Resiliência da empresa: a necessidade de operações ininterruptas: 24/7/365

IBM®

Preparado para IBM pela TechRepublic

TechRepublic.

ÍNDICE:

Sumário executivo 3
Introdução 4
Por que resiliência? 4
Calculando os custos 6
Virtualizados e replicados 10
Parceria 13

Sobre este relatório técnico: este documento foi preparado pela CBS Interactive em nome da IBM. A IBM especificou o assunto, o título e os principais temas deste guia e pode ter contribuído e exercido controle editorial sobre o conteúdo. Este relatório técnico só pode ser citado e reproduzido na íntegra pela IBM.

Sumário executivo

Os clientes e os parceiros de negócios de hoje em dia esperam operar 24/7/365. Paradas da infraestrutura de TI podem custar milhares de dólares por minuto. Consideramos os custos de remediação, a receita e a produtividade perdidas, os danos reputacionais e as penalidades associadas à não conformidade regulatória e acordos de nível de serviço (SLA). Muitas empresas não conseguem suportar os impactos de uma paralisação inesperada.

Diversos são os fatores causadores de paralisações inesperadas: as quedas de energia, o mau tempo, os problemas de hardware e até mesmo os erros humanos provocam interrupções regulares no serviço de TI e o tempo médio de recuperação é de 24 horas. Embora haja uma grande pressão, na verdade nem todas as empresas estão totalmente preparadas para momentos de contingência. Orçamentos limitados de TI, sistemas cada vez mais complexos e interdependentes, operações de negócios distribuídas e forças de trabalho cada vez mais móveis impactam este cenário.

Tecnologias como virtualização, replicação de dados e computação em nuvem evoluíram para ajudar as empresas a vencer esses desafios de resiliência. Virtualização e replicação estão presentes nos ambientes empresariais, e a adoção de serviços em nuvem cresce consistentemente. Os modelos de resiliência em nuvem incluem as modalidades privadas, compartilhadas, on site e off site. Muitas empresas empregam modelos híbridos para garantir alta disponibilidade para os seus sistemas de negócios mais críticos e recuperação eficiente em custos para componentes não essenciais.

Como algumas modalidades de serviços em nuvem são relativamente novas e complexas, muitos questionam os parâmetros de segurança. Por isso é importante trabalhar junto com um provedor especialista em serviços de resiliência, como a IBM. A IBM oferece um portfolio abrangente de serviços de continuidade e resiliência – além de consultoria especializada – para atender às necessidades de qualquer empresa. Através da sua combinação de data center, hardware, software, especialistas técnicos e serviços em nuvem, a IBM pode gerar um plano de resiliência assertivo e implementar uma solução sob medida que garanta transferência, recuperação, segurança de dados, remediação de eventos e conformidade regulatória. Além disso, a IBM pode administrar toda a solução sem sobrecarregar os recursos de TI internos do cliente.

Introdução

"O servidor está indisponível!" Quatro palavras temidas que podem significar coisas diferentes para pessoas diferentes, mas todas as conotações são negativas. Para o pessoal de TI, significa tentar garantir que os recursos afetados sejam trazidos de volta e estejam funcionando. E também restaurar dados de backup, se necessário. Para a equipe de trabalho, isso significa minutos ou horas de produtividade perdida, frustração e estresse. Para a gestão executiva, significa receita perdida, mais custos, danos para a reputação da empresa e até penalidades se os níveis de serviço exigidos não forem atendidos.

Neste documento, discutiremos os vários fatores que impulsionam a necessidade de resiliência e os custos potenciais de paralisação. Vamos ver os fatos que atualmente estão dificultando a alta disponibilidade e a continuidade dos negócios e vamos explorar novos modelos que permitam às empresas transferirem e recuperarem seus recursos de TI com rapidez e confiabilidade.

POR QUE RESILIÊNCIA?

Nos últimos anos, as empresas tem percebido o quão custoso é a indisponibilidade devida a uma paralisação. Já se foram os dias em que uma interrupção de serviço durante um fim de semana para manutenção podia ser considerada rotineira. Para se manter competitiva, as empresas de hoje devem estar engajadas – transacionando, processando, oferecendo manutenção para os clientes e reagindo às condições de mudanças o tempo todo, no modelo 24/7/365. No nível mais simples, a continuidade da empresa é essencial porque cada minuto de paralisação equivale a receita perdida. E no mais longo prazo, se suas operações forem interrompidas, os clientes poderão migrar seus investimentos para a concorrência.

SLAs

Além disso, muitas empresas estão sujeitas a acordos de nível de serviço que incluem penalidades por não conformidade. No seu "Guia para SLAs", o consultor de gestão de TI, Barclay Rae, explica que SLAs podem ser estabelecidos entre provedores e clientes, parceiros e até departamentos internos. Podem também ser formalizados como contratos de nível de serviço, com responsabilidades e penalidades executáveis.

SLAs forçam as organizações a quantificar e levar em conta todos os elementos da sua operação de serviços de TI, inclusive:

- descrições dos serviços;
- roteiros e mapeamento para remediação de problemas;
- horas de suporte;
- velocidade de resolução para incidentes;
- velocidade de execução de serviços não emergenciais;
- níveis de gravidade de incidentes;
- descrição de responsabilidades dos clientes;
- considerações especiais.

Cada minuto de paralisação equivale a receita perdida.

[1] Barclay Rae, "A Guide to SLAs," julho de 2012

Imergindo nos níveis de severidade das ocorrências, Rae delineia uma amostra de SLA que coloca incidentes de alta prioridade em recuperação de uma hora, incidentes de segundo nível em 4 horas e incidentes de terceiro nível em um dia útil. Mas, mesmo esse nível de responsividade está ultrapassado e pode custar milhares de dólares ou mais, como veremos.

Fonte: Forbes Insights, "How the cloud is changing resilience in the expanding universe of digital data", 2014

CONFORMIDADE REGULATÓRIA

Além dos acordos de nível de serviço com clientes e times internos, muitas organizações de TI estão vinculadas a normas industriais e governamentais, para manter redundância e disponibilidade de sistemas críticos e dados sensíveis. Empresas globais devem manter conformidade com as leis de proteção de dados pertinentes em todos os países onde operam, como por exemplo:

- Basel II, exigindo disponibilidade de sistemas para as instituições financeiras internacionais;
- Diretiva de proteção de dados da União Europeia, relacionadas a backup de dados e disponibilidade;
- Sarbanes-Oxley, relacionada aos dados financeiros em empresa de capital aberto nos EUA;
- HIPAA, exigindo disponibilidade de dados para informações de saúde dos EUA.

Essas normas exigem que as empresas mantenham recursos redundantes, além de backup de dados abrangente e seguro para manter a integridade das informações. Incluem penalidades financeiras significativas para as empresas que não estão em conformidade. Essas multas devem ser levadas em conta quando as empresas avaliam os custos de uma paralisação potencial.

CALCULANDO OS CUSTOS

De acordo com o estudo "2014 Cost of Data Breach Study" do Ponemon Institute, o valor em dólares que as empresas atribuem aos incidentes de dados devem incluir custos diretos, indiretos e de oportunidade para refletir os danos monetários corretamente. Esses fatores incluem:

- Detecção do incidente
- Contenção do incidente
- Recuperação de redes, dados e/ou sistemas centrais
- Perícia forense associada a investigação pós-evento
- Terceiros engajados para ajudar a remediar o problema e sistemas de auditoria
- Custas legais associadas às violações de conformidade e do cliente
- Treinamento/carga de trabalho aumentada para pessoal de serviços técnicos e de apoio
- Receita perdida por interrupção de negócios
- Oportunidades perdidas por rotatividade de clientes

Sessenta por cento desses incidentes foram causados por erro humano e falhas técnicas do sistema.

Levando isso em consideração e aplicando em uma amostra de pesquisa de 314 empresas em dez países, a Ponemon descobriu que o custo médio por incidente foi de US$145 globalmente, um aumento de 9% em relação a 2013. Os custos médios totais de incidentes vão de US$3 milhões a quase US$6 milhões, dependendo do país. É importante notar que essas violações não estão limitadas a ataques cibernéticos. Em média, 60% desses incidentes foram causados por erro humano e falhas técnicas do sistema, em outras palavras, interrupção de TI.

OS CUSTOS PODEM VARIAR

Naturalmente, nem toda empresa observará custos tão altos e outras podem ter custos ainda mais altos. Dependendo da indústria, violações e interrupções de serviço podem custar muito mais que a média. Violações do setor de assistência à saúde, por exemplo, custaram US$359 por incidente, de acordo com a Ponemon.

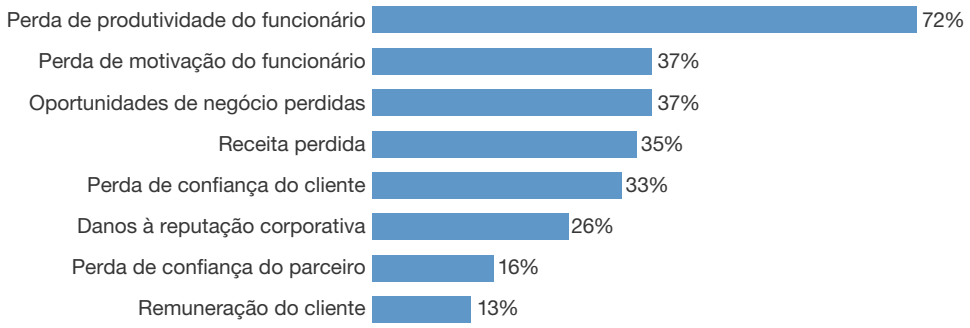
No caso de inscrições para cartões de crédito, que estão instaladas em muitas empresas, uma hora de paralisação pode custar até US$2,6 milhões e uma interrupção da página inicial de 49 minutos da Amazon.com, em janeiro de 2013, custou à empresa quase US$5 milhões, de acordo com estimativas citadas pelo Neverfail Group.[3]

[2] Ponemon Institute, "2014 Cost of Data Breach Study", maio de 2014

[3] Neverfail Group, "Downtime Report: Top Ten Outages in 2013", Dezembro de 2013

Atualizações ao plano de recuperação de desastres precisam mudar

"Considerando a interrupção mais significativa de sua empresa, quais das opções abaixo acabou ocasionando os maiores impactos na sua organização?"
(Classificação 1- 3)



Base: 66 tomadores de decisão e influenciadores globais de recuperação de desastres que declararam um desastre ou tiveram uma interrupção de negócios importante

Fonte: Forrester Research, "State of Business Technology Resiliency, Q2", maio de 2014

Num estudo conduzido no ano passado pela Continuity Software, 43% dos entrevistados disseram que cada hora de paralisação custa US$100.000 ou mais, e 12% disseram que cada hora custa mais de US$1 milhão. A ampla maioria dos entrevistados – 90% – disse que a disponibilidade dos serviços é fundamental para seus clientes. Além disso, 73 dos entevistados da pesquisa da Continuity disseram que suas metas de disponibilidade ficam acima de 99,91%, ou menos de oito horas de paralisação não planejada por ano. Esse número está crescendo em comparação com os dados de 2013 , que eram de 68%.[4]

O custo de paralisação vai divergir de uma empresa para outra, mas está crescendo consistentemente nas indústrias nos últimos quatro anos, e este cálculo é um bom exercício para entender e comunicar a necessidade de medidas de resiliência.

TENDÊNCIAS ATUAIS

É interessante observar que apesar das pressões existentes já citadas, as iniciativas de resiliência em muitas empresas continuaram relativamente estagnadas nos últimos anos.

O relatório da Forrester Research "State of Business Technology Resiliency, Q2 2014" (O estado da resiliência da tecnologia de negócios, 2º trimestre de 2014) mostra que, enquanto a demanda por objetivos de tempo de recuperação rápida (RTO) pode estar subindo no lado das empresas, o tempo real de recuperação foi em média de 24 horas em 2013, acima das 18,5 horas em 2010. Na verdade, apenas 2% dos entrevistados na pesquisa da Forrester de 2013 disseram que poderiam recuperar em menos de 1 hora.[5]

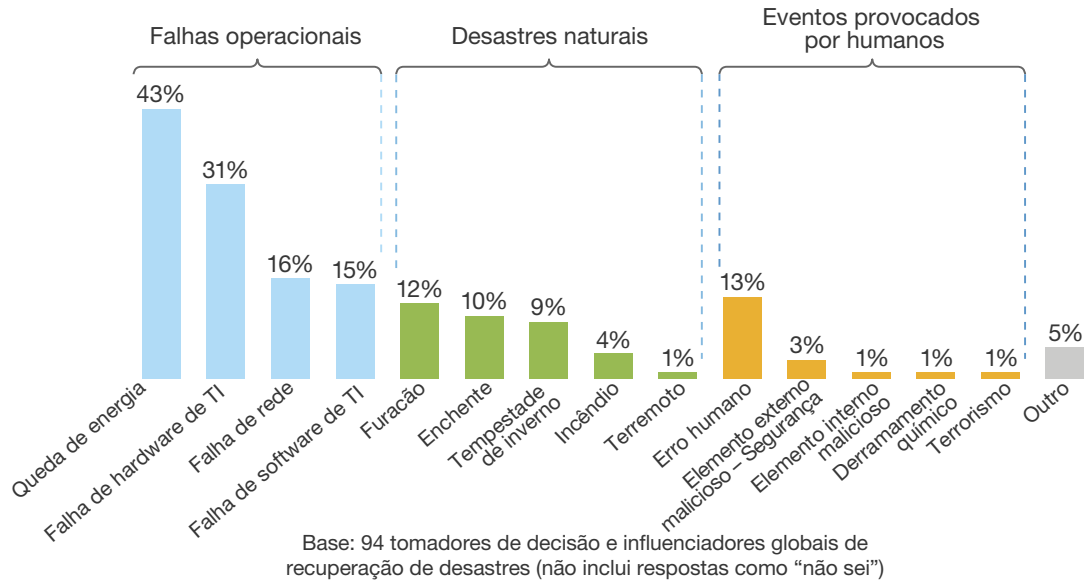
Entretanto, as causas da paralisação têm sido as mesmas. Os dados mostram que, apesar de desastres em larga escala, como o furacão Sandy que dominou as manchetes, quedas de energia, quedas de TI e erro humano são as causas mais comuns de paralisação de negócios, de acordo com a Forrester.

[4] Channel Insider, "Helping Combat Downtime, On-Premise and in the Cloud", junho de 2014

[5] Forrester Research, "The State of Business Technology Resiliency, Q2 2014", maio de 2014

Causas mais comuns de paralisação são eventos mundanos e não desastres

"Quais as causas de seus eventos de desastre mais significativas ou de suas maiores interrupções de negócios?"



Base: 94 tomadores de decisão e influenciadores globais de recuperação de desastres (não inclui respostas como "não sei")

Fonte: Forrester Research, "State of Business Technology Resiliency, Q2 2014", maio de 2014

Outros institutos também concordam com os dados. No estudo da Continuity Software acima mencionado, 87% dos entrevistados experimentaram um evento de paralisação durante os três meses da pesquisa, e as causas mais comuns foram falha de hardware, atualizações de equipamento, erro humano e quedas de energia.

Da mesma forma, o relatório da KPMG, "2013-2014 Continuity Insights", citou o mau tempo e as quedas de energia como a principal causa de paralisação, ficando os erros de TI em terceiro lugar.[6]

Assim, se as causas de paralisação estão sendo constantes, porque os custos e tempos de recuperação estão piorando de um ano para o outro?

Quedas de energia, falhas de TI e erro humano são as causas mais comuns de paralisação nos negócios.

MUDANÇA DE CENÁRIO

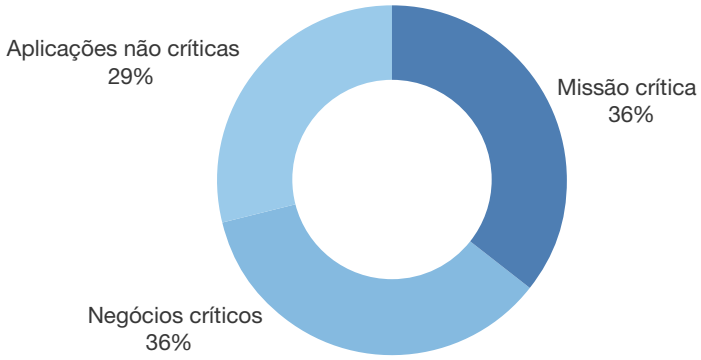
A resposta está nos ambientes de TI que se tornaram mais complexos e distribuídos, quando as empresas acompanham a concorrência global. Cada vez mais, os trabalhadores remotos e móveis de todo o mundo precisam de acesso a sistemas de negócios essenciais em todos os momentos, em vários dispositivos e, como referimos, qualquer interrupção cria uma bola de neve de danos financeiros.

A Forrester se refere a essa tendência como "a era do agora". No relatório acima mencionado, a analista Stephanie Balaouras explica que aplicações de comunicação tornaram-se elementos de missão crítica de todas as operações de negócios. As expectativas do cliente estão em sua maior alta e as interdependências entre as aplicações (uma ferramenta de vendas que depende de uma base de dados particular através de uma estrutura de gestão do processo de negócios, por exemplo) criam um ambiente onde mais componentes são considerados essenciais.

[6] KPMG, "The 2013-2014 Continuity Insights and KPMG LLP Global Business Continuity Management (BCM) Program Benchmarking Study", abril de 2014

Níveis de missão crítica e negócios críticos estão aumentando

"Qual a porcentagem das suas aplicações e dados que se encontram nos níveis abaixo?"



Base: 94 tomadores de decisão e influenciadores globais de recuperação de desastres
(não inclui respostas como "não sei"; as porcentagens não somam 100 por conta de arredondamento)

Fonte: Forrester Research, "The State of Business Technology Resiliency, Q2 2014", maio de 2014

Ao mesmo tempo, os orçamentos de TI continuaram virtualmente estáveis desde a recessão econômica de 2008, com a recuperação só começando a aparecer em 2015, de acordo com a empresa de pesquisas Corporate Executive Board. Isso significa que não tiveram os recursos para investir na atualização ou facilitação das suas estratégias de resiliência.

Além disso, a mobilidade está mudando a forma como os trabalhadores executam suas tarefas. Em 2012, o IDC estimou que o número de trabalhadores móveis chegaria a 1,3 bilhão em 2015, representando mais de 37% da força de trabalho global. Mais recentemente, o Gartner iberou uma previsão dizendo que até 2016, 38% dos empregadores exigiriam que seus trabalhadores usassem seus próprios dispositivos móveis para trabalhar, e esse número chegaria perto de 50% em 2017.[9]

Todos esses fatores oferecem obstáculos para as configurações de resiliência tradicionais, que envolvem hardware redundante (que tem manutenção dispendiosa) e cópias de segurança gravadas (que são demoradas nos cenários de recuperação). Criam também vários pontos de falha potencial, já que os caminhos da rede e as dependências dos dispositivos devem ser mapeadas com cuidado e correção. Qualquer erro durante a transferência pode destruir toda a infraestrutura.

Nesse cenário de negócios cada vez mais interconectado e de rápida evolução, as empresas procuram soluções de resiliência mais inteligentes para proteger sua infraestrutura, seus dados, suas operações e seus trabalhadores.

[7] Corporate Executive Board, "IT Budget Benchmark Key Findings", 2014

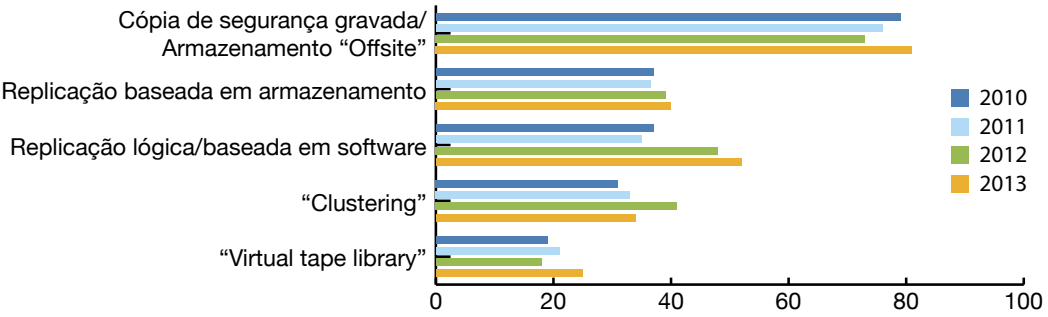
[8] Reuters, "Mobile Worker Population to Reach 1.3 Billion by 2015, According to IDC", janeiro de 2012

[9] Gartner, "Bring Your Own Device: The Facts and the Future", maio de 2013

VIRTUALIZADOS E REPLICADOS

Graças à virtualização – formação de uma rede de cargas de trabalho aplicadas ao hardware em que estão funcionando – a resiliência é uma meta mais atingível para as empresas de todos os portes e indústrias. Servidores inteiros, e até ambientes inteiros, podem ser modificados para recursos de contingência com mínima paralisação, e muitas empresas replicam todas as atividades de negócios em tempo real, de forma que o ambiente de contingência fica pronto para transferência quase instantânea.

Tecnologias de proteção de dados: 2010 a 2013



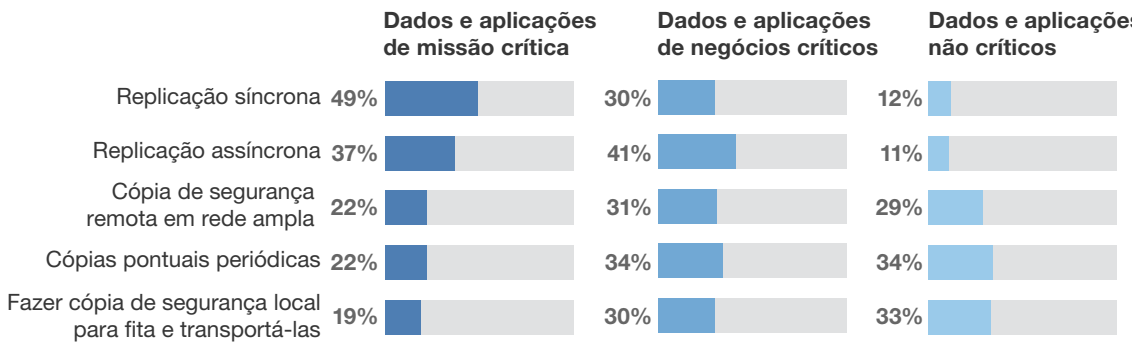
Fonte: Vision Solutions, "State of Resilience 2013", janeiro de 2014

A pesquisa de 2014 da Continuity Software descobriu que 72% dos entrevistados usam a virtualização para alta disponibilidade nos seus ambientes, acima dos 63% de 2013.

A Vision Solutions, na sua pesquisa "State of Resilience 2013" (Estado de resiliência 2013) com mais de 3.500 profissionais de TI, mostra um aumento marcante nas instalações de replicação baseada em software de 2010 para 2013. A Forrester encontrou uma tendência semelhante ao comparar 2010 com 2013, com o uso de replicação crescendo de 35% para mais de 50%. Cópia de segurança, acrescenta o relatório, ainda é o método mais popular de proteção de sistemas não essenciais.

Dados entre os principais sites de recuperação

"Como você copia dados entre seus principais sites de recuperação?"



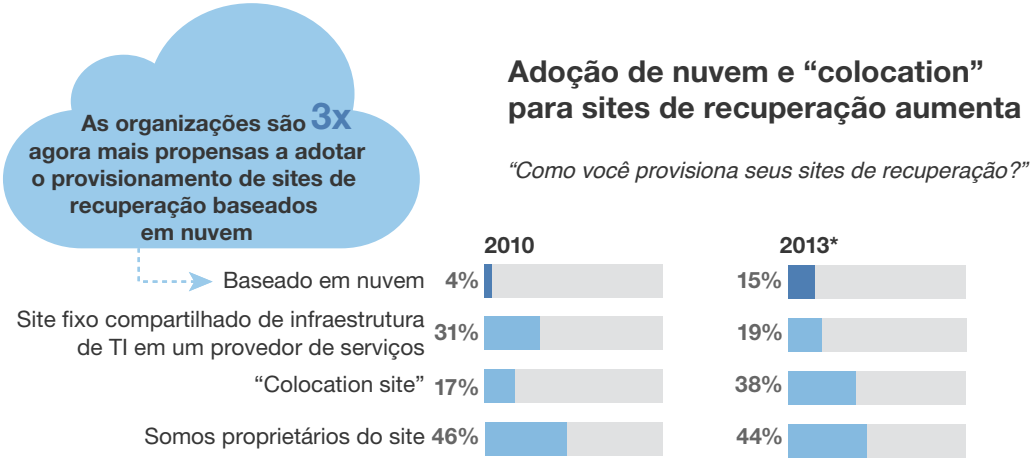
Base: 94 tomadores de decisão e influenciadores globais de recuperação de desastres (não inclui respostas como "não sei")

Fonte: Forrester Research, "The State of Business Technology Resiliency, Q2 2014", maio de 2014

[10] Vision Solutions, "State of Resilience 2013", janeiro de 2014

ADOTE O SERVIÇO NA NUVEM

Os componentes finais nos planos de resiliência da próxima geração são serviços em nuvem. A capacidade de hospedar recursos em infraestrutura redundante fora do local – e de transferir dados e componentes virtualizados em velocidades WAN ou melhor, cria várias opções de transferência para as empresas que querem garantir recuperação rápida em casos de interrupção.



Base: 180 tomadores de decisão e influenciadores globais de recuperação de desastres
*Base: 85 tomadores de decisão e influenciadores globais de recuperação de desastres (não inclui respostas como "não sei")

Source: Forrester Research, "The State of Business Technology Resiliency, Q2 2014", maio de 2014

Além dos recursos internos tradicionais, essas opções incluem:

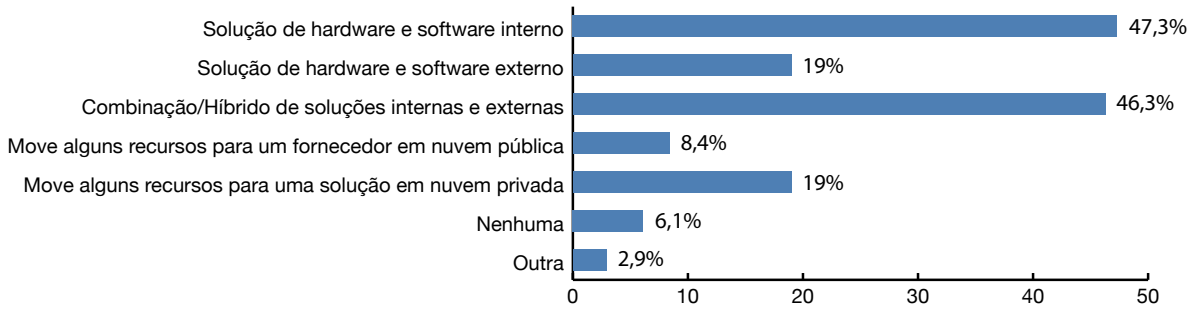
- Recursos dedicados off site, em sites de contingência
- Infraestrutura compartilhada em instalação off site
- Nuvem on site ou privada
- Nuvem pública

Setenta e dois por cento dos entrevistados usam a virtualização para elevada disponibilidade.

Muitas empresas estão buscando estratégias que combinem várias dessas opções em uma solução de resiliência híbrida. De acordo com a Forrester, a adoção de recuperação baseada em nuvem subiu de 4% em 2010 para 15% em 2013 e a sua adoção continua crescente. Um entre cinco disseram à Forrester que eles usam um mix de modelos para fornecer transferência rápida para sistemas críticos, e um modelo de recuperação mais faseado, para elementos não críticos.

A KPMG encontrou uma adoção um pouco maior para soluções híbridas e em nuvem de recuperação de desastres, com quase 20% citando a nuvem privada e apenas 8% indicando que usam serviços de nuvem pública para algumas cargas de trabalho.

Estratégias DR atuais de TI das organizações



Fonte: KPMG, "The 2013-2014 Continuity Insights and KPMG LLP Global Business Continuity Management (BCM) Program Benchmarking Study", abril de 2014

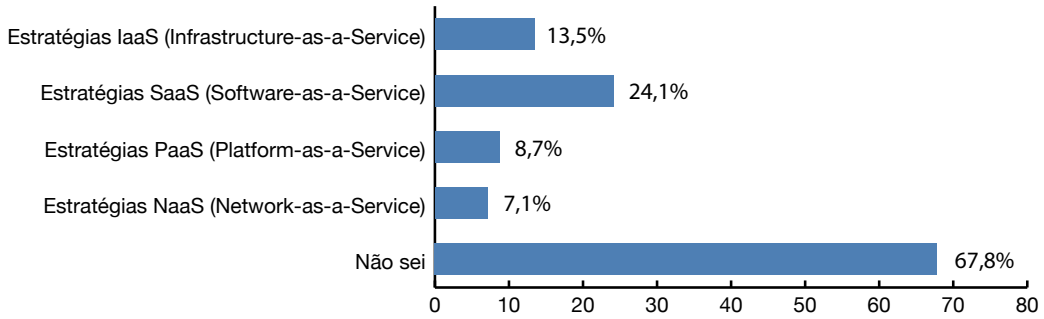
A COMPLEXIDADE NA ADOÇÃO DOS SERVIÇOS EM NUVEM

Como os serviços em nuvem são relativamente novos e sua adoção – especialmente em grandes organizações – é geralmente esporádica e descentralizada, existem também muitos questionamentos em torno de parâmetros de SLAs em nuvem; a proteção, propriedade e localização de dados, e quem é responsável por interrupções de serviço que afetam os provedores em nuvem.

Por exemplo, no estudo da Continuity Software, 44% dos entrevistados disseram que sua disponibilidade de serviços em nuvem está em paridade com seus sistemas internos. Quase 30% disseram que a disponibilidade dos seus serviços em nuvem é menor do que seus outros sistemas, e 26% disseram que a disponibilidade de serviços em nuvem é superior. Estes dados parecem indicar que as empresas não têm necessariamente um entendimento sólido dos indicadores de disponibilidade para seus serviços internos e baseados em nuvem.

Essa conclusão nasce dos achados da KPMG, que indicam que 68% dos entrevistados não entendem a natureza das suas medidas de recuperação de desastre de TI baseadas em nuvem. Apesar de os serviços de recuperação geralmente incluírem infraestrutura sob demanda (IaaS) e soluções de software hospedado (SaaS) – e as plataformas de computação hospedadas (PaaS) e soluções de rede (NaaS) em menor escala – a maioria dos profissionais pesquisados não tinham a menor ideia do que seus planos de resiliência em nuvem incluíam.

As organizações implementaram atualmente planos DR de TI em nuvem,



Fonte: KPMG, "The 2013-2014 Continuity Insights and KPMG LLP Global Business Continuity Management (BCM) Program Benchmarking Study", abril de 2014

PARCERIA

Nós entendemos que a resiliência é um fator importante para as empresas e, em muitas formas, difícil de ser implementada. Os serviços em nuvem podem levar a virtualização e a replicação para o próximo nível, fornecendo vários tipos de hospedagem de recursos fora do local.

Por causa da enorme confusão que ocorre em torno dos serviços em nuvem, é importante trabalhar junto com um provedor de serviços de resiliência especializados para garantir os SLAs e interdependências exigidas para uma instalação de recuperação híbrida bem-sucedida.

Felizmente, as empresas podem fazer parcerias com a IBM, a líder indiscutível e reconhecida de soluções de tecnologia de negócios, para serviços de resiliência que abrangem desde sites de contingência a ambientes de resiliência baseados em nuvem.

SERVIÇOS DE RESILIÊNCIA DA IBM

A IBM oferece um portfolio abrangente de serviços de continuidade e resiliência – além de consultoria especializada – para atender às necessidades de qualquer empresa. Através da sua combinação de centros de dados, hardware, software, especialistas técnicos e serviços em nuvem, a IBM pode gerar um plano de resiliência bem projetado e implementar uma solução sob medida que garanta transferência e recuperação, segurança de dados, remediação de eventos e conformidade regulatória. Ainda melhor, a IBM pode administrar toda a solução sem a necessidade do cliente expandir os recursos internos de TI.

Os serviços de resiliência da IBM incluem:

Consultoria de resiliência: profissionais especializados, experiência de décadas na área de continuidade e o histórico de instalações bem-sucedidas da IBM para planejar, desenhar, integrar e testar sua estratégia de resiliência e continuidade em toda a empresa, levando em conta aplicações e infraestrutura nas sedes e em todos os escritórios.

Recuperação de infraestrutura: a IBM conduz uma avaliação detalhada dos seus sistemas de TI e define uma estratégia de recuperação e proteção de dados, completa com cópias de segurança fora do local e assistência de recuperação no local em caso de incidente. Esse serviço é ideal para empresas com requisitos de conformidade regulatória e ambientes complexos.

Gestão de disponibilidade: consultores IBM especializados analisam incidentes anteriores e criam uma estratégia que se alinha aos seus processos comerciais e ajuda a evitar paralisações futuras. Um gerente de programa dedicado supervisiona cada fase do projeto, deixando seus recursos de TI internos livres para apoiar as operações e a inovação comercial.

Resiliência administrada: depois que você tiver designado a informação e os sistemas que você necessita que estejam disponíveis em caso de ruptura, a IBM oferece gestão de resiliência para você, com serviços proativos e de resposta a eventos que podem ser elaborados com base na criticidade.

Resiliência em nuvem: os serviços em nuvem da IBM incluem cópia de segurança, recuperação e gestão de dados virtualizada para oferecer acesso flexível e controle abrangente. Recupere servidores, aplicativos e dados em poucos minutos para reduzir os riscos, melhorar a conformidade e preservar a produtividade.

Recuperação de servidores em nuvem: garantindo seus recursos virtuais e não virtuais contra a inatividade,

os serviços de recuperação em nuvem da IBM automatizam os procedimentos de transferência e melhoram a confiabilidade das operações de negócios. Esse serviço apoia um amplo conjunto de sistemas e plataformas operacionais do servidor.

Backup gerenciado: se você estiver buscando uma solução de backup abrangente que inclua replicação no local e/ou fora do local, conheça os serviços de backup gerenciado da IBM. Essa solução apoia modelos em nuvem, tradicionais ou híbridos, e entrega ambientes escalonáveis dinamicamente, que reduzem o custo total e incluem criptografia/deduplicação para oferecer eficiência e proteção para as empresas.

A DIFERENÇA IBM

IBM Resiliency Services é o único provedor realmente global que habilita resiliência em todas as camadas da empresa. Ele suporta as instalações do cliente de várias maneiras:

- A IBM mantém mais de 312 centros de resiliência em todo o mundo que fornecem computação e formação de rede para apoiar a camada tecnológica, replicação e proteção de dados nas camadas de aplicação e dados, e metodologia de consultoria de resiliência de categoria internacional.
- Essas instalações incluem mais de 900 mil metros quadrados de espaço do centro de dados para operações de recuperação de desastres e resiliência, com mais de 41.000 posições de área de trabalho para recuperação de operações de local de trabalho.
- Os serviços de resiliência de IBM estão atualmente atendendo cerca de 6.000 clientes em 68 países.
- A IBM tem uma taxa de sucesso de 100% no cumprimento de compromissos com clientes que declararam desastre.

Junte-se à IBM e usufrua do seu histórico de mais de cinco décadas de proteção de dados e serviços de resiliência de negócios.

Para outras informações sobre os serviços de resiliência da IBM, acesse IBM Data Center Services.

Sobre a IBM

A IBM é uma empresa de consultoria e tecnologia integrada globalmente, com sede em Armonk, Nova York. Operando em mais de 170 países, a IBM ajuda a resolver problemas e a oferecer uma margem para empresas, governos e organizações sem fins lucrativos. A empresa desenvolve e vende software e hardware de sistemas e um amplo conjunto de serviços de infraestrutura, nuvem e consultoria. Hoje, a IBM focaliza três imperativos estratégicos para transformar indústrias e profissões com dados, para refazer a infraestrutura de TI empresarial para a era de nuvem e para habilitar “sistemas de engajamento” para empresas.