# AS ORGANIZAÇÕES AINDA TÊM DIFICULDADES COM A INOVAÇÃO E TRANSFORMAÇÃO DIGITAL

Examinando os impactos reais quando as metas de disponibilidade de serviço não são cumpridas.

## 2017 Veeam Availability Report

Relatório Completo

# Índice

# Introdução da pesquisa

Nunca fomos tão dependentes da tecnologia quanto somos hoje em dia, nem tivemos tantas pessoas e funções críticas para os negócios que contam tanto com seus dados. Para que as organizações atinjam suas metas de negócios, as empresas buscam que a transformação digital e a nuvem ofereçam serviços mais eficientes, ágeis e confiáveis para atender às necessidades dos usuários. Como parte dessa transformação, as equipes de TI precisam trabalhar cada vez melhor para garantir a proteção e a disponibilidade dos seus sistemas e estão buscando, em ambientes heterogêneos e híbridos, maneiras para motivar eficiências e otimização de desempenho.

A Veeam®, que ajuda organizações a atingir maior disponibilidade operacional há mais de uma década, encomendou para a Enterprise Strategy Group (ESG) a realização do sexto Veeam Availability Report anual. Este relatório almeja (1) quantificar se as organizações estão atingindo suas metas de disponibilidade, (2) avaliar os impactos nas organizações que são deficientes quanto aos seus níveis de serviço de TI e (3) compreender como esses desafios afetam iniciativas estratégicas de TI, tais como a transformação digital.

# Sumário Executivo

As organizações continuam tendo dificuldades em garantir disponibilidade em seus ambientes de TI:

**Quatro em cada cinco organizações reconhecem que têm uma "lacuna de disponibilidade".** Na pesquisa deste ano, 82% dos entrevistados reconheceram a inadequação de seus recursos de recuperação quando comparados com a expectativa de SLA de suas unidades de negócios, o que está consistente com o resultado das duas últimas pesquisas anuais. Ainda que algumas organizações estejam se esforçando para melhorar, as crescentes expectativas das unidades de negócios, combinadas com o cenário de TI em constante evolução e diversificação, além da mudança para ambientes heterogêneos e híbridos, continuam a criar desafios para o fornecimento de disponibilidade adequada de TI. Isso causa problemas maiores para os negócios em termos de confiança dos clientes e funcionários.

**Em média, as empresas tem perdas financeiras diretas de US$21,8 milhões devido às Lacunas de Disponibilidade e Proteção,** reconhecendo que estes números vão variar de acordo com a indústria, seu tamanho e localização. Estas lacunas de disponibilidade e proteção também impactam as iniciativas realmente estratégicas de modernização de negócios:

- **82% das implantações e estratégias de virtualização das organizações foram afetadas** por suas soluções de proteção de dados.
- **66% das organizações informam que as iniciativas de transformação estão sendo atrasadas** (de forma significativa ou não) pelo tempo de inatividade não planejado ou disponibilidade insuficiente de aplicações.

**Seis em cada sete organizações não tem alto nível de confiança em sua capacidade de proteger e recuperar seus dados em seus ambientes virtuais, de forma confiável.** 85% dos entrevistados se autoavaliaram como estando menos do que muito confiantes na capacidade atual de suas organizações, com relação ao backup e recuperação de máquinas virtuais. Com a virtualização sendo a tecnologia de sustentação de todos os ambientes de TI modernos, incluindo ambientes locais e baseados na nuvem, *qualquer* resposta diferente de "muito confiante" é inaceitável em 2017.

**Três em cada quatro organizações reconhecem que têm uma "lacuna de proteção."** Também consistente com a pesquisa dos anos anteriores, 72% dos entrevistados deste ano não são capazes de proteger seus dados com a frequência necessária para garantir que possam atender às expectativas das unidades de negócio, com relação à perda de dados.

82%

das corporações enfrentam uma lacuna entre as exigências dos usuários e o que a TI pode oferecer, ou seja, uma 'lacuna de disponibilidade'

US$ 21,8

milhões é a média do custo financeiro das lacunas de disponibilidade e proteção para as empresas

66%

das corporações admitem que as iniciativas de transformação digital estão sendo refreadas devido ao tempo de inatividade não planejado

Além disto, os impactos do tempo de inatividade e perda de dados podem atingir muito mais do que apenas perdas econômicas diretas:

- Externamente, metade das organizações acredita que os desafios da disponibilidade podem levar a perda de confiança dos clientes, impactar a integridade da marca, reduzir o preço das ações e causar cancelamento de licenças e certificações.
- Internamente, muitos acreditam que os desafios da disponibilidade podem levar à perda de confiança dos funcionários, o que frequentemente resulta em desvio de recursos de projetos de longo prazo ou essenciais para os negócios.

As conclusões desse estudo são consistentes com as pesquisas anteriores da ESG e relatórios da Veeam®, que ilustram claramente que as organizações devem reconsiderar seus recursos de disponibilidade, proteção e recuperação de dados. O fracasso da TI, em melhor alinhar esses recursos importantes de resiliência com as expectativas dos responsáveis pelo negócio, continuará a colocar em risco suas organizações e atrasar as estratégias de transformação digital e inovação.

# Por que a Disponibilidade e Proteção de Dados Continuam a Desafiar as Organizações?

Muitas organizações continuam tendo dificuldades com relação à recuperação de dados em seus esforços de garantir disponibilidade de seus sistemas virtualizados. Na verdade, somente 15% dos tomadores de decisão estão muito confiantes na capacidade de suas soluções atuais de fazer backup e recuperação de máquinas virtuais de forma confiável dentro de seus SLAs.

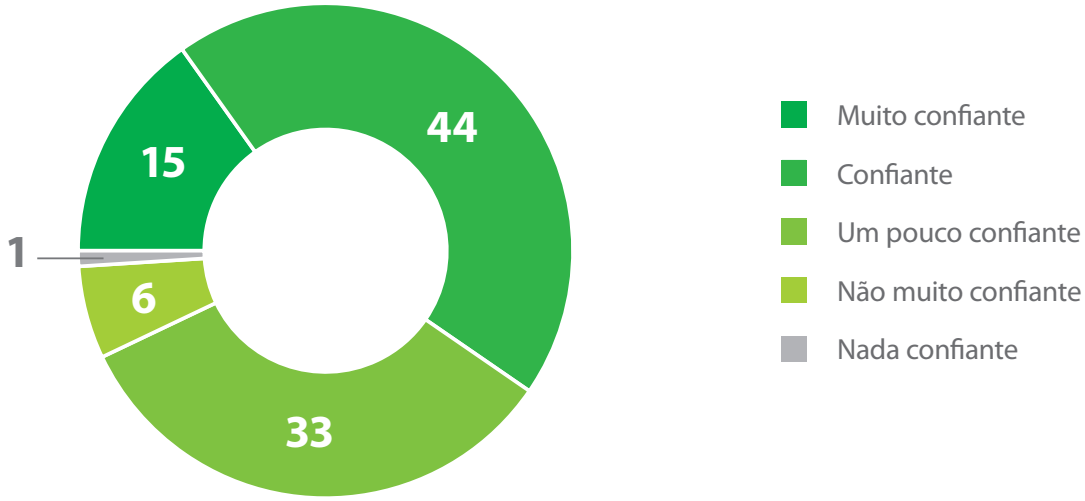


**Figura 1. Quão confiante você está na capacidade da solução primária de sua organização de fazer backup/recuperação de VMs de forma confiável e de recuperar o que você precisa dentro dos SLAs? (Porcentagem de respondentes, N=1.060)**

Esta é uma porcentagem terrivelmente baixa de confiança real. Qualquer organização que não esteja "muito confiante" em sua capacidade de proteger a estrutura fundamental de seu data center moderno, fornecer total dos dados e disponibilidade de aplicações, deve reexaminar suas estratégias e as tecnologias das quais são dependentes.

Infelizmente, esta falta de confiança largamente disseminada está bem fundamentada. Considere o fato de que os respondentes dizem que estão atendendo seus objetivos de tempo de recuperação (RTOs) e pontos de recuperação (RPOs) somente em 72% das vezes. Em mais de uma tentativa em quatro, seus esforços de recuperação falham, ou demoram muito tempo, ou recuperam uma quantidade inadequada de dados.

15%

dos tomadores de decisão estão confiantes na capacidade de suas soluções atuais de fazer o backup e recuperação de máquinas virtuais.

# Sensação Relacionada às Lacunas de Disponibilidade e Proteção

Em muitas empresas, quase todos os respondentes reconhecem que suas equipes de TI não conseguem recuperar de forma rápida o suficiente, com confiabilidade suficiente, ou em quantidade suficiente. A Veeam se refere a estes desafios como Lacuna de Disponibilidade e Lacuna de Proteção.

- **A Lacuna de Disponibilidade** se refere à diferença entre os níveis de serviço esperados pelas unidades de negócio, e a capacidade da organização de fornecer as aplicações e as informações que os usuários demandam.
- **A Lacuna de Proteção** se refere à tolerância a perda de dados da organização ser excedida pela incapacidade de TI de proteger os dados com a frequência necessária.

É alarmante a situação onde mais de quatro em cada cinco organizações pesquisadas reconhecem que têm uma Lacuna de Disponibilidade, e quase três em cada quatro organizações reconhecem que tem uma Lacuna de Proteção.

**4 de 5**

organizações pesquisadas reconhecem que tem uma Lacuna de Disponibilidade

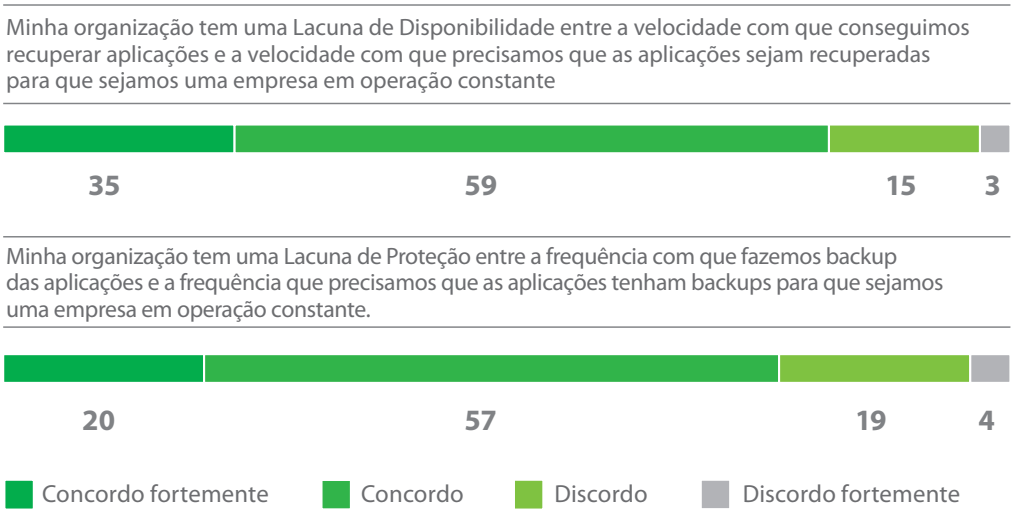


**Figura 2. Por favor, avalie se você está de acordo com as seguintes afirmações. (Porcentagem de respondentes, N=1.060)**

É notável o fato de que tantos tomadores de decisão estejam reconhecendo, pelo terceiro ano consecutivo, que continuam sofrendo da Lacuna de Disponibilidade, e que a mesma tendência esteja aparente com relação à Lacuna de Proteção — cada uma delas com quantidades quase iguais comparando ano contra ano.

Isto é mais do que apenas um problema disseminado; é também um problema contínuo.

**3 de 4**

organizações reconhecem que tem uma Lacuna de Proteção

# Realidades sobre Recuperabilidade e suas Ramificações

É de vital importância para uma organização reconhecer a precariedade de seus sistemas de TI e evitar banalizar o tempo de inatividade quando acontecer.

Na média, mais de um em cada quatro (27%) servidores passam por pelo menos uma ocorrência de tempo de inatividade por ano. Para entender como a ESG calculou estas médias, meios e medianas neste relatório, veja o apêndice 1[1].

**1em4**

servidores tem pelo menos uma interrupção não programada por ano

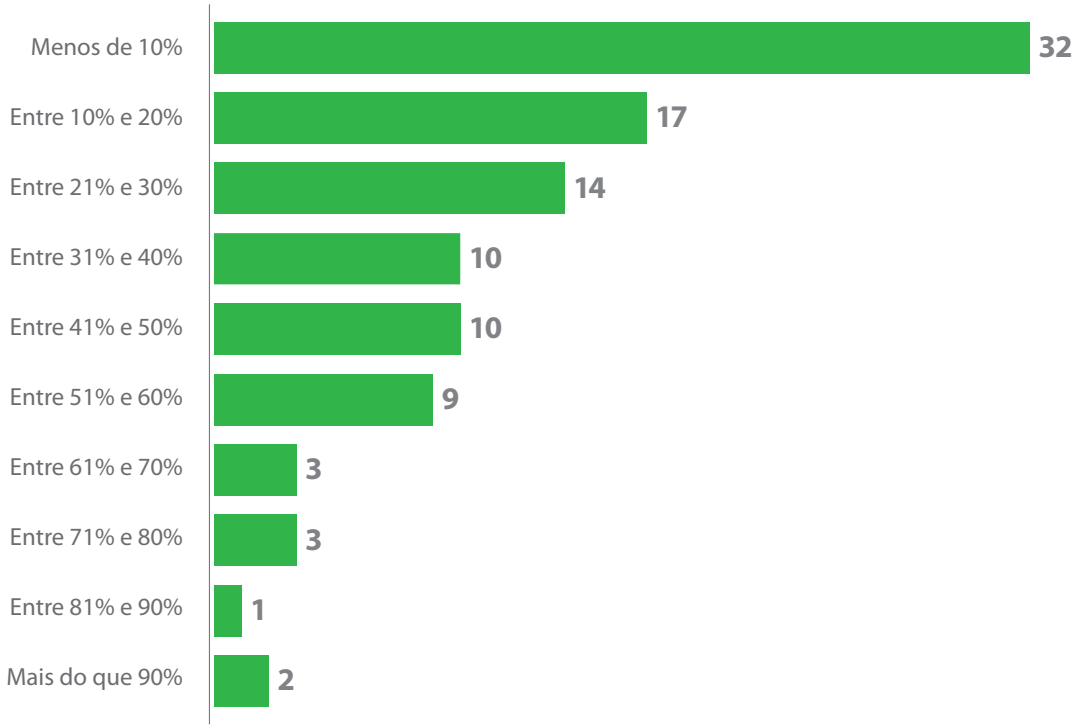


**Figura 3. Qual porcentagem dos servidores de produção de sua organização teve pelo menos um tempo de inatividade não programado por ano? (Porcentagem de respondentes, N=1.005)**

E algumas destas paradas duraram bastante tempo.

[1] Veja as Notas Relacionadas aos Cálculos e Dados Apresentados Neste Relatório no Apêndice: Metodologia de Pesquisa e Dados Demográficos dos Respondentes

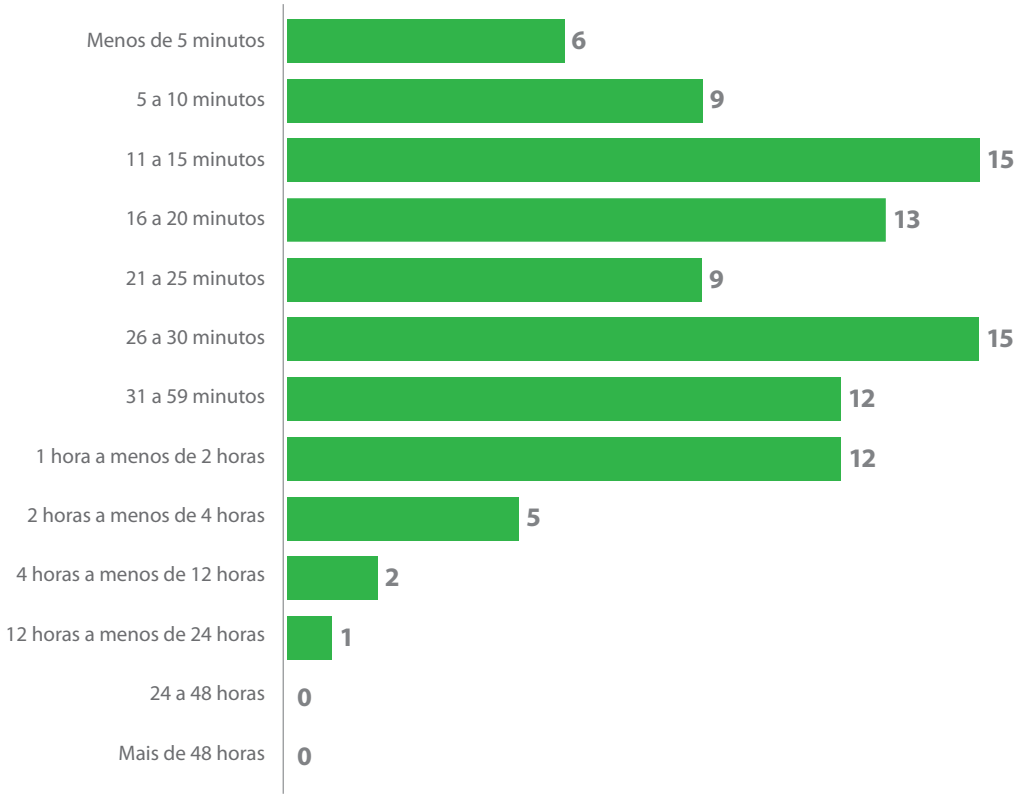


**Figura 4. Na média, quanto tempo dura uma parada não planejada? (Porcentagem de respondentes, N=989)**

A mediana da[2] duração de uma parada não programada é de 23 minutos. Embora isto possa não parecer muito tempo, considere:

- Qual o impacto a milhares de passageiros de uma empresa aérea cujos aviões não podem levantar voo por apenas 23 minutos?
- Qual o impacto para os clientes e para um varejista on-line cujo website está indisponível por 23 minutos?
- Qual o impacto para um paciente em um hospital cujos dados estão indisponíveis por somente 23 minutos?

23

minutos é a duração média de uma parada não programada

Qualquer profissional experiente de TI pode compartilhar histórias relacionadas a paradas não programadas, e como elas geraram crises. Mais ainda, a mídia publica novos eventos quase todas as semanas (dica: não seja um deles). Desde eventos que mudam sua vida à simples incapacidade de se comunicar com seus colegas, clientes, ou parceiros, todos os processos de negócio estão em risco quando a TI falha com seus usuários.

Considerando o potencialmente alto impacto de paradas não programadas em conjunto com a insuficiência de recursos de sistemas legados para fazer backup e recuperação de dados, o desejo entre os executivos de TI de buscar melhores ferramentas de disponibilidade é garantido.

[2] Ibid

# A Lacuna de Disponibilidade e Tempo de Inatividade

Se você olhar em detalhe o que as organizações pesquisadas classificam como cargas de trabalho de "alta prioridade" quando comparadas com cargas de trabalho "normais", uma surpreendente diferença fica aparente:

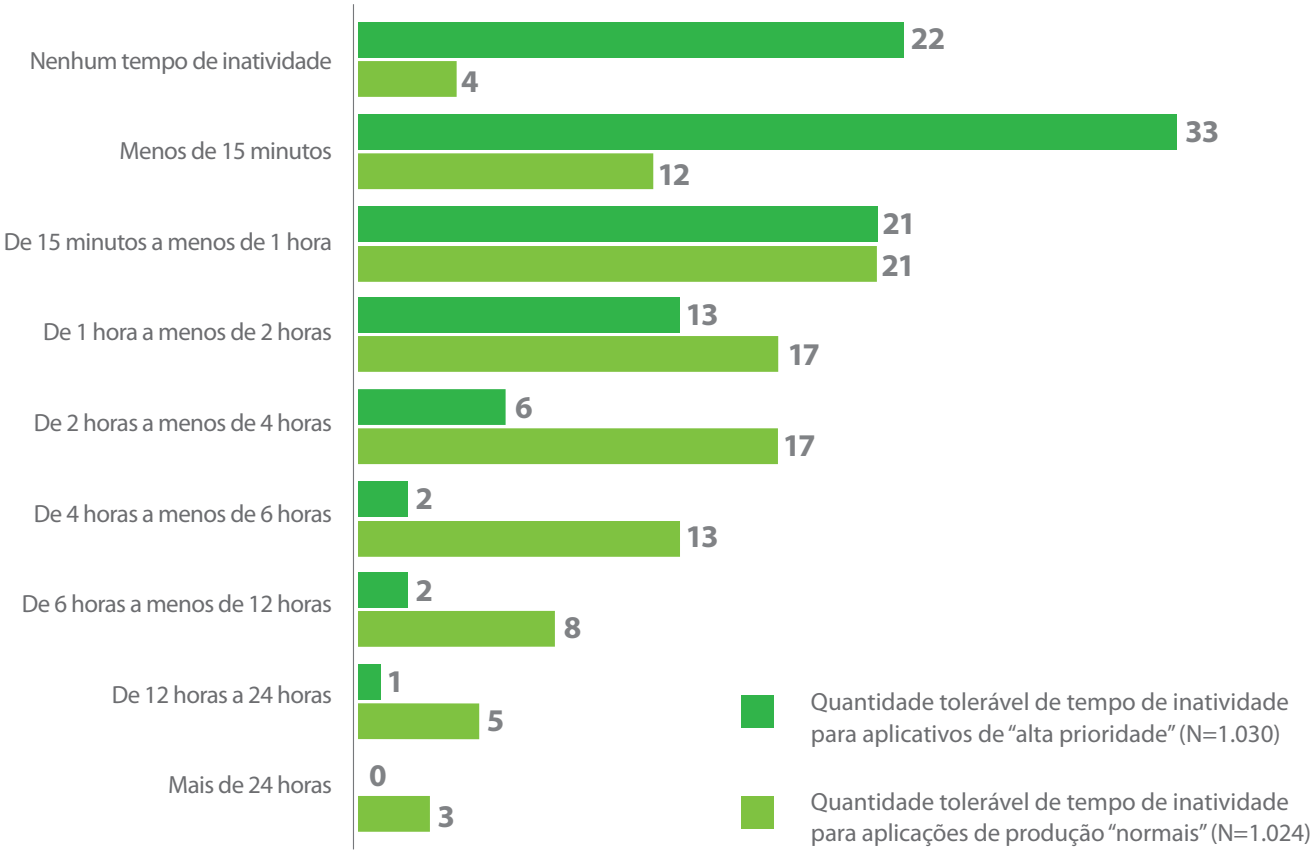


**Figura 5. Qual o tempo de inatividade que sua organização pode tolerar para suas aplicações de produção de "alta prioridade" comparado com o tempo das aplicações de produção "normais"? (Porcentagem de respondentes)**

- A mediana do tempo tolerável de inatividade entre aplicações de *alta prioridade* é de 7,5 minutos, onde uma parada não programada de "apenas 23 minutos" excederia o limite da maioria das aplicações de alta prioridade.
- A mediana de tempo de inatividade tolerável entre as aplicações *normais* é de 90 minutos. Embora a duração de 23 minutos possa parecer mais tolerável, muitas aplicações normais teriam seus SLAs extrapolados com uma parada não planejada desta duração.

# A Lacuna de Proteção e os SLAs de Perda de Dados

A disparidade entre a velocidade com que TI pode recuperar plataformas/cargas de trabalho e a expectativa de disponibilidade das unidades de negócio e outros usuários finais não é a única preocupação. As organizações também estão protegendo dados de forma inadequada:

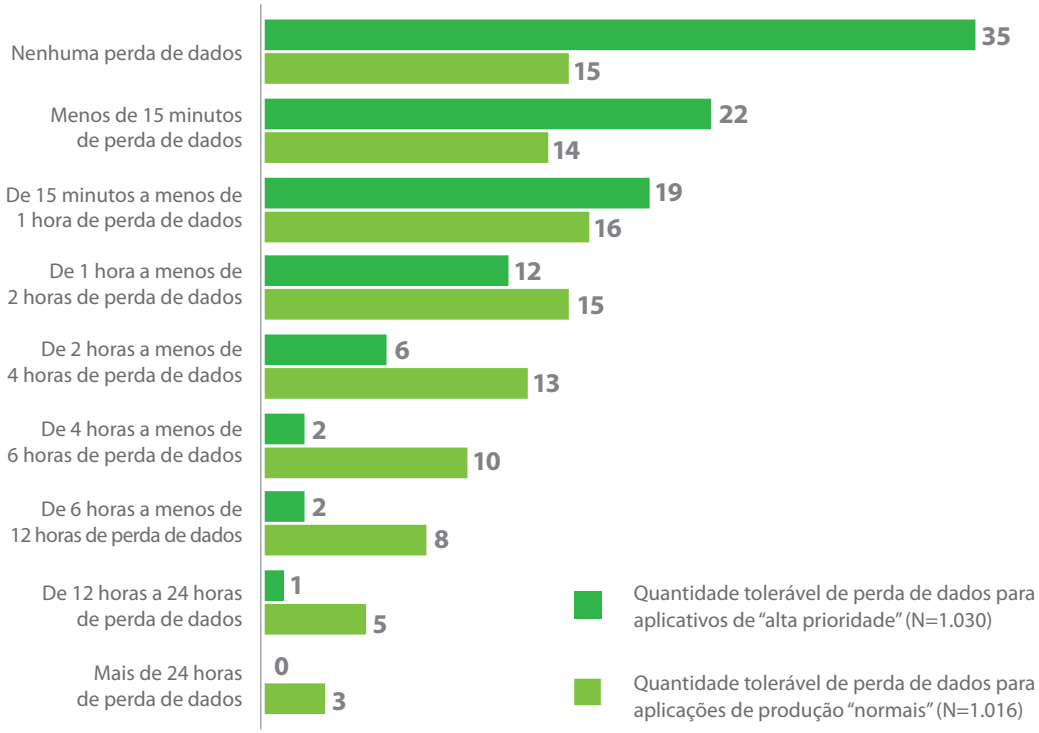


**Figura 6. Qual a quantidade de perda de dados que sua organização pode tolerar em suas aplicações de produção de "alta prioridade" comparadas com as aplicações de produção "normais"? (Porcentagem de respondentes)**

- A média aceitável de perda de dados entre aplicações de *alta prioridade* é de 72 minutos, conforme mostra a Figura 6. Mas as organizações pesquisadas somente protegem seus dados de alta prioridade aproximadamente a cada 127 minutos, em média.
- De forma similar, embora a média de perda de dados aceitável entre aplicações *normais* seja de 240 minutos, as organizações pesquisadas somente protegem seus dados normais aproximadamente a cada 352 minutos.

Este é um exemplo quantificável de Lacuna de Proteção. Para ser claro: muitas organizações acreditam que tem uma Lacuna de Disponibilidade, uma Lacuna de Proteção, ou ambos. Para superar estas lacunas, as organizações devem começar aumentando a frequência da proteção e incrementar a agilidade e confiabilidade da recuperação.

# Os Custos das Lacunas de Disponibilidade e Proteção

Em uma época onde VMs de missão crítica e VMs não essenciais podem conviver no mesmo host hoje, mas não poderão amanhã, e onde o número de usuários por VM varia muito, calcular o tempo de inatividade pode ser assustador para organizações de qualquer tamanho. Para efeito deste relatório, os custos dos tempos de inatividade incluíram as seguintes informações (a maioria de outros lugares neste relatório):

- A média do número total de servidores de produção (1.200) implantados nas organizações
- A porcentagem de servidores que tiveram pelo menos uma parada não programada por ano (27%)
- A duração média de paradas não planejadas (85 minutos)
- O custo médio por hora de aplicações de missão crítica (USD$ 108.000) e não missão crítica (USD$48.000) — ajustando para a taxa média de aplicações de missão crítica e não de missão crítica
- Média da taxa de aplicações por servidor da ESG (.81)

US$ 21,8

milhões organizações que participaram desta pesquisa sofrem com custos diretos de US$21,8 milhões por ano, em média

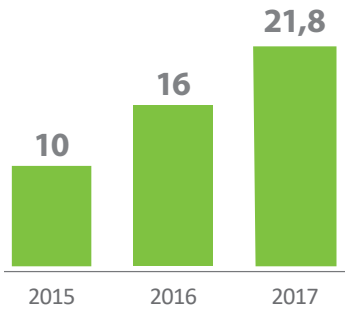


**Figura 7. Custo estimado anual de tempo de inatividade por organização respondente (em USD$Milhões)**

Usando estas informações, a ESG calculou que as organizações que participaram desta pesquisa sofreram custos financeiros diretos de USD$21.8M anualmente, em média. Este número dá sequência à tendência de aumento de custos por tempo de inatividade conforme vimos em 2016 (USD$16M) e 2015 (USD$10M).

Mas ainda tem mais ....

# Como as Organizações estão Lidando com estas Lacunas

Quando você examina as discrepâncias entre as abordagens arcaicas e as expectativas das unidades de negócio, surgem três "níveis de compreensão":

- **Em teoria**, o reconhecimento da existência da Lacuna de Disponibilidade e da Lacuna de Proteção também representam um reconhecimento conceitual ou intelectual de que os mecanismos de proteção, recuperação e estratégias de dados também precisam evoluir.
- **Na prática**, lacunas irrefutáveis, quantificáveis existem entre os recursos de proteção e recuperação de TI e as expectativas das unidades de negócio existem e são disseminadas.
- **Na realidade,** os custos associados ao tempo de inatividade e perda de dados também trazem uma variedade de outros impactos negativos. Sim, os impactos econômicos são os mais fáceis de visualizar, mas outras ramificações são igualmente, senão mais, danosas.

41%

reconhecem que problemas de disponibilidade conduzem à perda de confiança do cliente e do funcionário, e isso é um impacto dos mais preocupantes

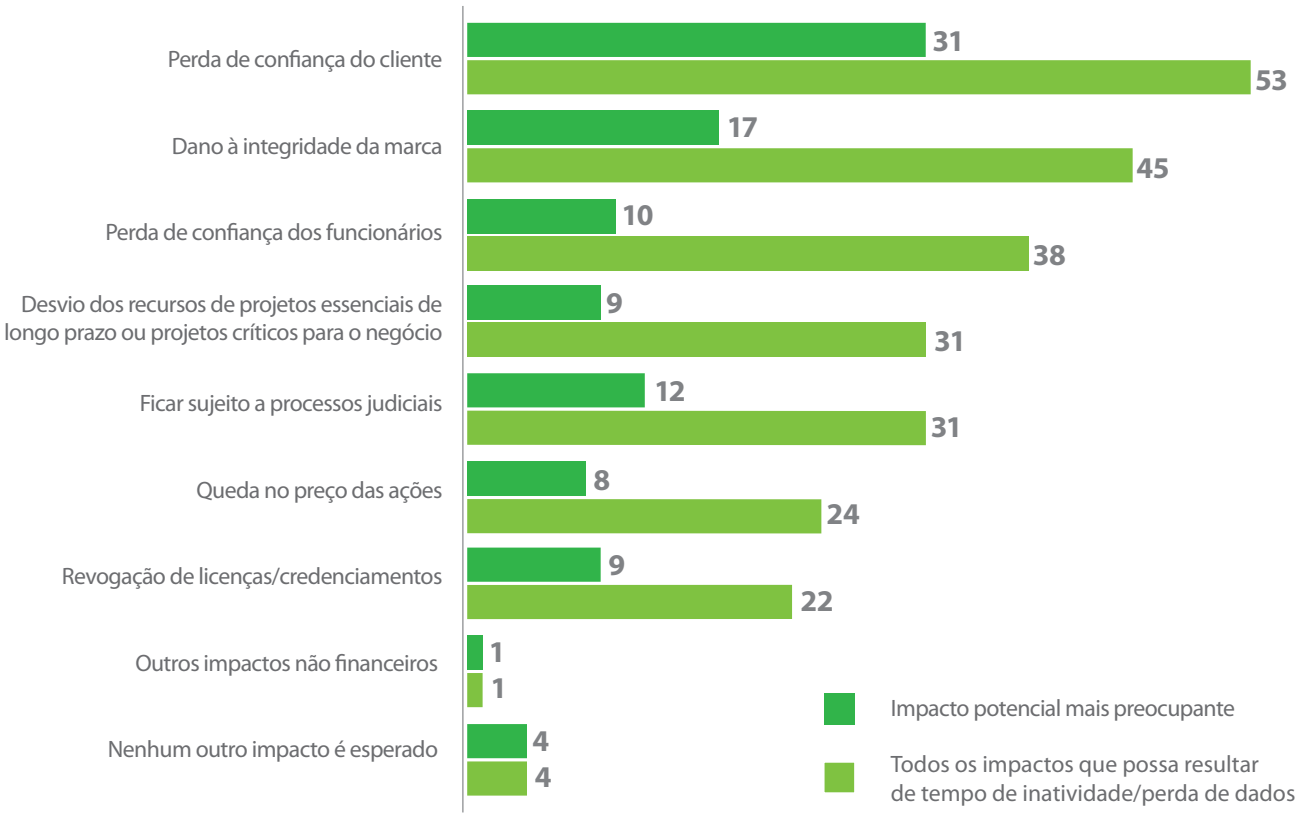


**Figura 8. Quais outros impactos – se existirem – a perda de dados ou o tempo de inatividade de aplicações podem causar à sua organização? Qual impacto mais preocupa você? (Porcentagem de respondentes, N=943)**

Considere, por exemplo, que somente 4% dos executivos acreditam que suas organizações sofrem apenas impactos monetários como resultado do tempo de inatividade ou perda de dados.

Muitos executivos reconhecem que os problemas de disponibilidade podem fazer com que suas organizações sofram problemas como redução na confiança dos clientes e funcionários, ou prejuízos para a integridade da marca.

Coincidentemente, a soma destes impactos é quase idêntica à da pesquisa do ano anterior, desde o fato da confiança de clientes e integridade da marca serem os mais preocupantes até o número minúsculo de pessoas que negam estes impactos não financeiros.

O problema só vai ficar pior com o passar do tempo. Somente 13% dos respondentes esperam que os custos de tempo de inatividade e perda de dados venham a diminuir no futuro. Para todos os demais, como as expectativas de disponibilidade das unidades de negócio continuem a crescer e TI continue a ter dificuldades, os impactos decorrentes do tempo de inatividade e perda de dados também deve crescer.

# Obstáculos às estratégias de virtualização das organizações

É extremamente importante reconhecer que os mecanismos de proteção e recuperação inadequados não dificultam apenas os sistemas e os processos de negócio de hoje. Eles também irão dificultar a capacidade da organização de continuar a modernizar seu ambiente de TI como parte de uma evolução pelo bem do negócio.

Servidores virtualizados são a fundação sobre a qual a maioria das infraestruturas mais modernas de TI estão baseadas. A maioria dos respondentes pesquisados (82%) reconhecem alguma relação entre a viabilidade de sua solução de backup e o sucesso relativo de sua estratégia de implantação de virtualização:

- Uma quantidade não trivial (33%) reconhece que o fato de sua solução de backup de VM ser inadequada tem ***reduziu a velocidade*** do esforço de implantação de virtualização de suas organizações.
- Uma constatação positiva, muitos (49%) reconhecem que uma solução de backup de VM efetiva permitiu às suas empresas ***acelerar de forma significativa*** sua estratégia de implantação de virtualização.

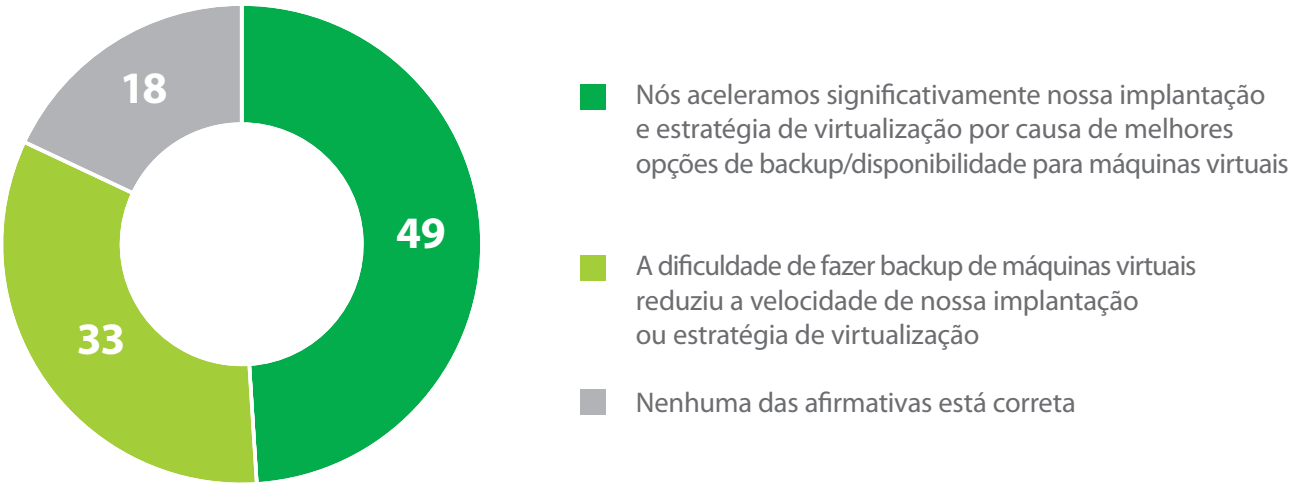


**Figura 9. Qual das afirmações a seguir sobre o relacionamento entre a virtualização de servidores e proteção de dados está mais correta? (Porcentagem de respondentes, N=964)**

# Obstáculos às estratégias de nuvem das organizações

Assim como a virtualização de servidores forçou novas abordagens para a proteção e recuperação de dados, o mesmo ocorre com "a nuvem" — em cada uma de suas formas:

- Esta movimentação das cargas de trabalho de produção para serviços hospedados IaaS ou PaaS, ou a adoção de SaaS, terão que repensar seus cenários de proteção e recuperação de dados; e muitas vão descobrir que é necessário mudar de fornecedor.
- Enquanto isto, soluções de storage na nuvem permitem novas opções para retenção de dados, especialmente quando combinadas com serviços de backup disponíveis na nuvem (BaaS), ou mecanismos de failover (DRaaS).

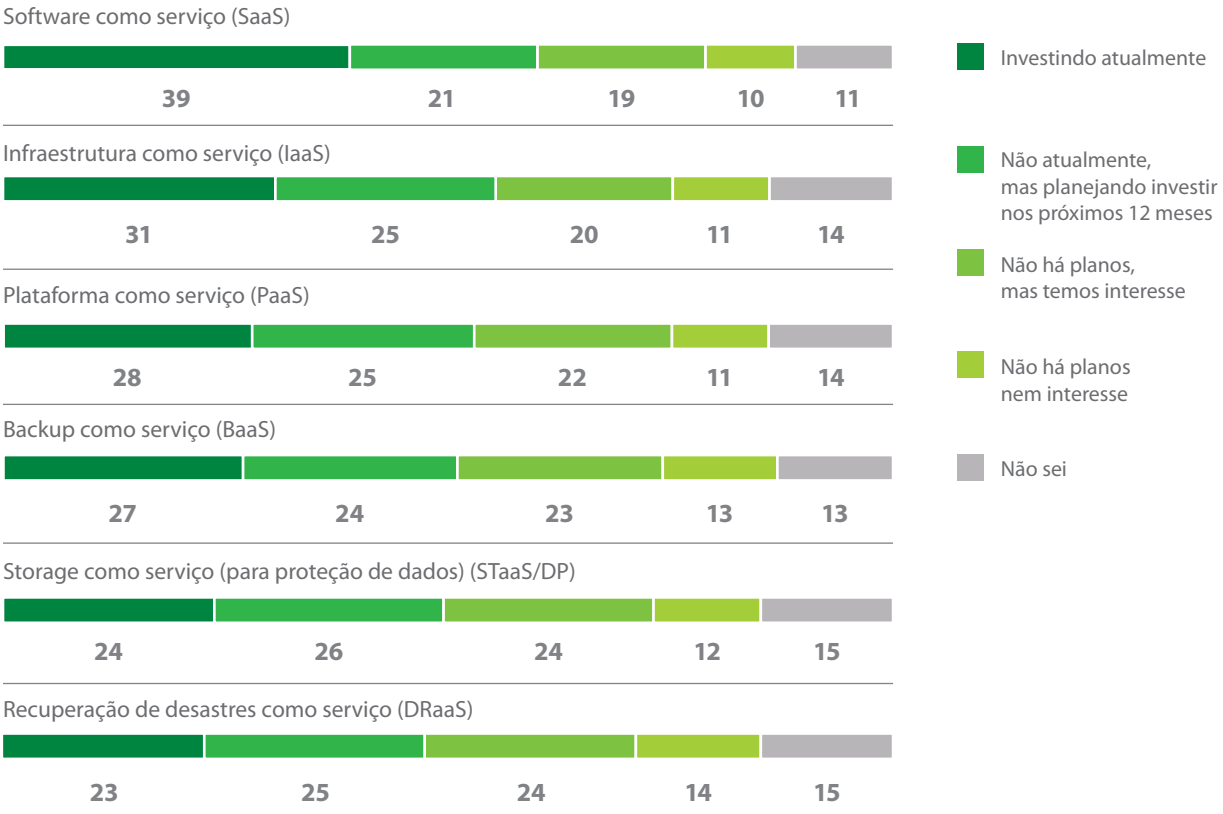


**Figura 10. Que tipos de serviços baseados na nuvem sua organização está usando atualmente ou planeja usar nos próximos 12 meses (se pretender)? (Porcentagem de respondentes, N=1.060)**

Dado o nível de investimento observado na nuvem, está claro que os serviços na nuvem irão mudar a forma como TI alcança ambos os objetivos de produção e proteção, mas nem todos os fornecedores estão preparados para a nuvem.

# Obstáculos às iniciativas de transformação digital das organizações

Embora algumas organizações ainda estejam modernizando as infraestruturas de base para virtualização, muitas outras reconhecem que uma estratégia de *transformação digital* vai demandar muito mais do que simplesmente a modernização da infraestrutura.

- Mais de dois terços dos respondentes pesquisados (69%) reconhecem que a transformação digital é crítica, ou muito importante, para o futuro de suas organizações.
- Dito isto, quase metade deles (45%) dizem que ainda estão na fase de planejamento ou ainda nas fases iniciais das iniciativas de transformação digital.

É preocupante que mais da metade dos respondentes cujas organizações tem iniciativas de transformação digital em seu cronograma (66%) declarem que estas iniciativas estão sendo restringidas por causa de inatividade não planejada ou disponibilidade insuficiente de aplicações.

66%

declaram que suas iniciativas de transformação digital estão sendo restringidas por tempo de inatividade não planejado ou disponibilidade insuficiente para aplicações.

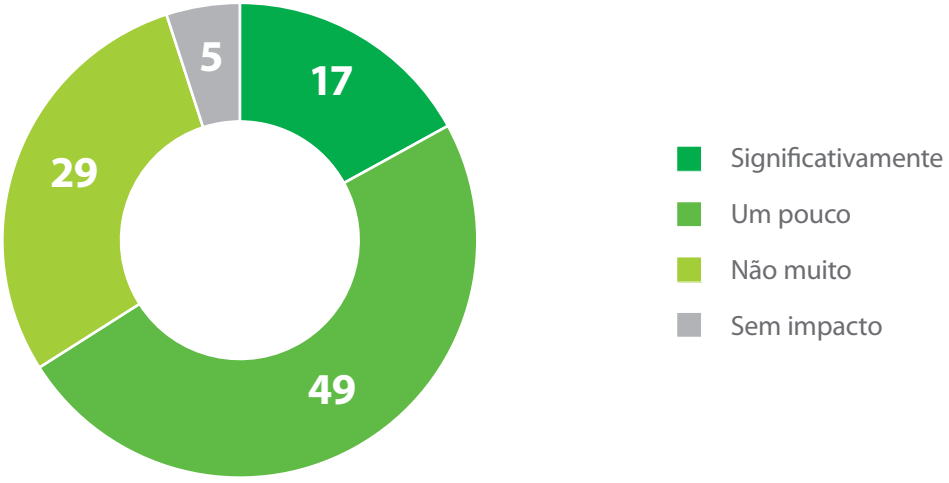


**Figura 11. Qual a extensão da restrição que o tempo de inatividade não planejado e insuficiência de disponibilidade das aplicações estão trazendo às iniciativas de transformação digital de sua organização? (Porcentagem de respondentes, N=970)**

Para que possam avançar em suas iniciativas críticas de transformação digital para além das fases iniciais, muitas organizações devem resolver suas deficiências de tempo de atividade e disponibilidade.

# Conclusão

A maioria das organizações reconhecem (e outras não, mas deveriam) que as lacunas em seus recursos de disponibilidade e proteção, resultam em fracasso em atender às expectativas de suas unidades de negócio, de seus executivos, de seus colegas funcionários, e de seus clientes. As razões para esta situação incluem:

- A maioria das infraestruturas de TI está em contínuo estado de modernização, o que inclui iniciativas de transformação digital, estratégias agressivas de virtualização, ampliadas através da adoção, muitas vezes experimental, de serviços de nuvem híbrida, diversificação das plataformas de produção e SLAs em crescimento, mas tudo sem o aumento proporcional do orçamento.
- Muitas organizações não alinham a frequência de sua proteção nem os mecanismos de recuperação com os SLAs definidos por suas unidades de negócio, o que resulta em disponibilidade inadequada.
- Muitas organizações não são capazes de quantificar efetivamente a miríade de custos e impactos do tempo de inatividade ou perda de dados, e com isto dificultam sua capacidade de obter suporte operacional e econômico para melhorar suas ferramentas e resultados.

Estes desafios não são triviais, mas são superáveis. As organizações devem resolver as Lacunas de Disponibilidade e Proteção que têm, ou vão colocar seus funcionários e instituições em risco de uma grande variedade de falhas de produtividade, econômicas, sentimentais e operacionais.

- **Qualquer organização que não consiga recuperar dados de forma granular ou VMs completas mais rapidamente do que definido pelos SLAs relacionados a tempos de inatividade aceitáveis, tem uma *Lacuna de Disponibilidade*.** A Lacuna de Disponibilidade resultará em perda de produtividade de usuários, não conformidade com a acessibilidade acordada (tanto entre parceiros de negócio e aplicáveis a regulações da indústria), e perda de confiança dos funcionários, cliente, e dos mercados em que atua.
- **Qualquer organização que não proteja seus dados em uma frequência maior do que demandado pelo SLA relacionado à perda de dados tem uma *Lacuna de Proteção*.** A Lacuna de Proteção resultará em perda de dados, que pode gerar problemas de produtividade de funcionários, tanto na recriação dos dados quanto em servir seus clientes sem informações completas.

Lacunas, seja de disponibilidade ou proteção, invariavelmente representam problemas para os ambientes operacionais de hoje, para as estratégias de virtualização e implantações que estão modernizando os data centers de hoje, e finalmente às iniciativas de transformação digital nas quais muitas instituições estão confiando para garantir sua relevância no mercado no futuro.

# Próximos Passos

**O primeiro, e mais crucial, passo para garantir a viabilidade dos seus sistemas de TI em servir suas unidades de negócio e clientes, é presumir que você tem uma Lacuna de Disponibilidade e uma Lacuna de Proteção,** até que você consiga provar o contrário. Muitas organizações que não possuem métricas acuradas ou processos de monitoramento presumem que seus sistemas são suficientes e, com isto, estão atrapalhando suas organizações através de sua ingenuidade. Ao invés disto, presuma que você tem o problema, e então quantifique-o. Apenas uma minoria das organizações (menos do que uma em cinco) vai fazer diferente, e muitas delas são provavelmente resilientes em função de grandes esforços de disponibilidade feitos em anos anteriores.

**Depois, quantifique os SLAs de suas unidades de negócio e avalie seus próprios mecanismos de proteção e capacidade de recuperação.** Somente ao comparar suas expectativas de disponibilidade e proteção com sua capacidade real, você será capaz de determinar o tamanho das lacunas em sua estratégia de TI.

**Converta suas lacunas em análises de impacto.** No mundo de BC/DR, este processo é chamado de análise de impacto no negócio (business impact analysis - BIA), que pode ser feito simplesmente perguntando, *"Se [sistema] falhar, quanto isto nos custaria [em termos econômicos, de processo, percepção, etc.]?"* Olhando os logs do sistema do passado, a maioria vai descobrir que estes sistemas tiveram interrupções no passado, que agora podem ser quantificadas como impacto ao negócio.

Com um entendimento claro da frequência e duração das paradas em seu ambiente, compare com as expectativas de SLA dos responsáveis pelo negócio, e a avaliação do impacto econômico e de percepção específicos de sua organização, **você está pronto para imaginar o que seria necessário para se tornar uma corporação em operação constante:**

1. *Reconheça que a virtualização será quase certamente a sustentação de sua infraestrutura*, e por isto você deve garantir que seus recursos de proteção e recuperação para sistemas altamente virtualizados exceda os SLAs de seu negócio. Isto já pode resolver uma parte significativa de suas Lacunas de Disponibilidade e Proteção.

2. *Entenda que os serviços na nuvem sem sombra de dúvida terão uma grande participação em sua estratégia,* embora os tipos de solução em nuvem possam a variar bastante entre storage na nuvem, serviços de proteção baseados na nuvem, infraestrutura baseada na nuvem em cenários de BC/DR e aplicações baseadas na nuvem (como o Office365). Cada uma destas escolhas de plataforma irá afetar suas opções de proteção e recuperação, que devem novamente ser medidas primeiramente para validar sua conformidade com os SLAs para garantir redução nas Lacunas de Disponibilidade e Proteção.
3. E finalmente, mas talvez o mais importante, *reconheça que o tempo de inatividade e perda de dados não são apenas conceitos teóricos, e que POR/RTO não são apenas métricas para o scorecard de TI.* A falta de mecanismos ágeis e confiáveis de recuperação/disponibilidade irão impactar a sustentação de sua virtualização hoje e vão atrasar as iniciativas de transformação digital que devem levar sua empresa ao futuro. *Tudo começa com seu comprometimento em estar em operação constante.*

# Apêndice: Metodologia de Pesquisa e Dados Demográficos dos Respondentes

## Metodologia da Pesquisa

A Veeam contratou The Enterprise Strategy Group, uma empresa líder em análise, pesquisa, e estratégia de TI, para desenvolver e realizar a pesquisa na qual este relatório está baseado.

Para coletar os dados para este relatório, a ESG conduziu uma ampla pesquisa on-line com 1.060 ITDMs de organizações do setor público e privado com pelo menos 1.000 funcionários em 24 países diferentes entre 18 de Novembro de 2016 e 31 de Dezembro de 2016.

A representação geográfica dos respondentes está apresentada na Figura 12.

| | |
|---|---|
| Estados Unidos | N=158 |
| Reino Unido | N=103 |
| França, Alemanha | N=78 |
| Benelux (Belgica, Holanda), Hong Kong | N=75 |
| Austrália, Japão, China, Brasil, Cingapura | N=50 |
| Canadá | N=49 |
| Itália, Nórdicos (Suécia, Dinamarca, Finlândia), Rússia, Tailândia, Índia, Oriente Médio (Emirados Árabes Unidos, Arábia Saudita, Israel), México | N=16-30 |

**Figura 12. Número de Respondentes Qualificados por País/Região**

Para se qualificar para esta pesquisa, os respondentes precisavam estar empregados em uma função de TI com conhecimento da operação diária e/ou familiaridade com o ambiente e estratégia de backup de dados/arquivos . Foi oferecido um incentivo na forma de prêmios em dinheiro e/ou equivalente a todos os respondentes para que completassem a pesquisa.

Todos os respondentes foram submetidos a um rigoroso processo de garantia de qualidade, que incluiu a filtragem de respondentes não qualificados, remoção de respostas duplicadas, e verificação das respostas completas restantes (em vários critérios) para garantir a integridade de dados.

Veja se seção de Informações Demográficas dos Respondentes deste relatório para maiores informações sobre os respondentes.

## Notas Relacionadas aos Cálculos e Dados Apresentados Neste Relatório

Neste relatório, as médias e medianas calculadas são estimadas para as perguntas em que as opções de respostas eram intervalos numéricos. Isto é feito usando o ponto localizado no meio de cada intervalo selecionado por cada respondente como o valor escolhido por ele, e calculando a média (seja média ou mediana) baseada na distribuição agregada das respostas dos respondentes para a pergunta. As referências a qualquer média apresentada neste relatório se refere à média matemática, a menos que a mediana seja informada explicitamente.

Adicionalmente, os totais apresentados nas figuras e tabelas neste relatório podem não somar 100% devido a arredondamentos.

## Informações Demográficas dos Respondentes

Os dados apresentados neste relatório são baseado numa pesquisa com 1.060 respondentes qualificados. As figuras 13 a 17 detalham as informações demográficas da base de respondentes, incluindo a função corrente do respondente, assim como o número total de funcionários da organização do respondente, indústria primárias, e volume de servidores.

## Respondentes por Função

A função corrente dos respondentes em suas organizações está apresentada na Figura 13.

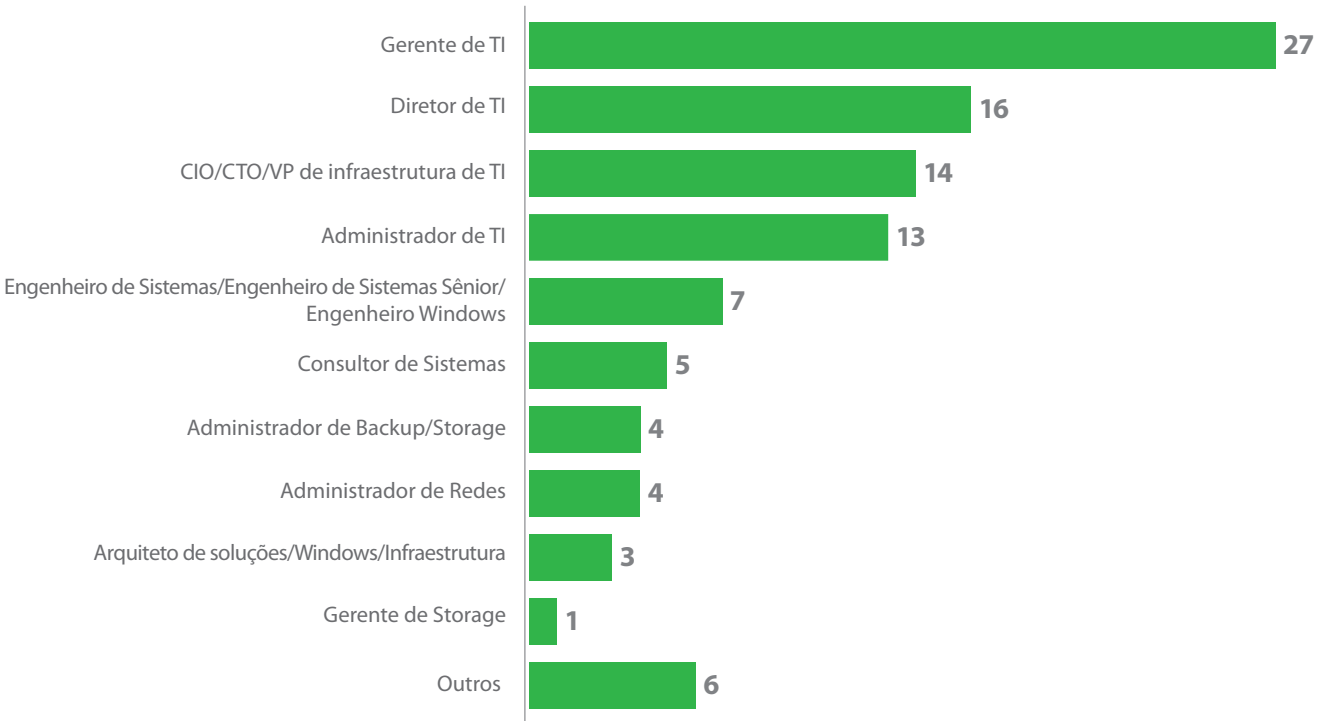


**Figura 13. Quais das afirmações seguintes descrevem melhor sua função em sua organização? (Porcentagem de respondentes, N=1.060)**

## Respondentes por Número de Funcionários

O número de funcionários na organização do respondente está apresentado na Figura 14.

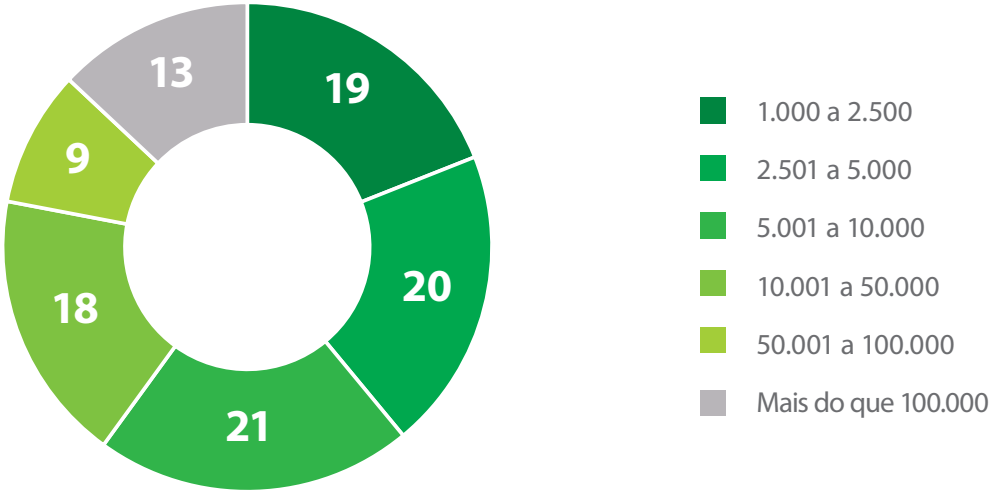


**Figura 14. Qual o número total de funcionários de sua organização mundialmente? (Porcentagem de respondentes, N=1.060)**

## Respondentes por Indústria

Pedimos aos respondentes que identificassem a indústria primária de suas organizações. Ao todo, a ESG recebeu respostas completas e qualificadas de indivíduos em 12 indústrias verticais, mais uma categoria de "Outras", apresentadas na Figura 15.

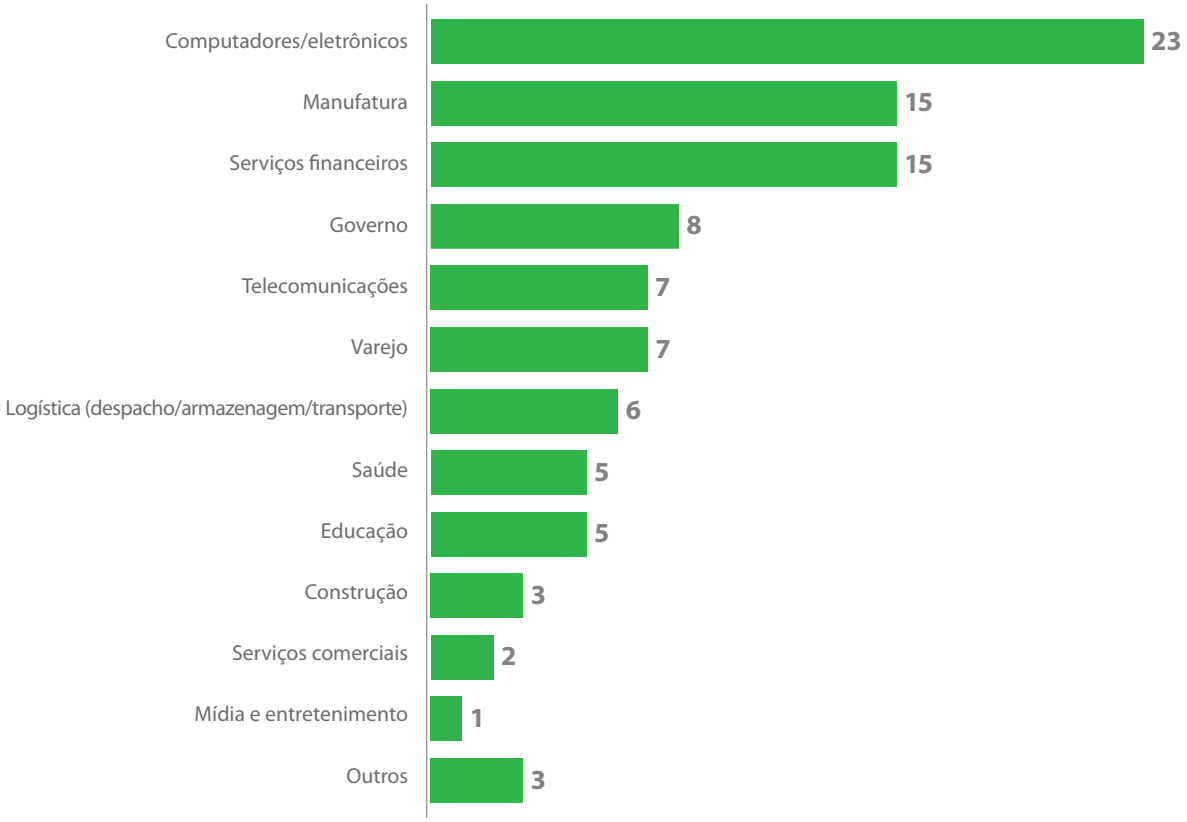


**Figura 15. Qual a indústria primária de sua organização? (Porcentagem de respondentes, N=1.060)**

## Respondentes por Número de Servidores de Produção

O número de servidores de produção físicos e virtuais da organização está apresentado na Figura 16.

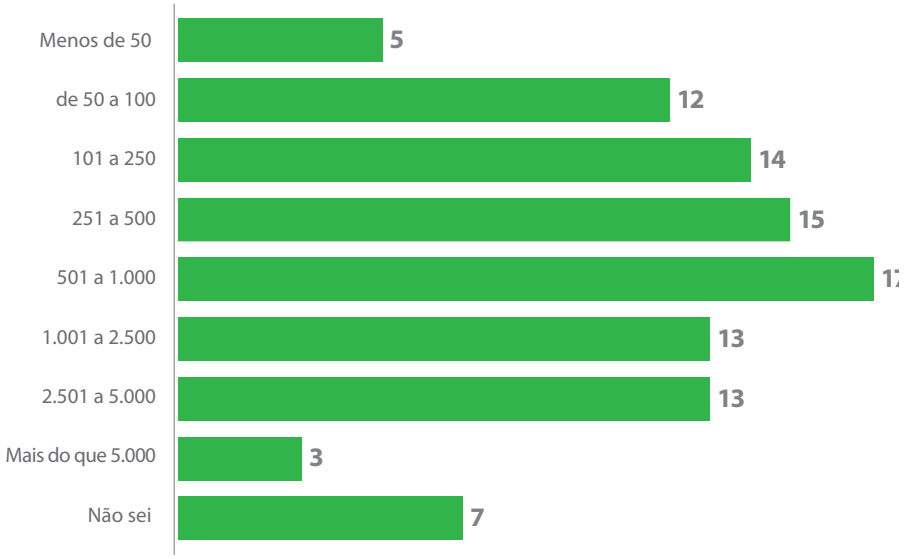


**Figura 16. Aproximadamente, quantos servidores de produção ao todo (isto é, ambos físicos e virtuais, mas não incluindo servidores de teste/desenvolvimento) estão atualmente instalados em sua organização? (Porcentagem de respondentes, N=1.035)**

## Respondentes por Porcentagem de Servidores Virtualizados X86

A porcentagem de servidores x86 que tenham sido virtualizados até a data, e como este porcentual deve mudar em dois anos, está apresentada na Figura 17.

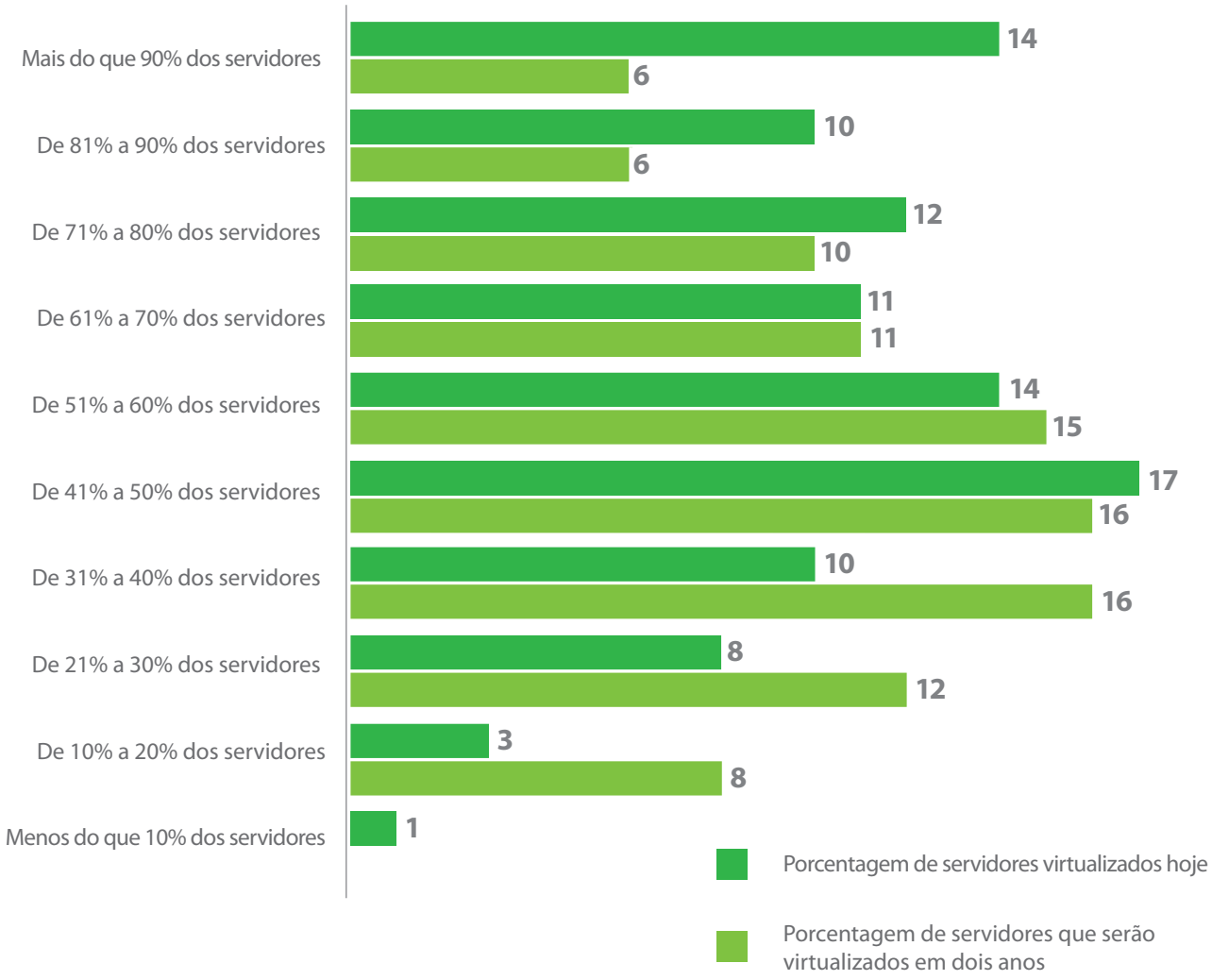


**Figura 17. De todos os servidores x86 em sua organização que podem ser virtualizados, qual porcentagem foi virtualizada? Olhando para os próximos dois anos, qual porcentual de servidores você acredita que estarão virtualizados? (Porcentagem de respondentes, N=1.060)**

**Sobre a Veeam Software:**
Veeam® reconhece os novos desafios que as empresas em todo o mundo enfrentam para manter os negócios em operação constante (Always-On Business™), um negócio que deve ter operações 24 horas, 7 dias por semana, 365 dias por ano. Para lidar com isso, a Veeam se tornou pioneira de um novo mercado de *Availability for the Always-On Enterprise™*, ajudando as organizações a cumprirem recovery time e point objectives (RTPO™) de menos de 15 minutos para todas as aplicações e dados por meio de um tipo de solução fundamentalmente nova, que fornece recuperação em alta velocidade, prevenção contra perda de dados, proteção verificada, aproveitamento de dados e visibilidade completa. O Veeam Availability Suite™, que inclui o Veeam Backup & Replication™, aproveita as tecnologias de virtualização, storage e nuvem que capacitam o data center moderno a ajudar as organizações a poupar tempo, reduzir riscos e diminuir consideravelmente os custos operacionais e de capital, ao mesmo tempo que apoia as metas de negócios atuais e futuras dos clientes da Veeam.

Fundada em 2006, a Veeam atualmente tem 41.000 ProPartners e mais de 205.000 clientes em todo o mundo. A sede global da Veeam está localizada em Baar, na Suíça, e a empresa tem escritórios espalhados pelo mundo. Para saber mais, visite www.veeam.com.

**Sobre a ESG**
A ESG é uma empresa de análise, pesquisa e estratégia de TI, fundada em 1999, com sua sede em Milford, Massachusetts. Ela realiza pesquisas com e para fornecedores de TI, profissionais de TI, profissionais de negócio, e canais. A ESG mantém cobertura constante de analistas sobre a computação em nuvem, redes, storage, proteção de dados, segurança cibernética, gerenciamento e análise de dados, mobilidade corporativa, gerenciamento de sistemas, e canais.

**Sobre o Analista Principal deste Estudo**
Jason Buffington é o Analista Principal da ESG focado em todas as formas de proteção, preservação e disponibilidade de dados. Ele atuou ativamente na implantação ou consultoria de soluções de proteção de dados e storage for 28 anos, trabalhando em parceiros de canal, múltiplos fornecedores de software de proteção de dados e na Microsoft. Jason tem sido um destacado palestrante em vários eventos de infraestrutura de servidores, continuidade de negócios e storage em todo o mundo, e seus artigos têm sido publicados em vários jornais da indústria de TI.