Informativo

Digital Insights

Temas de tecnologia e segurança da informação para executivos

Junho de 2006

Ernst & Young
Quality In Everything We Do

Ernst & Young

www.ey.com.br

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 com:

Hugo Pochettino
(hugo.pochettino@br.ey.com),

Wilson Gellacic
(wilson.gellacic@br.ey.com) e

Alberto Fávero
(alberto.favero@br.ey.com).

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

Jornalista Responsável: **Ana Paula Baltazar** (Mtb 18313-RJ)
Redação: **Erivelto Tadeu**
Projeto Gráfico e Ilustrações: **Rogério Weikersheimer**

Segurança: uma questão de identidade

Um estudo conduzido pela Ernst & Young no Brasil comprova que a profusão de senhas controladas pelo processo manual é a brecha para ocorrências de fraudes e a razão do aumento dos custos para gerenciar direitos de acesso. Por isso, hoje, é praticamente impossível pensar em uma política de segurança e confidencialidade eficaz sem uma solução de gerenciamento de identidades.

A pesquisa foi realizada no ano passado com executivos de 145 companhias brasileiras com faturamento médio anual entre R$ 250 milhões e R$ 1 bilhão. Ela revelou que mais da metade das empresas já foi vítima de, pelo menos, uma fraude interna nos últimos cinco anos. Em 46% dos casos descobertos, o prejuízo não foi recuperado. Os tipos de fraudes mais comuns foram desvios de ativos (65%), corrupção (13%), fraudes contábeis (12%), fraudes em sistemas (6%) e fraudes em seguros (4%).

Apesar do percentual aparentemente baixo de fraudes em sistemas, o número desse tipo de ação – e, conseqüentemente, o montante das perdas – aumentou de modo exponencial nos últimos três anos em todo o mundo. Nos Estados Unidos, por exemplo, as empresas perderam mais dinheiro em 2005 com o roubo de informações confidenciais do que com fraudes financeiras, principalmente por causa de problemas de segurança tecnológica, conforme apurou um levantamento realizado pelo FBI e pelo Computer Security Institute (CSI).

O mais espantoso é que a maior parte dos incidentes partiu de pessoas da própria empresa, por meio de acessos indevidos de funcionários e até mesmo de ex-funcionários. Os dados da pesquisa feita no Brasil pela Ernst & Young confirmam o crescimento desse tipo de crime, ao mostrar que, em 79% dos casos, a iniciativa de cometer a fraude nasce da porta para dentro. Historicamente, os incidentes de segurança no mundo com origem em funcionários representam 70% dos casos.

O aumento dos roubos de informações por parte de pessoal interno sinaliza que a maioria das empresas brasileiras não protege seus dados da maneira correta. Em geral, mais preocupadas com as ameaças externas, investem tudo nas chamadas ferramentas de borda (*firewall*, detector de intrusos, antivírus) e acabam esquecendo de se proteger dos riscos existentes dentro da própria casa. A prática mais usual por parte daquelas que mantêm algum controle para tentar evitar a ocorrência de fraudes é o uso de senhas, o que não tem se mostrado suficiente para coibir a ação de funcionários mal-intencionados. Pior ainda, tem dado margem a um ciclo incessante de senhas, o que obriga as empresas a criar verdadeiros exércitos de administradores e operadores de *help desk* para acrescentar, modificar, excluir e gerenciar direitos de acesso e senhas. Além dos altos custos que esse tipo de estrutura exige, ela não tem conseguido, devido ao volume de checagens manuais, garantir a segurança e o nível de satisfação dos usuários.

É nesse cenário que o emprego do conceito de gerenciamento de identidades (ou IAM - Identity and Access Management) começa a ganhar corpo, tanto no Brasil quanto no restante do mundo. Atualmente, com a expansão e a complexidade das infra-estruturas de TI, em decorrência do acréscimo de aplicações e serviços e da necessidade das empresas de interligar suas redes a clientes, fornecedores, parceiros de negócio e colaboradores, uma solução de IAM se torna parte essencial de uma política de segurança e confidencialidade eficaz.

Além disso, com a exigência de adequação das empresas aos critérios estabelecidos por regulamentações nacionais e internacionais, como a lei americana Sarbanes-Oxley, o acordo Basiléia II e as normas do Banco Central e da CVM, que têm como objetivo dar maior segurança, robustez e transparência às medidas administrativas das corporações ao mercado, o gerenciamento de identidade tem-se tornado cada vez mais indispensável. A Sarbanes-Oxley, por exemplo, exige um controle rigoroso na concessão de senhas e tem sido um dos principais impulsionadores dos investimentos em sistemas de IAM.

Mas, apesar de o gerenciamento de identidades ser um dos pontos mais importantes da política de segurança, as corporações ainda dão pouca atenção à questão, de acordo com Alberto Fávero, sócio da Ernst & Young na área de segurança da informação. Ele avalia, entretanto, que a crescente pressão por transparência e segurança das empresas para atender às demandas regulatórias, bem como a necessidade de buscar a melhoria de processos para aumentar a produtividade e a competitividade no mercado, deverá alterar radicalmente esse quadro. Uma das principais razões dessa mudança, segundo Fávero, está na necessidade de as empresas reduzirem custos com o controle de acesso a dados e informações.

O problema ganhou dimensão na última década com o avanço da informatização dos processos de negócios e o advento da internet, que causaram um crescimento desordenado de sistemas e plataformas de *hardware* e *software*. Isso deu margem ao surgimento de uma profusão de senhas e perfis de acesso e, conseqüentemente, elevou os custos com suporte ao usuário. Nos últimos anos, a essa multiplicidade de perfis se somou, com a expansão das operações das empresas, a complexidade de administrar o acesso de clientes, fornecedores e parceiros, além de funcionários espalhados por unidades de negócios em localidades geográficas dispersas.

Com a necessidade de adequação a regulamentações nacionais e internacionais, o gerenciamento de identidade tem-se tornado cada vez mais indispensável

É com base nesse contexto que as grandes corporações estão começando a descobrir a importância de ter um sistema consistente de gerenciamento de identidades. Entre os benefícios operacionais imediatos estão os ganhos de produtividade e eficiência. Isso sem falar na economia de custos com a redução do volume de checagens manuais.

A adoção de uma solução de gerenciamento de identidades permite a gestão integrada de acessos às informações e às diversas aplicações corporativas

Apenas para exemplificar, um estudo recente divulgado pelo instituto de pesquisas Gartner aponta que, em 2007, as soluções corporativas para gerenciamento de identidades proporcionarão uma economia de custos com segurança (operacionais e administrativos) de 21%. No ano passado, segundo o mesmo documento, os custos de *help desk* associados com alterações de senhas caíram cerca de 70% com a implementação de serviços *self-service* – tarefas mais simples como reinicialização de senhas ou atualização de dados pessoais feitas pelo próprio usuário.

Além desses ganhos, a adoção de uma solução de IAM, segundo Fávero, proporciona inúmeros outros benefícios. Um deles é o controle unificado das múltiplas identidades existentes na organização – por identidades entenda-se funcionários, clientes, fornecedores, etc. Isso, além de permitir o gerenciamento integrado de acessos às informações e às diversas aplicações corporativas, torna mais ágil a concessão, a revogação e a criação e manutenção de atributos dos usuários. Outro ponto favorável é que, por se tratar de um processo automatizado, não atrapalha também o dia-a-dia corporativo.

A vantagem em relação a um processo iminentemente manual é bastante significativa. Enquanto nesse método a concessão de acesso de um novo funcionário a aplicações básicas – e-mail, internet etc. – chega a demorar uma semana, com um sistema de IAM a mesma operação não leva mais que alguns minutos. Quando se trata de sistemas específicos, então, o tempo para autorização do usuário pode se arrastar por um mês. Na revogação ocorre a mesma coisa ou, em alguns casos, é até pior. "As empresas demoram, em média, seis meses para desativar a senha e o *login* do funcionário que se desligou da companhia", revela Fávero. Segundo ele, já ficou comprovado pelas auditorias, durante a apuração de eventos pós-fraude, que boa parte dos furtos de dados ou informações ocorre por meio dessa brecha na segurança.

Um outro grande diferencial de uma solução de gerenciamento de identidades, de acordo com o executivo, está na possibilidade de implementar adequadamente funções nos sistemas corporativos. O recurso que facilita a identificação dos usuários associados a cada transação executada nos sistemas é o Role-based Access Control (RBAC), um mecanismo para controle de acesso baseado em papéis. Em síntese, o RBAC define um conjunto de papéis que geralmente representam posições profissionais como diretor, gerente, administrador e atribui a cada um deles um conjunto de permissões. Ele também aperfeiçoa os processos de trabalho (*workflow*) relacionados à administração de usuários e acessos.

De acordo com Fávero, os sistemas de gerenciamento de identidades estão entre os melhores mecanismos para prevenção de fraudes e ameaças internas e externas às informações confidenciais das empresas. Mas ele faz questão de ressaltar que a implantação de um IAM envolve todo um processo e não somente tecnologia. E, como qualquer processo, exige um elevado grau de maturidade tecnológica e de gestão. "Se a empresa tiver um ambiente de TI descontrolado ou um nível de gerência básico, a implantação de um sistema de gerenciamento de identidades pode trazer mais um problema do que atender às suas necessidades", finaliza. ■

RETORNO DO INVESTIMENTO GARANTIDO

De acordo com um estudo recente do Gartner, o gerenciamento de identidades é uma das poucas áreas relacionadas à segurança da informação em que o retorno do investimento (ROI) pode ser claramente medido por meio da redução de pessoal e de ganhos de produtividade. Segundo o instituto de pesquisas, tomando por base uma empresa hipotética com 10 mil funcionários que automatizasse a gestão de 12 aplicativos, a economia seria de cerca de US$ 3,5 milhões em três anos, e o retorno sobre o investimento de 295%. Ainda segundo o Gartner, é possível economizar 14 mil horas em gestão e 6,6 mil horas em atendimento a usuários, anualmente.

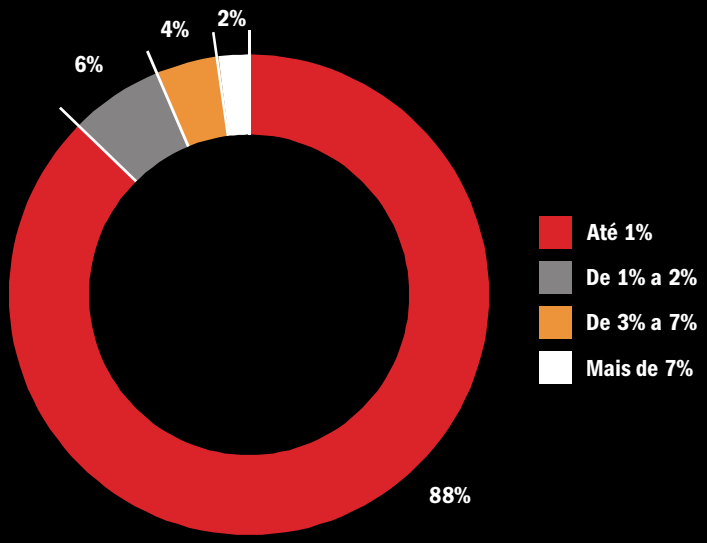
Para Alberto Fávero, sócio da Ernst & Young, o retorno está na redução de custos obtida pela empresa em relação ao processo manual de concessão e revogação de usuários. Como no primeiro caso normalmente o processo resulta em vários dias de improdutividade do novo funcionário, além do dinheiro gasto com o contingente de profissionais que faz a análise para conceder o acesso, a economia seria significativa. O sócio calcula que o custo hoje, por identidade, é de US$ 100. Considerando que o número mínimo de funcionários que uma empresa precisa ter para justificar a implementação de uma solução de gerenciamento de identidades é de 5 mil empregados, o retorno seria em torno de R$ 1,1 milhão. Segundo Fávero, esse ROI varia de seis meses à um ano e meio.

Os benefícios do gerenciamento de identidades

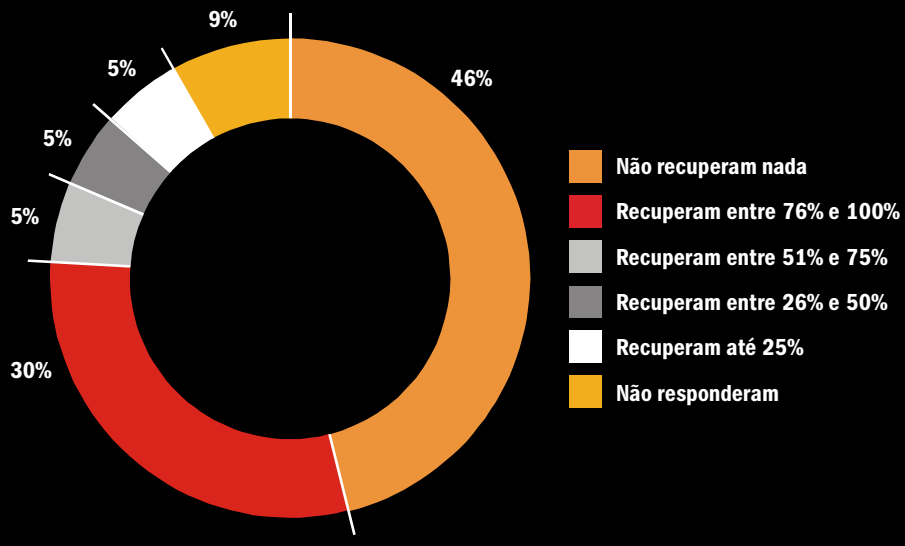
A implantação de uma solução de IAM traz benefícios tangíveis e intangíveis aos ambientes de TI e controles internos. Veja quais são eles.

- Ambiente de TI forte, com a melhoria da capacidade de *compliance* com regulamentações. Proporciona o aumento da confiança da alta administração nos controles internos;
- Aumento da eficiência operacional de TI e redução dos custos de administração;
- Redução do tempo de concessão, alteração e revogação de acessos;
- Aumento de produtividade dos usuários devido ao uso de senha únicas;
- Aumento da segurança, devido ao uso de senhas fortes, nivelando a segurança do ambiente de TI;
- Redução do risco de fraude, devido ao aumento do controle de acesso;
- Redução do risco de TI, devido ao controle mais forte do ambiente;
- Aumento da satisfação dos usuários;
- Melhoria dos controles internos.

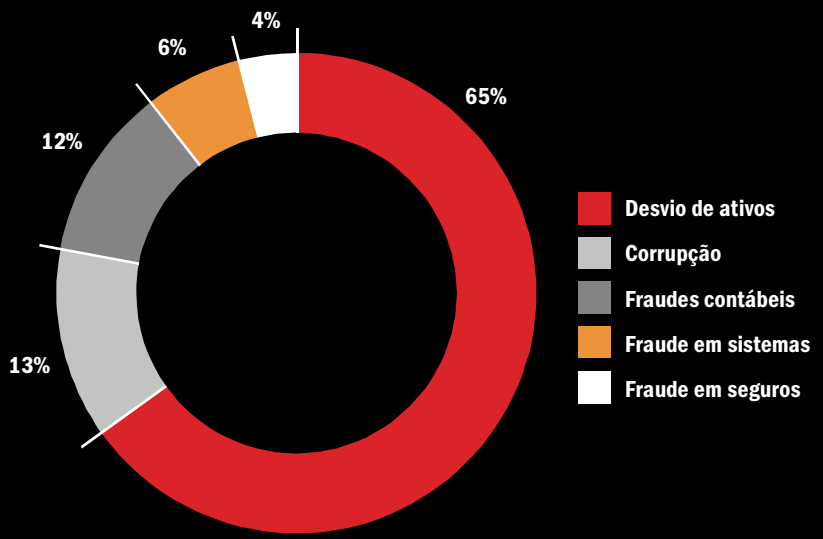
A CONTA DO PREJUÍZO
Quanto as empresas perdem com fraudes em relação ao faturamento



A CONTA DO PREJUÍZO
Quanto as empresas conseguem recuperar



OS TIPOS DE FRAUDES
Os desvios mais comuns dentro das empresas



FONTE: Ernst & Young. Pesquisa sobre Fraudes 2005

Ferramentas de análise de dados aprimoram a detecção de fraudes

As técnicas de análise de dados vêm sendo usadas com freqüência crescente como um mecanismo eficiente de detecção de fraudes. Muitas companhias de serviços financeiros fizeram investimentos pesados em *data warehouses* e em ferramentas de análise de dados para desvendar a ocorrência de atividades irregulares. O problema é que, sem a identificação correta dos indicadores que devem ser monitorados e do local em que eles podem ser encontrados nos dados, o sucesso dessas ferramentas para essa finalidade fica comprometido.

Um bom ponto de partida para qualquer esforço de análise de fraudes é estabelecer uma hipótese de trabalho para os resultados esperados. Isso envolve definir, juntamente com os *stakeholders* (clientes, administração, responsáveis por processos de negócios, equipes de auditoria e TI), quais são as expectativas deles sobre os indicadores de possível atividade irregular em um fluxo de dados. Um indicador pode ser qualquer atributo de uma transação que ultrapasse os "parâmetros razoáveis" para aquele tipo de transação. A equipe de análise documentará esses indicadores na forma de regras de negócios.

A análise deve ser feita com agilidade porque os fraudadores podem notar facilmente o uso de técnicas de detecção e alterar seus esquemas.

Uma lista completa de regras de negócios fornece à administração os "*benchmarks*" para a conclusão do esforço de análise. Esses *benchmarks* também identificam os pontos de dados específicos necessários para executar a análise. Com essa abordagem, é possível fazer um uso eficiente das informações fornecidas pelos *stakeholders* para simplificar a aquisição de dados e os esforços de análise.

Depois de definir as regras de negócios, o próximo passo é o desenvolvimento de testes analíticos para filtrar os dados com base nessas regras. Muitos testes geralmente envolvem a estratificação dos dados em torno de pontos ou intervalos-chave. Esse tipo de lógica indutiva, em que a análise se faz "das partes para o todo", é mais eficaz na identificação de situações em que uma ou mais transações parecem ser inconsistentes com relação à população de dados geral (por exemplo, pagamentos a fornecedores acima dos limites de autorização aprovados).

Um segundo tipo de testes emprega lógica dedutiva, ou "do todo para a parte", com o objetivo de pesquisar a ocorrência de situações específicas de risco. Por exemplo, se a gerência está preocupada com fraudes em contas a pagar envolvendo o uso de fornecedores fictícios, alguns testes específicos podem ser desenvolvidos para destacar fornecedores no "arquivo mestre" que não dispõem de informações importantes, como endereço e número de telefone. É melhor ser flexível na definição de tolerâncias para testes dedutivos porque isso permitirá que a equipe faça um trabalho de ajuste fino durante a análise, para minimizar a descoberta de falsos positivos.

Um tipo de análise ainda mais sofisticado serve para pesquisar padrões de transações suspeitas que ainda estejam em fase de desenvolvimento e que ocorram em múltiplas fontes de dados. Como exemplos, podem ser citadas as transferências entre contas não-relacionadas e as operações recorrentes de pagamento de cheques, instrumentos monetários e transferências eletrônicas. Uma análise de padrões de atividade pode ser eficaz para identificar indicadores de possíveis roubos de identidade e lavagem de dinheiro. Mas essa análise deve ser feita com agilidade porque os fraudadores podem notar facilmente o uso dessas técnicas de detecção e alterar seus esquemas para escapar delas.

A eficácia de qualquer esforço de análise está baseada na qualidade dos dados de origem. A ausência de dados de entrada apropriados e de controles de transações pode resultar em formato de dados inadequados. Isso apenas facilita o trabalho do fraudador, que pode tirar vantagem de controles frágeis de integridade de dados para ocultar um delito em um fluxo de dados.

A revisão quantitativa de qualquer fluxo de dados pode ser um primeiro passo importante na identificação de atividades irregulares e de fraudes. A disponibilidade sem precedentes de dados em formato eletrônico, a elevada capacidade de processamento computacional e as sofisticadas ferramentas de análise fornecem à administração atualmente um poderoso arsenal para combater fraudes. A análise quantitativa é apenas um primeiro passo. Para comprovar uma fraude verdadeira, é necessário confirmar, em primeiro lugar, a intenção de dolo. Só assim pode-se passar à próxima etapa da investigação: a revisão manual de transações específicas. ■

Prepare-se para o inesperado

Umberto Rosti

A dependência cada vez mais acentuada das organizações pelos recursos tecnológicos alterou profundamente os modelos de administração em Tecnologia da Informação (TI). O nível de exposição a riscos é crescente e isso obriga as empresas, comprometidas com a saúde financeira e a continuidade do negócio, a estarem preparadas para enfrentar adversidades. Algumas dessas adversidades são previsíveis e podem ser facilmente mitigadas, mas o desafio hoje para a alta administração é se proteger contra o que não pode ser previsto. É no gerenciamento da incerteza que a empresa se torna mais competitiva.

Atualmente, muitas companhias se vêem obrigadas por seus órgãos reguladores a contar com planos de continuidade de negócios – Business Continuity Management (BCM) - documentados e testados. Até mesmo organizações não regidas por regras procuram transmitir conforto e segurança a diretores, clientes e acionistas no que se refere à continuidade do negócio em caso de incidentes. Assim, elas se julgam preparadas para reduzir o impacto financeiro de uma interrupção na cadeia produtiva, seja por fatores simples, como falhas de *hardware* ou pane elétrica, por exemplo, seja por problemas mais complexos, como incêndios, explosões e inundações.

Não há dúvida de que um BCM bem-estruturado é capaz de minimizar as conseqüências negativas de uma situação inesperada. Há inclusive bons *frameworks* no mercado (como Cobit e ISO 27001, entre outros), com os quais é possível criar um modelo que atenda às necessidades da organização. Antes de elaborar esse plano, no entanto, é importante refletir um pouco mais sobre a questão. Para facilitar esse processo, listamos algumas perguntas que a alta administração e a gerência devem responder antes de optar por um pacote:

- Quais são as minhas prioridades de recuperação de negócio?
- Quais os meus processos críticos de negócio?
- O que pode dar errado?
- Eu conheço meus riscos de contingência?
- Quanto devo investir?
- Como tratar um incidente ou desastre?
- Quais são as nossas reais ameaças?
- Quais os meus objetivos de recuperação?

No caso em que os riscos são previstos, a equipe de TI deve se assegurar de que o plano de contingência considere todos os processos críticos que apresentem impacto significativo para o faturamento. É importante ainda que o plano de contingência seja amplamente divulgado e passe a fazer parte da cultura da organização, o que pode garantir à alta administração, em caso de situações inesperadas, a mitigação dos impactos financeiros e de imagem.

É preciso adequar o BCM de forma a prever interações inesperadas. Isso demanda tempo e envolvimento. Ou seja, é preciso estimular as pessoas a pensarem, a fugirem do óbvio.

É recomendado que o BCM da organização seja elaborado de acordo com as seguintes etapas:

- Análise dos riscos de contingência, ou seja, riscos inerentes à operação do negócio.
- Análise de Impacto ao Negócio, de forma a determinar e priorizar os processos críticos para o negócio e, conseqüentemente suas dependências de TI.
- Estratégia de Recuperação – análise das estratégias que poderão ser utilizadas para a recuperação dos processos críticos de negócio identificados na Análise de Impacto ao Negócio, possibilitando a operação em contingência.
- Gerenciamento de crises e incidentes, processo para análise e gerenciamento de eventos inesperados.
- Plano de Continuidade de Negócio, documento sistemático para os processos críticos de negócio, definição das equipes de recuperação e *contingency office*.
- Plano de Recuperação de Desastres, documento para recuperação do ambiente de TI que suporta os processos críticos de negócio.

Mas e como se proteger de problemas que não podem ser previstos? Antes de mais nada, vale a pena aprofundarmos as discussões sobre a diferença entre uma situação previsível e um evento incerto. Queda ou sobrecarga no servidor, falha elétrica, pane telefônica, indisponibilidade de acesso são riscos a que qualquer empresa está sujeita nos dias de hoje. E para isso os BCM oferecem respostas rápidas. Já um evento incerto, pela própria definição, é algo que foge do controle do administrador de TI e da alta administração.

Uma saída para esse impasse é a quebra de padrões. Não é raro usarmos linhas de pensamento predefinidas para gerenciar riscos. Pensamos em problemas relacionados ao ambiente de TI e avaliamos, na maioria das vezes, de forma previsível. Realmente não é possível determinar em um primeiro momento todas as variáveis – e principalmente as inter-relações – de um negócio. Mas é preciso adequar o BCM de forma a prever interações inesperadas. Isso demanda tempo e envolvimento. Ou seja, é preciso estimular as pessoas a pensarem, a fugirem do óbvio.

Um grande aliado nesse processo é a diversidade. Imagine uma sala repleta de pessoas com formação, conhecimento e históricos profissionais semelhantes. Provavelmente o resultado de um *brainstorm* com um grupo tão homogêneo não será tão surpreendente como seria desejável. A probabilidade de pessoas com perfis semelhantes seguirem uma mesma linha de pensamento é bastante grande. Por outro lado, se reunirmos para um debate um grupo com perfis diferenciados é bem provável que as discussões se acalorem e que os pontos de vista diferentes acabem convergindo para propostas mais interessantes e originais.

Um outro aspecto que não pode deixar de ser analisado pelas equipes responsáveis pelos planos de continuidade de negócios é a velocidade com que as inovações tecnológicas chegam ao mercado. Há 20 anos, a área de tecnologia se resumia a um centro de processamento de dados nas empresas. Mas esse cenário mudou radicalmente. Hoje, TI é uma das áreas mais dinâmicas nas organizações e com papel importante na vida em sociedade, resultado de inovações que permitiram a proliferação de serviços como Internet, telefonia móvel, redes de comunicação sem fio.

Assim, é preciso estar aberto para as novas possibilidades. No cenário atual, um BCM que contemple, não apenas situações previsíveis, mas que tangencie também a incerteza, pode se transformar em um diferencial de mercado importante. Essa é uma tendência irreversível. ■

Umberto Rosti é gerente de Security and Technology Solutions da Ernst & Young

SOX: TI exige esforço de remediação

A área de sistemas e tecnologia da informação foi a que exigiu mais esforço de remediação de controles internos durante o projeto-piloto conduzido em 2005 pelas empresas estrangeiras com ações negociadas nos EUA e que devem se adequar ao artigo 404 da Lei Sarbanes-Oxley. Segundo pesquisa realizada pela Ernst & Young, foram realizadas remediações nessa área em 76% das companhias, em comparação com 48% que tiveram de remediar controles relativos às operações do *core business* e 45% que o fizeram nos processos relacionados com as demonstrações financeiras.

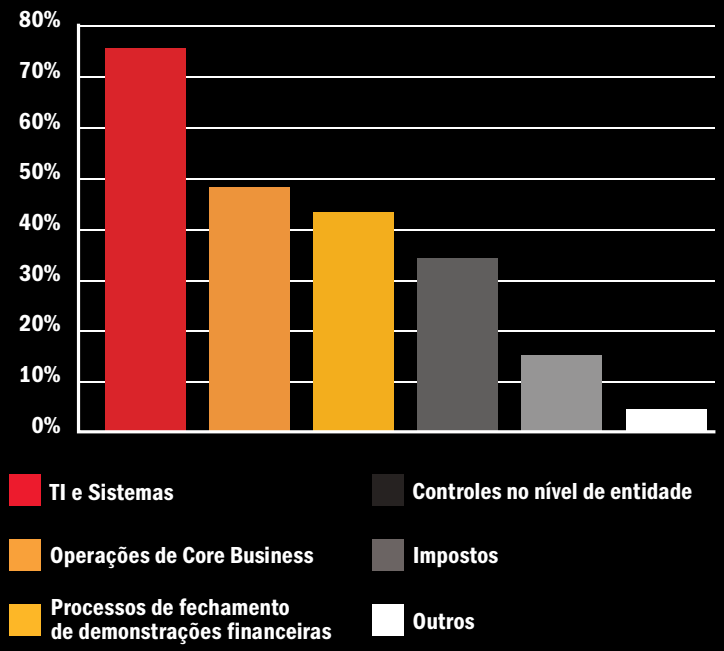
Falhas em controles de TI são um fator que leva à ocorrência de muitos outros problemas de controles internos em uma empresa e, por isso, é tão importante evitá-las. A Ernst & Young analisou os relatórios preenchidos entre janeiro e outubro de 2005 pelas empresas que já se adaptaram ao artigo 404 da nova lei e verificou que quase 7% das deficiências de controles internos identificadas em suas contas significativas estavam relacionadas à área de TI.

Aspectos de segurança e de gerenciamento de acesso de usuários são responsáveis por praticamente metade das falhas de controle de TI detectadas e merecem atenção especial (mais informações sobre gerenciamento de acesso nas páginas 3 a 6).

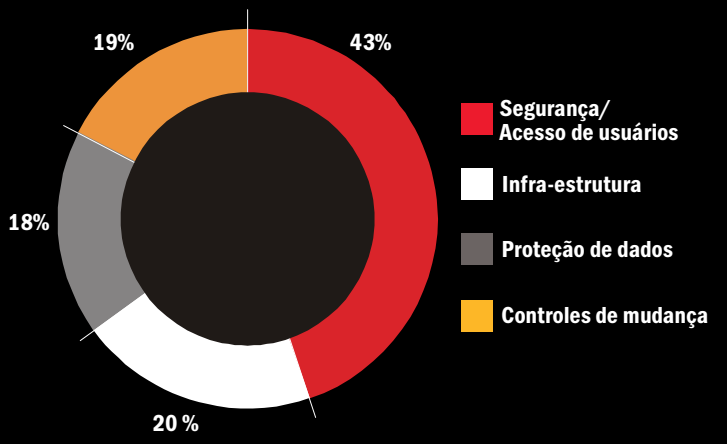
Um dos principais desafios para as equipes que trabalham no projeto SOX diz respeito à crescente tendência de terceirização nas empresas. Praticamente todas as companhias, em todas as faixas de faturamento, têm algum tipo de serviço terceirizado. No entanto, é muito difícil saber como avaliar controles em áreas nas quais fornecedores ou parceiros estão processando as transações.

Para solucionar esse problema, as empresas estão adotando ou planejando diferentes abordagens para lidar com controles relacionados a processos terceirizados e fornecedores. Em 58% das companhias entrevistadas, serão exigidas certificações SAS 70 adicionais para prestadores de serviços. Além disso, 54%

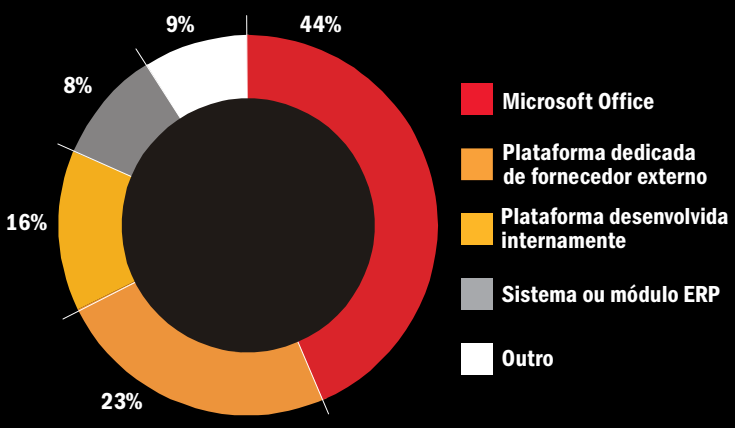
ÁREAS QUE EXIGEM REMEDIAÇÃO SIGNIFICATIVA DE CONTROLES RELACIONADOS AO ARTIGO 404



PERCENTAGEM DOS PROBLEMAS DE CONTROLES INTERNOS DE TI POR TIPO



PRINCIPAL PLATAFORMA TECNOLÓGICA QUE DÁ SUPORTE À IMPLEMENTAÇÃO



FONTE: Ernst & Young. Pesquisa Global sobre Segurança da Informação 2005

pretendem fortalecer os controles da organização e o monitoramento de fornecedores, enquanto 27% conduzirão testes locais dos procedimentos de controle das empresas fornecedoras. Diante dessa nova realidade, as empresas fornecedoras precisam antecipar-se para responder prematuramente às exigências de certificações SAS 70 e assim evitar as pressões de última hora.

Para muitas delas, o artigo 404 teve um papel importante no sentido de melhorar a eficiência e os processos de monitoramento dos controles que integram os modelos de terceirização. Como resultado dos esforços de adequação ao artigo 404, 71% das empresas pretendem realizar aprimoramentos nos sistemas de TI. Nesse processo, estão incluídas atividades como:

- Fazer um levantamento geral do relacionamento com terceiros;
- Identificar e classificar riscos associados;
- Revisar contratos para adicionar ou aprimorar cláusulas relacionadas a "direitos de auditoria"; e
- Trabalhar de modo cooperativo com fornecedores para desenvolver uma abordagem de teste confiável e sólida.

OFFICE É A PRINCIPAL PLATAFORMA DE APOIO À IMPLEMENTAÇÃO DO ARTIGO 404

A implementação das exigências do artigo 404 da Lei Sarbanex-Oxley é um processo de grande complexidade, mas a tecnologia pode desempenhar um importante papel no sentido de facilitar o trabalho. Em virtude do elevado volume de informações e atividades que precisa ser registrado, atualizado, coordenado e acompanhado, geralmente em prazos bem curtos e abrangendo unidades em diferentes cidades e até países, as empresas precisam investir na adoção de uma plataforma que satisfaça integralmente suas necessidades.

Atualmente, segundo pesquisa realizada pela Ernst & Young, 44% das empresas usam ou pretendem usar produtos do pacote Microsoft Office para coletar, monitorar e gerar relatórios relativos aos testes e à documentação do artigo 404 durante o primeiro ano do processo de adequação. Outras 23% pretendem adotar uma plataforma dedicada especificamente ao artigo 404, enquanto 16% utilizarão uma plataforma desenvolvida internamente. Apenas 8% informaram que vão empregar um módulo ERP. Acredita-se que o uso de plataformas dedicadas cresça com a expansão e o amadurecimento desse nicho de mercado fora dos Estados Unidos.

preparado para gerenciar riscos digitais?

Gerenciar o risco decorrente do uso de tecnologia, o risco digital, é fator crítico para o sucesso de uma organização. Sua empresa tem certeza de que as informações críticas para o negócio estão armazenadas de maneira segura? Confia plenamente nos dados gerados sobre receitas, despesas e impostos a recolher?

Faz idéia dos prejuízos que acarretam as chamadas feitas por clientes quando o sistema está fora do ar?

A Ernst & Young pode desenvolver modelos sustentáveis de administração de riscos digitais, que proporcionem eficiência de custos para a sua empresa. Oferecemos serviços de avaliação e implantação de sistemas de governança e gestão de riscos em TI e ajudamos a desenvolver e validar as estratégias de segurança da informação. Prestamos assessoria na revisão da função de auditoria interna de TI e também dos controles dos sistemas considerados essenciais para a organização.

Para decidir com segurança sobre as ameaças e oportunidades que surgem para a sua empresa, fale com a Ernst & Young. Uma decisão que minimiza seus riscos.