Auditoria dos Sistemas de Informação Aliada à Gestão Empresarial

Maicom Rafael Victor Simch
Tiago Squinzani Tonetto
E-mail:tiago-tonetto@hotmail.com, maravisi@hotmail.com

Resumo

Neste trabalho é proposta a auditoria dos sistemas de informações das empresas, bem como o acompanhamento permanente do ambiente informatizado. Desta forma, salienta-se a necessidade de oferecer informações seguras aos tomadores de decisão e, através da revisão de literatura, evidencia-se a relevância destas informações no ambiente empresarial. A intensa busca por dados, registros, informações e sistemas no meio empresarial sustenta-se em regras básicas de segurança que, quando observadas tornam-se ferramentas preparadas para o enfrentamento de uma realidade onde mais do que nunca "informação é poder".

Palavras-chaves: sistemas de informações, auditoria, gestão empresarial.

Introdução

Com a globalização a disseminação das informações tornou-se bastante abrangente, facilitando a vida dos usuários. As informações ficaram mais fáceis de serem interceptadas, gerando risco e receio por parte dos usuários. A cada tempo que passa os empresários ficam mais receosos e acabam retrocedendo no tempo em prol da própria segurança, por vezes, deixam de tomar decisões importantes ao futuro da empresa por não dispor da informação em tempo hábil ou então por não confiar na informação gerada pelo sistema de informações que é utilizado.

Estas informações após processadas geram os relatórios contábeis e financeiros que são apresentados aos interessados pelo seu desempenho econômico-financeiro. Estes usuários podem ser acionistas, investidores, ou analistas de mercado, entre outros. Tais usuários avaliam o valor das ações e outros títulos emitidos pela empresa, e a cada dia a dinâmica do mercado financeiro tem exigido uma maior velocidade das informações, colaborando com isso a internet vem

sendo considerada um canal de divulgação que potencializa as oportunidades melhorando a qualidade das informações.

Toda empresa que prime por controles internos e processos definidos deve utilizar-se de sistemas de informações. Entretanto, uma empresa que dispõe de um sistema integrado informatizado e, não respeita alguns aspectos de suma importância estará exposta a riscos. Os riscos podem ser identificados internamente e externamente. Sua avaliação dependera da análise da probabilidade de ocorrência e de seus impactos identificados, de maneira quantitativa e qualitativa. Não esquecendo, entretanto, de avaliar sempre os efeitos positivos e negativos da aplicação da auditoria destes sistemas. O controle de risco deverá estabelecer um processo formal de identificação, avaliação e desenvolvimento das respostas aos riscos do projeto de auditoria, para que a sua situação seja constantemente monitorada e seus planos de contingência estejam sempre atualizados e prontos para serem implementados.

Diante disso, este artigo tem por objetivo analisar a prática de procedimentos de auditoria nos sistemas de informações visando, sobretudo, evidenciar a necessidade de informações úteis e confiáveis para o processo de gestão. Complementando a proposta, discorre-se sobre os componentes que necessitam de maior atenção em um uma auditoria nos sistemas de informações voltados a gestão.

O cumprimento dos objetivos dar-se-á por meio da revisão da literatura, determinando-se a relação entre gestão, segurança e auditoria de TI (Tecnologia de Informações), no que diz respeito a dados e informações. Discute-se a auditoria das informações como atitude aliada aos processos de gestão na empresa, no sentido de oferecer às organizações um maior controle sobre os dados relevantes e uma conformação maior com os mecanismos de tomada de decisão e confidencialidade dentro das instituições.

Tecnologia da Informação como Suporte à Gestão da Informação

A tecnologia da informação alterou o mundo dos negócios de forma irreversível. Desde que foi introduzida sistematicamente, em meados da década de 50, houve uma mudança radical no modo de operar das organizações (Mcgee, Prusak, 1994). Na atualidade, tanto sob a perspectiva acadêmica quanto do mundo dos negócios, é uma questão de grande relevância. Antonialli (1996) concorda que

as fortes tendências e fatores tecnológicos são os responsáveis por contínuas adaptações da postura estratégica empresarial.

Corroborando com isso, Wang (1998) afirma que a informação tecnológica pode ser a maior ferramenta dos tempos modernos, mas é o julgamento de negócios dos humanos que a faz poderosa.

De acordo com Rezende e Abreu (2000), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. Ela ajuda na identificação das ameaças e das oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz.

Assim, a tecnologia da informação abrange uma gama de produtos de hardware e software capazes de coletar, armazenar, processar e acessar números e imagens, que são usados para controlar equipamentos e processos de trabalho e conectar pessoas, funções e escritórios dentro das empresas e entre elas (Walton, 1993).

A importância da Informação nos Processos de Gestão

A informação, na visão de Rezende e Abreu (2000), é o dado com uma interpretação lógica ou natural agregada pelo usuário. A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegido (NBR ISO/IEC 17799, 2003). Como salienta Dias (2000), a informação é o principal patrimônio da empresa e está sob constante risco.

Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, uma determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja ainda será menor que o custo de não dispor dela adequadamente. Boran (1996) e Wadlow (2000) classificam a informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa:

- Pública. Informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital.

- Interna. O acesso livre a este tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital.
- Confidencial. Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.
- Secreta. Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Ativos de Informação

Conforme Souza (2006), os ativos de informação são aqueles mecanismos que usamos para armazenar, transmitir e processar informações (Ex.: pedaço de papel, computadores, redes, discos rígidos, banco de dados, fitas etc..).

Constituem basicamente os chamados Ativos de Informação:

- A informação (conceitualmente): mensagens, textos, dados de um sistema, informações de funcionários, programas de rádio e TV, etc.
- As tecnologias que suportam a informação: papel, correio eletrônico, editor de texto, sistemas de informação, rádio, TV, telefone, arquivos de aço, computadores, etc.
- As pessoas e processos que utilizam as informações: vendedores, gerentes, fornecedores, clientes, processo de compra, processo de venda, etc.
- Os ambientes: CPDs, salas de arquivos, depósitos de mídias e equipamentos, etc.

Vulnerabilidade dos ativos da informação

Souza (2006) ressalta ainda que, na área de tecnologias podemos identificar as seguintes deficiências:

- computadores sem proteção contra vírus;
- arquivos de aço sem controle de acesso;

- equipamentos em locais públicos (impressoras, fax)
- cabos de redes expostos;
- redes locais com senha padrão ou pública;
- sistemas sem controle de acesso lógico;
- falta de controle a áreas críticas;
- problemas de manutenção em equipamentos;
- problemas com energia elétrica.

Com relação às pessoas e processos os ativos da informação podem estar comprometidos no que diz respeito a:

- ausência de controle interno estruturado e bem aplicado;
- ausência de política institucional de segurança na organização;
- inexistência de especialistas em segurança na organização;
- inexistência de regulamentação para acesso às informações da organização;
- procedimentos ineficientes para análise e conferencia das informações;
- colaboradores não-treinados em segurança;
- ausência de procedimentos disciplinares para o tratamento das violações da política de segurança;
- ausência de planos de contingência.

O ambiente no qual a empresa esta inserida também propicia algumas formas de “ataque” ao ativo da informação da empresa, conforme segue:

- ausência de mecanismos contra incêndio;
- inexistência de mecanismos de prevenção à enchente;
- inexistência de proteção contra poluentes diversos que possam prejudicar mídias e equipamentos.

Critérios para Segurança da Informação

É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam proporcionar confidencialidade, integridade e disponibilidade. Segundo Albuquerque e Ribeiro (2002) há três princípios básicos para garantir a segurança da informação:

- Confidencialidade. A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.
- Disponibilidade. A informação deve estar disponível no momento em que a mesma for necessária.
- Integridade. A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

O item integridade não pode ser confundido com confiabilidade do conteúdo (significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

Rezende, Abreu (2000) e Sêmola (2003) defendem que para que uma informação seja considerada segura, o sistema que o administra ainda deve respeitar os seguintes critérios:

- Autenticidade. Garante que a informação ou o usuário da mesma é autêntico.
- Não repúdio. Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; não é possível negar o envio ou recepção de uma informação ou dado.
- Legalidade. Garante a legalidade (jurídica) da informação; a aderência de um sistema à legislação; e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação nacional ou internacional vigente.
- Privacidade. Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve poder ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade à informação). É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.
- Auditoria. Rastreabilidade dos diversos passos de um negócio ou processo, identificando os participantes, os locais e horários de cada etapa. A

auditoria aumenta a credibilidade da empresa e é responsável pela adequação da empresa às políticas legais e internas.

Implementado e Auditando Políticas de Segurança

Conforme Dias (2000), os aspectos de segurança apresentados a seguir podem ser utilizados como uma lista de controle, tanto pela gerência de segurança de sistemas, como pela equipe de auditoria. Para a gerência de segurança, essa lista pode servir como um conjunto de tarefas a serem realizadas na implementação da política de segurança.

Lista de política de segurança de informações:

- Elaborar, divulgar e manter atualizado documento que descreva a política de segurança de informações;
- A alta gerência deve estar comprometida com a política de segurança de informações, a qual deve ser implantada de acordo com o documento formal por ela aprovado;
- Definir uma estrutura organizacional responsável pela segurança, a qual deve aprovar e revisar as políticas de segurança, designar funções de segurança e coordenar a implantação da política;
- Estabelecer procedimentos de segurança de pessoal, com intuito de reduzir ou evitar erros humanos, mau uso dos recursos computacionais, fraude ou roubo, por meio de um processo rigoroso de recrutamento de pessoal e de controle sobre acessos a dados confidenciais;
- Todos os funcionários devem ter conhecimento dos riscos de segurança de informações e de suas responsabilidades com relação a esse assunto. É aconselhável que haja um treinamento de segurança para difusão de boas práticas e padrões de segurança, promovendo uma cultura de segurança na organização;
- Implantar controle de acesso lógico aos sistemas de forma a prevenir acessos não autorizados. Esse controle pode ser feito via processo seguro de logon, senhas fortemente seguras, registro formal de usuários, monitoramento por trilhas de auditoria;

- Definir procedimentos de backup e de restauração dos sistemas computacionais para garantir a integridade e a disponibilidade de dados e software. A freqüência de backup deve ser apropriada e pelo menos uma cópia do backup deve ser guardada em local seguro. Os procedimentos de restauração devem ser periodicamente testados para garantir sua efetividade quando forem necessários; e
- Auditar regularmente todos os aspectos de segurança a fim de determinar se as políticas estão sendo efetivamente cumpridas ou se são necessárias modificações.

Antigamente, a atenção sobre a segurança da informação estava focada na tecnologia. Hoje, o desafio é construir uma relação de confiabilidade com clientes e parceiros. Conforme Rezende e Abreu (2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório.

Auditoria da Tecnologia da Informação

Auditoria da TI é uma auditoria operacional[1], analisa a gestão de recursos, com o foco nos aspectos de eficiência, eficácia, economia e efetividade. A abrangência desse tipo de auditoria pode ser o ambiente de informática como um todo ou a organização do departamento de informática (PUCRS, 2007):

- Ambiente de informática:
    - Segurança dos outros controles;
    - Segurança física;
    - Segurança lógica;
    - Planejamento de contingências;
    - Operação do centro de processamento de dados.
- Organização do departamento de informática:
    - Aspectos administrativos da organização;

[1] Para Araújo (2001, p.34) a auditoria operacional é "o exame objetivo e sistemático da gestão operativa de uma organização, programa, atividade ou função e está voltada para a identificação das oportunidades para se alcançar maior economia, eficiência e eficácia"

- Políticas, padrões, procedimentos, responsabilidades organizacionais, gerência pessoal e planejamento de capacidade;
- Banco de dados;
- Redes de comunicação e computadores;
- Controle sobre aplicativos:
  - Desenvolvimento;
  - Entradas, processamento e saídas.

A auditoria da segurança de informações determina a postura da organização com relação à segurança. Avalia a política de segurança e controles relacionados com aspectos de segurança institucional mais globais, faz parte da auditoria da TI. Seu escopo envolve:

- Avaliação da política de segurança;
- Controles de acesso lógico;
- Controles de acesso físicos;
- Controles ambientais;
- Planos de contingência e continuidade de serviços.

Os aplicativos (softwares) necessitam de atenção especial, ao que da-se o nome de auditoria de aplicativos. Segurança e controle de aplicativos específicos, incluindo aspectos intrínsecos à área a que o aplicativo atende:

- Controles sobre o desenvolvimento de sistemas aplicativos;
- Controles de entradas, processamento e saída de dados;
- Controle sobre conteúdo e funcionamento do aplicativo, com relação à área por ele atendida.

Conclusões

A informação contábil é uma ferramenta extremamente importante para o sucesso empresarial, mas não deve apenas se restringir ao atendimento das determinações legais, pois, mais que a legalidade, a informação contábil deve contribuir decisivamente para a tomada de decisão pelos gestores da empresa.

Neste sentido, pode-se observar que a auditoria de TI deve estar inserida na rotina de processos de qualquer empresa que busca tomar decisões baseando-se

em relatórios gerados a partir de um sistema informatizado. No entanto, nota-se que o elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas), que por sua vez, é a responsável por garantir a fidelidade da informação. Assim, a melhor forma de garantir a segurança da informação estratégica é atuar junto às pessoas que de alguma forma manipulam a informação com políticas de treinamento, prevenção e auditoria dos processos relacionados.

Enfim, as práticas da Segurança da Informação garantem que a informação certa, esteja disponível na hora certa, para que os responsáveis possam tomar a decisão estrategicamente adequada em tempo hábil.

Referências Bibliográficas

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. 2002. **Segurança no Desenvolvimento de Software** – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro.

ANTONIALLI, L.M. (1996). **Tecnologia da informação e estratégia de uma cooperativa de cafeicultores**: o caso Cooxupé. In: MARCOVITCH, J. Tecnologia de Informação e Estratégia Empresarial. São Paulo: FEA/USP. cap.3, p.13-24.

ARAÚJO, I. da P. S. (2001). **Introdução à auditoria operacional**. Rio de Janeiro: FGV.

BORAN, Sean. **IT Security Cookbook**. 1996. Disponível em http://www.boran.com/security/. Acesso em: 15/09/2007.

DIAS, Cláudia. 2000. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books.

MCGEE, J. V.; PRUSAK, L. (1994). **Gerenciamento estratégico da informação**. Rio de Janeiro: Campus.

NBR ISO/IEC 17799. 2003. **Tecnologia da Informação**. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro.

PUCRS. 2007. **Auditoria da Tecnologia da Informação**. Disponível em http://pucrs.campus2.br/~annes/sas_audit.doc. Acesso em 15/09/2007.

REZENDE, Denis Alcides e ABREU, Aline França. 2000. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas.

SÊMOLA, Marcos. 2003. **Gestão da Segurança da Informação** – Uma visão Executiva. Editora Campus. Rio de Janeiro.

SOUZA, Celso. 2006. **Auditoria da Tecnologia de Informação**. Disponível em: http://www.trueaccess.com.br/pagina-artigos.html. Acesso em 20/09/2007.

WADLOW, Thomas. 2000. **Segurança de Redes**. Editora Campus. Rio de Janeiro.

WALTON, R. (1993). **Tecnologia da informação: o uso da TI pelas empresas que obtêm vantagem competitiva**. São Paulo: Atlas.

WANG, C. B..(1998). **Techno Vision II - Um Guia para Profissionais e Executivos Dominarem a Tecnologia e Internet.** São Paulo: Makron Books.