



O Acronis Global Disaster Recovery Index: 2012

Uma classificação mundial anual da confiança internacional na prontidão, recursos e práticas de backup e recuperação de desastres.

Juntamente com o
Ponemon Institute



Índice

Sumário Executivo	3
O que é o Acronis Global Disaster Recovery Index?	4
O formato da pesquisa.....	4
Principal constatação: a confiança está aumentando	5
As classificações do índice: quanto maior a mudança, mais as coisas ficam como estão	6
Principais Constatações Globais	9
Adoção da virtualização por SMBs superará a das corporações em 2012	10
Dados virtuais em maior risco que os dados físicos	12
A nuvem avança, mas ainda não atende às expectativas	13
Estratégia de backup externo ainda insuficiente	14
Erros humanos são a maior causa de indisponibilidade de sistemas	15
O dilema do fornecedor especializado: empresas ainda não consolidaram	16
Recomendações para backup e DR – uma perspectiva do patrocinador da pesquisa	17
Apêndices	18

Sumário Executivo:

Proteção de dados em um mundo tumultuado

2011 foi um ano de conflitos políticos, agitação econômica e desastres ambientais em uma escala global sem precedentes, afetando as vidas e o sustento de bilhões de pessoas.

- Com inundações devastadoras na Austrália, Brasil e Tailândia, terremotos mortais na Nova Zelândia, um tsunami quase apocalíptico no Japão, tufões nas Filipinas e cerca de 100 tempestades atingindo diversas partes dos EUA, o mundo observou o poder destrutivo da mãe natureza.
- Ao mesmo tempo, levantes populares em todo o mundo alimentaram a agitação civil, levando, em alguns casos, à guerra civil, e ditadores implacáveis foram implacavelmente derrubados.
- A desaceleração global, as debilidades econômicas e a crise na zona do Euro adicionaram outra dimensão brutal a um ano já extremamente tumultuado.

Durante 2011, incontáveis milhares de negócios foram direta ou indiretamente afetados por agitação política, crises econômicas e desastres ambientais que moldaram o ano. Muitos dos atingidos mais duramente, talvez a maioria, nunca se recuperará.

Os líderes e executivos sênior de empresas em todo o mundo foram alertados para reavaliar o backup e a recuperação de desastres (DR). Eles devem preparar-se para o pior e assegurar que têm as ferramentas e os meios para suportar o inesperado.

Poucas empresas atualmente podem sobreviver a perdas de dados significativas sem uma estratégia abrangente de backup e DR implementada. No entanto, a maioria das empresas enfrenta um desafio comum: seus dados de negócio estão crescendo a um ritmo insano, enquanto que seus orçamentos de TI permanecem, em termos reais, inalterados. De acordo com as constatações da pesquisa

Uma SMB típica produz cerca de 40 TB de dados novos a cada ano

relacionadas neste relatório, uma SMB típica administra hoje mais de 100 servidores, computadores de mesa e laptops e produz cerca de 40 TB de novos dados a cada ano. É uma enorme quantidade de dados para proteger. Os gerentes de TI descreveram os níveis crescentes de dados a administrar da seguinte forma:

- *“Confuso e caótico... as perdas de dados aumentam”*
- *“Afeta a lucratividade e a produtividade”*
- *“Aumenta os riscos do negócio”*

As constatações da pesquisa sugerem que os desastres de 2011 catalisaram mudanças positivas, levando a maioria das empresas a testarem suas operações de backup e DR. No entanto, apesar das constatações positivas da pesquisa, persiste um número muito elevado de pontos negativos no nível estratégico quando se trata de preservar a segurança, proteção e disponibilidade imediata dos bens digitais essenciais para o negócio da empresa.

O Acronis Global Disaster Recovery (DR) Index 2012 é a maior referência de backup e recuperação de desastres do setor. As empresas podem examinar este relatório e entender o que é necessário para se tornarem líderes na recuperação de desastres. O índice analisa o que mudou nos últimos 12 meses e se as empresas em todo o mundo estão tomando as medidas corretas para proteger o seu ativo mais importante depois de seus funcionários: os dados.

Os desastres de 2011 podem ter provocado mudanças positivas, levando a maioria das empresas a testar suas operações de backup e DR. No entanto, apesar das constatações positivas da pesquisa, persiste um número muito elevado de pontos negativos no nível estratégico quando se trata de preservar a segurança dos bens digitais essenciais para o negócio da empresa.

O que é o Acronis Global Disaster Recovery (DR) Index?

No seu segundo ano, o Acronis Global DR Index é um indicador anual que classifica os países de acordo com os níveis de confiança e os recursos das empresas em relação a backup e DR. O objetivo do índice é oferecer a todas as empresas um melhor entendimento sobre como sua confiança e recursos se comparam às de seus pares em outros países.

Embora as atitudes e percepções de confiança variem entre diversas culturas, o índice oferece a todas as empresas um modelo de tendências e estratégias que ajudará a melhorar sua confiança e seus recursos em relação a backup e DR.

O índice é baseado em um estudo contratado pela Acronis e realizado pelo Ponemon Institute, uma empresa internacional de pesquisa e um respeitado grupo de pensadores sobre as tendências da proteção de dados. A pesquisa foi baseada nas respostas de quase 6.000 profissionais de TI (o dobro dos 3.000 do ano anterior e a maior pesquisa do setor) nos treze países originais e em cinco países adicionais: Arábia Saudita, Alemanha, Austrália, Brasil, China, Cingapura, Estados Unidos, França, Holanda, Hong Kong, Índia, Itália, Japão, Noruega, Reino Unido, Rússia, Suécia e Suíça. Com os mercados emergentes sendo a esperança de crescimento econômico para o resto do mundo, a adição dos países do BRIC oferecerá uma referência sólida para examinar o desempenho desses países em termos de excelência técnica. O índice foi calculado considerando uma grande variedade de setores (Apêndices 1 e 2).

O formato da pesquisa

A pesquisa usou uma combinação de métodos de amostragem omnibus e personalizados, incluindo a amostragem proprietária de profissionais de TI, em empresas de pequeno e médio porte (empresas do mercado intermediário com menos de 1.000 funcionários). O Ponemon Institute executou todas as fases da pesquisa, realizada entre setembro e outubro de 2011

Com os mercados emergentes em evidência em todo o mundo, a adição dos países do BRIC oferecerá uma referência sólida para examinar o desempenho desses países em termos de excelência técnica

Para criar o índice, cada país foi classificado com base nas respostas agregadas a 11 perguntas sobre sua prontidão, seus recursos e suas práticas de backup e DR (Apêndice 3).

As perguntas avaliaram a confiança dos gerentes de TI em sua recuperação de desastres com de acordo com:

- a capacidade e a disposição para adotar novas tecnologias
- a confiança em seus procedimentos e políticas
- o nível de apoio executivo e orçamento/recursos
- a capacidade de recuperação rápida após uma indisponibilidade

Os participantes usaram as seguintes respostas ponderadas para cada pergunta:

Concordância total com uma declaração	5
Concordância com uma declaração	2.5
Neutro	0
Discordância com uma declaração	-2.5
Discordância total com uma declaração	-5

Todos os números de pesquisa comparativos são baseados nos 13 países originais pesquisados em 2010 em relação aos mesmos 13 países em 2011.

O índice é baseado em um estudo realizado pelo Ponemon Institute, uma empresa internacional de pesquisa e um respeitado grupo de pensadores sobre as tendências da proteção de dados. A pesquisa foi baseada nas respostas de quase 6.000 profissionais de TI (o dobro dos 3.000 do ano anterior e a maior pesquisa do setor) nos treze países originais e em cinco países adicionais (BRIC e Arábia Saudita).

Principal Constatação:

A confiança está aumentando

A pesquisa constatou que a confiança global nas mesmas bases de avaliação cresceu 14% nos últimos 12 meses. O aumento mais evidente na confiança foi em relação à disponibilidade suficiente de recursos adequados (ferramentas e ambiente) e da tecnologia adequada para lidar com um desastre. Em ambos os casos, a confiança das empresas cresceu mais que o dobro nos últimos 12 meses (142% e 109%, respectivamente).

A disponibilidade de ferramentas necessárias parece afetar diretamente a capacidade de recuperação rápida em caso de falha de sistema, com um aumento de confiança de 45%. Essa constatação é apoiada por um aumento de 66% na confiança de que as empresas não sofrerão indisponibilidades substanciais em caso de um evento ou incidente sério.

No entanto, essas constatações não permitem ignorar o fato de que cerca de um terço (32%) das empresas ainda está preocupado com falhas nas suas operações de backup e recuperação de desastres em caso de um incidente sério e um número semelhante (34%) considera que sofrerá uma indisponibilidade substancial como consequência.

Há um número crescente de oportunidades de melhoria em diversas áreas:

- Procedimentos e políticas de backup aparentam estar consideravelmente menos bem documentados e a confiança nesta área caiu 44% durante 2011.
- Da mesma forma, as empresas estão 16% menos confiantes sobre a disponibilidade suficiente de controles e procedimentos implementados.

47% consideram que os executivos da empresa não apoiam sua operação de recuperação de desastres, apesar de 2011 ter sido um dos anos mais tumultuados já registrados.

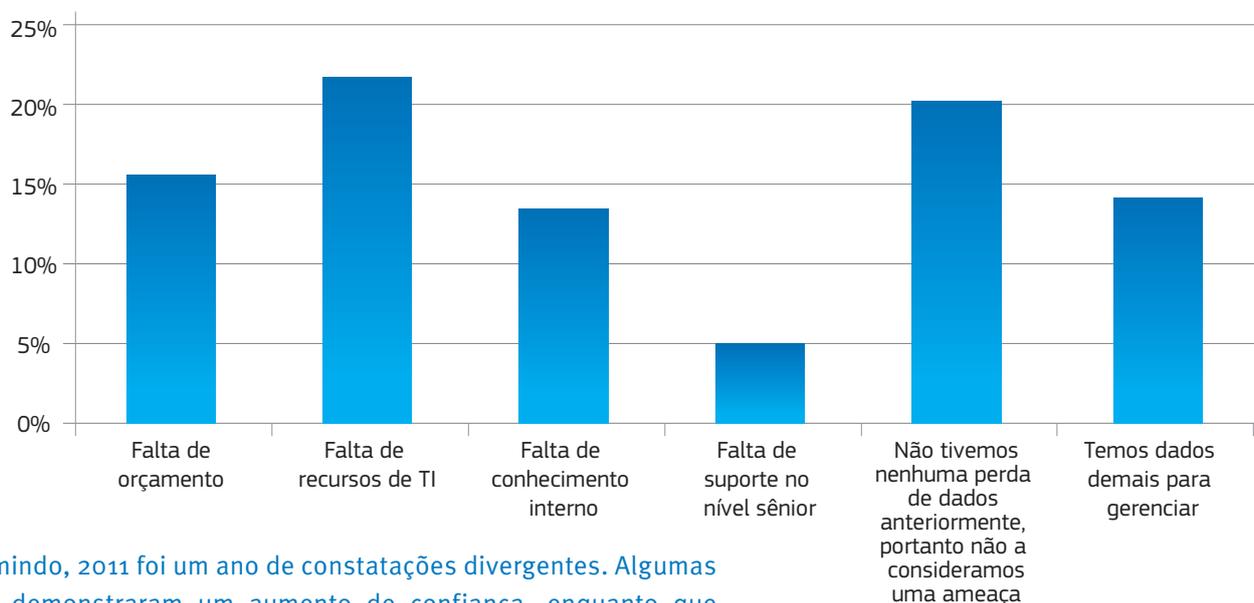
- As empresas não abordaram a carência de equipes qualificadas em 2010. Em 2011, constatou-se um decréscimo de 8% na confiança de que as equipes estão suficientemente qualificadas para lidar com um desastre ou com uma interrupção importante, possivelmente causado pelo ambiente econômico desfavorável.

O dado mais desanimador é uma queda de 13% no apoio da alta administração. Praticamente a metade (47%) considera que os executivos da empresa não apoiam suas operações de backup e recuperação de desastres, apesar de 2011 ter sido um dos anos mais tumultuados já registrados. Os motivos relacionados incluem:

- *“Os executivos querem ouvir boas notícias. A recuperação de desastres é sempre uma má notícia”*
- *“Tenho vergonha do nosso backup e DR”*
- *“TI opera de forma isolada em relação aos outros departamentos”*

Os orçamentos permaneceram inalterados no ano, sem mudanças nos gastos com backup e recuperação. Cerca de dois terços (67%) admitem gastar 10% ou menos de seus orçamentos de TI em operações de backup e recuperação e 22% admitem não gastar nada. Os maiores desafios em relação ao backup e à recuperação permanecem os mesmos do ano anterior, com dois em cada cinco mencionando indisponibilidade de orçamento e recursos de TI como o maior obstáculo para a implementação adequada de DR.

Gráfico: qual o seu maior desafio em relação ao backup e à recuperação de desastres?



Resumindo, 2011 foi um ano de constatações divergentes. Algumas áreas demonstraram um aumento de confiança, enquanto que outras recuaram. Embora o aumento geral seja positivo, diversas lições ainda precisam ser aprendidas.

As classificações do índice: Quanto maior a mudança, mais as coisas ficam como estão

Apesar de um aumento de 14% na confiança geral, a maioria das classificações dos países permaneceu quase que exatamente a mesma, pois o crescimento foi geral. Algumas pequenas mudanças ocorreram nas classificações. Por exemplo, Suécia e Noruega melhoraram, ultrapassando Cingapura, que não progrediu nos últimos 12 meses.

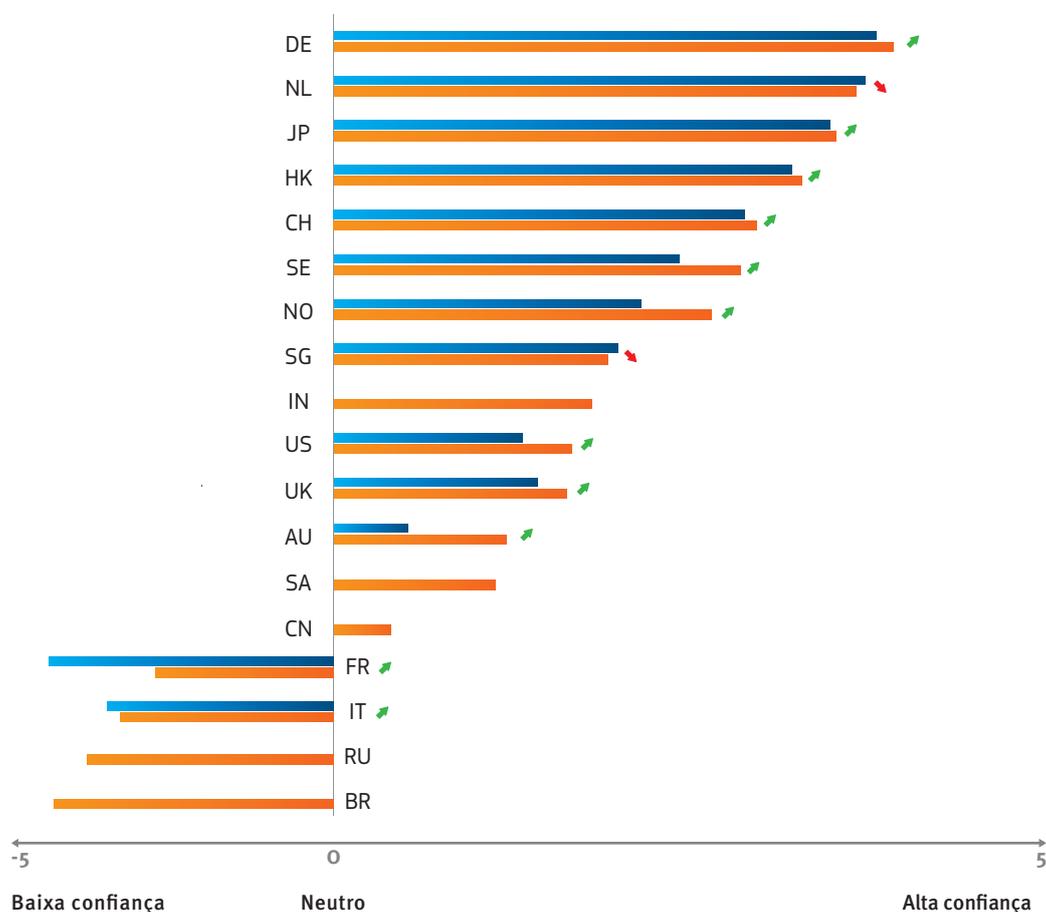
Dos cinco novos países adicionados à pesquisa no ano anterior, apenas um se posicionou entre os 10 primeiros – o índice de confiança da Índia foi 1,21, correspondente ao 9º lugar.

O Reino Unido, ultrapassado em 2011 pelos EUA e pela alta classificação inicial da Índia, caiu da 9ª para a 11ª posição. Entre as regiões que mais melhoraram, estão a Noruega (melhora de 35%) e a França (melhora de 48%). O exemplo mais notável é o da Austrália, onde a confiança aumentou mais que o dobro no ano anterior, demonstrando um aumento de confiança em seus recursos de DR em caso de desastres.

Apesar de um aumento de 14% na confiança geral, a maioria das classificações dos países permaneceu quase que exatamente a mesma, pois o crescimento foi geral.

Acronis Global Disaster Recovery Index 2012

■ 2011 ■ 2012



Média de 2011: 1,14 (média de 2010: 1,00)

A) Líderes invictos: Alemanha e Holanda

Embora os líderes de 2010 tenham mantido as duas primeiras posições no índice pelo segundo ano consecutivo, o seu crescimento de confiança ficou abaixo do aumento médio do mercado de 14%. A confiança alemã cresceu menos que 1%, enquanto que a coragem holandesa na verdade recuou 2% em termos reais. A confiança obviamente tem um limite, mesmo entre as regiões mais completamente organizadas, altamente qualificadas e com ampla disponibilidade de recursos, possivelmente um sinal de que a crise da zona do Euro está se fazendo sentir.

- A confiança alemã nas operações de backup e DR aumentou 21% em 2011, com 70% tendo pouca preocupação com falhas nessas operações em caso de um incidente sério.
- Ao mesmo tempo, as organizações holandesas estão 25% mais confiantes de que têm os recursos adequados (crescimento de 51% para 64%) e 30% mais confiantes de que têm as tecnologias adequadas para abordar backup e DR.

78% dos gerentes de TI japoneses demonstraram pouca preocupação com falhas em suas operações de backup e DR, um possível sinal de que, quando exigida, a nação está amplamente preparada para desastres.

B) Os desafiados: nórdicos e suíços se aproximam rapidamente da Ásia

Japão e Hong Kong mantiveram respectivamente a 3ª e a 4ª posições, mas Suíça, Suécia e Noruega se aproximaram bastante neste ano. A distância também diminuiu porque a confiança de Cingapura diminuiu em 2011 e o país desceu duas posições. Assim como os líderes Alemanha e Holanda, o crescimento marginal da confiança no Japão e Hong Kong, 1% e 2% respectivamente, foi muito menor que o crescimento geral do índice, outra indicação de que há um limite para a alta confiança.

- O Japão tem a maior confiança nas operações de backup e DR, com 78% demonstrando pouca preocupação com falha nessas operações, um possível sinal de que, quando exigida, a nação está amplamente preparada para desastres.

- Nesse grupo, as empresas de Hong Kong são as que têm maior dificuldade para obter apoio da alta administração. Quase um terço (31%) afirma que os executivos da empresa não apoiam suas estratégias de backup e DR, um aumento de 35% sobre o ano anterior (11%).
- Em relação ao ano anterior, as organizações norueguesas estão 28% mais confiantes de que contam com o apoio da alta administração, 33% mais confiantes de que têm recursos suficientes e 12% mais confiantes de que têm as tecnologias necessárias, o que explica a sua posição comparativamente mais alta no índice.
- Da mesma forma, as organizações suecas estão 22% mais confiantes de que têm o apoio da alta administração, 42% mais confiantes de que contam com equipes devidamente qualificadas e 23% de que têm as tecnologias necessárias, em relação ao ano anterior.

A Índia merece uma menção especial, pois embora este seja o primeiro ano em que a confiança foi medida naquele país, alcançou a 9ª posição, com um índice de 1,21, que é o segundo em confiança entre países falantes de inglês, atrás de Cingapura.

A Índia merece uma menção especial. Alcançou a 9ª posição, com um índice de 1,21, que é o segundo em confiança entre países falantes de inglês, atrás de Cingapura.

C) Os intermediários: países falantes de inglês desapontam outra vez

Apesar de Estados Unidos, Reino Unido e Austrália relatarem níveis de confiança abaixo da média pelo segundo ano consecutivo, as regiões demonstraram uma melhoria nos níveis de confiança.

Embora a Austrália tenha a menor pontuação entre os três, sua confiança aumentou mais que o dobro em 2011, crescendo 136%. As organizações australianas estão 36% mais confiantes de que suas operações de backup e DR não apresentarão falhas. Assim como o Japão, a confiança em backups aparenta crescer quando o país se defronta com desastres naturais. Esse aumento em relação ao ano anterior é apoiado pela constatação de que as organizações australianas demonstraram:

- confiança 22% maior de que contam com o apoio da alta administração;
- confiança 32% maior de que têm recursos suficientes;
- confiança 39% maior de que têm as tecnologias necessárias.

A confiança entre as organizações americanas aumentou duas vezes mais que no Reino Unido (35% contra 17%) e, como resultado, os EUA superaram o Reino Unido na classificação. No entanto, ambos ainda têm muito a ser melhorado.

D) O retardatário: China

Embora a confiança entre as organizações chinesas seja extremamente baixa, fica entre os intermediários e os últimos colocados. É interessante observar que, em algumas áreas, os chineses estão razoavelmente confiantes: 36% acreditam que seu backup e DR são bem gerenciados e 46% acreditam que têm a equipe qualificada de TI necessária para gerenciar backup e DR. Ao mesmo tempo, 43% demonstram preocupação com possíveis falhas em operações de backup e recuperação de desastres como resultado de um incidente ou evento sério e a falta de suporte executivo está abaixo da média do setor (39%). Não é uma constatação confortável para a segunda maior economia do mundo.

E) Oportunidades de melhoria: Arábia Saudita, Brasil, França, Itália, Rússia

Das regiões pesquisadas no ano anterior, Itália e França permanecem como as menos confiantes em seu backup e DR, muito provavelmente porque alegam ter o menor suporte, menos recursos e as piores práticas e processos.

Na mesma categoria, Rússia, Brasil e Arábia Saudita têm muito a ser feito para corrigir suas estratégias de backup e recuperação de desastres. A Índia é o único membro do BRIC que demonstra níveis de confiança acima da média.

Embora os níveis de confiança da Itália praticamente não tenham sofrido alteração, a França experimentou um dos maiores aumentos de confiança sobre o ano anterior: 48%. Os principais motivos para o crescimento da confiança francesa incluem:

- confiança 12% maior de que têm os recursos necessários;
- confiança 21% maior na documentação de processos e procedimentos de backup e DR.

43% dos gerentes de TI chineses estão preocupados com possíveis falhas nas operações de backup e recuperação de desastres como consequência de um incidente sério. Não é uma constatação confortável para a segunda maior economia do mundo.

Principais Constatações Globais

Principal Constatação Global 1: A adoção da virtualização por SMBs superará a adoção corporativa em 2012

Principal Constatação Global 2: Dados virtuais em maior risco que os dados físicos

Principal Constatação Global 3: A nuvem avança, mas ainda não atende às expectativas

Principal Constatação Global 4: Estratégia de backup externo ainda insuficiente

Principal Constatação Global 5: Erros humanos são a maior causa de indisponibilidade de sistemas

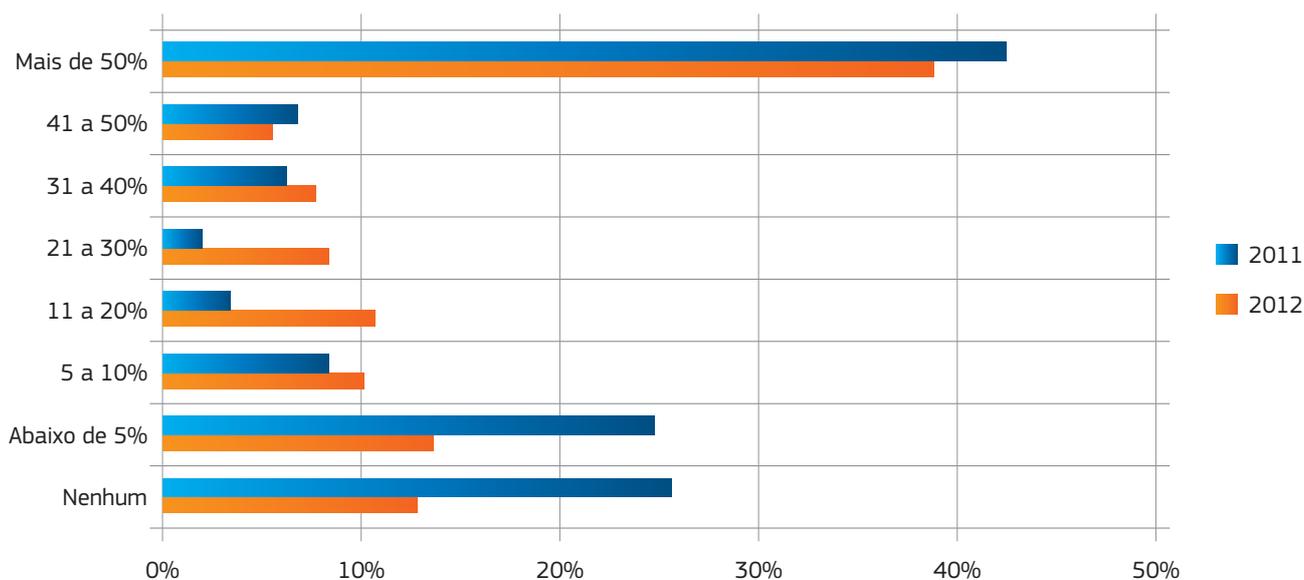
Principal Constatação Global 6: O dilema do fornecedor especializado. Empresas ainda não consolidaram ferramentas de backup e DR

Principal Constatação Global 1: A adoção da virtualização por SMBs superará a adoção corporativa em 2012

A pesquisa constatou que, pela primeira vez, a virtualização de servidores será adotada em um ritmo muito mais rápido entre pequenas e médias empresas (SMBs) que entre as corporações. Um relatório recente do Gartner demonstrou que a adoção de virtualização crescerá 14% nas corporações em 2012. Ao mesmo tempo, o Acronis Global Disaster Recovery Index mostra que a adoção entre SMBs crescerá 21% nesse ano (Gartner's Virtualisation Research Virtual machines will slow in the Enterprise, Grow in the Cloud, Thomas J Bittman, Lydia Leong, 4 de março de 2011, RA1010182011).

Apesar da agitação em volta da virtualização, as constatações da pesquisa sugerem um ritmo de adoção menor que o esperado. As empresas previram que a porcentagem de servidores virtuais utilizados em 2011 atingiria 33%. De acordo com essa pesquisa, a porcentagem média de servidores virtuais utilizados em 2011 foi apenas 24%. As empresas revisaram suas previsões com valores menores e esperam que 29% de seus servidores sejam virtuais até o final de 2012, embora isso ainda represente um crescimento anual de 21%.

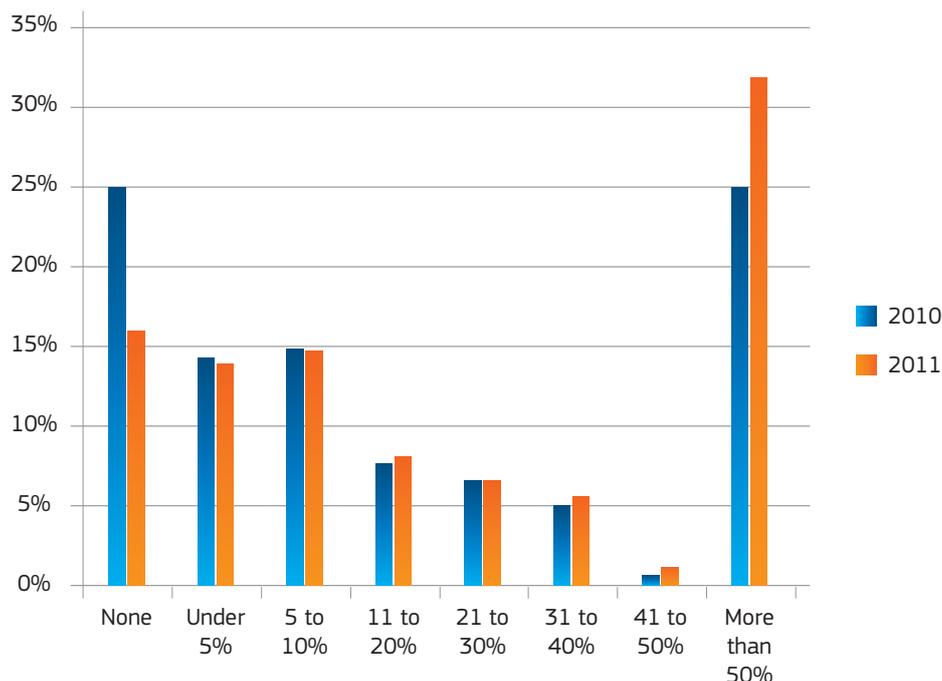
Gráfico: crescimento previsto. Que porcentagem dos seus servidores de produção será virtualizada no próximo ano?



Apesar desses números aparentemente menores que o esperado, quase um terço (32%) dos pesquisados afirmou que mais da metade dos seus servidores de produção eram virtuais em 2011. A virtualização, embora claramente conquistando uma grande base em diversas empresas em todo o mundo, ainda representa uma grande oportunidade de longo prazo.

Em 2012, pela primeira vez, a virtualização de servidores será adotada em um ritmo muito mais rápido entre SMBs que entre as corporações.

Gráfico: crescimento real. Qual a porcentagem de virtualização dos seus servidores de produção hoje?



Os motivos mais citados por empresas globais para a adoção da virtualização foram:

1. maior eficiência (24%);
2. flexibilidade e rapidez de implantação (20%);
3. redução de custo (18%)

Para as SMBs, o principal motivo para a virtualização não é a redução de custos, mas o aumento de eficiência e agilidade.

No entanto, as tendências de virtualização variam consideravelmente em todo o mundo. Hong Kong foi identificado como o usuário mais prolífico de servidores virtuais, com 55% das empresas afirmando que mais da metade dos servidores de produção eram virtualizados. A escassez de espaço físico e a superutilização das fontes de energia podem ser dois grandes motivos para a agressiva taxa de adoção de servidores virtuais em Hong Kong.

Na outra ponta da lista, 41% das empresas de porte médio da Itália ainda não têm uma única máquina virtual. Apenas uma entre dez empresas italianas adotou a virtualização com mais da metade de seus servidores de produção virtualizados. Apesar dessas limitações, a Itália experimentou o dobro do crescimento global médio (18% contra 9%) da porcentagem de servidores virtuais implantados em 2011.

A virtualização ainda tardará para as regiões no final da lista do índice. A Itália e o Brasil são dois países em que respectivamente 39% e 27% das empresas aparentam não ter absolutamente nenhum planejamento para virtualizar um único servidor em 2012.

Para a maioria das regiões, 2012 promete ser outro ano ocupado para a virtualização, à medida que SMBs aproveitam ao máximo sua infraestrutura existente de servidores e armazenamento. Uns consideráveis 38% das organizações pesquisadas esperam ter mais da metade dos servidores de produção virtualizados em 2012.

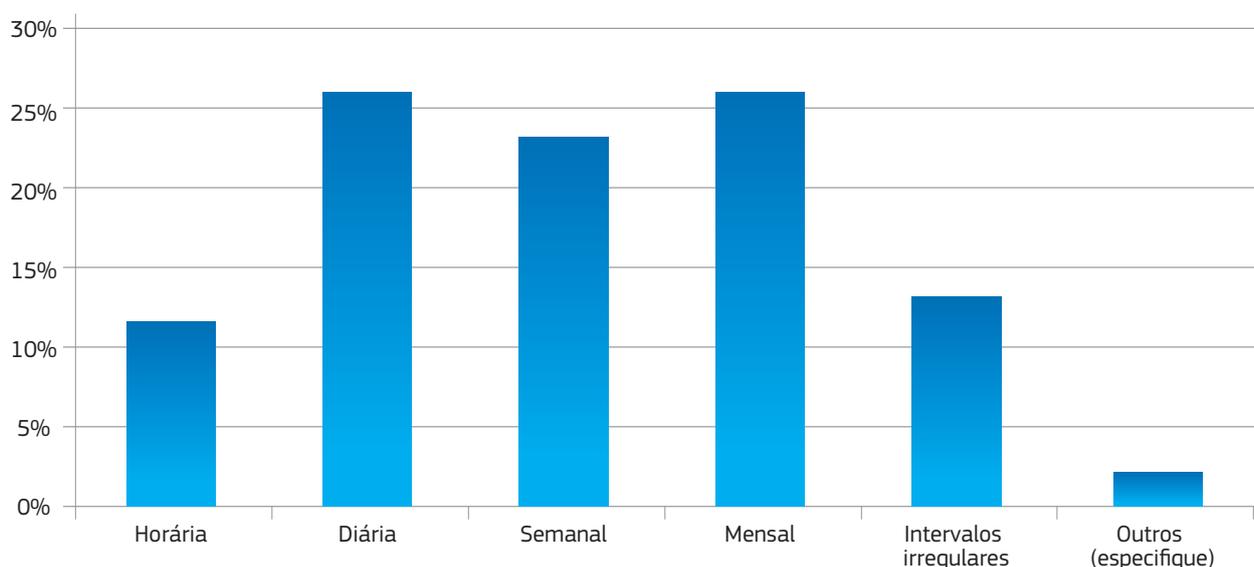
Uns consideráveis 38% das organizações pesquisadas esperam ter mais da metade dos servidores de produção virtualizados em 2012.

Principal Constatação Global 2: Dados virtuais em maior risco que os dados físicos

Apesar do aumento da adoção de virtualização entre as SMBs, a maioria das empresas não está protegendo adequadamente os dados acumulados em máquinas virtuais.

- Um terço (33%), o mesmo que há 12 meses, admitiu que não faz backup de servidores virtuais com a mesma frequência que os servidores físicos.
- Quase a metade (49%) faz backup de máquinas virtuais semanalmente ou mensalmente.
- Pouco mais que um terço (37%) faz backup de máquinas virtuais diariamente.

Gráfico: qual a frequência de backup dos servidores virtuais?



Os maiores culpados estão na Inglaterra (60%), França (58%), Itália (56%) e Brasil (57%), onde mais da metade das organizações pesquisadas admitiu não fazer backup dos servidores virtuais com a mesma frequência que os servidores físicos.

Considerando que o valor monetário dos dados hospedados em servidores virtuais é, de acordo com os participantes da pesquisa, praticamente equivalente ao dos dados hospedados em servidores físicos, essa constatação é preocupante.

Um terço das organizações não fazem backup de seus servidores virtuais com a mesma frequência que fazem de seus servidores físicos.

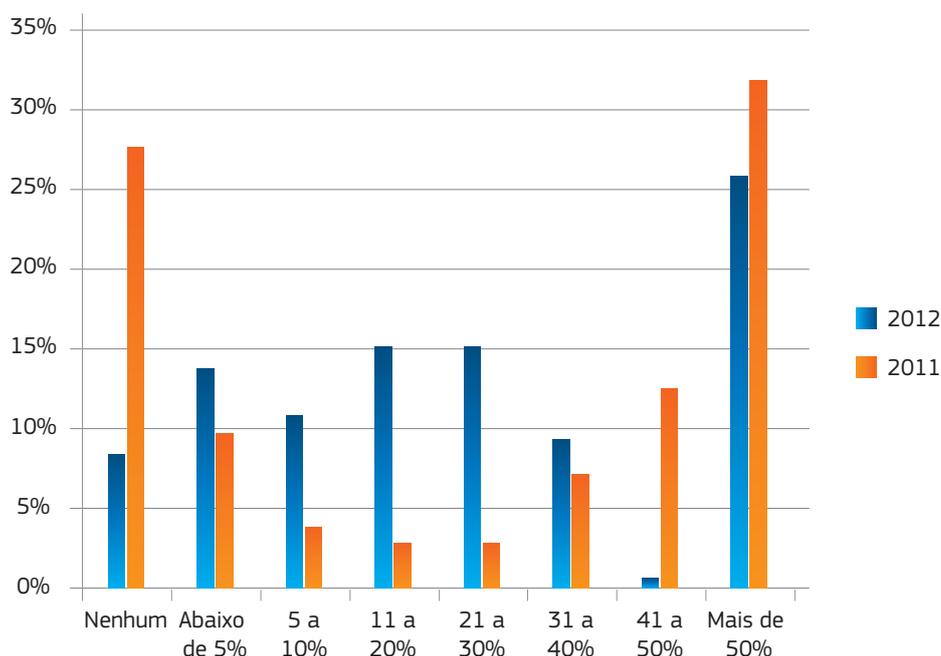
Principal Constatação Global 3: A nuvem avança, mas ainda não atende às expectativas

Dos 6.000 participantes questionados, 83% têm agora alguma forma de infraestrutura baseada em nuvem, o que é um crescimento de 13%. Porém, no geral, a nuvem representa apenas 19% de toda a infraestrutura.

Em 2010, as empresas previram que teriam 30% da infraestrutura na nuvem durante os próximos doze meses, um crescimento de 87% (de 16% para 30%). Entretanto, na verdade, o crescimento da infraestrutura baseada em nuvem nas empresas foi de apenas 19% (de 16% para 19%).

No entanto, a expectativa poderá tornar-se realidade, pois mais de um quarto (26%) estimam que mais de 50% de sua infraestrutura de TI estará baseada na nuvem em 2012.

Gráfico: crescimento previsto. Qual a porcentagem aproximada de sua estrutura de TI que será baseada em nuvem no próximo ano



A expectativa poderá tornar-se realidade, com mais de um quarto estimando que mais de 50% de sua infraestrutura de TI será baseada em nuvem em 2012

Ainda persistem algumas preocupações sérias a respeito do uso da nuvem como parte das operações de backup e recuperação de desastres que precisam ser abordadas. Os participantes da pesquisa citam a recuperação de dados em caso de desastre (56%), riscos de segurança na nuvem (39%) e carga de trabalho e complexidade (33%) como os três principais problemas, os mesmos do ano anterior.

Uma quantidade significativa das empresas citou a falta de confiança real em provedores de nuvem. Mais de uma em cinco empresas na Suécia (25%), França (19%), Itália (23%), Noruega (23%) e Brasil (21%) ainda não tem nenhuma parte de sua infraestrutura atual na nuvem.

Apesar disso, existem alguns progressos, com a Itália mostrando a maior taxa de crescimento de adoção de nuvem, 325%. Para efeito de comparação, a Noruega demonstrou a segunda maior taxa de crescimento, 86%.

Os três principais benefícios do uso da nuvem para backup e recuperação de desastres incluem menores custos operacionais de TI (50%), espaço de armazenamento adicional ou flexível (20%) e melhor conformidade. Os primeiros benefícios são idênticos aos do ano anterior, mas o backup em nuvem por motivos de conformidade cresceu 60% (16% contra 10% em 2010).

Os três principais benefícios do uso da nuvem para backup e recuperação de desastres incluem menores custos operacionais de TI (50%), espaço de armazenamento adicional ou flexível (20%) e melhor conformidade (16%).

Principal Constatação Global 4:

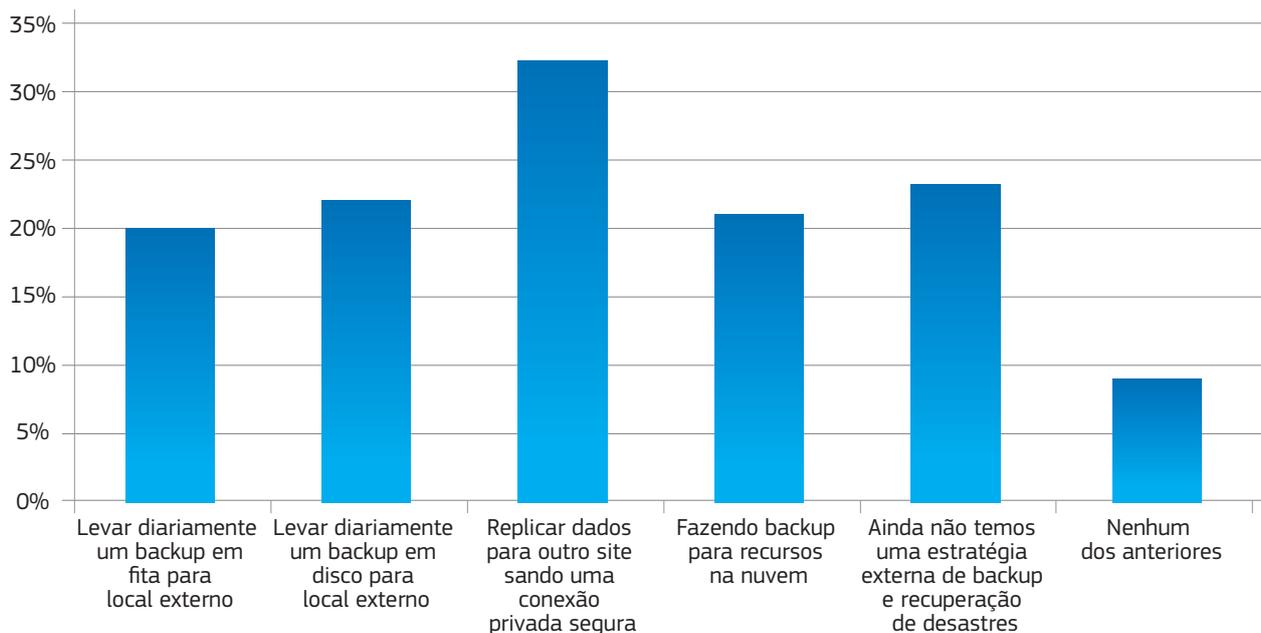
Estratégia de backup externo ainda insuficiente

O software para backup e recuperação locais é essencial para a recuperação de problemas como arquivos excluídos por engano ou quebra de um servidor ou estação de trabalho. Mas os backups locais não podem proteger dados contra as severas consequências de desastres naturais ou causados pelo homem, envolvendo danos físicos a equipamentos de TI e sua possível destruição. A perda permanente de dados e a indisponibilidade de backup externo faz com que muitas empresas não consigam recuperar-se e, muito provavelmente, cessem as operações logo em seguida.

Quase um quarto de todas as empresas ainda não dispõe uma estratégia de backup externo implementada no momento. Essa constatação é praticamente idêntica à do ano anterior e indica que a atitude em relação ao backup externo não foi alterada.

Apesar dos riscos, quase um quarto (23%) de todas as empresas ainda não dispõe de uma estratégia de backup externo implementada no momento.

Gráfico: o que está incluído na sua estratégia de backup externo e recuperação de desastres?



Na Austrália, onde inundações terríveis ocorreram no começo de 2011, mais de um terço (36%) ainda não tem uma estratégia de backup externo, o mesmo que no ano anterior.

- França, Reino Unido e Rússia estão em situação igualmente ruim, com respectivamente 37%, 35% e 33% das organizações desses países ainda sem uma estratégia de backup externo.
- Brasil e Itália estão na pior situação, com quase a metade, 43% e 49% respectivamente, não executando nenhum backup externo.

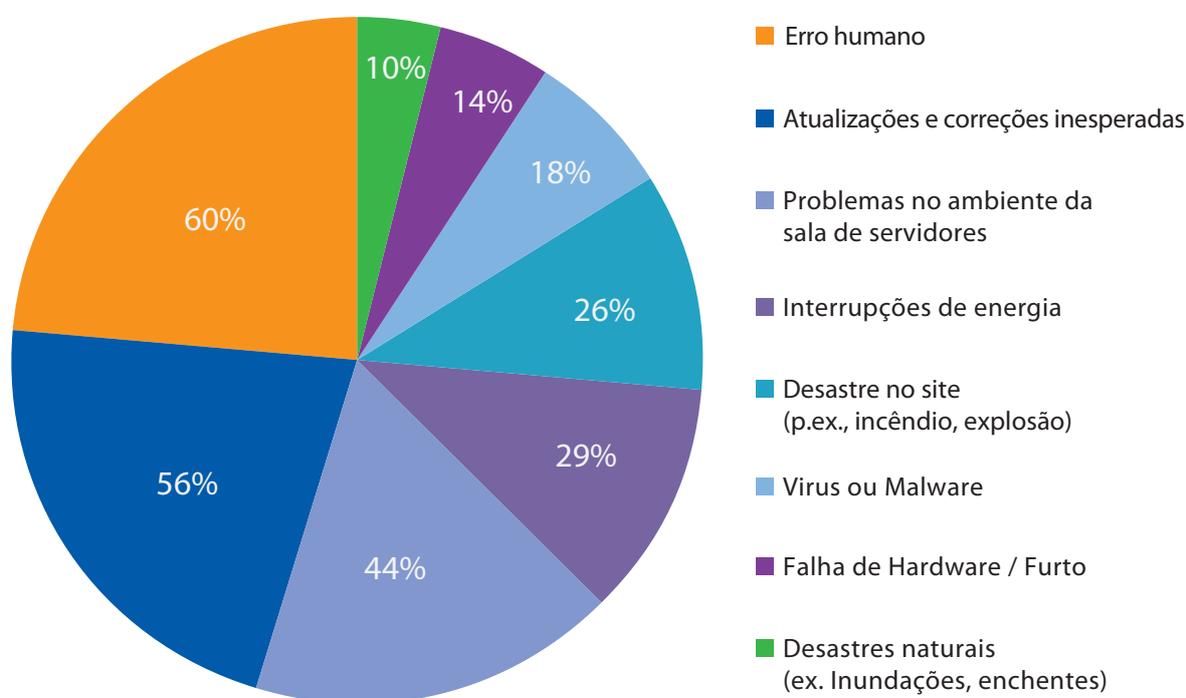
Em vez de automatizar os backups externos, cerca da metade (42%) das empresas aparentemente ainda confia no método tradicional de backup físico no local e em um backup em fita ou em disco e seu armazenamento externo todos os dias. Como esses procedimentos dependem de funcionários individuais, responsáveis pela execução diária dessa tarefa, é aqui que erros humanos podem ocorrer.

Principal Constatação Global 5: Erros humanos são a maior causa de indisponibilidade de sistemas, que custa às empresas US\$ 366.363 por ano

Embora a natureza possa ser a causa dos mais dramáticos desastres que podem atingir uma empresa, os erros humanos ainda são a causa mais comum (60%) da indisponibilidade de sistemas. A incapacidade de recuperação imediata em casos de falha de sistema, especialmente como resultado de erro humano, tem um alto custo.

A grande maioria das organizações pesquisadas (86%) experimentou um ou mais casos de indisponibilidade de sistemas durante os últimos 12 meses, com duração média de 2,2 dias. As empresas calcularam que a perda de produtividade causada diretamente pela indisponibilidade custou a elas aproximadamente US\$ 366.360 por ano.

Gráfico: quais são as principais causas de indisponibilidade não planejada de sistemas?



Um dos problemas é que 44% ainda executam backups apenas de arquivos, em vez de backups de sistema e arquivos. A imagem de backup de um sistema completo, incluindo sistema operacional, aplicativos e preferências de sistema, permite que as organizações recuperem um servidor ou estação de trabalho completo com rapidez. Essa abordagem elimina a necessidade de executar a delicada tarefa de carga e configuração manual de software que, frequentemente, é a parte mais longa do procedimento de recuperação.

Embora o volume de dados tenha crescido, os orçamentos de DR permaneceram inalterados em comparação ao ano passado, estáveis no nível de 10% dos gastos totais com TI. Cerca de um terço cita a falta de orçamento como um motivo para a falta de prioridade para backup e recuperação. Como os dados da empresa são a sua essência vital, é preocupante notar que a proteção desses dados contra desastres ainda não é priorizada nas agendas das empresas.

Principal Constatação Global 6: O dilema do fornecedor especializado. Empresas ainda não consolidaram ferramentas de backup e DR

Um dos motivos pelos quais as empresas têm um histórico de backup de servidores virtuais tão ruim pode ser que mais da metade (53%) usa soluções de backup separadas para ambientes físicos e virtuais. As empresas claramente ainda estão comprando ferramentas separadas de fornecedores especializados para cada um dos ambientes, em vez de comprar uma solução que atenda a todos os ambientes. As razões citadas para o uso de soluções separadas incluem:

- *“Pessoas diferentes estão envolvidas no backup físico e virtual”*
- *“É mais fácil fazer backup de servidores físicos que de servidores virtuais”*
- *“Os aplicativos legados não são compatíveis”*

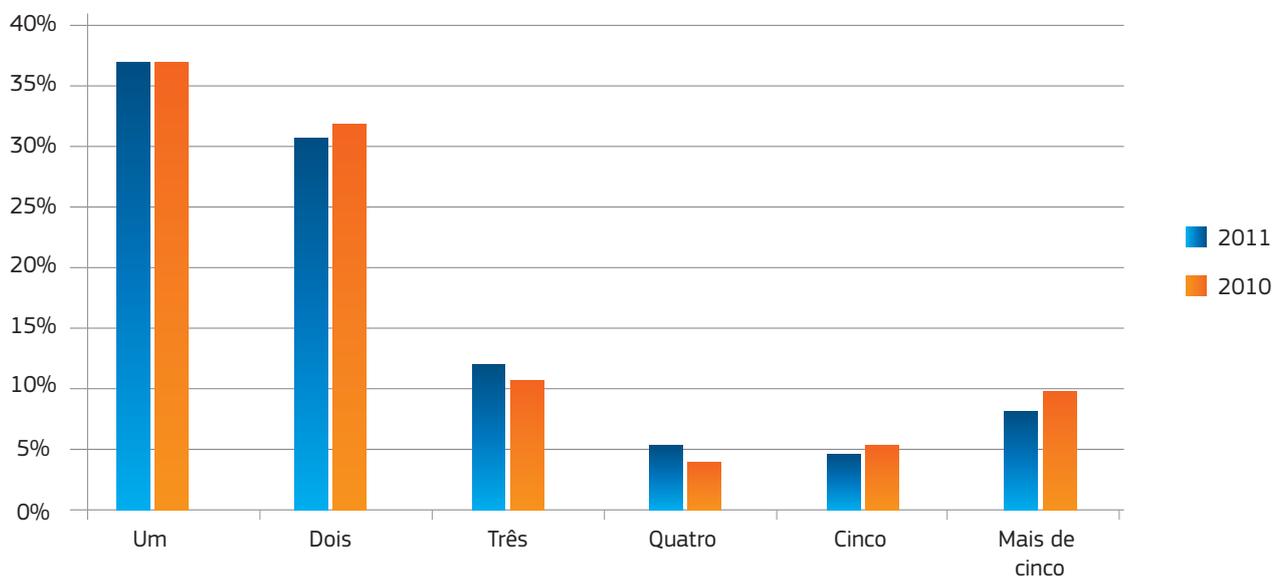
Quase um terço (32%), o mesmo que no ano anterior, usa três ou mais soluções diferentes como parte de sua estratégia de DR, o que é caro e ineficiente. As empresas ainda não consolidaram as ferramentas de DR, tornando o gerenciamento de backup e DR, além da migração de dados entre ambientes diferentes, desnecessariamente mais complicados e demorados. Na verdade, 76% dos pesquisados reconhecem que uma solução abrangente para proteção física, virtual e em nuvem ofereceria a mais significativa melhoria para as operações de backup e recuperação de desastres, pelos seguintes motivos:

- *“Dormiríamos melhor à noite”*
- *“Reduziria risco, complexidade e TCO”*
- *“Nosso CIO prefere uma única solução”*

76% desejam uma única solução para ambientes físicos, virtuais e em nuvem

Está claro que muitas empresas ainda têm um longo caminho a percorrer antes de conseguir ter confiança nas operações de backup e DR. Uma solução única de backup e DR para todos os ambientes facilitaria as operações. 94% das empresas desejam soluções confiáveis e fáceis de usar, um pequeno crescimento em relação aos 91% do ano anterior, e são os revendedores que podem ajudá-los a escolher a solução correta e orientá-los na obtenção de uma estratégia sólida e backup e DR.

Gráfico: número de aplicativos diferentes de backup usados pelas organizações pesquisadas



Recomendações para backup e recuperação de desastres – Uma perspectiva do patrocinador da pesquisa

A comparação de atitudes e níveis de confiança globais a respeito de recursos de backup e DR regionais oferece às organizações uma oportunidade para uma comparação com seus pares muito mais abrangente que a comparação com a organização vizinha.

A pesquisa identificou novamente diferenças extremas nos níveis de confiança em todo o mundo e essas diferenças refletem a natureza diversificada das empresas globais.

A única coincidência em todas as empresas, independentemente de sua origem, é a vontade de tomar as medidas corretas para proteger seus ativos digitais essenciais para o negócio. Além da necessidade de levar o backup e DR mais a sério em termos de investimento e recursos, a maioria das regiões também precisa de um grau mais alto de convencimento dos executivos. A pesquisa mais recente demonstrou que está ocorrendo o contrário em relação ao apoio da alta administração.

Para a maioria das empresas, o sucesso de um serviço é caracterizado pela capacidade de oferecer facilidade de uso, economia e flexibilidade e pela capacidade de implementar medidas com rapidez suficiente para obter um impacto positivo praticamente imediato. Na verdade, poucas empresas podem sobreviver a uma perda de dados significativa sem uma estratégia abrangente de backup e DR implementada. Quanto maior o tempo de recuperação devido a ferramentas, processos ou políticas insuficientes, maior será o impacto direto negativo na produtividade.

Com os orçamentos de TI sendo pressionados, os investimentos futuros em soluções de backup e DR provavelmente não serão aumentados. As empresas enfrentam um triplo desafio em 2012. Precisam proteger mais dados, financiar essa proteção usando um orçamento cada vez menor e implementar essa proteção em um número de ambientes cada vez maior.

Isso exige que os gerentes de TI ajam com maior inteligência. Uma abordagem holística de backup e DR exige ferramentas que possam lidar com backup e DR em ambientes físicos, virtuais e em nuvem.

As empresas enfrentam um triplo desafio em 2012. Precisam proteger mais dados, financiar essa proteção usando um orçamento cada vez menor e implementar essa proteção em um número de ambientes cada vez maior.

A proteção de dados e sistemas de TI é uma jornada, pois está em constante evolução. Mesmo os países mais confiantes precisam monitorar e gerenciar continuamente sua infraestrutura à medida que novas tecnologias afetam suas empresas. Este ano, por exemplo, o uso contínuo de dispositivos móveis para finalidades comerciais trará uma nova dimensão à função do administrador de backups

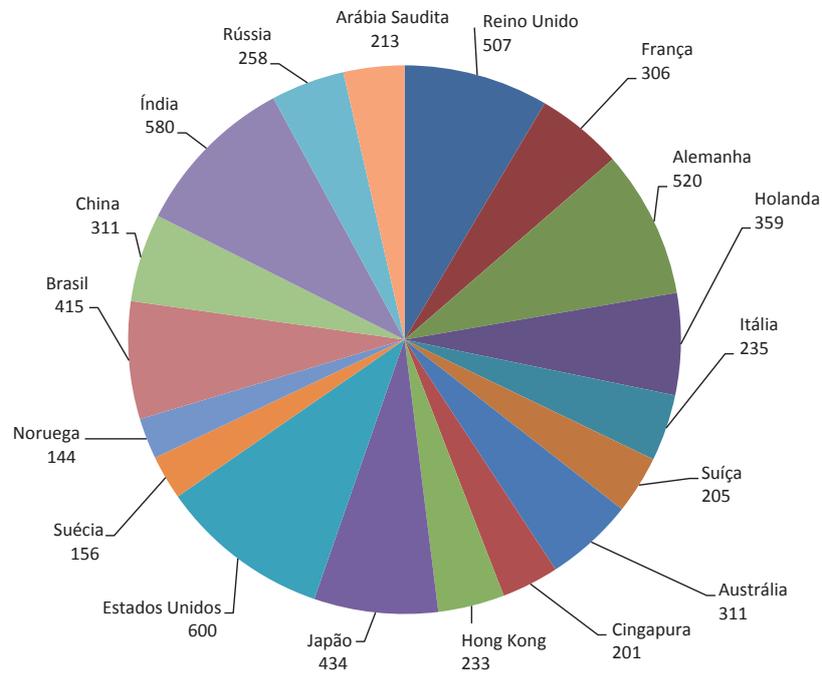
O fato é que os ambientes híbridos continuarão a florescer e que veremos um deslocamento na direção de mais fornecedores desenvolvendo soluções de múltiplos hipervisores e múltiplos ambientes. O gerenciamento de dados em um mundo híbrido permanece um desafio e parte dele é devido à falta de compreensão das tecnologias disponíveis. As empresas precisam certificar-se de que têm uma única solução de backup e DR para proteger seu mundo híbrido.

Para saber mais sobre os resultados da mais ampla pesquisa de DR do setor e para participar dessa pesquisa, visite: <http://acronisinfo.com>.

Está claro que muitas empresas ainda têm um longo caminho a percorrer antes de conseguir ter confiança nas operações de backup e DR. Uma solução única de backup e DR para todos os ambientes facilitaria as operações.

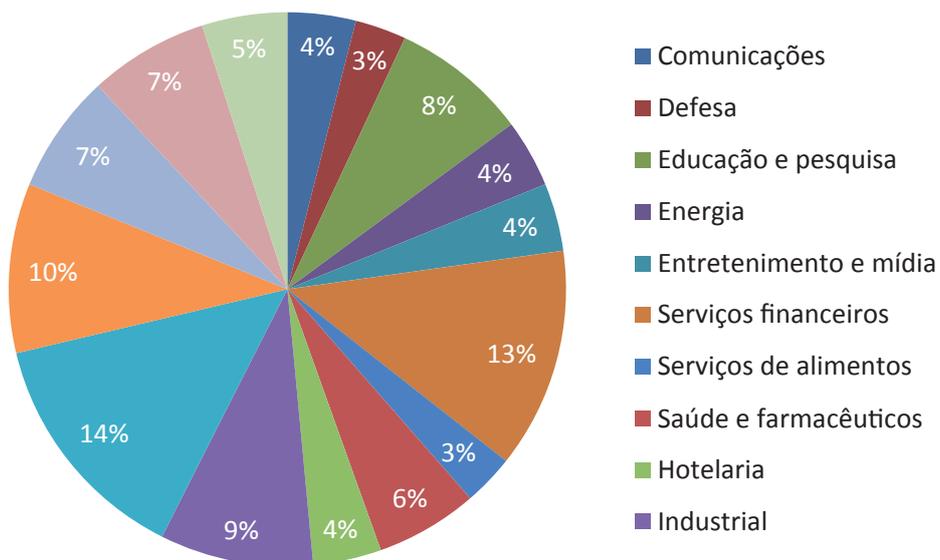
Apêndices

Apêndice 1: distribuição dos participantes por país



*Todas as respostas foram filtradas para garantir o envolvimento da amostragem com backup e DR

Apêndice: Gráfico: distribuição do setor dos participantes



Resumindo: Para saber mais sobre os resultados da mais ampla pesquisa de DR do setor e para participar dessa pesquisa, visite <http://acronisinfo.com>.

Apêndice 3: Perguntas de avaliação de confiança para o índice de recuperação de desastres da Acronis

Classifique a sua opinião sobre as 11 declarações a seguir usando a escala fornecida abaixo de cada item.

Nossas operações de backup e recuperação de desastres são bem gerenciadas.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Temos pouca preocupação com falhas nas operações de backup e recuperação de desastres após um incidente ou evento sério.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Os executivos da empresa apoiam as operações de backup e recuperação de desastres.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Temos amplos recursos que nos permitem operações abrangentes de backup e recuperação de desastres.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Temos amplas tecnologias que nos permitem operações abrangentes de backup e recuperação de desastres.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Temos amplos controles e procedimentos que nos permitem operações abrangentes de backup e recuperação de desastres.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Nossos procedimentos e políticas de backup e recuperação de desastres são bem documentados.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Não sofreríamos indisponibilidades substanciais se nossa organização enfrentasse um incidente ou evento sério (como eventos climáticos, ataques cibernéticos e similares).

Concordância total Concordância Não tenho certeza Discordância Discordância total

Nosso pessoal de TI e segurança está qualificado para executar operações de backup e recuperação de desastres após um incidente ou evento sério (como eventos climáticos, ataques cibernéticos e similares).

Concordância total Concordância Não tenho certeza Discordância Discordância total

A migração para novas tecnologias, como computação em nuvem e virtualização, ajudará a garantir que as operações de backup e recuperação de desastres sejam gerenciadas com eficiência.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Podemos nos recuperar rapidamente em caso de indisponibilidade de sistemas.

Concordância total Concordância Não tenho certeza Discordância Discordância total

Sobre a Acronis

A Acronis é o principal fornecedor de soluções fáceis de usar para recuperação de desastres e proteção de dados para ambientes físicos, virtuais e em nuvem. Sua tecnologia patenteada de imagens em disco possibilita que corporações, SMBs e clientes protejam seus ativos digitais. Com o software de recuperação de desastres, implantação e migração da Acronis, os usuários protegem

suas informações digitais, mantêm a continuidade do negócio e reduzem a indisponibilidade. O software da Acronis é vendido em mais de 90 países e está disponível em até 14 idiomas. Para obter informações adicionais, visite <http://br.acronis.com> Siga a Acronis no Twitter: <http://twitter.com/acronis>.

Sobre o Ponemon Institute LLC

O Ponemon Institute é dedicado à pesquisa e educação independente para a promoção de práticas de gerenciamento de informações e privacidade responsáveis em empresas e órgãos públicos. Nossa missão é realizar estudos de alta qualidade e empíricos sobre questões essenciais que afetam o gerenciamento e a segurança de informações confidenciais sobre pessoas e organizações. Como membro do Conselho Americano de Organizações de Pesquisa (CASRO), cumprimos padrões rígidos de

confidencialidade de dados, privacidade e pesquisa ética. Não coletamos nenhuma informação de identificação pessoal de indivíduos ou de identificação comercial de empresas durante nossas pesquisas comerciais. Além disso, temos padrões rígidos de qualidade para assegurar que os participantes não tenham que responder a perguntas estranhas, irrelevantes ou inadequadas. Para obter mais informações, visite www.ponemon.org.

Para obter informações adicionais sobre o Acronis DR Index 2012, visite <http://acronisinfo.com>



Os detalhes dos escritórios da Acronis podem ser encontrados em <http://br.acronis.com/company/international/>

Para obter informações adicionais ou comprar produtos Acronis, envie um email para brasil@acronis.com

Copyright © 2002-2012 Acronis, Inc. Todos os direitos reservados. "Acronis" e o logotipo da Acronis são marcas comerciais da Acronis, Inc. Os outros nomes mencionados podem ser marcas comerciais ou marcas registradas de seus respectivos proprietários e como tal devem ser considerados. Eventuais diferenças ou erros na reprodução ou publicação de marcas comerciais e marcas registradas não resultarão em prejuízo dos direitos legais. 2012-02