Informativo

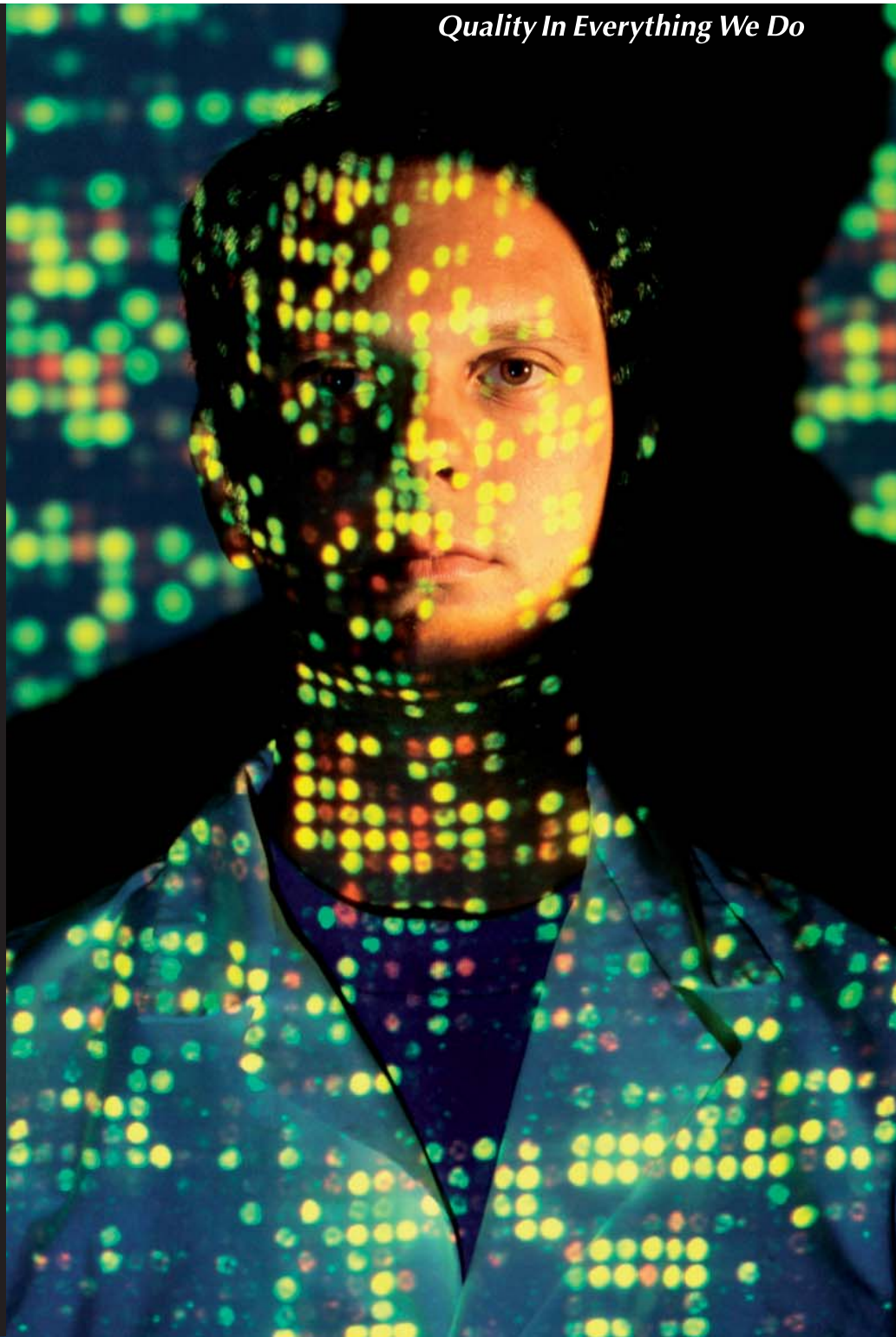
Digital Insights

Temas de tecnologia e segurança da informação para executivos

Junho/2007

Ernst & Young

Quality In Everything We Do



Digital Insights é uma publicação destinada a clientes e colaboradores da Ernst & Young, que aborda questões relevantes para as empresas na área de tecnologia da informação. Alertamos os leitores para o fato de que as opiniões aqui expressas não devem ser utilizadas, de maneira isolada, para a tomada de decisão por parte das empresas. Isto porque existem particularidades atinentes a cada empresa que podem, eventualmente, alterar o enfoque transmitido na opinião. Recomendamos que, antes de a decisão ser tomada, as empresas discutam esses pontos de vista com seus consultores. Estamos à disposição para discutir nossas opiniões e sua aplicação em cada caso concreto.

Mais informações sobre a área de Riscos Tecnológicos e Segurança da Informação com:
Alberto Fávero (alberto.favero@br.ey.com) e
Wilson Gellacic (wilson.gellacic@br.ey.com)
ou pelo e-mail tsrs@br.ey.com

Digital Insights é uma publicação da:
Área de Comunicação e Gestão da Marca da Ernst & Young Brasil

Jornalista Responsável: **Rejane Rodrigues** (Mtb 22.837-SP)

Textos: **Inaldo Cristoni, Nelson Rocco e Rejane Rodrigues**

Projeto Gráfico: **Rogério Weikersheimer**

Compliance e privacidade de dados pessoais são prioridades em segurança da informação

Pesquisa global da Ernst & Young traz impressões de executivos de 1.200 organizações e agências governamentais em 48 países

A conformidade com leis e regulamentos tornou-se um dos principais fatores de impacto na segurança da informação das organizações. Essa é uma das conclusões da Pesquisa Global sobre Segurança da Informação 2006, realizada pela Ernst & Young com cerca de 1.200 companhias, em 48 países. Para 56% dos entrevistados, a conformidade (*compliance*) com leis e regulamentos afetou suas práticas de segurança da informação nos 12 meses anteriores à pesquisa, enquanto 50% acham que ela irá influenciar a área nos 12 meses seguintes.

> Deixar de atender aos requisitos regulatórios é um dos mais sérios riscos que as empresas podem enfrentar

"Houve um amadurecimento dos negócios que acabou exigindo um controle maior sobre *compliance*. A Lei Sarbanes-Oxley é um dos carros-chefes para isso, mas há outros fatores vindos dos bancos centrais de todo o mundo", diz Alberto Fávero, sócio da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young Brasil. Segundo ele, o próprio alinhamento dos negócios da área de Tecnologia da Informação fez com que houvesse uma mudança das preocupações do setor com temas como fraude e *hackers* para *compliance*.

O destaque que a conformidade com as exigências regulatórias recebeu na pesquisa mostra que, nesta época de atenta vigilância por parte de governos e investidores, deixar de satisfazer plenamente os requisitos regulatórios, principalmente no que se refere aos controles internos, é um dos mais sérios riscos que as empresas podem enfrentar. Segundo o estudo, os participantes acreditam firmemente que o trabalho relacionado à conformidade resultou em avanços na proteção contra os riscos enfrentados pelas empresas.

Os dados indicam ainda que deve haver um alinhamento contínuo das atividades de negócio, governança, TI e segurança da informação nas empresas. A governança corporativa e a conformidade regulatória exigem o alinhamento efetivo dos controles de gestão financeira, operacional e de segurança da informação. Nesse sentido, a conformidade impõe uma melhora à segurança da informação.

Amadurecimento

De acordo com a pesquisa, quase 80% dos participantes acreditam que os esforços para atingir a conformidade regulatória melhoraram a segurança da informação. "Esse resultado sugere que as empresas do segmento estão mais maduras na forma como encaram os quesitos de *compliance*", afirma o relatório da pesquisa.

As organizações passaram a entender, segundo o estudo, que *compliance*, embora exigente, não deve ser tratado como obstáculo. "Na realidade, as empresas perceberam que o trabalho relacionado a *compliance* pode ser um catalisador para a solução de problemas que teriam de ser resolvidos de qualquer forma e para o desenvolvimento pró-ativo de novos controles e processos", diz o texto.

Proteção à privacidade

A privacidade e a segurança dos dados pessoais é outro tema de preocupação por parte das empresas. Os resultados dão conta de que 52% das companhias adotam pro-

cedimentos formais para a proteção da privacidade e de dados pessoais, enquanto 31% usam procedimentos informais. Apenas 7% da amostra têm na validação por terceiros uma garantia contra esses riscos e outros 8% não abordam a proteção da privacidade e dos dados pessoais.

"Os executivos financeiros, de TI e de negócios passaram a perceber que os dados não estão mais restritos às suas fronteiras", afirma Fávero. "E o risco da perda de informação, de acontecer algo que está fora de seu controle e do fornecedor, pode afetar o seu negócio. Hoje falamos em processo colaborativo. Não é mais uma empresa única, mas um processo que envolve várias organizações", completa.

AS PRIORIDADES EM SEGURANÇA DA INFORMAÇÃO

A Pesquisa Global sobre Segurança da Informação 2006 detectou cinco prioridades para as organizações na área de segurança da informação. Conheça as ações que devem estar na pauta de melhorias:

- Integração da segurança da informação;
- Ampliação do impacto de *compliance*;
- Administração dos riscos de terceiros;
- Proteção da privacidade e de dados pessoais;
- Desenvolvimento de segurança da informação.

O relatório da pesquisa afirma que a proteção à privacidade e de dados pessoais continuará a ser uma prioridade para as empresas. Exigirá supervisão rigorosa por parte das organizações e a formalização cada vez maior de medidas para a diminuição dos riscos. “A empresa que está preocupada com isso sairá na frente. A que ignora ou age de má-fé perde em vantagem competitiva”, avalia Fávero.

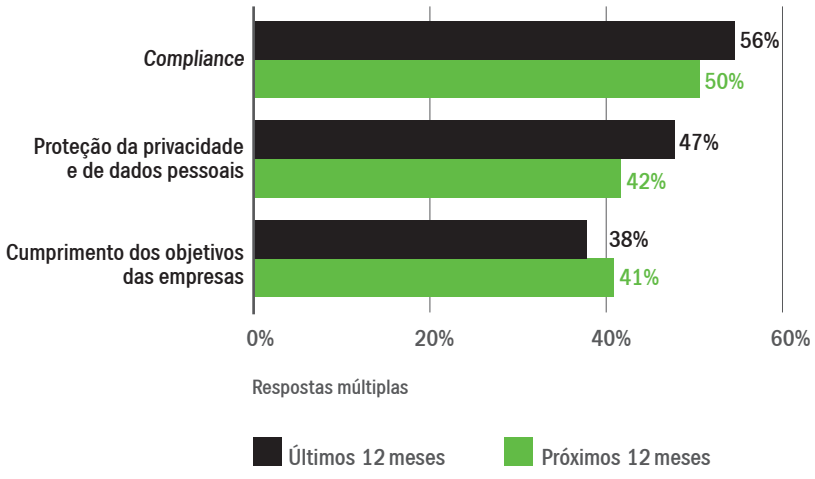
O sócio da Ernst & Young conta que a privacidade dos dados tem sido um tema muito discutido nos Estados Unidos. Em sua avaliação, lá o consumidor é mais exigente que o brasileiro, as pessoas cobram muito mais das empresas com as quais se relacionam. Ainda segundo ele, a convergência de mídias e tecnologias irá “exacerbar” ainda mais essa necessidade de proteção à privacidade dos dados e informações sobre as pessoas.

Riscos de terceiros

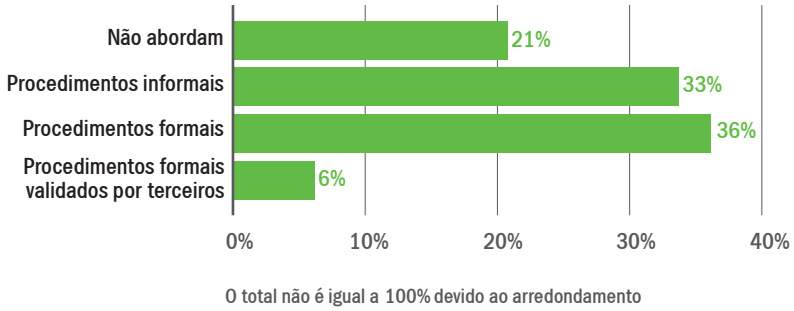
Nesse sentido, certificar-se de que os fornecedores também têm consciência dos riscos a que estão sujeitos dados e informações pessoais é muito importante. De acordo com a pesquisa, mais de um terço dos participantes afirmou ter procedimentos formais de administração do risco de fornecedores. Para muitos, essa atitude leva à confiança de que a administração do risco de fornecimento está sob controle. Na realidade, afirma o relatório da pesquisa, dois terços das empresas consultadas acreditam que seus fornecedores e parceiros são capazes de cumprir suas políticas, procedimentos e normas.

Uma tendência apontada no estudo é que os fornecedores, por sua vez, reconhecem cada vez mais a importância da segurança da informação nas suas negociações com terceiros. Esse grupo informou que, neste ano, deverá investir mais tempo cumprindo os requisitos de certificação de segurança da informação estabelecidos nos contratos firmados. “Por esse motivo, esperamos ver as auditorias SAS 70 e as certificações ISO 27001 continuarem a ganhar destaque como meio para avaliar os controles da segurança da informação e demonstrar aos clientes a qualidade desses controles”, afirma o relatório.

Prevê-se que *compliance* será prioridade para a segurança da informação nos próximos 12 meses



Como as organizações abordam a administração do risco de fornecimento:



Um aliado estratégico para o negócio

O emprego dos conceitos de *IT Governance* e *IT Effectiveness* é imprescindível para que as empresas possam cumprir o desafio de promover o alinhamento da área de tecnologia da informação com a estratégia de negócio

A busca pelas melhores práticas de gestão ocupa, hoje, boa parte da agenda dos executivos das grandes corporações. Transparência, eficiência operacional, maximização e retorno dos investimentos, adequação dos processos internos às leis e normas internacionais, como Sarbanes-Oxley e Basiléia II, são requisitos essenciais no mercado cada vez mais globalizado. Nesse cenário, as empresas enfrentam o desafio de promover o alinhamento da área de tecnologia da informação com a estratégia de negócio para dar sustentação ao avanço de suas atividades.

No meio corporativo é forte o movimento no sentido de transformar a área de TI em uma aliada estratégica. Mas, para atingir esse objetivo, é preciso contar cada vez mais com iniciativas que garantam o uso eficaz dos recursos tecnológicos. As práticas mais usuais para atender com agilidade e eficiência às demandas de negócio são a *IT Governance* e o *IT Effectiveness*, que ajudam a estabelecer critérios de definição, gestão e acompanhamento de resultados de investimentos em TI. A aplicação desses dois conceitos tornou-se uma tendência mundial por causa da importância do setor de TI no dia-a-dia das organizações. Enquanto o primeiro indica os caminhos que a área deve seguir para atender as metas da empresa, o *IT Effectiveness* é utilizado para medir os benefícios decorrentes da utilização dos recursos tecnológicos. "É uma abordagem sobre o papel da área de TI na estrutura de governança corporativa de uma organização", define Zunara Carvalho, diretora-executiva da área de Risk Advisory Services da Ernst & Young.

> O Brasil é hoje o país de maior destaque na implantação de programas de Governança de TI na América do Sul

Estudo divulgado pelo Massachussets Institute of Technology (MIT), dos Estados Unidos, indica que os lucros das empresas que adotam as boas práticas de governança de TI são, em média, 20% superiores ao das demais. Segundo Sergio Kogan, diretor-executivo da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young, por causa do porte das empresas e do tamanho do mercado, o Brasil é o país de maior destaque na implantação de programas de governança de TI na América do Sul. "Os executivos estão empenhados em saber como melhorar os resultados da organização", afirma.

Mais investimentos em TI

Um olhar sobre as pesquisas mais recentes comprova esse movimento. Nos últimos anos, os investimentos na área TI avançaram de forma expressiva no país e tendem a seguir em ritmo forte em 2007. O estudo Brasil IT Spending by State 2007, elaborado ela IDC Brasil, mostra que no exercício passado as empresas brasileiras aplicaram o equivalente a R$ 39 bilhões em TI. A projeção para este ano gira em torno de R$ 45 bilhões. Com isso, a participação de TI no Produto Interno Bruto (PIB) poderá passar de 2% para 2,2%.

Já o Instituto Sem Fronteiras (ISF) fez um mapeamento das tendências de investimentos em TI para 2007 a partir de consultas a 940 empresas de diversos setores, como finanças, governo, manufatura, óleo e gás, mineração, comércio, serviços públicos e agronegócio, que faturam acima de R$ 50 milhões por ano. E concluiu que o orçamento de TI crescerá dois dígitos pelo terceiro ano consecutivo, com os investimentos chegando a R$ 44 bilhões em 2007.

A mesma pesquisa atestou que a adoção de programas de governança de TI é uma prioridade para este ano. Do universo de empresas consultadas pelo ISF, apenas 13% disseram que estão experimentando níveis mais avançados de utilização do conceito. O levantamento constatou, ainda, que o grande interesse no tema não decorre da imposição da alta direção das empresas, mas da constatação da necessidade de adotar uma metodologia capaz de melhorar os serviços prestados pela área de TI.

As vantagens do alinhamento de TI aos processos de negócios são muitas. Uma delas é que desmistifica a idéia, tão comum quanto equivocada, de que a área de TI serve apenas para solucionar problemas dentro do ambiente corporativo, além de contribuir para diminuir a complexidade do ambiente, eliminar atividades redundantes e gerar aumento de produtividade. Mais que isso, ela vem sendo requisitada para auxiliar

no planejamento, na implantação e na viabilização de ações que permitam a concretização dos objetivos das empresas. “Uma organização de TI efetiva cria valor para a empresa como um todo ao entregar benefícios que superam os custos envolvidos”, comenta Sergio.

Por outro lado, o alinhamento permite programar melhor os investimentos na infra-estrutura tecnológica, evitando a aquisição de sistemas e máquinas que não atendem às necessidades da corporação. “Há situações em que o projeto não contempla fatores inerentes ao ambiente de TI, como a escalabilidade dos equipamentos. Quando adquire uma solução, a empresa precisa levar conta que a sua infra-estrutura cresce à medida que os negócios evoluem”, explica Zunara.

Um novo perfil do CIO

O papel do CIO (*chief information officer*) ganhou uma nova dimensão na busca pelas melhores práticas de governança de TI. A esses profissionais cabe a missão de coordenar o processo de alinhamento da área de TI com a estratégia de negócio e, talvez o mais difícil, demonstrar de forma clara e objetiva como os investimentos em tecnologia podem gerar resultados e melhorar o desempenho da companhia. A tarefa é ainda mais árdua nas situações em que a área de TI é vista como um centro de custo ou no caso de empresas para as quais a área de TI não é considerada um fator crítico para o negócio. Zunara reforça a idéia de que o trabalho do CIO não pode ser dissociado do restante da companhia. Como responsável pela área de TI, ele deve ter assento obrigatório nos comitês da estrutura de governança corporativa e participar ativamente das grandes decisões. “Parte da visão do CIO está focada no negócio e parte, na avaliação sobre como TI responde à estratégia da empresa”, explica.

> Hoje, as empresas cobram do CIO uma visão de processos, produtividade, retorno sobre investimentos e custos

Nesse sentido, há uma mudança no perfil profissional do CIO. Há algum tempo habilidades técnicas e conhecimento profundo da tecnologia deixaram de ser um diferencial para os profissionais que atuam na área de TI. Hoje, as empresas cobram do CIO uma visão de processos, produtividade, retorno sobre investimentos e custos. Em uma palavra, o CIO precisa entender do negócio. Esse é um fator preponderante para o esforço de atrelar as iniciativas na área de TI à estratégia de negócio, bem como para o relacionamento do dia-a-dia com o CFO (*chief financial officer*), com o CEO (*chief executive officer*) e com os diversos organismos de gestão e de governança.

Como garantir a continuidade do negócio

Em uma época em que as informações trafegam em nanossegundos, dispor de um plano de gerenciamento de crise consistente é condição essencial para a empresa evitar riscos com a indisponibilidade dos recursos tecnológicos, que podem causar impactos negativos ao negócio.

Apenas metade dos planos de continuidade dos negócios foi testada no último ano, como revela a Pesquisa Global sobre Segurança da Informação 2006 realizada pela Ernst & Young com executivos de aproximadamente 1.200 organizações globais. Mais: um terço dos entrevistados declarou que os prazos para recuperação não foram acertados com a empresa, o que pode resultar em esforços aplicados a processos e sistemas errados, no caso de recuperação de desastres. São dados que alertam para a necessidade de uma empresa estar preparada para lidar com situações que podem prejudicar a sua imagem, comprometer a sua saúde financeira ou, até mesmo, levá-la ao extremo da falência.

Na verdade, a ocorrência de eventos adversos faz parte da dinâmica do mundo dos negócios e atinge todas as organizações independentemente do seu porte, ramo de atividade, grau de credibilidade e solidez. Por isso, um ramo da gestão empresarial que está ganhando força no mercado corporativo é o gerenciamento de crises, que nada mais é que um processo estabelecido pelas organizações para enfrentar situações adversas.

Mas quais ações o gerenciamento de crises deve contemplar? Depende da empresa e dos tipos de risco aos quais está exposta. Antes de mais nada, é preciso avaliar se a ocorrência consiste, de fato, em uma crise ou pode ser classificada como apenas um problema. Essa definição é muito importante para definir a melhor estratégia de trabalho. Em linhas gerais, um problema é um evento localizado que pode ser resolvido internamente sem impactos significativos. Já a crise, ao contrário, extrapola os limites do ambiente corporativo e, além dos funcionários, pode afetar clientes, fornecedores e parceiros. O ideal é que a análise e a classificação de eventos sejam conduzidas por um comitê multidisciplinar de gestão de crise, mas não são todas as companhias que contam com essa figura em seu organograma.

> Um fator decisivo para a indisponibilidade de tecnologia é a ineficácia do planejamento de infra-estrutura ou de sistemas

Como lembra Andréa Thome, gerente sênior da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young, as empresas atualmente estão expostas a diversos tipos de crises. Existem aquelas associadas à imagem, às finanças, à sucessão (mudanças na cúpula administrativa), entre outras. Mas a mais freqüente delas diz respeito à indisponibilidade dos recursos tecnológicos, que guarda relação direta com temas como recuperação de desastres, contingenciamento e redundância do ambiente de tecnologia da informação. “A questão é mais crítica quanto mais o negócio da empresa depende de TI”, observa a gerente, acrescentando que eventos relacionados à indisponibilidade de tecnologia não resultam, necessariamente, da falta de planejamento ou de um planejamento mal-elaborado dos investimentos em TI. “Muitas vezes as empresas possuem as soluções adequadas, mas os negócios crescem de tal forma que fica difícil atender às novas demandas”, explica.

Falhas de planejamento

Na avaliação de Andréa, um fator que pode ser decisivo para a indisponibilidade de tecnologia é a ineficácia do planejamento da capacidade da infra-estrutura ou dos sistemas em operação. Em outras palavras, as empresas pecam por não fazer simulações das situações relacionadas à indisponibilidade dos recursos ou por não disporem de estruturas alternativas (sistemas, plataformas, infra-estrutura redundantes etc.) para situações de emergência. “Às empresas faltam, ainda, planos bem definidos de continuidade de negócio e de recuperação de desastres”, observa. Andréa adverte que, dependendo da gravidade da crise, nem sempre os planos convencionais de geração e armazenamento de backups adotados pelas empresas são suficientes para garantir a continuidade da operação.

O gerenciamento de crises está mais fortemente ligado a um dos três pilares da segurança da informação:

disponibilidade (os outros dois são confiadencialidade e integridade). Entretanto, em muitos casos o assunto não recebe a atenção que a sua importância exige ora porque o orçamento previsto não é suficiente ora porque a abordagem é equivocada. É verdade que as empresas procuram adotar medidas de prevenção, mas elas podem não ser eficazes se não estiverem no nível exigido para garantir a alta disponibilidade dos seus sistemas. Por outro lado, uma empresa pode investir em *backups* e enfrentar problemas de indisponibilidade de sistemas ou montar um ambiente de alta disponibilidade e ter problemas com a infra-estrutura.

Para a gerente da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young, no que tange ao gerenciamento de crises, as companhias devem levar em consideração dois fatores essenciais. Um deles é que a estratégia de negócio precisa ser suportada pelas ações de tecnologia que serão colocadas em prática. O outro ponto refere-se à necessidade do alinhamento entre a estratégia de negócio e a estratégia de tecnologia. “Isso é muito importante porque, por exemplo, se uma empresa pretende aumentar em 30% as suas vendas, a sua infra-estrutura tecnológica tem de ser redimensionada para atender essa meta”, exemplifica.

Como evitar crises

Planos de contingência, de recuperação de desastres e de continuidade da operação são algumas das medidas previstas para o enfrentamento de crises de indisponibilidade de recursos tecnológicos. O problema costuma ser abordado, também, sob o prisma da redundância do ambiente, ou seja, a duplicação dos sistemas e plataformas instalados. De acordo com Andréa, uma vez identificada a natureza da crise, recomenda-se às corporações seguir alguns passos considerados indispensáveis para elaboração do que ela denomina plano de tratamento e gestão de crises. A primeira providência é fazer uma análise do negócio, levantando suas necessidades e os cenários de crise temidos. Depois, devem ser feitas simulações dos riscos, que permitirão identificar os pontos vulneráveis e as principais ameaças para o ambiente corporativo. A fase de avaliação dos riscos deve ser complementada com a análise do impacto de um evento adverso para os processos de negócio, dando embasamento para selecionar e delinear as estratégias adequadas, as prioridades de recuperação dos processos de negócio no advento de crises e as medidas de controle necessárias.

Enquanto cuida da elaboração dos planos, a empresa deve se ocupar da implementação de um planejamento adequado de comunicação como forma de garantir a transparência dos fatos. Também durante as crises é fundamental fornecer informações sobre a ocorrência do incidente para o público interno e externo, sua evolução e as ações em curso para solucioná-las. Apesar da importância do tema, menos da metade das organizações contam com estratégias de comunicação interna e externa, de acordo com resultados da Pesquisa Global sobre Segurança da Informação 2006 da Ernst & Young. “Infelizmente, muitas empresas ainda não se deram conta de que um plano de comunicação em paralelo a todo o processo de gestão de crise é essencial para o sucesso da operação”, reitera Andréa.

Segregação de funções, uma arma contra fraudes

Ao permitir que os funcionários tenham acesso ao mínimo necessário para a execução de suas atividades, a empresa reduz a possibilidade de falhas e fortalece o ambiente de TI

Se no passado a proliferação de perfis de acesso foi a solução para manter a continuidade de negócios, hoje ela tira o sono dos profissionais da área de TI. Não é para menos: são cada vez mais comuns os casos em que funcionários mal-intencionados valem-se do acesso a diferentes tipos de operações, especialmente financeiras, em benefício próprio. Infelizmente, na maioria das vezes, quando a fraude é descoberta é tarde demais.

Para evitar situações desse tipo, vêm ganhando força nas empresas os projetos de segregação de funções.

Em linhas gerais, a segregação de funções busca reduzir o acesso de funcionários de uma organização ao mínimo necessário para a execução de suas atividades, tendo em vista que a maioria das invasões aos sistemas é feita por pessoal com acesso autorizado. Para piorar, o volume de usuários nas empresas e a complexidade de sistemas e aplicações são cada vez maiores. "Em um primeiro momento, no final da década de 90, a segregação de funções estava mais relacionada à continuidade de negócios. Foi uma época de proliferação de perfis de acesso. Mas as empresas já começam a ver na restrição de autorizações um recurso importante para ampliar a segurança das informações e preservar os ativos da companhia. Hoje este é um tema notadamente financeiro", pondera Alberto Fávero, sócio da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young.

> A Lei Sarbanes-Oxley contribuiu para que a segregação de funções fosse inserida na agenda de trabalho dos gestores

A introdução da Lei Sarbanes-Oxley (SOX) e de outras exigências regulatórias também contribuiu para que a questão fosse inserida na agenda de trabalho dos gestores. Principalmente em razão do impacto que o grande número de perfis de acesso pode provocar nos balanços financeiros. Nessa linha de raciocínio, a segregação de funções surge como um mecanismo de controle interno que contribui para evitar fraudes ou, no mínimo, determinar a probabilidade de ocorrência desse tipo de problema. Um programa eficiente de segregação de funções pode ajudar uma organização a:

- **Identificar deficiências em operações financeiras;**
- **Determinar quais operações não devem ser combinadas;**
- **Determinar quantos problemas de segregação de funções existem na organização;**
- **Definir uma estratégia de remediação ou mitigação dos problemas;**
- **Executar de maneira adequada os planos de remediação ou mitigação de riscos;**
- **Manter processos apropriados de segregação de funções e processos para minimizar problemas futuros.**

Se a organização segue essas orientações ou mesmo que recorra a apenas algumas delas, o gestor da área de TI já terá uma perspectiva da extensão do problema. Esse quadro poderá inclusive auxiliar o executivo a manter-se informado sobre decisões acerca da segregação de funções e outros aspectos de negócio que impactam as demonstrações financeiras. No Brasil, ao contrário do que já ocorre nos Estados Unidos, esse é um tema ainda incipiente, mas em razão dos benefícios que traz para a organização vem ganhan-

do espaço na pauta não apenas de CIOs, mas principalmente de CEOs e CFOs. “A segregação de funções já ultrapassa os limites da área de segurança da informação. É um tema de interesse para toda a empresa”, resume Márcio Lopes, gerente da área de Riscos Tecnológicos e Segurança da Informação da Ernst & Young.

Para os profissionais da área de TI que ainda não colocaram o tema em sua agenda de trabalho, o primeiro passo rumo a um projeto para segregar funções é fazer um diagnóstico dos perfis de acesso na organização, de modo a identificar os planos de mitigação mais indicados para cada caso. Essa avaliação preliminar oferece uma visão geral da maioria dos problemas. Com o diagnóstico em mãos, é possível desenvolver planos de mitigação ou de desenho de controles compensatórios. No primeiro caso, pode-se optar por fazer as correções por área, por departamento, por empresa (em caso de grandes grupos) ou por produto. A grande vantagem é que esse serviço é modular e customizado. Já nos modelos de controles compensatórios é preciso desenvolver um estudo mais aprofundado do negócio para escolher a melhor estratégia de mitigação dos riscos.

Uma terceira possibilidade é a reengenharia de perfis, modelo mais efetivo atualmente, por redefinir por completo os perfis de acesso dos usuários à informação. Trabalhos realizados pela Ernst & Young com grandes empresas nessa área comprovam que é possível reduzir o número de perfis de acesso em até 70%, com vantagens que vão do aumento da segurança dos sistemas à melhorias no processo de administração dos perfis e controles internos, além da otimização de TI de forma geral. É preciso, porém, ficar alerta sobre a necessidade de checar os perfis mapeados de tempos em tempos, para que o modelo não se torne obsoleto. Outra ação importante para o sucesso de um projeto de segregação de funções é a conscientização dos usuários sobre o benefício da iniciativa. “Sem o comprometimento dos usuários, o processo de gestão de mudança será muito mais difícil”, avalia Fávero. É importante lembrar ainda que a segregação de funções possui relação íntima com os processos de gestão de identidades da empresa.

Na opinião de Alberto Fávero, a segregação de funções continuará como um dos principais controles internos para garantir a segurança e a integridade das informações. “A segregação de funções representa a interseção entre *compliance* e o valor real de negócio, além de contribuir para tornar os sistemas de TI mais eficientes”, avalia.

ERNST & YOUNG

www.ey.com.br