

Continuidade dos negócios: novos riscos, novos imperativos e uma nova abordagem



Liderança planeada

Introdução

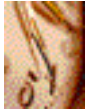
“A maravilha da Web é que o cliente fica ao corrente dos problemas das TI ao mesmo tempo que nós. Não há qualquer possibilidade de camuflagem.”

– VP Sênior de tecnologia de corretagem electrónica¹

O seu centro de dados está a operar na perfeição, a sua rede está activa e o seu centro de chamadas está a funcionar normalmente. Mas nas últimas 24 horas a sua empresa perdeu milhões de dólares de capitalização de mercado. Uma degradação no desempenho de um servidor da Web, aliada a faltas de pessoal, originou um período de inactividade total dos seus negócios online.

Teria sido possível impedir este desastre? Até há bem pouco tempo, o planeamento clássico de recuperação incidia no recuperação de centros de dados centralizados em caso de catástrofes naturais ou provocadas pelo Homem. Este tipo de planeamento não incidia sobre a necessidade de garantir a operação contínua dos processos críticos para os negócios. Embora as medidas tradicionais continuem a ser importantes, estão longe de ser adequadas a ambientes informáticos distribuídos. Os requisitos relativos à continuidade das operações num mundo onde impera o *e-business*, à velocidade da Web, são ainda mais complexos e exigentes.





Tendências e direcções, para além da recuperação de desastres

Quando a recuperação de desastres surgiu como disciplina formal e actividade comercial na década de 80, incidia principalmente sobre a protecção dos centros de dados, o ponto fulcral de qualquer estrutura de TI, altamente centralizada, de uma empresa. Este modelo começou a sofrer alterações no início da década de 90, para acomodar o tratamento distribuído de dados e a tecnologia cliente/servidor. Simultaneamente, as tecnologias de informação passaram a estar interligadas com praticamente todos os aspectos de uma empresa. O processamento de informações deixou de ser algo que era feito em segundo plano. De facto, os dados críticos para os negócios passaram a ser acedidos em toda a empresa através de PCs e de redes locais departamentais, e no centro de dados.

Esta evolução continua a registar-se. As iniciativas-chave para os negócios, como, por exemplo, o planeamento dos recursos da empresa, a gestão da cadeia de fornecimentos, a gestão das relações com os clientes e o *e-business*, tornaram um acesso contínuo e simultâneo às informações, essencial para qualquer organização. Ou seja, hoje em dia as empresas já não podem funcionar sem as tecnologias de informação: dados, software, redes, centros de atendimento telefónico e até computadores portáteis.

Uma empresa que comercialize os seus produtos na Web, por exemplo, ou que preste suporte aos seus clientes através de um centro de chamadas activo 24 horas por dia, tem de estar operacional 24 horas por dia, 7 dias por semana, senão os clientes mudam de fornecedor. Uma empresa que utilize o *e-business* para adquirir e distribuir peças e produtos fica dependente tanto da sua própria tecnologia como da dos seus fornecedores. É por isso que a protecção dos processos críticos para os negócios, com todas as suas interdependências complexas, assumiu um papel tão vital como a protecção dos próprios dados.

O objectivo das empresas cujos negócios não admitem qualquer tempo de inactividade é alcançar um estado de continuidade dos negócios no qual os sistemas e as redes críticas estejam sempre disponíveis, seja o que for que se esteja a passar. Isto implica um pensamento proactivo: disponibilidade para introduzir alterações técnicas e imbuir os processos de negócio de segurança e fiabilidade desde o seu início, em vez de alterar um plano prévio de recuperação de desastres de modo a acomodar os requisitos actualmente colocados à continuidade dos negócios.



Continuidade dos negócios: a quem cabe a responsabilidade?

Muitos quadros superiores e gestores de negócios são de opinião que a responsabilidade pela continuidade dos negócios cabe ao departamento de TI. Contudo, actualmente já não é suficiente nem prático atribuir a responsabilidade exclusivamente a um grupo. O processamento distribuído e baseado na Web dos dados tornou os processos demasiado complicados, descentralizando-os. Além disso, o que está em jogo é a reputação da empresa, a base de clientes e, obviamente, as receitas e os lucros. Por isso, todos os quadros, gestores e colaboradores devem participar no desenvolvimento, implementação e suporte constantes do planeamento e da avaliação da continuidade.

As mesmas tecnologias de informação, ao criarem novas fontes de vantagem competitiva, deram ainda origem a novas expectativas e vulnerabilidades. Na Web, as empresas ficam aptas a satisfazer - ou não satisfazer - imediatamente milhões de pessoas. Nos ambientes de planeamento dos recursos da empresa e da cadeia de fornecimentos, as organizações podem colher os frutos da melhoria de eficiência ou sentir o impacto de uma interrupção em qualquer ponto dos seus processos integrados.

Numa época em que as interrupções dos negócios, em vez de serem medidas em horas, são medidas em minutos, até o êxito pode causar um desastre para a empresa. Actualmente, as empresas que actuam na Web estão mais preocupadas com a sua capacidade de enfrentar picos inesperados no tráfego de clientes do que com incêndios ou inundações. De facto, têm boas razões para isso. Por exemplo, uma infra-estrutura que não esteja apta a acomodar um aumento súbito de 200 % no tráfego registado no seu site da Web, fruto de uma campanha de publicidade bem sucedida, pode dar azo à perda de

oportunidades, a menos receitas e a uma má imagem de marca.

Dada a velocidade a que as transacções e as comunicações electrónicas se desenrolam, a quantidade de trabalho e de negócios perdidos numa hora excede largamente a das décadas anteriores. Segundo um relatório publicado pela Strategic Research Corporation, uma empresa de estudos de mercado e de consultoria de Santa Bárbara, na Califórnia², o impacto financeiro de um período considerável de inactividade do sistema pode ser enorme: 6,5 milhões de dólares por hora no caso de uma operação de corretagem; 2,6 milhões de dólares por hora no caso de um sistema de autorização de compras com cartões de crédito; ou uns meros 14 500 dólares por hora em taxas de máquinas multibanco (ATM) se um sistema ATM estiver fora de serviço.

Até o que chegou a ser considerado um problema "menor", como, por exemplo, um disco rígido com defeito ou uma falha do software, pode agora afectar um processo crítico para os negócios e provocar perdas similares às incorridas por uma falha de corrente ou pela inundação de um centro de dados. Por exemplo, a FIND/SVP, uma empresa de investigação sediada em Nova Iorque, calcula que a perda financeira média por hora de tempo de inactividade de matriz de disco corresponde a 29 301 dólares para a indústria de acções e obrigações, a 26 761 dólares para uma empresa de produção, a 17 093 dólares para a banca e a 9435 dólares para as empresas de transportes.³ Mais difíceis de calcular são os danos intangíveis que uma empresa pode sofrer: quebra da moral, diminuição da produção, aumento da tensão dos colaboradores, atrasos nos prazos de projectos-chave, desvio de recursos, investigações regulamentares e uma imagem pública prejudicada.

Neste clima, os executivos responsáveis pelo desempenho da empresa vêem agora em jogo as suas reputações pessoais. É normal as empresas que sofreram interrupções nos seus negócios online, seja por que motivo for, estarem nas parangonas dos jornais na manhã seguinte, tendo a imprensa o cuidado de identificar as pessoas que estão por trás delas. Além disso, os directores e os quadros das empresas podem ser responsabilizados pelas consequências da interrupção dos negócios ou pela perda de informações críticas para esses mesmos negócios. A maior parte das grandes empresas estipula contratualmente que os fornecedores têm sempre de fornecer os seus serviços e produtos, sejam quais forem as circunstâncias. Por outro lado, a lei pode exigir uma protecção adequada dos dados, em particular no caso de

empresas públicas, instituições financeiras, empresas fornecedoras de serviços de utilidade pública, organizações de saúde ou departamentos governamentais.

Aliados, estes factores fazem com que a continuidade dos negócios seja uma responsabilidade partilhada por todos os quadros superiores de uma empresa, desde o Director Geral aos executivos responsáveis pelos processos cruciais para os negócios. Embora as TI continuem a desempenhar um papel fundamental para a continuidade dos negócios, a gestão das TI por si só não pode determinar quais os processos que são críticos para os negócios e quais as verbas que a empresa deverá dispende na protecção desses recursos.

A Internet acarreta novos riscos

Segundo uma investigação recentemente promovida pela IBM junto de 226 gestores empresariais de recuperação de negócios, só 8 % das empresas presentes na Internet estão preparadas para enfrentar um desastre do sistema informático. E, no entanto, o facto de trabalharem online implica a exposição de inúmeras aplicações críticas para os negócios, a inúmeros novos riscos.

Se, por um lado, a Internet oferece inúmeras oportunidades de vantagem competitiva, pelo outro também pode dar aos parceiros, fornecedores, clientes, colaboradores e piratas informáticos acesso a infra-estruturas de TI da empresa. Actos maliciosos ou não intencionais podem resultar num importante período de inactividade das TI. Além disso, a operação de um site na Web cria interdependências

organizacionais e relacionadas com o sistema que são impossíveis de controlar pela empresa, desde os fornecedores de serviços Internet e os operadores de redes de telecomunicações a centenas de milhões de utilizadores da rede pública.

Por isso, o maior risco que as operações de TI de uma empresa têm de enfrentar pode já não ser um terramoto, um furacão, uma grande cheia, uma falha de energia ou até um cano rebentado. O planeamento da continuidade num ambiente de e-business tem de abordar tanto a vulnerabilidade da rede, as intrusões de piratas informáticos, os vírus e a sobrecarga de mensagens de e-mail não solicitadas, como as falhas nas linhas dos fornecedores de serviços Internet e dos operadores de telecomunicações.



Planeamento da continuidade dos negócios: uma abordagem proactiva

Poucas são as organizações que têm quer a necessidade, quer os recursos para garantir a continuidade uniforme dos negócios em todas as áreas funcionais. Por isso, uma empresa que tenha adoptado uma única estratégia de continuidade dos negócios para toda a organização, provavelmente não estará preparada ou estará a gastar mais do que o necessário.

O segredo para garantir a continuidade dos negócios consiste na compreensão dos mesmos, na determinação dos processos críticos para manter esses negócios e a identificação de todos os elementos cruciais para esses processos. Conhecimentos e aptidões especiais, boas instalações, formação e satisfação dos colaboradores, a par das tecnologias de informação, são factores que devem, todos eles, ser tidos em conta. Através de uma análise exaustiva destes elementos pode identificar, com precisão, potenciais riscos, e tomar decisões comerciais conscientes sobre a aceitação, atenuação ou transferências desses riscos. Depois de desenvolver um programa para garantir a disponibilidade dos processos críticos 24 horas por dia, assuma que esse programa poderá falhar e empenhe-se em manter o seu programa a par das alterações da infra-estrutura tecnológica e dos negócios.

Uma estratégia à prova de falhas parte do princípio de que nenhum programa de continuidade dos negócios pode assegurar uma protecção total contra todos os tipos de danos, independentemente de quão abrangentes sejam as suas estratégias de alta disponibilidade, redundância, tolerância de falhas, agrupamento e

replicação. Actualmente, os desastres que, mais provavelmente, forçarão a sua empresa a interromper os seus negócios resultam de erros humanos ou de acções mal-intencionadas: o colaborador que elimina acidentalmente um bloco de dados fundamental; o ex-colaborador ressentido que se procura vingar através da introdução de um vírus prejudicial; o ladrão que rouba segredos comerciais vitais de um sistema central; ou o pirata informático que invade uma rede. Segundo um estudo promovido conjuntamente pelo FBI e pelo Computer Security Institute, a quantidade e a gravidade dos negócios de pirataria empresarial bem sucedidos estão a aumentar drasticamente, nomeadamente as intrusões praticadas por entidades internas à própria empresa. De acordo com outro estudo, das 1000 principais empresas segundo a Fortune, 250 reportaram prejuízos no total de 137 milhões de dólares em 1997, o que representa um aumento de 37 % relativamente ao ano anterior.⁴

O assumir de um compromisso, por parte dos quadros da empresa, no sentido de testar, validar e actualizar regularmente o programa de continuidade dos negócios da sua empresa pode ajudá-lo a protegê-la contra aquele que talvez seja o maior risco de todos: a complacência. Neste ambiente de rápidas mudanças tecnológicas e comerciais, mesmo a alteração mais ínfima de uma aplicação ou de um sistema crítico pode provocar uma falha imprevista na continuidade dos seus negócios. Um planeamento eficaz de protecção dos negócios tem em conta não só as suas necessidades actuais mas também as suas necessidades futuras, seja num futuro próximo, seja num mais distante.



Optar por uma solução interna ou recorrer aos serviços de um fornecedor de continuidade dos negócios?

As empresas com uma taxa elevada de sucesso reconhecem o valor de um fornecedor de soluções tecnológicas que pode ajudar a planear, implementar e gerir um programa permanente de continuidade dos negócios.

À medida que o processamento de dados cliente/servidor se foi difundindo cada vez mais no início dos anos 90 e que a relação preço/desempenho do processamento e armazenamento de dados continuou a melhorar, muitas empresas optaram pela implementação de replicação de dados interna, conjuntos redundantes de armazenamento de dados e outras técnicas de alta disponibilidade para criar cópias duplicadas de dados, online ou praticamente online.

Embora estas estratégias possam garantir uma disponibilidade de dados praticamente contínua a preços muito atraentes, as empresas que testam e validam a respectiva capacidade de recuperação de uma interrupção consciencializaram-se de que a continuidade dos negócios envolve muitos outros desafios. Para garantir uma verdadeira continuidade dos processos críticos para os negócios, e não apenas dos dados críticos, as empresas que optarem por uma abordagem interna do problema terão ainda de:

- Assegurar a disponibilização imediata de uma capacidade latente suficiente para garantir uma eliminação de falhas e uma recuperação rápidas
- Dispor de capacidades de teste sem provocar interrupções nas operações em curso
- Instalar uma rede redundante dedicada à continuidade dos negócios
- Instalar equipamento interno de recuperação de falhas num local separado do equipamento de produção principal e prever e instalar outras redundâncias, como a obtenção de energia eléctrica de diferentes redes ou sectores
- Estabelecer e manter relações com fornecedores que assegurem um fornecimento rápido de PCs de substituição, hardware de redes, secretárias, cadeiras, telefones, etc., para o caso de um desastre que afecte todas as instalações
- Assegurar a obtenção de fundos adequados junto de departamentos de utilizador-final para implementar e manter uma protecção adequada à continuidade dos negócios críticos
- Adquirir, formar e manter pessoal qualificado, apto a gerir as interdependências complexas, e elementos especializados em continuidade dos negócios
- Tomar as medidas apropriadas para adicionar pessoal de apoio à recuperação, em caso de um desastre regional ou natural.

O recurso a um fornecedor de uma solução tecnológica para parte ou para a totalidade destes requisitos pode ser atraente para empresas que preferem concentrar os seus já poucos recursos no aumento das receitas e do valor dos accionistas. Ao estabelecer uma relação estratégica a longo prazo com um fornecedor de serviços mundialmente reconhecido como a IBM Global Services, as empresas podem obter uma vantagem competitiva com um plano de continuidade à medida, ao mesmo tempo que evitam os custos inerentes à actualização da tecnologia e da formação.

A contratação de um fornecedor de continuidade dos negócios permite a essas organizações:

- Tirar proveito dos vastos investimentos que o fornecedor fez nas tecnologias mais recentes, nos melhoramentos contínuos das metodologias e em pessoal qualificado
- Beneficiar da experiência adquirida com a resolução de problemas para inúmeros clientes com requisitos semelhantes
- Eliminar, da folha de balanço, itens tecnológicos redundantes e dispendiosos
- Utilizar as instalações e os recursos de segurança do fornecedor
- Tirar proveito das economias de escala do fornecedor em bens, recursos e aquisições, para ajudar a garantir um custo de operação mais reduzido e um risco significativamente menor
- Concentrar-se em alcançar os objectivos relacionados com o crescimento da actividade principal da empresa.



Prontidão da continuidade dos negócios

Esta auditoria interna, muito simples de realizar, irá ajudá-lo a proceder a uma avaliação extremamente importante: a prontidão da sua empresa para assegurar a continuidade dos negócios.

Mesmo que responda “Não” ou “Não sei” a apenas uma destas perguntas, os processos críticos para o seu negócio podem ser vulneráveis a uma interrupção e pôr o seu negócio em perigo.

Consegue identificar as actividades críticas para o seu negócio que satisfazem as expectativas dos seus clientes e suportam o funcionamento dos seus negócios em geral?

Sim Não Não sei

Consegue identificar quais são as informações críticas para o seu negócio de que necessita para que essas actividades tenham êxito?

Sim Não Não sei

Dispõe de informações sobre a frequência, impacto e causas do tempo de imobilização?

Sim Não Não sei

Essas informações permitem-lhe identificar e classificar as actividades mais vulneráveis?

Sim Não Não sei

Os seus sistemas centrais antigos e recursos de TI estão devidamente protegidos contra intrusões de piratas informáticos e vírus?

Sim Não Não sei

Elaborou uma lista de verificações, por área funcional, do que a sua empresa irá necessitar para prosseguir os negócios com eficácia em caso de interrupção ou de emergência?

Sim Não Não sei

Você e os seus colegas do departamento de TI tiveram êxito em tornar a continuidade do negócio numa das prioridades da direcção?

Sim Não Não sei

Trabalhou com os seus colegas do departamento de TI com vista a elaborar um plano de continuidade aprovado que tenha em conta todos os aspectos da continuidade e da recuperação dos negócios?

Sim Não Não sei

O seu plano de continuidade do negócio tem sido testado com regularidade?

Sim Não Não sei

Dispõe de um processo de controlo de alterações que lhe permite manter o seu plano de continuidade a par das alterações organizacionais, tecnológicas e processuais?

Sim Não Não sei

Está certo de que, se neste exacto momento ocorresse uma interrupção ou um desastre, a sua organização estaria apta a recuperar com rapidez e sem problemas para impedir que os seus negócios fossem afectados?

Sim Não Não sei



Factores-chave para o êxito

Que exigir de um fornecedor de serviços de continuidade dos negócios

Hoje em dia, muitos são os fornecedores que oferecem serviços e soluções de continuidade dos negócios e recuperação de desastres. Estes serviços podem incluir consultoria, planeamento, hardware, software e instalações alternativas equipadas para TI ou operações de centros de atendimento telefónico.

O apoio do fornecedor de serviços que escolher terá de versar os processos críticos para os negócios da sua empresa. A lista que se segue inclui alguns factores-chave para o êxito, que deverão ser tidos em conta ao avaliar a capacidade de um fornecedor de serviços para fornecer verdadeiras soluções de continuidade dos negócios:

- A capacidade de compreender a integração das TI na estratégia comercial e de definir os riscos e os impactos de uma interrupção em infra-estruturas de TI críticas
- A compreensão das dependências do *e-business* e dos requisitos críticos para os negócios
- A concentração na continuidade dos negócios, independentemente dos serviços tradicionais de recuperação de desastres
- A compreensão das dinâmicas inerentes à cadeia de fornecimentos
- Capacidades e recursos para gerir programas de continuidade complexos num ambiente de TI em rede e em constante mudança
- A capacidade de utilizar recursos exteriores às capacidades de recuperação e de continuidade essenciais
- Um sistema formal de gestão de capital intelectual que permita a partilha, a nível mundial, das melhores práticas e de procedimentos actualizados
- Uma vasta experiência adquirida em várias indústrias, regiões geográficas e cenários de desastre
- Recursos suficientes para acomodar diversos clientes de recuperação em caso de um desastre que abranja uma área alargada
- O suporte de ambientes de TI de plataformas e fornecedores múltiplos
- O acesso aos melhores investigadores, instalações e responsáveis pelo desenvolvimento de tecnologias
- Um investimento significativo em instalações e ferramentas modernas e a capacidade financeira para continuar a investir
- Soluções integradas para assegurar a disponibilidade de recursos não relacionados com centros de dados, incluindo redes, área de trabalho de utilizadores-finais e centros de atendimento telefónico
- Uma experiência comprovada em recuperação e suporte tecnológico
- Uma interface contínua e perfeita com serviços e suporte adicional
- O acesso à tecnologia mais recente, constantemente actualizada para reflectir as necessidades do mercado.



A IBM Global Services

Sendo uma das maiores empresas mundiais e um dos maiores fornecedores de serviços tecnológicos, a IBM Global Services dispõe dos conhecimentos, da competência, da experiência e de um leque único de capacidades para gerir e assegurar a continuidade dos negócios e serviços de recuperação.

Oferecemos inúmeras soluções, desde a consultoria, o planeamento e o teste para implementação da continuidade dos negócios à gestão global da continuidade dos negócios para os seus processos críticos de planeamento dos recursos da empresa, de *e-business* e estratégicos. Fornecemos ainda serviços de recuperação e instalações para ambientes de processamento de dados de grande ou médio porte, distribuídos e de plataforma múltipla, bem como de recuperação de redes e de centro de atendimento telefónico.

A nossa força baseia-se nos nossos colaboradores - mais de 130 000 profissionais em mais de 164 países. As suas capacidades e experiências são variadas: peritos na continuidade dos negócios, consultores em *e-business*, profissionais de disponibilidade elevada, especialistas em tecnologias para ambientes de fornecedores múltiplos, profissionais em gestão operacional de TI e especialistas em suporte a TI.



Conclusão

Actualmente, a continuidade dos negócios é tão essencial ao êxito dos negócios que já não pode ser uma responsabilidade exclusiva do departamento de TI. O tempo, o dinheiro e a confiança dos clientes que pode ser perdida devido a tempos de imobilização ou à interrupção dos negócios pode prejudicar gravemente uma empresa de qualquer dimensão e arruinar a reputação dos seus executivos tanto a curto como a longo prazo.

Os riscos são ainda maiores para o *e-business* e as empresas que operam num ambiente global 24 horas por dia, 7 dias por semana. Para garantir a sobrevivência, as empresas têm não só de adoptar estratégias comprovadas para proteger os processos e as informações vitais para os negócios como de implementar programas de gestão da continuidade e da recuperação a nível de toda a empresa.

Para obter informações mais detalhadas sobre as vantagens que a sua empresa pode usufruir da inclusão dos colaboradores da IBM Global Services na sua equipa, visite o nosso site www.ibm.com/services/continuity, contacte o seu representante de vendas ou envie-nos um e-mail para o endereço bcrs@pt.ibm.com.



Bibliografia

¹Dalton, Gregory. "E-Business Emergency — The High-Stakes Battle For Online Customers and Market Share Has Turned Crisis Management Into A Top Priority." *InformationWeek*, 6 de Setembro de 1999.

²Strategic Research Corporation, Peterson, Michael and Newton, Kris, "1998 DATABASE OPERATING PRACTICES High Availability and Data Protection, Executive Summary." http://www.sresearch.com/oper_prac98.htm.

³Patrowic, Lucie Juneau, "A River Runs Through It." *CIO Magazine*, 1 de Abril de 1998.

⁴DiDio, Laura, "Computer Crime Costs on the Rise." *Computerworld*, 20 de Abril 1998.

Companhia IBM Portuguesa, SA

Praça de Alvalade, 7
1700-036 Lisboa
Portugal
Tel: 351-217915584

A página dos IBM Global Services pode ser consultada na Internet em www.ibm.com/services.

IBM é uma marca comercial registada da International Business Machines Corporation.

* O logotipo e-business é uma marca comercial da International Business Machines Corporation.

Outros nomes de empresas, produtos e serviços, podem ser marcas comerciais ou marcas de serviços de outras companhias.

As referências, nesta publicação, a produtos, programas ou serviços IBM não implicam a intenção por parte da IBM de os comercializar em todos os países em que a IBM opera. Qualquer referência a um produto, programa ou serviço da IBM não significa que apenas esse produto, programa ou serviço possa ser utilizado. Qualquer produto, programa ou serviço, funcionalmente equivalente, poderá ser utilizado em sua substituição.

Esta publicação destina-se apenas a servir de consulta.

Impresso em Inglaterra por Carwin

Printed in England by Carwin

© International Business Machines Corporation 1999.

GSOPG40 (09/99) LB