Mestres em recuperação de desastres

Como organizações altamente resilientes atingem a excelência

IBM

IBM **Center for Applied Insights**
ibm.com/ibmcai | ibmcai.com

Nuvem, mobilidade, social, Internet das Coisas – tecnologias como essas estão mudando os negócios, nos tornando mais produtivos, flexíveis, conectados e responsivos. Mas nossa crescente necessidade de estarmos conectados 24/7 também nos expõe a mais riscos quando uma interrupção acontece.

Por que algumas empresas conseguem dominar melhor a recuperação de desastres diante do mundo sempre conectado de hoje? A diferença está em uma estratégia integrada que utiliza tecnologias avançadas e um programa robusto de testes.

Na TI corporativa de hoje, tudo está mais conectado. Tudo precisa estar disponível o tempo inteiro. Tudo está sendo direcionado por dados. Seus funcionários, clientes e parceiros esperam que as informações, os produtos e os serviços dos quais precisam estarão sempre disponíveis onde, quando e como eles desejarem.

Para atender essa demanda, os sistemas estão cada vez mais integrados, distribuídos e interdependentes, o que pode criar muitas vulnerabilidades em potencial. A ligação de mais sistemas importantes para atender a maiores expectativas complica a recuperação de desastres e a segurança. Quando um elo da cadeia se quebra ou é atacado, o impacto pode repercutir em toda a empresa.

Quase **40%** das organizações precisaram executar seu plano de recuperação de desastres devido a uma interrupção no serviço nos últimos dois anos.

Em nosso estudo com 310 profissionais de continuidade de negócios (BC) e recuperação de desastres (DR), quase 60% das organizações executaram seu plano de recuperação de desastres devido à interrupção de um serviço. E cerca de 40% das empresas tiveram de fazer isso nos últimos dois anos. Para ampliar o problema: o tempo de recuperação não está melhorando e o impacto do tempo de inatividade nos negócios está aumentando.[1]

Interrupções acontecem. Antecipar problemas é essencial. Mas mesmo com as melhores medidas preventivas implantadas, você precisa ter um plano de recuperação comprovado na prática.

O problema: nunca foi tão desafiador dominar a recuperação de desastres.

SOCIAL SIGNALS

Mais de **99.000** discussões sobre a recuperação de desastres e continuidade de negócios aconteceram nas mídias sociais durante os seis meses de pesquisa.[2]

Sobre o estudo

Para entender melhor as mais eficientes estratégias atuais de recuperação e continuidade de negócios, o IBM Center for Applied Insights entrevistou 310 profissionais de recuperação de desastres e continuidade de negócios nos Estados Unidos e no Canadá. A base de participantes consistiu em líderes de BCDR principalmente em funções executivas e gerenciais, incluindo mais de 60% de diretores de TI ou CIOs. Os participantes da pesquisa trabalham para empresas em 19 segmentos de mercado, com tamanhos entre 100 e mais de 10.000 funcionários.

Sobre o IBM Center for Applied Insights

ibm.com/ibmcai | ibmcai.com

O IBM Center for Applied Insights apresenta novas maneiras de pensar, trabalhar e liderar. Através de pesquisa baseada em evidências, o Centro municia líderes com orientação pragmática e argumentos para mudanças.

Equipes de recuperação e continuidade de negócios enfrentam um caminho desafiador

Os profissionais de recuperação de desastres e continuidade de negócios trabalham em um ambiente muito exigente e complexo. Cerca de 55% dos participantes do estudo dizem que seu maior desafio é incorporar a seus planos de recuperação um número cada vez maior de sistemas essenciais para os negócios. Por exemplo, cada vez mais empresas consideram aplicativos móveis como ferramentas essenciais. Isso significa que esses aplicativos precisam de um nível de proteção igual àquele dado a sistemas críticos tradicionais, como logística, centrais de atendimento ou volume de emails.

Como o número de aplicativos críticos e volume de trabalho aumenta, também aumenta o grau de integração da TI. O resultado: mais pontos de falha em potencial que as equipes de DR precisam gerenciar. O crescimento no número de pontos de conexão com fornecedores e parceiros de negócios serve apenas para ampliar o problema.

Quase metade dos líderes de DR citam violações de segurança e cybercrime, cujo escopo e sofisticação estão aumentando, representando outro grande desafio para a resiliência de suas organizações. E está claro que muitas organizações estão perdidas, com metade dos líderes de resiliência de negócios admitindo que suas organizações não estão preparadas para lidar com interrupções de serviço causadas por cyberataques.

Ainda assim, um grupo de empresas se destaca das demais, demonstrando um maior domínio da recuperação de desastres. O que as torna diferentes?

O terreno hostil da recuperação de desastres

Profissionais de recuperação e continuidade de negócios enfrentam diversos obstáculos para atender as expectativas de disponibilidade contínua.

30%
Usam análise para prever melhor interrupções de serviço

33%
Estão buscando profissionais de TI com conhecimento sobre DR

37%
Cumprem RTOs e RPOs mais apertados*

38%
Estão demonstrando forte ROI de investimentos em DR

49%
Lidam com riscos de segurança cibernética

55%
Estão incluindo um número maior de sistemas importantes em planos de DR

48%
Gerenciam mais pontos de interrupção devido à maior integração de TI

45%
Obtêm o financiamento necessário para atingir objetivos de DR

30%
Atendem às expectativas cada vez maiores dos líderes de negócios em relação a recursos de DR

*Objetivos do tempo de recuperação (RTOs) e objetivos do ponto de recuperação (RPOs)

Um grupo de elite atinge o topo

Apesar dos desafios significativos, um grupo de organizações altamente resilientes lidera seus colegas nas estratégias de recuperação de desastres que englobam planos integrados e testes robustos. Menos de um terço dos profissionais de BCDR fazem parte desse segmento de elite dos Mestres de recuperação de desastres. Em comparação, cerca de 44% se classificam como Especialistas, enquanto 26% são Táticos.

Mestres adotam uma estratégia corporativa para recuperação de desastres com testes mais frequentes e rigorosos.

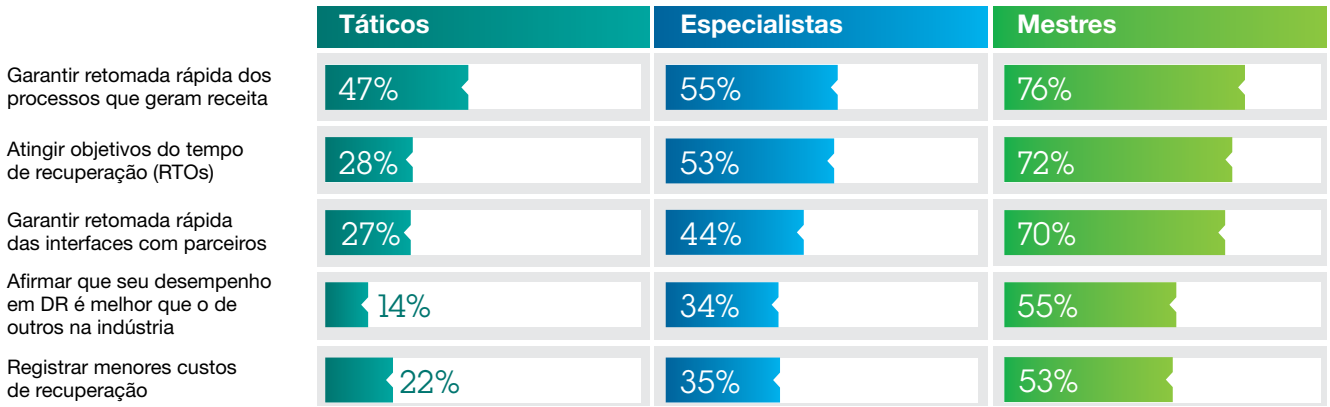
Especialistas começaram a melhorar seus testes e segurança, mas ainda não conseguiram passar para uma abordagem integrada.

Táticos ainda estão testando os sistemas individualmente e com pouca frequência, tratando o recuperação de desastres como um problema principalmente de TI.

Os resultados não deixaram margem para dúvida: os Mestres têm resultados melhores que os demais. Eles relatam uma melhora significativa nas principais métricas de recuperação de desastres. Por exemplo, Mestres são 1,5 vez mais propensos que os Táticos a relatar que estão garantindo a retomada rápida de processos de negócios que geram receita – o que é essencial para manter relacionamentos com clientes – quando ocorrem interrupções.

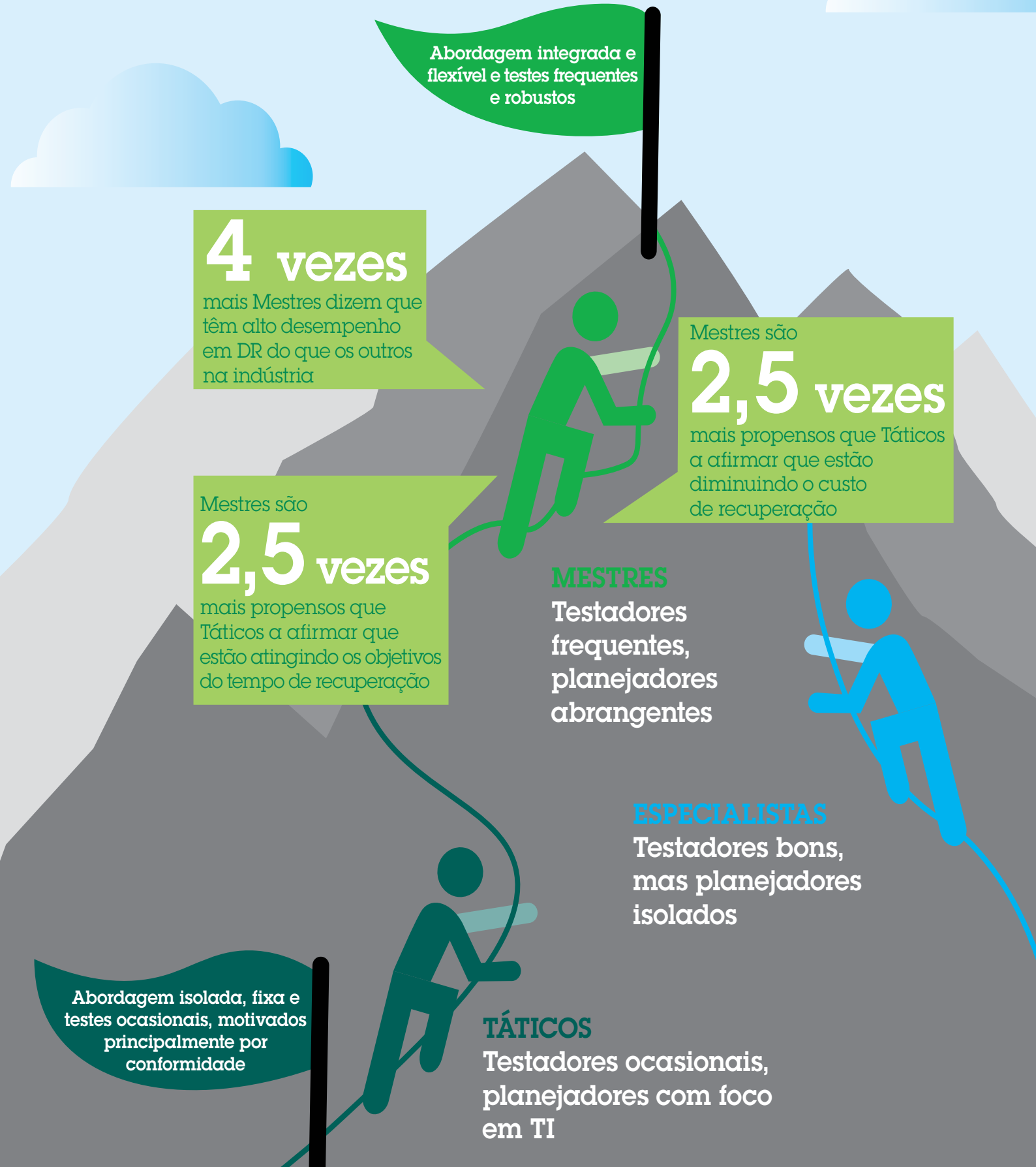
Os Mestres também são 2,5 vezes mais propensos a relatar o cumprimento das metas de tempo de recuperação e de controle de custos, conquistas que demonstram o valor que a equipe de DR oferece para o sucesso da organização em que estão inseridos.

No geral, os Mestres são quatro vezes mais propensos que os Táticos a relatar que sua capacidade de recuperação de desastres (recuperação de desastres) é melhor que a de outros na indústria.



Quem está liderando a escalada para uma resiliência melhor?

Encarando os desafios de frente, um grupo de organizações altamente resilientes supera as demais com planos integrados de BCDR e testes robustos e frequentes.



Alcançando o pico da recuperação e continuidade de negócios

Os Mestres se antecipam e fazem planos. Eles criam uma cultura sólida de colaboração entre TI e negócios, levando em conta novas tecnologias, prioridades de negócios e riscos ao fazer planos para recuperação de desastres.

Eles testam e avaliam. Praticam cada vez mais. É assim que os Mestres melhoram seu tempo de resposta e estendem o escopo de seus programas de recuperação e continuidade de negócios.

Os Mestres também respondem e se recuperam mais rapidamente. Eles exploram as tecnologias certas para fazer com que processos importantes de negócios voltem à atividade rapidamente.

Textron eleva o nível de recuperação de desastres[3]

Textron, uma empresa que atua em vários segmentos de mercado, famosa por marcas como Bell Helicopter e Cessna, entende os altos riscos da recuperação e continuidade de negócios.

As abordagens de recuperação de desastres em algumas empresas nem sempre incluem infraestrutura crítica e serviços de segurança, nem consideram dependências mais amplas ao decidir quais ativos devem ser colocados on-line novamente. A Textron adota uma abordagem mais abrangente para o planejamento da resiliência, começando com um planejamento dos ativos críticos e dependências obscuras. “Antigamente você perguntaria ‘quais aplicativos são necessários para manter seus negócios funcionando?’”, diz a CIO da Textron, Diane Schwarz. “Você avaliava ERP, sistemas de manufatura e inventário, mas talvez não considerasse alguns dos sistemas mais amplos necessários para suportar as operações. As empresas precisam levar em conta os ativos críticos em uma rede, não apenas aqueles com importância financeira”, diz ela.

A Textron também reconhece a importância de ter a flexibilidade para ajustar as estratégias de resiliência segundo as mudanças nas necessidades de negócios. A empresa utiliza tecnologia e parcerias confiáveis para ajudá-los a se movimentarem entre soluções na nuvem, compartilhadas e híbridas.

A prática leva à perfeição. A empresa testa seus planos de recuperação três vezes por ano. Ao colocar seu plano de desastre corporativo em teste com frequência, a empresa se prepara para os incidentes menores que ela, como outras, enfrenta diariamente.

A Textron acredita que não basta colocar tudo em uma instalação fora da cidade e saber que aquilo estará lá quando você precisar. “Um aspecto que geralmente é ignorado é a perspectiva dos talentos”, diz Schwarz. “Você precisa de resiliência não apenas na arquitetura tática; você precisa disso nas equipes”.

Os testes na Textron incluem pessoas de unidades de negócios, suporte a aplicativo, suporte a infraestrutura, gerentes de projeto e usuários avançados, juntamente com equipes de suporte de provedores de serviço.

Avance na recuperação de desastres como um mestre

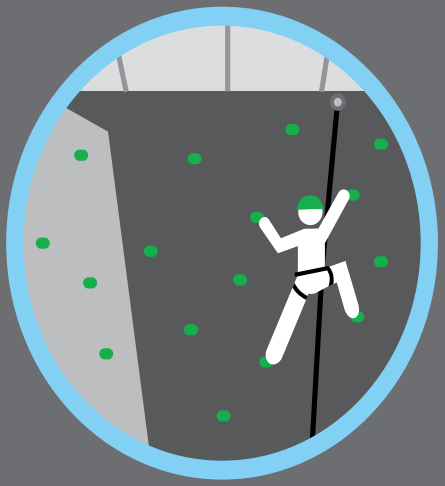
Mestres superam os demais em quatro áreas importantes de recuperação de desastres.

Abordam DR estrategicamente

Integram segurança

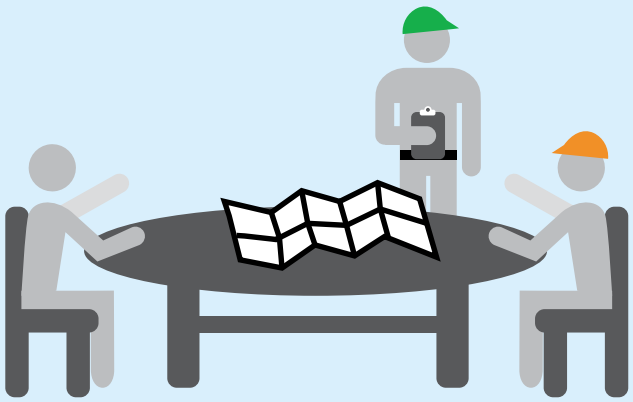
Utilizam novas tecnologias

Testam rigorosamente



Os Mestres abordam recuperação de desastres de maneira estratégica

2,5 vezes
mais propensos a manter um plano de DR integrado



Esses líderes são duas vezes mais propensos que os Táticos a manter um plano de recuperação de desastres integrado. Os Mestres envolvem o gerenciamento sênior por toda a organização no planejamento de resiliência. Afinal, com riscos tão altos assim, o conselho fica de olho. Os Mestres sabem disso e incluem ativamente o conselho na priorização de investimentos com base nas necessidades de negócios mais importantes.

O envolvimento da liderança vem com ordens claras. Setenta e um por cento de todos os participantes dizem que os líderes de negócios esperam que os riscos de segurança da informação sejam incluídos nos planos de recuperação de desastres. E metade dos profissionais de DR participantes explica que seus investimentos em DR vêm com ordens decisivas para obter ROI. Os Mestres também incluem parceiros externos confiáveis com mais frequência em suas avaliações de recuperação de desastres – parceiros de ecossistema e especialistas em planejamento de DR.

SOCIAL SIGNALS

Aconteceram **9.000** discussões nas mídias sociais sobre estratégias de recuperação de desastres e planejamento end-to-end durante os seis meses de pesquisa.

	Táticos	Especialistas	Mestres	*Mestres vs. Táticos*
Envolvem o conselho no planejamento de DR	34%	47%	73%	**2,0 vezes**
Mantêm um plano de DR integrado	19%	26%	46%	**2,5 vezes**
Envolvem especialistas externos em planejamento de DR, execução e avaliação	21%	34%	44%	**2,0 vezes**
Integram fornecedores nos testes gerais	9%	12%	39%	**4,5 vezes**

Mestres colaboram com especialistas em risco e segurança

Uma visão corporativa das possíveis vulnerabilidades pode tornar os planos de recuperação de desastres mais direcionados e efetivos. Os Mestres fazem do gerenciamento de segurança e risco uma parte importante do planejamento de recuperação de desastres e continuidade de negócios. São 3,5 vezes mais propensos que os Táticos a envolver o CISO de sua empresa no planejamento de recuperação de desastres e cinco vezes mais propensos a envolver o CRO. Também incluem políticas de segurança nos testes de recuperação de desastres, verificando ao mesmo tempo tanto seu plano de recuperação quanto suas práticas de segurança.

SOCIAL SIGNALS

8.000 discussões sociais sobre recuperação de desastres relacionadas a tópicos de segurança.

	Táticos	Especialistas	Mestres	*Mestres vs. Táticos*
Envolvem CISO no planejamento de DR	16%	36%	57%	3,5 vezes
Integram segurança corporativa e gerenciamento de riscos em DR	21%	32%	52%	2,5 vezes
Têm políticas de segurança implantadas e funcionando durante testes de DR	4%	16%	47%	12,0 vezes
Envolvem CRO em planejamento de DR	6%	19%	30%	5,0 vezes

Mestres utilizam novas tecnologias

Estes vanguardistas usam com frequência inovações como computação em nuvem, analytics e mobilidade para restaurar rapidamente processos cruciais para os negócios. Durante uma interrupção, eles são mais propensos a fornecer atualizações em tempo real, via dispositivos móveis, e a usar a computação em nuvem para recuperação.

Como o tempo de inatividade destrói renda, os Mestres também são mais propensos a implementar redes virtuais, replicação e armazenamento para melhorar a recuperação e a continuidade e recolocar as operações em funcionamento mais rapidamente.

E, por fim, os Mestres não esperam para reagir. Eles são 15 vezes mais propensos que os Táticos a descobrir riscos e vulnerabilidades usando análises preditivas. Também são mais propensos a usar análise preditiva para descobrir interrupções em potencial. Essas ferramentas são implementadas não apenas para recuperação, mas também para diagnosticar a causa raiz dos problemas, antecipar o risco e evitar interrupções.

SOCIAL SIGNALS

Uma em cada cinco discussões sociais sobre recuperação de desastres está centrada em tecnologia.

E **67%** dessas discussões sobre tecnologia têm a computação em nuvem como foco.

	Táticos	Especialistas	Mestres	*Mestres vs. Táticos*
Permitem atualizações móveis em tempo real durante interrupções	16%	34%	51%	**3,0 vezes**
Usam análises preditivas para identificar riscos de DR	3%	18%	46%	**15,0 vezes**
Implementam a nuvem para recuperação (por exemplo, DR como serviço)	12%	23%	25%	**2,0 vezes**
Usam análise preditiva para antecipar interrupções de serviço	0%	5%	22%	**–***

** Impossível calcular porque o denominador é 0 – nenhum Tático declarou usar análise preditiva.*

Mestres fazem testes rigorosamente

Esse grupo de elite adapta seus planos de recuperação através de testes mais frequentes e rigorosos. Por exemplo, são 2,5 vezes mais propensos que os Táticos a fazer testes seus planos de recuperação de desastres ao menos uma vez por ano e, em muitos casos, até uma vez por mês ou por semana. E eles se adaptam, atualizando os planos futuros com base no que aprenderam nos testes.

Os Mestres são vigilantes, incluindo requisitos de teste em acordos de nível de serviço. São também deliberados, mantendo a consistência entre os testes de recuperação de desastres e os ambientes de produção.

SOCIAL SIGNALS

Mais de **2.500** conversas nas mídias sociais com foco em testes de recuperação de desastres no período da pesquisa.

	Táticos	Especialistas	Mestres	*Mestres vs. Táticos*
Fazem testes ao menos uma vez por ano	34%	68%	89%	**2,5 vezes**
Incluem requisitos de teste em SLAs	33%	43%	64%	**2,0 vezes**
Mantêm consistência entre teste de DR e ambientes de produção	13%	19%	55%	**4,0 vezes**
Adaptam planos futuros com base em resultados de teste	21%	34%	45%	**2,0 vezes**

Como sua organização pode dominar a recuperação de desastres?

Estabeleça uma abordagem estratégica e integrada para recuperação de desastres

- Trabalhe com os líderes internos, incluindo o conselho de administração, e com parceiros da cadeia de suprimentos e especialistas da indústria.
- Baseie sua estratégia em um entendimento profundo dos requisitos de conformidade.
- Leve em consideração as necessidades da empresa e dos clientes.

Crie um programa de testes robusto

- Faça testes ao menos uma vez por ano, e desenvolva a capacidade de fazer testes em tempo real com consultas ad hoc em qualquer dispositivo.
- Melhore os testes continuamente incorporando aos planos de DR as percepções adquiridas em testes anteriores.
- Estenda os testes à infraestrutura interna, aos novos aplicativos móveis e baseados na nuvem e às conexões com parceiros da cadeia de suprimentos.
- Faça comparações com os líderes da indústria em DR para identificar possíveis melhorias.

Colabore com líderes em segurança e risco

- Faça parcerias com equipes de risco para aprimorar a conformidade e a governança de DR.
- Garanta a participação de sua equipe de segurança para integrar segurança cibernética no planejamento de DR.
- Considere solicitar que equipes internas de auditoria avaliem os planos de DR para cumprir os requisitos regulamentares.

Incorpore novas tecnologias em planos de DR

- Explore o uso da nuvem, de analytics avançado e de dispositivos móveis para responder com maior eficácia e evitar interrupções futuras em serviços.
- Use tecnologias sociais não apenas para informar sobre o status do sistema e eventos adversos em tempo real, mas também para monitorar eventos externos econômicos, ambientais e de outros tipos que podem interromper os negócios.

Sobre os autores

Mike Errity é vice-presidente da IBM Resiliency Services North America para IBM Global Technology Services. Sua equipe de consultoria, vendas e entrega trabalha de forma colaborativa com clientes em todos os segmentos de mercado para avaliar, conceber e implementar soluções para mitigar riscos técnicos e operacionais. Mike têm duas décadas de experiência profissional em resiliência de negócios, vendo as necessidades dos clientes mudarem para "sempre disponível" nos Estados Unidos e mundialmente, pois ele antigamente liderava esta linha de negócios no Reino Unido. Entre em contato com Mike pelo e-mail merrity@us.ibm.com e pelo Twitter em @MikeErrity.

Rasheq Rahman é o líder do IBM Center for Applied Insights na América do Norte, fornecendo percepções direcionadas por dados sobre resiliência, segurança e transformação do cliente. Antes de fazer parte da IBM, ele esteve envolvido na comercialização de tecnologias de energia e passou quase uma década desenvolvendo operações de comércio para vários bancos de investimento globais. Entre em contato com Rasheq pelo e-mail rsrahman@us.ibm.com e pelo Twitter em @rasheqrahman. Ele também escreve no blog do Center.

Kelly McKenna é Senior Analyst do IBM Center for Applied Insights, oferecendo liderança inovadora para provocar discussões fundamentadas entre líderes na era digital. Em sua função atual, ela realiza pesquisa direcionada por dados sobre tendências emergentes de tecnologia para pensadores avançados e pioneiros de indústria. Antes de fazer parte do IBM Center, ela era consultora da divisão IBM Global Technology Services. Entre em contato com Kelly pelo e-mail mckennak@us.ibm.com e pelo Twitter em @k_mck120. Ela também escreve no blog do IBM Center.

Contribuidores

Angie Casey
Laura DeLallo
Anurag Goyal
Tyler Kettle
Lindsey Reichelt

Notas e fontes

1 “2015 Cost of Data Breach Study: Impact of Business Continuity Management”, Ponemon Institute, junho de 2015. **ibm.com**/security/data-breach/

2 As estatísticas incluídas em Social Signals se baseiam no monitoramento social de termos sobre recuperação de desastres e continuidade de negócios em blogs, fóruns e tweets mundiais em língua inglesa de junho a novembro de 2015.

Para ver mais Social Signals sobre diversos tópicos de negócios, confira a série de blogs do IBM Center for Applied Insights.

3 Extraído de “Case study: Building resiliency into recuperação de desastres”, Forbes Insights, janeiro de 2016. http://www.forbes.com/forbesinsights

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

A página inicial da IBM encontra-se em:
ibm.com

BUE03004-BRPT-01