Auditoria em Segurança da Informação

Vanessa Mota Alves[1], Millys Fabrielle Araújo Carvalhaes[2]

[1,2] Bacharelados em Computação - Centro Universitário de Anápolis (UniEVANGÉLICA) – Anápolis - GO

[1]millys.carvalhaes@docente.unievangelica.edu.br

Resumo. *A nova era tecnológica tem trago importantes ganhos para a humanidade, proporcionando crescimento e produtividade; mas, em contrapartida, tem colocado as organizações diante de riscos inerentes ao acesso ou ao ataque às informações armazenadas nos sistemas computacionais corporativos. A informação, ativo cada vez mais valorizado, impacta diretamente na continuidade dos negócios e na sua credibilidade. Por conta disso, as empresas têm buscado soluções para mitigar esses riscos, estabelecendo um conjunto de boas práticas por meio de políticas de segurança gerenciadas em diferentes instâncias com funções e responsabilidades bem definidas. Tudo isso para assegurar o nível de segurança adequado ao negócio. A segurança é essencial para proteger os dados de uma empresa, por conta disso devemos praticar os pilares da segurança, segundo as normas da série 27000.*

1. Introdução

O alicerce de uma organização é gerado pelas pessoas presentes nela a partir da informação disponível, portanto a informação é o combustível dessa nova economia. É necessária uma ressalva, não pode ser qualquer informação, ela deve ter qualidades, ser confiável, estar disponível na hora certa. E é nesse contexto que entra a auditoria, que vai verificar se essa informação é criada com as qualidades necessárias para o negócio, identificando os pontos de falhas e sugerindo as correções necessárias.

Para que uma auditoria seja bem conduzida é necessário que haja por parte da organização um investimento em melhores práticas de gestão do negócio. Como estamos falando de segurança da informação, deve haver uma atenção especial para a gestão da Tecnologia da Informação (T.I.), principalmente no que tange a Segurança da Informação, pois em quase todas as empresas a informação é transmitida principalmente por meios computacionais.

2. A importância da informação

A informação é tida hoje como um dos maiores e mais importantes patrimônios de uma empresa no século em que vivemos. E não é de se estranhar, já que hoje podemos ver empresas que tem nela praticamente o núcleo do seu negócio (core business), quase não tendo ativos tangíveis e ainda assim valendo bilhões de dólares. Um exemplo claro disso é o Google, empresa de software para internet dos Estados Unidos da América e uma das maiores empresas do mundo.

Todas as decisões de uma organização se baseiam em informações, portanto ela tem que ser precisa, tendo uma importância e um valor. Para Rezende e Abreu (2000),

> a informação tem valor altamente significativo e pode representar grande poder para quem a possui, indivíduos ou instituição. Ela está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos e tecnologia.

Rezende e Abreu (2000) ainda completam que "a informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade.".

3. A Auditoria

Damos o nome de auditoria à atividade responsável na organização de avaliar se os processos e procedimentos estão sendo cumpridos, se os sistemas de informação estão sendo bem alimentados, se os princípios contábeis estão sendo seguidos, entre outros. Dessa forma a empresa pode aferir se está tomando decisões com base em informações verídicas, se as demonstrações contábeis refletem a realidade da empresa, se as metas, planos e objetivos da organização estão sendo seguidos, avaliando também se os recursos disponíveis estão sendo usados com eficiência e eficácia.

Basicamente há dois tipos de auditoria: a interna, que é executada pela própria organização e a externa, normalmente conduzida por empresas especializadas em auditoria. Apesar desta distinção, o trabalho de ambas é praticamente o mesmo.

Ter uma auditoria, portanto, seja ela interna ou externa é muito importante para a organização que quer ter mais confiança em suas informações e controles, constatando assim a integridade dessa empresa, tendo como objetivo final a emissão de um parecer sobre as adequações necessárias e ajudando a assegurar o princípio contábil da continuidade, pois dessa forma as decisões serão tomadas com base em informações corretas e com veracidade averiguada pela auditoria.

Para avaliar, revisar e adequar o uso das tecnologias de informação dentro das organizações existe dentro da auditoria a chamada Auditoria de Sistemas de Informação, que pretende sobre tudo aprimorar os controles internos que passam pelos sistemas da empresa. Conforme define Karapetrovic e Willborn (2000) “a finalidade principal da Auditoria de Sistemas é atender às necessidades dos usuários, através de uma análise dos sistemas contábeis de forma prática, clara e consistente.”.

4. A Segurança da Informação e sua importância

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto aos pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

Imagine por exemplo se o e-mail, arquivos e sistema de uma empresa estejam à disposição de pessoas com segundas intenções? Nem sempre os gestores do negócio se preocupam com isso e muitas vezes acreditam que essa situação não deve ocorrer em suas empresas. Conforme destaca Laureano (2005) há o seguinte cenário atual:

> Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças (Laureano 2005, p. 11).

Como podemos ver, da mesma forma que nos preocupamos com a segurança de qualquer outro bem tangível de uma organização como carros e imóveis, temos que nos preocupar com o bem intangível que é a informação e que conforme vimos pode ser inclusive de maior valor que os bens tangíveis dependendo do negócio da empresa. Para ajudar nesse problema, há uma área da tecnologia da informação especializada no estudo desse assunto, ela é chamada de Segurança da Informação.

5. As Normas ISO/IEC 27001 e 27002

As normas ISO/IEC 27001 e 27002 falam sobre os atributos básicos da informação, também chamado de princípios básicos da segurança da informação por alguns autores e podemos entendê-los da seguinte maneira:

- Confidencialidade: Para garantir esse princípio, o acesso às informações deve ser feito somente pelas pessoas explicitamente autorizadas. Exemplo de quebra da confidencialidade: acesso a um sistema, como por exemplo um e-mail, usando a senha de outra pessoa sem que o titular saiba.
- Integridade: Para garantir esse princípio é necessário ter a segurança que a informação acessada é confiável, estando completa e sem alterações. Exemplo de quebra da integridade: ao enviar um arquivo por e-mail o mesmo é alterado no caminho antes de chegar ao destinatário.
- Disponibilidade: Para garantir esse princípio a informação deve estar disponível (acessível) para as pessoas autorizadas sempre que necessário. Exemplo de quebra da disponibilidade: o sistema fica "fora do ar", não possibilitando o acesso ao mesmo, consequentemente às informações estão indisponíveis.

Além desses princípios apresentados, ainda temos outros não menos importantes como a autenticidade, privacidade, não-repúdio que juntos completam os principais conceitos relacionados a segurança da informação, mas que nesse momento não são alvo desse artigo e requerem um estudo mais detalhado.

É necessário que dentro da organização haja no setor de Tecnologia da Informação (TI) uma equipe preparada para criar as políticas relacionadas à tecnologia e dentre elas a política de segurança da informação, uma das políticas mais importantes da empresa e que dará norte ao uso da informação dentro da organização. Para auxiliar nisso, a ABNT (Associação Brasileira de Normas Técnicas), em sintonia com a ISO (*International Standardization Organization*) desenvolveram um padrão internacional de normas e procedimentos para garantir a segurança da informação nas organizações, são as normas ISO/IEC 27001 e 27002.

Cuidar da segurança da informação em uma empresa não é algo simples. Somente ler as normas ISO/IEC 27001 e 27002 e fazer uma política não significa que estará tudo pronto e as informações estarão seguras. Assim como outras áreas da organização, a empresa tem que investir na criação e manutenção da área de TI com a infraestrutura necessária, profissionais especializados e incluindo um projeto, planejamento e acompanhamento, mapeando todas as situações que possam ferir os princípios da segurança da informação, sendo esse um fator que pode definir o sucesso ou o fracasso de uma empresa que pretende ter as informações gerenciais necessárias para a tomada de decisão.

Para melhorar a gestão e o controle da área de TI e seus processos, buscando padronizar e facilitar a implantação de uma política de segurança da informação e tentando garantir o retorno do investimento junto com melhorias nos processos organizacionais existe um movimento chamado de Governança de TI, ou "*IT Governance*" que Fagundes (2013) define como:

> uma estrutura de relações e processos que dirige e controla uma organização a fim de atingir seu objetivo de adicionar valor ao negócio através do gerenciamento balanceado do risco com o retorno do investimento de TI.

Existem algumas metodologias que auxiliam na Governança de TI, estando adequada as normas ISO/IEC 27001 e 27002, ajudando assim diretamente no seu cumprimento. Dentre elas podemos citar o CobiT (*Control Objectives for Information and related Technology*).

6. Política Nacional de segurança da informação

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios

Consciente da importância das informações processadas nos órgãos, entidades e administrações, o Presidente da República decretou leis por meio do qual foi instituída a política nacional de segurança das informações. Com esse ato normativo, o governo brasileiro despertou de vez para a necessidade de proteção de assuntos que mereçam tratamento especial, adotando medidas para prevenir o risco de sua vulnerabilidade, lançando os seguintes decretos:

O **Decreto 3.505** estabelece diretrizes, critérios e procedimentos para a elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (PoSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta.

O **Decreto 4.553**, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

7. Considerações Finais

Conforme entendimento da ISO/IEC 27002, um dos principais objetivos da Segurança da Informação, sendo também esse um dos princípios contábeis, que a correta utilização da auditoria ajuda a assegurar. Dessa forma podemos entender que para ter resultado (e continuidade) o negócio necessita de decisões acertadas que por sua vez precisam de informações corretas que devem ser sempre acompanhadas através da auditoria e asseguradas através de uma boa gestão da segurança da informação. Ou seja, a segurança da informação auxilia tanto na manutenção das informações da organização mantendo os seus atributos de confidencialidade, integridade e disponibilidade, quanto possibilita o correto trabalho da auditoria, que por sua vez garante a qualidade das informações necessárias à organização.

Segurança da informação não deve ser considerada um fim, mas um meio para que as decisões e a gestão da organização sejam baseadas em dados e informações corretas, tornando mais acertada as decisões que podem definir o futuro e a continuidade do negócio. A realização deste trabalho tinha como proposta principal mostrar como a segurança da informação e a correta gestão da tecnologia da informação são importantes para uma auditoria de sistemas, portanto importante para a própria organização e esse objetivo ficou evidente no decorrer deste artigo.

Referências

Araújo, I. P. S. (1998) Introdução à Auditoria: breves apontamentos de aula - aplicáveis à área governamental e aos programas de concursos públicos. Salvador: Egba.

Chiavenato, I. (2000) Administração nos novos tempos. São Paulo: Campus.

Laudon, K. C., Laudon, J. P. (2004) Sistemas de Informação Gerencial: administrando a empresa digital. 5 ed. São Paulo: Prentice Hall, 2004.

Rezende, D. A., Abreu, A. F. de (2000) Tecnologia da informação aplicada a sistemas de informações empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas.