

IBM Institute for Business Value

# A evolução do papel de gerentes e diretores de TI

*Resultados do Estudo Global da IBM em 2010 sobre Riscos de TI*



---

## IBM Institute for Business Value

A IBM Global Business Services, através do IBM Institute for Business Value, desenvolve perspectivas estratégicas factuais para executivos de alto escalão a respeito de problemas dos setores público e privado. Este relatório executivo baseia-se em um estudo detalhado da equipe de pesquisa do Instituto. Ele é parte do compromisso permanente da IBM Global Business Services de oferecer análises e pontos de vista que ajudem as empresas a concretizar o valor de negócio.

Você pode entrar em contato com os autores ou enviar um e-mail para [iibv@us.ibm.com](mailto:iibv@us.ibm.com) a fim de obter mais informações.

Outros estudos do IBM Institute for Business Value podem ser encontrados na página [ibm.com/iibv](http://ibm.com/iibv)

---

*Pela Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Rick Telford e Mark Ernest*

## **Exigências normativas que crescem,**

a expansão dos negócios online 24x7 e a sombra constante de uma economia incerta aumentam a importância da administração de riscos em todas as suas formas – estejam eles relacionados aos negócios, dados ou eventos. O Estudo Global da IBM em 2010 sobre Riscos de TI revela os desafios inerentes aos riscos de TI e as providências que gerentes e diretores de TI estão tomando para melhor entender, confrontar e resolver este problema. Dentre os gerentes de TI entrevistados, a maioria acha que as suas responsabilidades decorrentes de riscos vão aumentar. Está claro que a administração dos riscos de TI vai longe e pode afetar diretamente a posição competitiva de uma empresa, tanto quanto sua reputação junto a clientes, parceiros, regulamentadores e outros grupos de interesse.

Do ponto de vista da perspectiva empresarial, a infraestrutura de TI tem função cada vez mais relevante, não só por amparar e resguardar os principais recursos da empresa, garantindo governança e adaptação apropriadas, como também por seu estímulo à expansão dos negócios. Em consequência, a gestão dos riscos de TI já não é mais vista como uma função estritamente técnica, mas como um dever crucial da administração, capaz de trazer benefícios comerciais diretos para toda a organização.

Para melhor entender o que as empresas estão fazendo para controlar e atenuar os riscos em todas as suas atividades – particularmente no que se refere a TI –, a IBM deu início ao seu Estudo Global em 2010 sobre Riscos de TI, parte da pesquisa que ela vem realizando na área de riscos de TI e o primeiro de uma série de estudos investigativos a

examinar o assunto. A investigação, realizada em maio e junho de 2010 em cooperação com a Economist Intelligence Unit (EIU), busca melhor entender as áreas a que se dedicam hoje os gerentes de TI e onde enxergam as oportunidades e desafios a curto prazo. Pesquisas futuras deverão explorar essas questões a fundo, examinando as opções e decisões que confrontam todos os quadros de administração de riscos.

---

*“Durante o período em que a TI tornou-se essencial para as atividades de mais empresas, a gestão de riscos não ganhou importância proporcional.”*

Entrevistado, Ramo de Viagens e Turismo, Europa Ocidental

---

*“Apesar de alguns dizerem que a tecnologia amadureceu e universalizou-se nos negócios, vemos a ‘revolução’ tecnológica como apenas começando. Nossa leitura da evidência sugere que o valor estratégico da tecnologia para os negócios ainda está crescendo.”*

Brynjolfsson, Erik e Adam Saunders. “Wired for Innovation: How Information Technology is Reshaping the Economy.” Massachusetts Institute of Technology, 2010.

Os resultados deste estudo baseiam-se numa abrangente investigação online com 556 gerentes de TI e outros elementos envolvidos primariamente nas funções de TI em suas empresas (incluindo 131 Diretores de TI). Representando as regiões de América do Norte, Europa Ocidental, Ásia-Pacífico, Oriente Médio e África, Europa Ocidental e América Latina, o estudo permeia vários segmentos do mercado – desde TI, serviços financeiros, assistência de saúde e produtos farmacêuticos, até biotecnologia, manufatura e o setor governamental. As empresas estudadas informaram faturamentos variando de US\$ 500 milhões até mais de US\$ 10 bilhões.

Os principais objetivos do estudo foram:

- Investigar uma amostra representativa de empresas a fim de determinar com precisão o estado vigente da gestão de riscos de TI.
- Identificar fatores capazes de promover (ou impedir) as estratégias de administração de riscos de uma organização.
- Descobrir até que ponto as empresas estão implementando novas estratégias, programas e políticas de risco.
- Entender de que forma avanços de TI, tais como a computação em nuvem, acompanham as estratégias gerais de risco das empresas.
- Examinar a evolução do papel dos gestores de TI, incluindo o diretor de Informação.

De um modo geral, os resultados da investigação foram uniformes para todas as regiões, porte das empresas, ramos e funções. (Todas as regiões representadas no estudo confirmaram a importância da administração dos riscos de TI e vêm trabalhando na aplicação de melhorias a esse respeito). De um modo geral, os participantes do estudo expressaram confiança no seu gerenciamento de riscos e esforços de adaptação (ver Figura 1).

Ainda assim, apesar de mais de 50% dos entrevistados tenha dito que seus orçamentos permaneceram iguais ou aumentaram, 36% continuam lutando pela garantia de verbas suficientes para tratar dos desafios das situações de risco. Além disso, apesar de reconhecer que a gestão dos riscos de TI pode trazer vantagens comerciais concretas, conquistar o apoio do primeiro escalão continua sendo algo muito problemático. Os comentários dos entrevistados parecem indicar um

#### Política geral de atenuação dos riscos de TI



#### A política geral melhorou nos últimos 12 meses

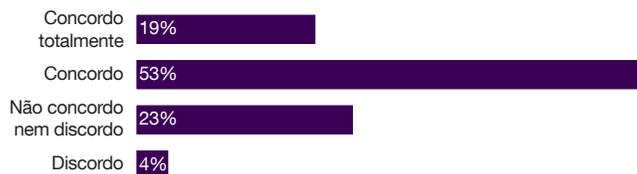


Figura 1: As organizações dão notas altas à sua política de atenuação dos riscos de TI.

distanciamento da diretoria entre sua percepção do custo para melhorar a gestão dos riscos de TI e o benefício que se possa derivar disto.

### Abrindo espaço para melhorar

Reconhecendo o retorno do gerenciamento eficaz dos riscos de TI sob a forma de possíveis negócios, muitos dos entrevistados pensam em ampliar suas iniciativas a respeito do assunto durante os próximos três a cinco anos. Apesar de tudo, houve algumas divergências notáveis. Atualmente, apenas cerca da metade das companhias entrevistadas tem um departamento formal de gerenciamento de riscos (46%) ou uma estratégia bem elaborada de continuidade dos negócios (54%). Além disso, questões de risco operacional na linha de negócios e outros (estratégia financeira/comercial, por exemplo) não constituem áreas de atenção primárias.

---

*“As organizações de TI tradicionalmente efetuam longos testes antes de introduzir novos serviços empresariais habilitados por TI, com o objetivo primário de evitar sua interrupção. Mas os executivos de TI modernos precisam entender o verdadeiro custo desses testes para a empresa. Não se trata só dos custos de TI, mas do custo das oportunidades perdidas devido ao atraso no acesso a tais serviços. Cada dia em testes é um dia a menos na geração de receitas e lucros. Qual é o risco se o serviço falhar, comparado ao benefício de colocá-lo em plena atividade?”*

Mark Ernest, IBM Distinguished Engineer

---

Quando se pediu que descrevessem a política geral da organização para atenuar os riscos da TI, 66% dos entrevistados classificou-a entre boa e ótima. Embora isto represente a maioria das empresas, mais de 30% delas as considera entre medianas e insatisfatórias nesta área. Porém, 72% dos entrevistados informaram que a política de risco da empresa melhorou durante os últimos 12 meses.

Não é de surpreender que 47% dos entrevistados tenham dito que o planejamento dos riscos de TI é, para a maior parte, uma função discreta cumprida a portas fechadas. Em consequência, fazer com que setores da organização trabalhem juntos representa um desafio significativo. Outro fato revelador: muitos dos entrevistados disseram que, apesar de estarem bastante envolvidos em uma série de atividades de gestão e adaptação a riscos, gostariam de participar mais. (Embora cerca da metade dos entrevistados tenha dito que sua empresa tem um setor de gerenciamento de riscos, muitos acreditam que ela deixa a desejar em termos de instruir seus funcionários e mantê-los informados sobre as políticas e problemas que enfrenta nesta área.)

Uma nota positiva: mesmo em um ambiente econômico de agruras, a gestão e adaptação a riscos de TI continuou praticamente a salvo de cortes orçamentários ou reduções de custos. Quando perguntados sobre o orçamento de 2010 da sua organização para gerenciamento de riscos, 14% (80 entrevistados) esperavam um aumento de verbas significativo, enquanto 39% notaram um certo aumento. 36% disseram que as verbas para este setor continuariam as mesmas.

Os entrevistados concordam que investir em gerenciamento de riscos de TI pode trazer expressivas vantagens comerciais, principalmente no que tange a continuidade dos negócios (74%) e resguardo da reputação da empresa (32%, veja a Figura 2). De acordo com os entrevistados, administrar riscos de TI deve ser visto mais como tática defensiva; pode aumentar a agilidade da empresa (19%), criar oportunidades de crescimento (12%) e ainda reduzir custos (18%). Mesmo assim, a maioria dos gerentes de TI (57%) concentra-se mais nos riscos ligados à infraestrutura.

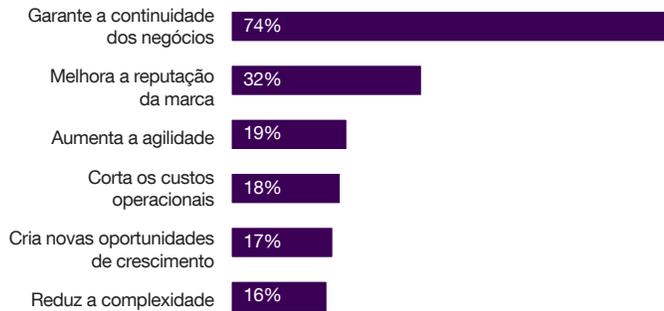


Figura 2: Vantagens de se aprimorar a gestão dos riscos de TI.

#### Em primeiro na lista: segurança em TI

Apesar dos riscos em TI existirem para processos, atividades e sistemas, sua segurança (vulnerabilidade a ataques e acesso/uso não autorizado de sistemas da empresa) é a preocupação número um de 78% dos profissionais de TI entrevistados. Defeitos de hardware e do sistema vieram a seguir – citados por 63%. Falta de energia e segurança física (40%) não ficaram muito atrás, seguindo-se roubo, qualidade dos produtos, adaptação, desastres naturais, revelação forense compulsória, falhas na cadeia de suprimento e terrorismo, nesta ordem.

Os gerentes de TI tem opiniões claras sobre a importância do gerenciamento de riscos, assim como das específicas áreas de interesse. Mesmo assim, ocorrem lacunas importantes quando se trata da confiança que depositam na capacidade da organização de lidar com o risco e reagir a ele de maneira apropriada. Por exemplo, apenas 22% dos entrevistados acreditam que suas organizações estejam bem

*“Continuidade dos negócios abrange muito mais do que se programar para desastres naturais ou planejados. Na verdade, tem a ver com formar uma cultura de percepção dos riscos – providenciando a disponibilidade dos necessários instrumentos, processos e metodologias, com todos os indivíduos da organização cientes de suas responsabilidades em termos de segurança e integridade dos dados. Finalmente, na implementação dos instrumentos e processos, é vital equilibrar a velocidade de atendimento às demandas do mercado com o risco aceitável.”*

Jessica Carroll, Managing Director Information Technologies,  
United States Golf Association

preparadas em termos de segurança de TI. 23% pensam o mesmo sobre a prontidão da empresa frente a falhas de equipamentos e sistemas. A proteção contra faltas de energia teve mais apoio – com 32% dos entrevistados declarando que suas empresas estavam bem preparadas nesta área. Porém, existe uma clara separação entre a aceitação pelos entrevistados da importância de se tratar os riscos de TI como um todo e a confiança que depositam na capacidade de suas companhias de controlar e atenuar esses riscos de modo apropriado.

---

## Estudo de Caso

Na primeira metade de 2010, a equipe da IBM X-Force Research and Development documentou 4396 novas vulnerabilidades – uma expansão de 36%, comparada ao mesmo período do ano anterior. De acordo com o relatório, vulnerabilidades de programas para a Internet continuam sendo a principal ameaça – respondendo por mais da metade de todos os vazamentos para o público. Apesar disso, o relatório observou que as organizações vinham fazendo mais para identificar e expor vulnerabilidades de segurança do que jamais haviam feito. Isto, por sua vez, vem tendo efeitos positivos sobre o mercado, estimulando uma colaboração mais franca para identificar e eliminar vulnerabilidades antes que os criminosos cibernéticos consigam explorá-las.<sup>1</sup>

---

## O desafio das comunicações

Não resta dúvida que a gestão dos riscos de TI pode trazer efetivas vantagens comerciais. No entanto, apesar dos vários métodos usados pelas empresas para distribuir informações relativas a riscos, a comunicação aparece como verdadeiro obstáculo. Conquistar o apoio da direção continua a ser um desafio, de acordo com 25% dos entrevistados. Comunicar políticas e procedimentos de risco aos funcionários também foi um problema para 30% deles.

Ao invés de agir preventivamente, muitas organizações assumem uma atitude passiva quanto ao controle e redução dos riscos de TI. Em muitos casos, as informações são colocadas na intranet da empresa, cabendo aos funcionários gastar seu tempo procurando-as por lá. Algumas organizações incorporam políticas de gestão de risco em materiais de treinamento para novos contratados – sem atentar para a necessidade de fazê-las chegar a todos. (Somente 22% dos gerentes de TI disseram que políticas de gestão de riscos são parte do treinamento formal de todo funcionário). E, talvez, o mais surpreendente: Menos de 15% incorporaram um plano integrado de gestão de riscos na infraestrutura física e técnica de suas empresas.

---

*“Esforçamo-nos para fazer com que a direção e os funcionários da empresa aceitem que é preciso modificar seu comportamento para melhorar as práticas de segurança.”*

Entrevistado, Setor Manufatureiro, Europa Ocidental

---

*“Está cada vez mais difícil conseguir verbas para tratar de riscos de TI, mesmo quando os custos de NÃO fazê-lo são claramente demonstrados para os executivos. Costuma haver uma má-vontade generalizada de investir.”*

Entrevistado, Setor Aeroespacial e de Defesa, América do Norte

Dada a variedade de canais de comunicação e educação disponíveis para despertar a atenção das pessoas para os riscos, seria bom que as empresas assumissem uma postura mais organizada e detalhada para dominar esses problemas, levando-os ao conhecimento dos funcionários e incorporando o gerenciamento de riscos de TI em todas as áreas da empresa. Em resposta à pergunta “Qual a principal atitude de sua empresa para manter-se em dia sobre os riscos?”, a maioria dos entrevistados declarou que ameaças à segurança eram tratadas com recursos internos e externos (38%), uma equipe multifuncional de executivos (26%) ou um departamento designado para gestão de riscos (19%).

*“Normalmente, usuários, dirigentes e parceiros encaram o risco sob diferentes perspectivas. Preciso fazer esses extremos se encontrarem de maneira sensata.”*

Entrevistado, Setor Manufatureiro, Europa Ocidental

## Avaliação de tecnologias emergentes

Perguntou-se aos entrevistados como se encontram suas organizações em termos de aquisição e implementação de cinco tecnologias emergentes (ver Figura 3):

- Ferramentas de interação social (fóruns na intranet/Internet, mensagens instantâneas, bibliotecas, blogs e wikis, por exemplo)
- Plataformas portáteis (Windows® Mobile, BlackBerry OS e Google Android OS, para citar três)
- Computação em nuvem
- Virtualização
- Arquitetura orientada para serviços (AOS)



Figura 3: Redes sociais, plataformas portáteis e computação em nuvem apresentam as maiores preocupações com riscos.

Dessas cinco tecnologias, redes sociais, plataformas portáteis e computação em nuvem apresentaram os maiores motivos de preocupação. As ferramentas de interação social assumiram a ponta, com 64% dos entrevistados, seguidas de perto por plataformas portáteis e computação em nuvem (54% e 43%, respectivamente). A maioria dos riscos tem a ver com acessibilidade, uso e controle de dados, especialmente referindo-se a redes sociais e ao perigo de sofrer acesso não autorizado a informações privativas e confidenciais. (Muitas organizações ainda não instituíram processos e métodos para integrar ferramentas de interação social em sua infraestrutura e fluxo de trabalho).

Quando solicitados a citar os dois maiores riscos que associam à computação em nuvem, a maioria dos entrevistados apontou para a proteção e privacidade dos dados (ver Figura 4). A continuidade dos negócios está nitidamente na mente de mais da metade dos entrevistados, dos quais 44% acreditam que nuvens privadas são mais arriscadas do que os serviços de TI tradicionais e 77% manifestaram preocupação com a privacidade.

*“A nuvem só é uma oportunidade de resolver um problema quando se consegue aproveitar suas melhores vantagens. Portanto, isto é um fator que tem de ser computado.”*

Entrevistado, Setor de Tecnologia da Informação, América do Norte



Figura 4: Riscos associados à computação em nuvem.

A transmissão de dados para terceiros também foi considerada fator de risco por 61% dos entrevistados, ficando apenas 23% preocupados com invasões na rede.

Somente 26% dos entrevistados indicaram a virtualização como risco significativo para suas empresas. Da mesma forma, a arquitetura orientada para serviços (AOS) preocupou apenas 25%.

---

## Baseados na Nuvem

Os gerentes de TI estão sentindo a pressão para reduzir gastos com infraestrutura, aumentar eficiências e melhorar o nível dos serviços para toda a empresa. Muitos buscam a computação em nuvem para ajudá-los a atingir esses objetivos. A computação em nuvem representa um grande avanço dentre os modelos de computação – assim como foram seus antecessores, os modelos cliente/servidor e de mainframe. Executa-se o processamento através de uma rede distribuída de acesso global com recursos de TI que são liberados sob demanda, como serviços. A computação em nuvem oferece uma alternativa dinâmica e altamente automatizada para a aquisição e fornecimento de serviços de TI – permitindo que usuários acessem nuvens públicas, privadas e híbridas em busca de recursos e serviços de computação sem atentar diretamente para a tecnologia que os sustenta. Hoje, as empresas estão se valendo da grandiosa capacidade de ampliação e colaboração da computação em nuvem para resolver problemas de formas até então impossíveis. Com isto, estão implementando novos serviços mais depressa e sem outros investimentos de capital. Apesar de tudo, as organizações precisam ser prudentes e estar bem-informadas ao escolher um provedor, principalmente quanto a questões de risco.

---

## Implicações para os gerentes de TI

Dentre os gerentes de TI entrevistados, a maioria espera que suas responsabilidades – desde a execução de políticas e procedimentos e o fornecimento de insumos para estratégias de redução de riscos até a colaboração para definir e/ou supervisionar estratégias de risco de TI para a organização – aumentem durante os próximos três anos (ver Figura 5). Mais de 65% dos entrevistados concordaram que a redução dos riscos está se tornando mais presente em seus trabalhos, com 83% acreditando que a categoria deve se envolver mais com o assunto.

Quando se considera o aumento da interdependência de negócios e TI, essas respostas não surpreendem. Na verdade, os gerentes de TI e diretores de Informação entrevistados acreditam que seus trabalhos deverão incorporar mais apoio à estratégia geral da empresa, tanto quanto à marca corporativa (por exemplo, em marketing e atendimento ao cliente). À medida que mais empresas estabilizam ou “endurecem” suas estratégias, processos e procedimentos de gestão de risco, a responsabilidade pela infraestrutura pode migrar para um fornecedor ou parceiro – liberando os gerentes de TI para se concentrar mais na segurança, resiliência e continuidade dos negócios.

Também é interessante notar que, ao fazer o cruzamento de dados dos 131 diretores de Informação que responderam à pesquisa, as respostas não variaram muito em relação àquelas dos gerentes de TI.

Apesar do significado da gestão de riscos de TI e sua adaptação às regulamentações ser prontamente reconhecida por organizações de todos os ramos, e de haver muita gente trabalhando para melhorar esses aspectos em suas empresas, poucos estão totalmente preparados para todos os riscos e adaptações a situações que possam ocorrer.

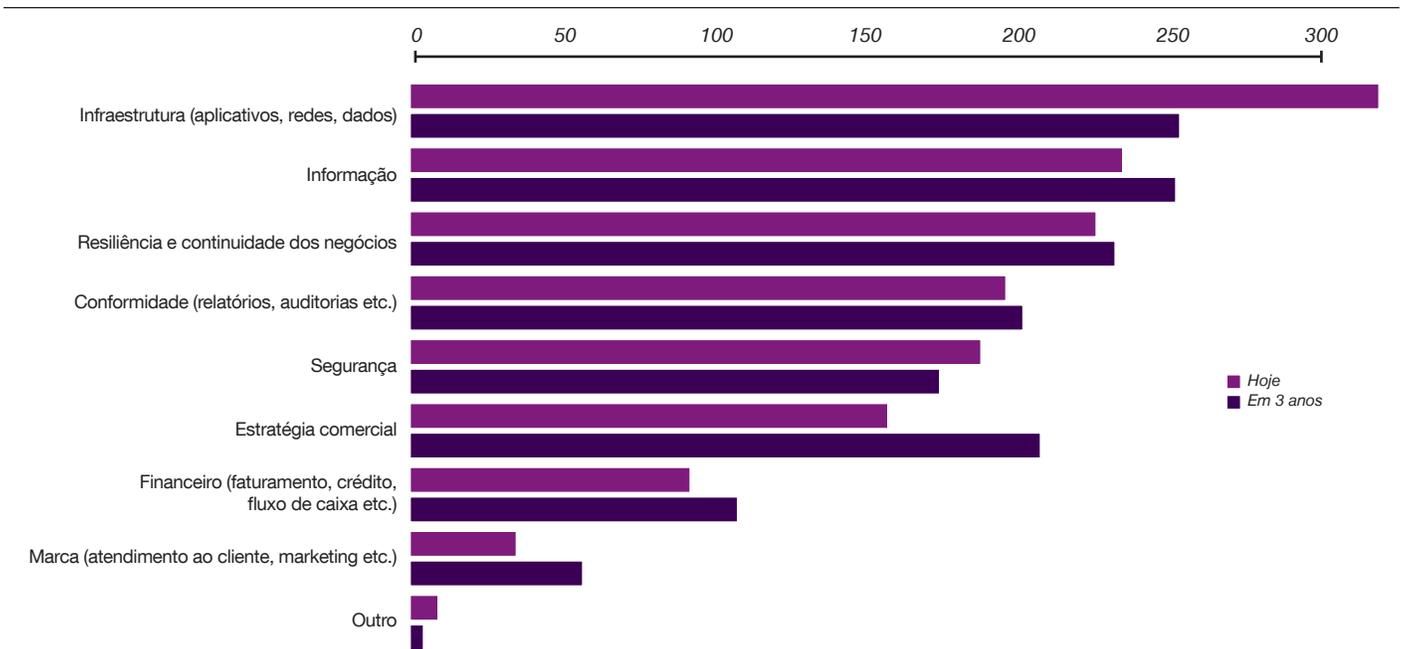


Figura 5: Os gerentes de TI acham que suas áreas de responsabilidade vão se alterar durante os próximos três anos.

Os resultados do Estudo da IBM Global em 2010 sobre Riscos de TI revelou campos de interesse que podem ajudar os gerentes de TI a avaliar seu grau de preparo frente aos riscos, apontar lacunas, definir prioridades e desenvolver estratégias em diversos planos:

- No âmbito da empresa, a consciência do risco é responsabilidade de todos. No entanto, a menos que políticas e procedimentos contra riscos estejam enraizados na cultura corporativa, muitas iniciativas para gestão e redução dos riscos de TI deixarão a desejar ou fracassarão por completo. Os resultados do estudo confirmam que é

preciso trabalhar mais nas empresas para educar, comunicar e apoiar as iniciativas de gestão e adaptação a riscos em toda a sua hierarquia.

- Dados constituem uma preocupação comum em todos os aspectos da gestão de riscos de TI desde a segurança, a resiliência e continuidade dos negócios até sua disponibilidade, recuperação de desastres, invasores, adaptação, infraestrutura e gestão de dados. Com isto em mente, as empresas devem assumir um enfoque unificado e holístico dos riscos de TI – levando em conta todos os seus elementos a fim de alcançar os objetivos gerais de ampliar os retornos e as eficiências.

- Ao adotar tecnologias, arquiteturas e estratégias emergentes, desenvolver novas aplicações ou integrar sistemas existentes, a redução dos riscos deve ser um ponto de discussão fundamental. Levar em conta tanto os riscos positivos (que a companhia deflagra por causa da oportunidade que o acompanha) e os negativos (possíveis incidentes capazes de prejudicar os negócios) pode agregar mais valor comercial e talvez aumentar o faturamento – mas somente se incluir verbas adequadas para a gestão dos riscos de TI. Nem todas as tecnologias emergentes nascem iguais, mas algumas – como a virtualização e a computação em nuvem – podem trazer muitas vantagens em termos de suporte e opções para redução dos riscos. Apesar da computação em nuvem exigir atenção com a segurança dos dados, se propriamente desenvolvida ela pode ajudar a reduzir custos e atenuar os riscos associados à resiliência dos negócios. Porém, é vital contar com processos ativos para lidar com os riscos inerentes a qualquer tecnologia nova.

---

*“Às vezes tendemos a considerar um plano de projeto de forma muito simplista, achando que sabemos onde estão os riscos, e assim tratamos da alocação de recursos com base nisto.”*

Entrevistado, Setor de TI e Tecnologia, África e Oriente Médio

---

## **O caminho do sucesso**

A gestão eficaz dos riscos de TI constitui um esforço multifacetado. Para assumir esta tarefa, os gerentes de TI devem considerar o seguinte:

### ***Examinar e avaliar a capacidade de risco de TI da organização***

- Instituir um planejamento geral para todas as categorias de risco (dados, segurança, resiliência e recuperação de desastres, novas tecnologias).
- Considerar a variedade de desafios de risco, confirmar se existe um plano para tratar de cada um (dar prioridade e reduzir riscos de depreciação como falhas de sistema e violações de segurança, por exemplo) e investigar como tirar proveito dos riscos de valorização (menos tempo de atendimento às demandas do mercado e novos pontos de contato com o cliente, por exemplo).

### ***Buscar defensores entre a diretoria***

- Tornar-se consultor de confiança e auxiliar valioso do CIO; articular os benefícios trazidos por ele e outros dirigentes ao tratar de riscos de TI.
- “Vender” as vantagens da redução do risco, tais como a expansão mais vigorosa dos negócios, com mais agilidade e melhor percepção da marca.

### ***Determinar como aumentar a percepção do risco em todos os níveis e dentro da própria cultura organizacional***

- Incorporar a percepção do risco no cotidiano dos negócios e dos processos de TI. Providenciar para que haja uma variedade de métodos para instrução da empresa inteira.
- Criar uma estratégia para a comunicação regular da amplitude da gestão de riscos, assim como de tópicos e problemas de conformidade – ressaltando tratar-se de mais do que uma simples atividade isolada.

---

### ***Buscar meios inovadores de implementar procedimentos de redução de riscos***

- Incorporar procedimentos contra riscos na infraestrutura de TI ao invés de agregá-los aos aplicativos de modo fragmentado.
- Examinar processos de trabalho quanto a possíveis problemas de risco e estabelecer um plano específico de governança de riscos de TI capaz de ser executado em toda a organização.

### ***Garantir a existência de salvaguardas que ajudem a impedir o acesso não autorizado aos dados e sistemas da empresa***

- Analisar planos de continuidade dos negócios. A continuidade dos negócios envolve mais do que preparar-se para um desastre natural; ela cobre um amplo leque de cenários de interrupção das atividades – desde falhas de servidor até pandemias.
- Conscientizar as pessoas de sua responsabilidade pela segurança e proteção dos dados – e como executar essa responsabilidade.
- Identificar instrumentos, processos e metodologias para manter os dados seguros e protegidos. Lembrar-se de que muitos já existem (acesso e controle de identidades; gestão de dados de referência; gestão dos ciclos de vida das informações; processos de propriedade dos dados).

Já não se trata mais de se novas tecnologias serão introduzidas na organização, mas *quando*. Como já foi dito, nem todas as tecnologias emergentes nascem iguais, mas algumas podem ter vantagens expressivas em termos de gestão dos riscos de TI. As tecnologias mais modernas, como virtualização e computação em nuvem, oferecem esplêndidas opções de atenuação de riscos e redução de custos.

---

### **Você está pronto?**

- Como a sua empresa avalia seu nível de preparo frente aos riscos e os controla tanto em termos dos negócios quanto em sua infraestrutura e recursos de TI?
  - Que estratégias sua organização implantou para acompanhar as melhores práticas do ramo e de TI visando a redução dos riscos – começando com segurança e incluindo resiliência e continuidade dos negócios?
  - De que maneiras as iniciativas da sua empresa contra riscos ajudam a melhorar sua visibilidade e controle, garantindo conformidade com contratos, normas do ramo, regulamentos e controles internos?
  - Como a sua infraestrutura de TI dá apoio aos atuais objetivos de desempenho da empresa em termos de flexibilidade, segurança, disponibilidade, escalabilidade, resiliência e governança?
  - Que tipo de plano sua organização tem para assegurar que capital humano, processos e sistemas consigam se recuperar e reagir a um evento destrutivo?
-

A governança cíclica e vigorosa dos riscos de TI – sob as perspectivas da tecnologia e dos negócios – avalia de forma contínua a vulnerabilidade da empresa a esses riscos, definindo suas respectivas prioridades e atuando sobre cada um deles. Por conseguinte, é importante incorporar protocolos de gestão de risco às novas tecnologias assim que elas forem implementadas.

Finalmente, considerar as necessidades da empresa durante a implementação de instrumentos e processos. Equilibrar a velocidade de atendimento às demandas do mercado com o risco aceitável. Ao assumir uma postura proativa quanto à gestão dos riscos de TI, as empresas podem se posicionar de modo a manter-se na dianteira das vulnerabilidades e reforçar sua segurança e resiliência em face de incidentes planejados ou imprevistos.

### Para mais informações

Para saber mais sobre este estudo do IBM Institute for Business Value, entre em contato conosco pelo endereço [iibv@us.ibm.com](mailto:iibv@us.ibm.com). Para um catálogo completo da nossa pesquisa, visite:

[ibm.com/iibv](http://ibm.com/iibv)

Para acessar outros recursos de gerenciamento de riscos de TI, visite:

[ibm.com/smarterplanet/security](http://ibm.com/smarterplanet/security)

### Autores

Linda Ban é a CxO Study Program Director e AIS Lead do IBM Institute for Business Value. Nesta função, ela lidera uma equipe global responsável pelo desenvolvimento, implementação e suporte de formadores de opinião da IBM em torno do programa de diretores da Informação, assim como da sua organização de Application Innovation Services (AIS). A formação diversificada de Linda compreende uma longa experiência em tecnologias emergentes e de colaboração, estratégia comercial e de operações, desenvolvimento de sistemas e gestão de operações. Além do seu trabalho com os clientes, ela tem vários títulos publicados sobre vários temas, desafios e soluções empresariais. Para entrar em contato com Linda, escreva para [lban@us.ibm.com](mailto:lban@us.ibm.com).

Richard Cocchiara é um IBM Distinguished Engineer e o Chief Technology Officer for Business Continuity and Resiliency Services na IBM Global Services. Ele acumula mais de 28 anos de experiência em I/S, tendo prestado consultoria para muitas empresas da classe Fortune 500, particularmente nos segmentos financeiro e do mercado de capitais. No momento, Rich é responsável pela pesquisa e desenvolvimento de soluções e serviços de Business Continuity and Resiliency no âmbito da IBM Global Technology Services. Ele pode ser encontrado no endereço [rmcoccb@us.ibm.com](mailto:rmcoccb@us.ibm.com).

Kristin Lovejoy é a Vice-Presidente responsável pela Estratégia de Segurança da IBM. Ela foi reconhecida como uma das Top 25 CTOs pela InfoWorld em 2005 e como uma das executivas mais influentes pelo prêmio Top 25 Most Influential Security da revista Security em 2006. Ela detém patentes nos EUA e na UE por seu Modelo e Metodologia de Gerenciamento de Riscos Orientados por Objetos. Para entrar em contato com Kristin, escreva para [klovejoy@us.ibm.com](mailto:klovejoy@us.ibm.com).

Ric Telford é o Vice-Presidente da IBM Cloud Services e o responsável pela definição de novas oportunidades e serviços como parte do volumoso portfólio da IBM de ofertas para computação em nuvem. Durante sua permanência na IBM, Telford desempenhou uma série de funções relevantes em várias iniciativas de software e serviços para a empresa, incluindo gestão de documentos, redes, gestão de sistemas e serviços de infraestrutura de TI. Antes disso, Ric atuou como vice-presidente da Autonomic Computing, liderando o desenvolvimento de sistemas com maior auto-gestão. Ric pode ser encontrado em [rtelford@us.ibm.com](mailto:rtelford@us.ibm.com).

Mark Ernest é um IBM Distinguished Engineer e membro da IBM Academy of Technology. Ele ajuda clientes a projetar e implementar sistemas de gerenciamento de TI para maximizar o valor do seu investimento nesta área e aprimorar a eficiência e eficácia no uso que fazem da tecnologia da informação. Mark pode ser contactado pelo [lernest@us.ibm.com](mailto:lernest@us.ibm.com).

## A parceira certa para um mundo em transformação

Na IBM, colaboramos com nossos clientes, trazendo concepções empresariais, pesquisa e tecnologia avançada que lhes proporcione uma vantagem nítida no rápido ambiente de transformações da atualidade. Através de nosso enfoque integrado de projeto e execução de negócios, ajudamos a transformar estratégias em ações. E com a experiência em 17 segmentos de atividade e recursos globais que abrangem 170 países, podemos ajudar o cliente a prever mudanças e aproveitar novas oportunidades.

## Referência

- 1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.



---

© Copyright IBM Corporation 2010

IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Produzido nos Estados Unidos da América do Norte  
Setembro de 2010  
Todos os Direitos Reservados

IBM, o logo IBM e [ibm.com](http://ibm.com) são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos, em outros países ou ambos. Se estes e outros termos registrados da IBM estiverem assinalados em sua primeira ocorrência neste informativo com o símbolo de marca comercial (® or ™), esses símbolos indicarão marcas comerciais registradas ou consuetudinárias nos EUA pertencentes à IBM na época em que este informativo foi publicado. Essas marcas também podem ser registradas ou consuetudinárias em outros países. Uma relação atualizada das marcas comerciais da IBM está disponível na Internet, sob o título "Copyright and trademark information" no endereço [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Windows é marca registrada da Microsoft Corporation nos Estados Unidos e em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou nomes-fantasia de terceiros.

As referências nesta publicação a produtos e serviços da IBM não implica que a IBM pretenda disponibilizá-las em outros países onde opere.



Por favor recicle