O Ato Sarbanes-Oxley e o Impacto sobre a Governança de TI das Corporações

Professor Especialista José Maurício dos Santos Pinheiro (Curso Tecnológico de Redes de Computadores – UniFOA) – jm.pinheiro@projetoderedes.com.br

Resumo

Cada empresa é diferente em sua operação e abordagem filosófica, o que nos leva a reconhecer a importância da análise apropriada das circunstâncias de controle específicas apresentadas por cada ambiente corporativo. Este ambiente encontra-se cada vez mais apoiado na tecnologia, apresentando-se em constante mutação e exigindo formas cada vez mais ágeis e flexíveis no gerenciamento dos recursos. Num cenário de extrema competitividade, as novas estratégias de negócios estão cada vez mais associadas à área de Tecnologia da Informação, entretanto, sem um conhecimento detalhado da estrutura existente e das práticas gerenciais em vigor é impossível tecer recomendações apropriadas para um ambiente de trabalho específico. Neste contexto, o Ato Sarbanes-Oxley afeta as empresas, tornando-se um requisito que exige dos administradores um nível elevado de entendimento das mudanças nos mecanismos e processos empresariais que este Ato acarreta sobre cada corporação. Este artigo tem como objetivo apresentar os efeitos do Ato Sarbanes-Oxley sobre a governança de TI e mostrar como os colaboradores de uma corporação são afetados em algum nível por ele.

Palavras-chave: Governança; Auditoria; Informação; Controle; Responsabilidade.

1- Governança Corporativa e Governança em TI

Governança é, segundo os dicionários, o ato de governar-se. O conceito de Governança Corporativa surgiu nos Estados Unidos e na Inglaterra no final dos anos 1990 e está relacionado à forma como as empresas são dirigidas e controladas. A governança surgiu visando garantir o componente ético da organização, representado por seus diretores e outros funcionários, na criação e proteção dos benefícios para todos os acionistas. Isto significa dizer que as empresas precisam saber quem toma as decisões e quais os processos pelas quais essas decisões são tomadas. Não vale para qualquer atitude adotada na empresa, deliberações sem grande relevância. Vale para decisões importantes, de grande valor para a organização.

Governança em TI (Tecnologia da Informação) é uma derivação de Governança Corporativa, termo que tem hoje grandes aplicações no mundo empresarial. A Governança em TI inclui estruturas de relacionamentos e processos que tem como objetivos dirigir e controlar a organização para que esta alcance seus objetivos mas que, simultaneamente, devem equilibrar os riscos em relação ao retorno da tecnologia de informação e a seus processos. São estruturas e processos que permitem controlar a execução e a qualidade dos serviços, viabilizando o acompanhamento de contratos internos e externos, ou seja, a Governança em TI define as condições para o exercício eficaz da gestão com base em conceitos consolidados de qualidade.

1.1- Desenvolvendo uma estrutura de Governança em TI

A Governança em TI visa designar os direitos de decisão nas questões relevantes com o propósito de atingir os objetivos de negócio da organização. Em muitas organizações este processo se inicia pela demonstração dos riscos envolvidos na falta de controle sobre o ambiente de TI. Assim, foram identificadas cinco áreas de domínios relevantes para as decisões de TI:

Princípios de TI – regras que norteiam o direcionamento e o controle dos processos dentro da estrutura corporativa;
Arquiteturas de TI – capacidade instalada de tecnologia da informação, padrões de tecnologia, modelos de dados etc;
Aplicações de negócios de TI – como decide e quem decide em relação às soluções de negócios;
Estratégia de infra-estrutura de TI – como vai dispor da capacidade instalada;
Investimentos em TI – como priorizar os recursos aplicados em TI.

Internamente, a governança deve desenvolver competências e designar os direitos de decisão nas questões de real valor tendo por fim atingir os objetivos de negócio. Neste aspecto, a governança em TI se apresenta como uma estrutura bem definida de relações e processos que controlam e dirigem uma organização dentro de um cenário de extrema competitividade. O foco é permitir que as perspectivas de negócios, de infra-estrutura, de pessoas e de operações sejam levadas em consideração no momento de definição do que mais interessa à empresa, alinhando a tecnologia da informação à essa estratégia.

1.2- Dificuldades na adoção da Governança em TI

A adoção acelerada de processos de gestão de infra-estrutura nas empresas, dentro do conceito de Governança em TI, tem como principal motivação, internamente, a cobrança sobre os responsáveis pelas operações de tecnologia da informação quanto à maximização do uso dos investimentos já realizados. Por trás desta iniciativa está a preocupação das empresas com melhorias nos seus processos operacionais, redução de custos, aumento da eficiência de seus colaboradores, aperfeiçoamento de relações com fornecedores, parceiros e clientes.

Entretanto, com a contínua evolução da infra-estrutura de TI, incluindo a tarefa de gerenciar soluções heterogêneas de diferentes fornecedores, as organizações têm hoje uma grande dificuldade em manter os custos operacionais sob controle. A elevada complexidade de gerenciamento é uma das principais razões pelas quais as organizações têm sido forçadas a incrementar seus orçamentos e equipes de TI, dedicando entre 70% a 80% dos recursos disponíveis somente para a manutenção dos sistemas e aplicações existentes.

1.3- Motivação para uma Governança em TI

Recentemente, a Governança em TI ganhou um novo impulso dentro do contexto das corporações devido as crescentes preocupações com a governança corporativa, como resultado dos escândalos financeiros ocorridos nos Estados Unidos com empresas de grande expressão, o que gerou prejuízos financeiros aos investidores comparáveis ao *crack* da Bolsa de Valores de Nova York em 1929.

Em dezembro de 2001, a empresa norte-americana Enron entrou em falência, dando início a uma série de outros escândalos corporativos envolvendo outras grandes empresas

(Tyco, Global Crossing, Qwest, Merck, Halliburton, Lucent, Vivendi, Xerox e Parmalat entre outras), o que colocou na ordem do dia questões como ética nos negócios, transparência, governança corporativa, conflitos de interesse entre acionistas e gestores das corporações, conflitos entre acionistas minoritários e os controladores, conflitos entre as corporações e a sociedade. Por fim, a crise colocou em xeque os sistemas de gestão até então vigentes.

O mercado reagiu à esta onda de escândalos adotando várias iniciativas, próprias ou derivadas de leis, que obrigam uma maior transparência da gestão. Podemos citar o Acordo de Basiléia II, em 2001, voltado para os aspectos financeiros e de transparência das empresas e o Ato Sarbanes-Oxley, de 2002, com leis voltadas para definição de critérios de governança. Essas leis criaram regras que se espalharam pelas organizações no mundo todo e chegaram até as áreas de Tecnologia da Informação.

2- O Ato Sarbanes-Oxley

Em 30 de julho de 2002, o congresso americano promulgou o Ato Sarbanes-Oxley, elaborado pelos senadores americanos Michael Oxley e Paul Sarbanes. O escopo da legislação federal "*The U.S. Public Company Accounting Reform and Investor Protection Act of 2002*", mais conhecida como Sarbanes-Oxley Act of 2002, ou simplesmente SOX, contém 11 títulos e foca principalmente a responsabilidade penal da alta administração. Esta lei, que teve como objetivo restabelecer e aumentar a confiança do investidor e a sustentabilidade das corporações, afetou a forma como as empresas de capital aberto passaram a relatar suas operações financeiras.

A SOX acabou apresentando um impacto significativo sobre a área de Tecnologia da Informação das organizações ao nível mundial uma vez que se insere no âmbito da governança corporativa e apresenta artigos diretamente voltados para a área de TI. Com a lei, rígidos parâmetros legais foram impostos às companhias de capital aberto e suas respectivas subsidiárias, cujas ações são negociadas em Bolsas (NYSE e Nasdaq), o que inclui também algumas corporações estrangeiras que negociam ADR’s (American Depositary Receipts – recibos de depósito americano de ações de empresas estrangeiras) não negociáveis no país de origem. No Brasil, essa lei se aplica às empresas com ações negociadas nos mercados de capitais dos Estados Unidos, ou seja, multinacionais de capital americano e empresas brasileiras com ações naquele país. No entanto, as responsabilidades criadas pela lei são de interesse de todas as empresas que queiram se atualizar sobre práticas de gestão de riscos, que estão entrando em vigor nos Estados Unidos e que, em curto prazo, terão ressonância mundial.

2.1- Responsabilidades da Lei

Em suas 1107 seções, o Ato Sarbanes-Oxley imputa responsabilidades nunca vistas perante os diretores de corporações, que vão desde o pagamento de multas ao cumprimento de penas de reclusão e sanções estendidas aos auditores que atestarem balanços com números fraudulentos. As seções 302 e 404 são as mais comentadas, sendo que a seção 302 trata da responsabilidade pessoal dos diretores executivos e diretores financeiros e a seção 404 determina uma avaliação anual dos controles e procedimentos internos para fins de emissão dos relatórios financeiros. É, portanto, a seção que mais impacta a área de TI.

Como não é possível separar processos de negócios e tecnologia no panorama corporativo atual, uma avaliação da infra-estrutura operacional e pessoal de TI das empresas é igualmente requerida. A Seção 404 do Ato Sarbanes-Oxley é o principal foco de atenção das

empresas neste particular, por trazer as determinações sobre os controles de processos internos e sistemas contábeis da empresa. Esta seção determina uma avaliação anual dos controles e processos internos para a realização de relatórios financeiros, com a obrigação de emissão de relatório a ser encaminhado à SEC (Security Exchange Comission - órgão regulador das empresas de capital aberto dos EUA), uma instituição equivalente à Comissão de Valores Mobiliários (CVM) no Brasil, que ateste estes parâmetros. Este relatório deve conter:

Atestado de responsabilidade dos administradores da empresa e manutenção da estrutura dos controles internos e demais procedimentos;

- Avaliação e relatório de cumprimento de metas, ao final de cada ano fiscal, da eficácia dos procedimentos internos adotados para emissão de relatórios financeiros;

Declaração que o auditor independente da companhia atestou a avaliação dos procedimentos elaborada pela administração.

É importante salientar que o Ato Sarbanes-Oxley requer mais do que a documentação citada ou o estabelecimento de controles financeiros. Ao regular a atividade de contabilidade e auditoria das empresas de capital aberto, a SOX reflete diretamente seus dispositivos nos sistemas de tecnologia da informação.

2.2- Segurança da Informação e SOX

Por força do Ato Sarbanes-Oxley, temos a obrigatoriedade da observância de práticas de segurança em sistemas e redes e critérios rígidos para uso de aplicações terceirizadas por companhias que se encontram ao alcance da lei. Invasão de sistemas, ataques, vírus, acesso indevido a bancos de dados, fraudes de senhas e demais ameaças à segurança da informação de uma corporação podem, se não houver prova suficiente de adoção de medidas preventivas coordenadas com os parâmetros da seção 404, implicar em responsabilidade direta dos administradores, surgindo daí possibilidades concretas de sanções civis e penais.

Neste momento, dois pontos devem ser observados cuidadosamente no que se refere ao uso dos sistemas de informação inserido no âmbito do Ato Sarbanes-Oxley:

- **Segurança de sistemas de informação -** A adequação do conteúdo da SOX deve ocorrer entre toda a cadeia de comunicação da empresa, principalmente nos recursos concernentes a informações financeiras. Sistemas de gestão - ERP (*Enterprise Resource Planning*), aplicativos contábeis, sistemas de relacionamento com clientes - CRM (*Customer Relationship Management*), Sistemas de gerenciamento de cadeia de suprimentos (*Supply Chain Management*), em conjunto com as demais aplicações de comunicação, banco de dados e armazenamento de informações precisam estar em sintonia com as regras adotadas na legislação. Consequentemente, a atenção do administrador deve se estender à utilização de todo e qualquer recurso tecnológico da empresa por parte dos funcionários e as políticas de segurança da informação adotadas devem ser adaptadas ao teor do Ato Sarbanes-Oxley. Uma atenção especial também deve ser conferida a terceirização (*outsourcing*) de serviços;

Controle de registros - Um arquivo de registros de procedimentos é fundamental para a tranqüilidade dos administradores. Estes registros devem ser tanto tangíveis (em papel) ou intangíveis (arquivos digitais e demais mídias) e a redundância em sistemas de backup é altamente recomendada. No bojo da lei encontram-se disposições que penalizam severamente a falsificação, destruição e perda de documentos e registros,

bem como prevêem a observação de prazos para seu armazenamento após o fechamento de cada exercício fiscal.

3- SOX é eficaz?

A Lei Sarbanes-Oxley é extensa e detalhada, apresentando diversas regras que devem ser implementadas. No entanto, seu principal objetivo é transformar os princípios de uma boa governança corporativa em leis, evitando assim o surgimento de fraudes nas empresas. Todavia, grande parte da discussão – e das incertezas – em torno da eficácia da SOX está centrada nas seções 302 e 404. Por exemplo, os requisitos da SOX não fazem nenhuma distinção com base no tamanho da receita de uma empresa, ou seja, empresas de tamanho pequeno a médio (departamento de TI) enfrentam os mesmos desafios tanto orçamentários quanto com pessoal, em seus esforços para corresponder a SOX. Isto leva a concluir que empresas de maior porte encontrarão desafios pouco diferentes das de pequeno e médio porte. Entretanto, a proporção da estrutura de controles internos em prática terá influência significativa sobre as atividades de cada uma.

Embora a maioria dos profissionais que conhecem os requisitos para a conformidade com o Ato Sarbanes-Oxley reconheça na lei um objetivo interessante, há controvérsia sobre se os requisitos de relatório existentes seriam suficientes para atender todas as necessidades. Entretanto, todos concordam que o mais importante é que a conformidade SOX seja vista como um processo contínuo, não como um evento único. Se executado adequadamente, o processo dará aos CFO's (*Chief Finance Officer*), CIO's (*Chief Information Officer*) e CEO's (*Chief Executive Officer*) a oportunidade para abordar questões importantes para o fluxo de informações na empresa como sistemas desatualizados, questões de falta de pessoal e de documentação e processos obsoletos. Neste caso, a implementação de novos processos, procedimentos ou aplicativos para a conformidade SOX deve beneficiar a empresa como um todo e a Tecnologia da Informação se torna crítica para o sucesso da conformidade SOX, assim como o suporte dos diversos ambientes empresariais será crítico para o sucesso da TI.

4- Padrões de procedimentos e controles internos

A conformidade Sarbanes-Oxley apresenta um impacto significativo sobre a estrutura de TI da maioria das empresas. No entanto, um grande problema se apresenta: não existem especificações sobre que controles têm de ser estabelecidos dentro da estrutura de TI para a conformidade com a nova legislação.

A seção 404 da SOX determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Além disso, o auditor independente da empresa deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros. A avaliação fornecida aos auditores independentes deve ser bem documentada e abrangente. Um *checklist* resumido com essa finalidade inclui:

Informações acerca do ambiente de controles gerais da empresa;

- Descrição do processo adotado pela administração para identificar, classificar e avaliar riscos que possam impedir que a empresa alcance seus objetivos de emissão de relatórios financeiros;

Descrição completa dos objetivos de controle criados pela administração para direcionar os riscos identificados e as respectivas atividades de controle;

- Descrição dos sistemas de informática e procedimentos de comunicação adotados para fornecer suporte ao tópico anterior;
- Resultados e documentação-suporte da avaliação mais recente feita pela administração sobre a eficácia do desenho e das operações das atividades individuais de controle;
  Relação de todas as deficiências encontradas no desenho e na implementação das atividades de controle, bem como os procedimentos propostos para sua correção;
- Descrição do processo adotado para comunicar deficiências significativas e insuficiências materiais aos auditores independentes e ao Comitê de Auditoria;
  Descrição dos procedimentos de monitoramento executados para assegurar que a estrutura de controles internos está operando conforme planejado e que os resultados dos procedimentos de monitoramento são revisados e executados;
- Descrição do processo de criação da divulgação e das atividades de controle relacionadas.

Para possibilitar agilidade, flexibilidade e inovação para a organização, uma das necessidades que devem ser satisfeitas é o estabelecimento de uma nova arquitetura de sistemas de informação, aliada aos novos recursos de interconexão, Internet, ferramentas de *workflow*, bancos de dados e algoritmos de *datawarehouse*, *dataming* e sistemas de *business intelligence*.

4.1- Adoção de padrões de documentação e controle

Como não há menção específica sobre o que a TI precisa fazer para atender a conformidade SOX, existe a possibilidade de utilizar um dos vários padrões disponíveis para definir e documentar os controles internos da empresa. Esta tarefa tem sido facilitada pela adoção de ferramentas, indicadores e metodologias que auxiliam os profissionais no dimensionamento e uso efetivo dos sistemas.

Segundo a seção 404 da SOX, os aplicativos e correspondente infra-estrutura que sustentam processos-chave, objetivos do controle e afirmações relevantes relacionadas a contas e divulgações significativas nas demonstrações financeiras devem ser incluídos no escopo do processo de avaliação dos controles internos da administração. Considerando que os aplicativos de TI freqüentemente suportam o início, a autorização, o registro, o processamento e a divulgação de transações financeiras, os controles de TI devem representar uma parte integrante do controle interno sobre os relatórios financeiros (ICOFR – *Internal Control Over Financial Reporting*).

Convém ressaltar que aplicativos de TI voltados ao usuário final, tais como planilhas eletrônicas e relatórios, podem apresentar uma empresa com um conjunto exclusivo de necessidades de controles gerais de TI. Isso porque ao disponibilizar para o usuário final tais tipos de ferramentas mais flexíveis, aumenta o risco de erros nas demonstrações financeiras derivados de dados incompletos ou incorretos. Uma vez que o resultado proveniente desses aplicativos freqüentemente toma o caráter de documento oficial, no qual a administração irá confiar no processo de preparação dos seus relatórios financeiros, eles deverão ter os seus controles internos identificados e incluídos no processo de documentação e testes.

Atualmente, somam-se às soluções conhecidas e tradicionais, como BSC (Balanced *ScoreCard)*, ROI (*Return on Investment*), TCO (*Total Cost of Ownership*), EVA (*Economic Value Added*), outros modelos que começam a ser empregados pelo setor corporativo, como o COBIT (*Control Objectives for Information and Related Technology*), ITIL (*IT Infrastructure Library*), e CMM (*Capability Maturity Model*).

A seguir será feita uma breve descrição das principais características das metodologias BSC, COBIT, ITIL E CMM:

4.1.1- BSC

A metodologia BSC foi criada no início da década de 1990 por Robert Kaplan e David Norton, professores da Harvard University (EUA). Ela permite a uma empresa obter uma base mais ampla para a tomada de decisão, considerando quatro perspectivas: a financeira (segundo a visão dos acionistas), a dos clientes, a de processos internos de negócios e a de inovação. Ela permite mostrar o que é mais crítico, possibilitando direcionar os recursos para os processos que de fato adicionarão valor à empresa.

A tecnologia é uma peça importante para colocar o BSC em funcionamento, mas não é suficiente porque a metodologia interage com a cultura da corporação. Por ser complexa e envolver toda a estrutura empresarial, a adoção desse modelo deve partir da alta direção ou mesmo do próprio presidente da empresa.

Trata-se de um modelo flexível, que permite ajustes ao longo do tempo. O emprego dessa metodologia possibilita uma visão ampla, geral e integrada da empresa, através de diversos painéis e o seu projeto de construção se aplica a qualquer empresa, independente do ramo de atividade e porte.

O BSC permite ainda:

Visão dos negócios a partir de perspectivas diferentes;
- Melhor elaboração e monitoramento das estratégias;

Análise das relações de causa e efeito a partir de um macro indicador;
- Alinhamento e compartilhamento da visão e metas desde o nível estratégico até o tático e operacional;

Melhor definição dos planos de ações;
- Agilidade no processo de decisão;

Colaboração por meio de mecanismos para compartilhar a informação analítica.

Tendo a metodologia BSC como uma opção de gestão na Governança em TI pode-se realizar a avaliação e a gestão de uma organização não apenas de forma restrita às medidas tradicionais de resultados e desempenho financeiro, mas, complementá-la com medidas de outras três dimensões: a atenção na satisfação dos clientes, nos processos internos e na capacidade de inovação e aprendizado. Essas dimensões adicionais garantem, quando integradas, resultados futuros e não simplesmente uma visão dos resultados passados, obtidos dentro de uma perspectiva de gestão puramente financeira.

4.1.2- COBIT

Desenvolvida em 1996 nos Estados Unidos, a metodologia COBIT foi criada pelo *Information System Audit and Control Association* (ISACA) a partir de ferramentas de auditoria, funcionando como uma espécie de guia para a gestão da TI nas empresas.

A metodologia apresenta padrões independentes de plataforma com aproximadamente 300 objetivos genéricos agrupados sob um conjunto de componentes: sumário executivo, *framework*, controle de objetivos, mapas de auditoria e um conjunto de processos de trabalho já estabelecidos e empregados pelo mercado entre os quais se inclui o CMM, a ISO 9000

(para qualidade), BS7799/ISO 17799 (normas para segurança da informação) e o ITIL (para gestão do departamento de TI).

O COBIT independe das plataformas de TI adotadas pelas empresas e seu uso é orientado a negócios, no sentido de fornecer informações detalhadas para gerenciar processos. Ao examinar e aplicar as diretrizes e práticas do COBIT é necessário personalizar esses objetivos de acordo com as necessidades específicas do ambiente. A maioria dos auditores para a conformidade SOX adotou o COBIT com uma quantidade reduzida de controles visando melhor atender o ambiente.

A metodologia é voltada para três níveis distintos: para gerentes que necessitam avaliar os riscos e controlar os investimentos de TI; para os usuários que precisam assegurar a qualidade dos serviços prestados para clientes internos e externos; e para auditores que necessitam avaliar o trabalho de gestão da TI e aconselhar o controle interno da organização.

O foco principal é apontar onde devem ser feitas melhorias. Nos casos onde é necessário o exame, desenvolvimento e implementação de novos procedimentos e controles manter uma política de revisão constante com o objetivo de manter a eficácia os mesmos é muito importante.

Cabe aqui apresentar algumas recomendações práticas sobre os controles:

A freqüência da revisão dos itens de controle pode ser semanal, mensal, trimestral etc, conforme as necessidades;

- Os objetivos de controle devem ser tão simples quanto possível;
- As atualizações da revisão devem ser devidamente documentadas e armazenadas;
- O processo de revisão deve perturbar o mínimo possível as funções rotineiras;

Preferencialmente o processo de revisão deve ser automatizado e as atualizações produzidas sistematicamente.

4.1.3- ITIL

Criado no final dos anos 1980 pela *Central Computing and Telecommunications Agency* para o governo britânico, o ITIL reúne um conjunto de recomendações, sendo dividido em dois blocos: suporte de serviços (*service support*), que inclui cinco disciplinas e uma função e entrega de serviços (*service delivery*), com mais cinco disciplinas.

Complementar ao COBIT, o ITIL é uma série internacional de documentos usados como auxílio à implementação de uma estrutura de gerenciamento de serviços de TI. Trata-se de uma biblioteca que descreve as melhores práticas de gestão, especificamente elaborada para a área de Tecnologia da Informação. Os pontos focados apresentam as melhores práticas para a central de atendimento, gerenciamento de incidentes, gerenciamento de problemas e gerenciamento financeiro para serviços de TI. O objetivo da estrutura é definir como o gerenciamento de serviços será aplicado dentro de empresas específicas e, como a estrutura é composta por diretrizes, independe de qualquer aplicativo ou plataforma e, portanto, pode ser aplicada em qualquer empresa.

4.1.4- CMM

O CMM destina-se a auxiliar as empresas a melhorar a produtividade dos processos de desenvolvimento de software e a organizar o funcionamento de seus ambientes de tecnologia da informação. É uma metodologia que mostra as metas a serem alcançadas, atuando como um modelo de orientação e qualificação dos estágios de maturidade.

O CMM define cinco níveis de maturidade para os ambientes de desenvolvimento de software (inicial, repetível, definido, gerenciado e otimizado), sendo que cada um deles é composto por um conjunto de áreas-chave de processo (KPA - Key Process Areas) que descrevem as questões e grandes temas que devem ser abordados e resolvidos para se atingir um determinado nível.

5- Por que se adequar a SOX?

O primeiro reflexo para uma empresa que não se adequar ao Ato Sarbanes-Oxley é a possibilidade de se expor a processos legais e pesadas multas para a gerência executiva, além de publicidade negativa. As corporações que se negam a instituir os controles exigidos podem se colocar em situações similares àquelas que levaram à promulgação da SOX, o que poderá vir a acarretar:

- Maior exposição à fraude;
- Penalidades impostas pela SEC;
- Publicidade desfavorável;
- Impacto negativo sobre o valor do acionista;
- Queixas ou outras ações judiciais impetradas por acionistas.

Por outro lado, uma estrutura de TI que conta com pouco pessoal, onde não se executam políticas e procedimentos de avaliação ou atualização tecnológica (aplicativos / hardware) periódicos e a documentação é colocada em segundo plano, uma adequação a SOX pode ser altamente positiva, uma vez que surgirão oportunidades para resolver as deficiências quanto à própria necessidade de conformidade a Lei, bem como aplicar as boas práticas da Governança Corporativa.

Segundo Souza & Fraga (2003):

> As regras contidas na SOX visam, em última análise: (i) transparência na divulgação de informações – *full and fair disclosure*; (ii) prestação de contas – assegurar a adequada e eficiente laboração e divulgação das demonstrações financeiras e demais informações da companhia e (iii) tratamento justo, e equânime às partes interessadas. Estas indicações representam os princípios fundamentais de boas práticas de Governança Corporativa.

6- Resistência à mudança

Apesar do entendimento da gerência executiva sobre a necessidade de se adequar a SOX, podemos encontrar dentro da estrutura da organização certa resistência à mudança por parte de outros membros e até mesmo a equipe de TI pode não abraçar abertamente a mudança.

De acordo com Lahti & Peterson (2005):

> Você pode ter as melhores políticas, aplicativos, ferramentas e controles, no entanto, nunca conseguirá eliminar completamente o “Fator Humano”. Logo, se não conseguir incorporar a área de gerenciamento de mudança, talvez não consiga se adequar ao Ato Sarbanes-Oxley independente de seus outros esforços.

Algumas das principais razões desta resistência à mudança incluem:

Medo do desconhecido;

A crença de que as coisas estão boas e não é preciso mudar;
- O desconhecimento dos motivos que levam à mudança;
A idéia de que a mudança é mais outra prática que pode ser ignorada;
- A clássica pergunta: “O que eu ganho com isso?”.

Devido a esses fatos, para que o processo de mudança seja bem-sucedido, a comunicação entre os membros da organização é fundamental. Neste ponto é preciso conhecer e gerenciar os processos pessoais para que a comunicação ocorra com facilidade e de várias formas, sejam através de memorandos, e-mails, reuniões presenciais, conversas individuais, etc. O objetivo é produzir um efeito consistente demonstrando a necessidade da conformidade SOX e, principalmente, as conseqüências da não-conformidade.

7- Conclusões

A Lei Sarbanes-Oxley de 2002 reescreveu as regras para a governança corporativa, relativas à divulgação e à emissão de relatórios financeiros. Sob suas páginas encontramos uma premissa muito simples: a boa governança corporativa e as práticas éticas do negócio não são mais requintes – são leis. Na mesma medida, a Governança em TI traz para as empresas uma nova cultura de gestão baseada em medições que consideram aspectos não só financeiros, mas outros que controlam fatores que apontam para o futuro, através de outros indicadores, como a criação e manutenção de capital intelectual, que permitirão garantir a perenidade da corporação.

O cumprimento da Lei Sarbanes-Oxley pode ser uma tarefa difícil, mas com pesquisa e planejamento adequados ela pode ser usada para corrigir deficiências adicionais na estrutura de TI das empresas adequando-as à nova realidade que se apresenta. A partir da promulgação do Ato Sarbanes-Oxley, o que era recomendável passa a ser obrigação legal: uma boa governança corporativa e a ética nos negócios das corporações com presença no mercado financeiro de capital aberto.

1. Referências Bibliográficas

DELOITTE. **Lei Sarbanes-Oxley: Guia para melhorar a governança corporativa através de eficazes controles internos.** Disponível em http://deloitte.com.br>. Acesso em 08 out. 2005.

FAGUNDES, Eduardo Mayer. **A lei Sarbanes-Oxley e seu impacto em TI.** Artigo disponível em: <http://www.efagundes.com/artigos/Sox_e_o_impacto_em_TI.htm>. Acesso em: 08 set. 2006.

LAHTI, Christian B., PETERSON, Roderick. **Sarbanes-Oxley – Conformidade TI usando COBIT e ferramentas open source**; tradução de Aldir José Coelho. AltaBooks, Rio de Janeiro, 2005.

NEXT GENERATION CENTER. **Módulo Governança de TI.** Disponível em: <http://www.nextg.com.br/br/modulo.aspx>. Acesso em: 18 set. 2005.

PEIXOTO, Rodney de Castro. **Implicações da Lei Sarbanes-Oxley na Tecnologia da Informação**. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/rodney_peixoto/sarbanes_oxley.html>. Acesso em 08 set. 2006.

SARBANES, P., OXLEY, M. **Sarbanes-Oxley Act of 2002.** Disponível em <http://www.findlaw.com>. Acesso em 08 jul. 2006.

SOUZA, Almir Ferreira, FRAGA, Rodrigo Mariti. **Governança Corporativa: Efeitos decorrentes da vigência da Sarbanes-Oxley Act nas empresas brasileiras.** Artigo disponível em <http://www. > . Acesso em 07 set. 2006.

WEILL, Peter, ROSS, Jeanne W., **Governança de TI, Tecnologia da Informação;** tradução de Roger Maioli dos Santos. M Books do Brasil, São Paulo, 2006.

Informações bibliográficas:
Conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT), este texto científico publicado em periódico eletrônico deve ser citado da seguinte forma:
PINHEIRO, J. M. S.. O Ato Sarbanes-Oxley e o Impacto sobre a Governança de TI das Corporações. Cadernos UniFOA , Volta Redonda, ano 1, n. 2, nov. 2006. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao/02/33.pdf>