

A SEGURANÇA DA INFORMAÇÃO E A SUA IMPORTÂNCIA PARA A AUDITORIA DE SISTEMAS

DALVAN CUNHA ¹

MARCOS ALEXANDRE FENATO ²

¹ Autor do Estudo – Graduado em Administração de Empresas com Habilitação em Análise de Sistemas pela Faculdade São Francisco de Barreiras – FASB, Barreiras - BA.

² Orientador do Estudo – Especialista em Redes de Computadores pela UNOPAR, bacharel em Ciências da Computação pela UNIPAR. Atualmente atua como coordenador do setor de tecnologia da informação e Comunicação (TIC) do IAESB – Instituto Avançado de Ensino Superior de Barreiras que tem como mantida a Faculdade São Francisco de Barreiras – FASB, Barreiras - BA.

RESUMO

A tecnologia mudou o rumo da administração nas organizações, antes baseado em um modelo industrial e atualmente em um modelo baseado em conhecimento. Para manterem-se na atual conjuntura econômica mundial as empresas passaram a dar valor e importância à informação, agora avaliado como um dos principais bens da organização e sendo ela considerada o principal combustível da economia contemporânea. Com o advento dos meios de comunicação, especialmente a internet, tornou-se um desafio filtrar dentro de todas as informações disponíveis aquelas que são importantes para a empresa e que embasa suas decisões. Para isso o presente artigo fez uso de estudos bibliográficos, composto por temas relacionados à auditoria e segurança da informação e aborda a importância da Segurança da Informação (SI) para a Auditoria de Sistemas dentro de uma organização, onde a SI cuidará da informação e seus atributos como a confidencialidade, integridade e disponibilidade e apoiado por ela, a auditoria certificará que as informações disponíveis tenham qualidade e sejam confiáveis, identificando os pontos de falha e sugerindo as correções necessárias.

PALAVRAS-CHAVE: Tecnologia da Informação, Segurança da Informação, Auditoria de Sistemas, ISO/IEC 27002, Sistemas de Informação.

THE INFORMATION SECURITY AND ITS IMPORTANCE TO THE SYSTEMS AUDIT

ABSTRACT

Technology has changed the direction of management in organizations, before based on an industrial model, and currently a model based on knowledge. To keep up on current world economic enterprises have come to value and importance to information, now rated as one of the main assets of the organization and which is considered the main fuel of contemporary economics. With the advent of mass media, especially the Internet, has become a challenge in filtering all the information available to those that are important and the company that bases its decisions. For this article it made use of bibliographical studies, composed of topics related to audit and information security and addresses the importance of Information Security (IS) Audit for System within an organization, where the IS handle the information and its attributes such as confidentiality, integrity and availability and supported by it, the audit shall certify that the information they have available quality and are reliable, identifying failure points and suggesting any necessary corrections.

KEYWORDS: Information Technology, Information Security, Systems Audit, ISO / IEC 27002, Information Systems.

1 Introdução

Passou o tempo em que para manter uma empresa era necessário domínio apenas da área em que a organização atuava. Atualmente as organizações tem que ter domínio em diversas frentes que vão das técnicas de produção mais baratas e ainda assim mantendo a qualidade, passando por gestão de estoque e logística, organização financeira e contábil, gestão de pessoas e até o domínio das tecnologias de informática em ascensão. Tudo isso para manter-se nessa conjuntura atual da economia mundial, que passou de um modelo industrial para um modelo baseado em conhecimento.

O conhecimento de uma organização é gerado pelas pessoas presentes nela a partir da informação disponível, portanto 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 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 evolução recente da tecnologia

A evolução cada vez maior da tecnologia, principalmente relacionada à internet e computação móvel – que de 2007 até 2012 teve saltos mais significativos do que nos 10 anos anteriores – tem alterado bastante a forma como a uma organização cria, filtra, organiza, cuida e usa a informação. Para ter ideia dessa mudança, a sete anos nós não tínhamos nada parecido com os celulares inteligentes (os *smartphones*) que temos hoje, onde o acesso a informação está a um toque de distância e podemos em qualquer lugar de forma prática e rápida acessar

os mais diversos sistemas empresariais, responder e-mails, ler notícias, ver previsão do tempo, situação do trânsito, acessar sites diversos. Tudo isso sem a necessidade de um computador/notebook por perto.

Há outro grande exemplo. Até 2010 nem os departamentos de Tecnologia da Informação (TI) das maiores empresas do mundo tinham em mente que teriam que integrar ao seu parque mais um equipamento de acesso a recursos da empresa, o *tablet*. Esses pequenos *gadgets* (equipamentos) além de agregar as funções existentes nos *smartphones* (com o conforto de uma tela maior), substituem boa parte das funções dos notebooks e computadores usados pelas pessoas. O surgimento destes dispositivos pode afetar indiretamente todas as empresas do mundo, tanto que o sistema operacional mais usado em computadores, o Windows® foi modificado pela Microsoft (sua fabricante) de uma forma como nunca antes nos seus 25 anos de existência, somente para ser viável seu uso em *tablets*.

Toda essa mudança em relação aos *tablets* iniciou-se a menos de três anos, mostrando como de um momento para outro a realidade pode mudar, forçando pessoas e empresas a se adaptarem. Veja por exemplo que somente pela massificação dos *smartphones* e *tablets* junto com a disponibilidade e mobilidade cada vez maior da internet temos uma grande vantagem, que é a informação disponível em quase todos os lugares, cabendo às organizações aproveitarem isso para o seu negócio.

3 A informação e sua importância

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.

Mas o que vem a ser esse bem tão importante chamado informação?

Para responder a essa pergunta temos primeiro que compreender o que são "dados", pois deles que são formadas as informações.

Conforme a precisa definição de CHIAVENATO (2008), “dados são os elementos que servem de base para a formação de juízos ou para a resolução de problemas. Um dado é apenas um índice ou um registro. Em si mesmo, os dados têm pouco valor. Todavia, quando classificados, armazenados e relacionados entre si, os dados permitem a obtenção da informação. Assim, os dados isolados não são significativos e não constituem informação. Os Dados exigem processamento (classificação, armazenamento e relacionamento), para que possam ganhar significado e conseqüentemente informar. A Informação apresenta significado e intencionalidade, aspectos que a diferenciam do dado simples.”.

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.”.

4 Sistemas de Informações

Já sabemos do valor que a informação tem para uma empresa, mas agora analisaremos a evolução da criação, armazenamento e extração das informações dentro das organizações e a importância atual dos sistemas de informações.

Em tempos passados as informações das empresas ficavam primeiramente disponíveis no papel, tendo que ser analisadas de forma manual mesmo. Com as empresas crescendo cada vez mais e sua atividade se tornando mais complexa era necessário que pudessem automatizar vários processos e atividades a fim de facilitar a gestão e a tomada de

decisão e isso foi possível com a disseminação dos computadores a partir da década de 80 que já permitiam as empresas o armazenamento e análise de informações por meio de planilhas eletrônicas, inclusive usado até hoje como único meio de armazenamento e análise de informações por algumas pequenas empresas.

As planilhas eletrônicas ajudam muito, pois são bastante personalizáveis para o fim a que se destina, mas para tomada de decisão e gestão ainda temos o problema da análise. Enquanto a empresa é pequena não é difícil analisar uma ou duas planilhas, mas quando cresce e tem filiais, as informações já não são tão confiáveis (já que a planilha pode ser modificada de qualquer maneira) e tão rápidas para análise em curto tempo. Imagine uma empresa com 10 (dez) filiais ter que receber na matriz todas as informações de vendas e produção através de planilhas para poder analisar e tomar uma decisão rápida? O trabalho torna-se custoso e pouco ágil, algo que nessa nova economia não serve, pois as empresas devem ter a informação em mãos tão rápido quanto a mesma é produzida de forma a estar preparada para as decisões e desafios diários.

Para melhorar o controle, planejamento e organização de uma empresa surgiram os Sistemas de Informações que aliado a outras ferramentas de tecnologia de informação serão os responsáveis pela entrada, processamento, armazenamento e recuperação da informação para auxiliar na tomada de decisões dentro da organização.

O'Brien (2004) define que um sistema de informação "é um conjunto organizado de pessoas, hardware, software, redes de comunicação e recursos de dados que coleta, transforma e dissemina informações em uma organização." A figura 1 a seguir contextualiza esse pensamento:

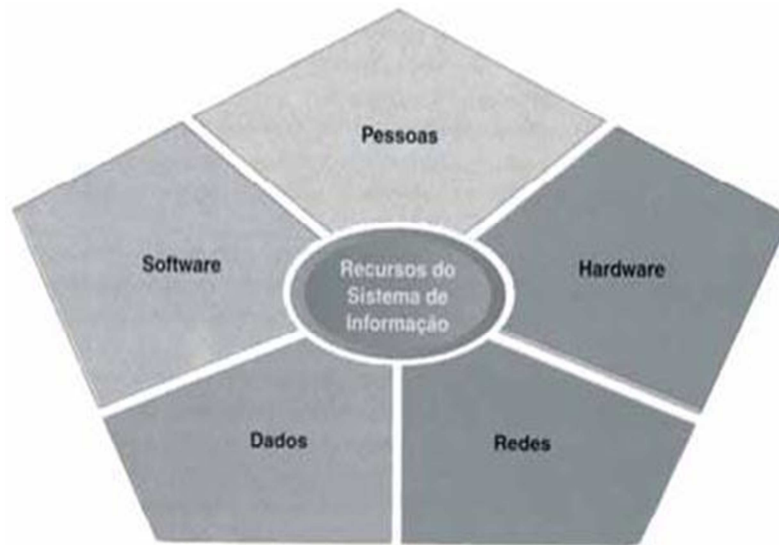


Figura 1 - Recursos do Sistema de Informação Fonte: O'Brien (2004, p. 06)

Já LAUDON e LAUDON (2004), determinam que um sistema de informação pode ser definido tecnicamente como “um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. Além de dar suporte ao processo decisório, à coordenação e ao controle, sistemas de informação podem também auxiliar gerentes e trabalhadores a analisar problemas, visualizar situações complexas, e criar novos produtos.”.

Vimos que auxiliar no processo decisório, ou seja, ajudar as pessoas a decidirem dentro das organizações é uma das principais funções dos sistemas de informação e como bem define CHIAVENATO (2000) decisão é “o processo de análise e escolha entre várias alternativas disponíveis do curso de ação que a pessoa deverá seguir”. Dessa forma para termos qualidade na decisão significa ter qualidade nas informações presentes no sistema que subsidiam essa decisão. A organização deve ter uma preocupação com a coerência dos dados inseridos em seu sistema, avaliando e filtrando, pois esses dados vão gerar as informações que serão usadas no processo decisório. Portanto é necessário ter uma rotina de auditoria (conforme abaixo) que irá conferir se todos os processos relacionados aos sistemas de informação estão ocorrendo de forma correta e garantindo assim uma informação mais confiável para o negócio.

5 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.

A auditoria é muitas vezes classificada com o uma especialização da contabilidade. ATTIE (1998) diz que “a auditoria é uma especialização contábil voltada a testar a eficiência e eficácia do controle patrimonial implantado com o objetivo de expressar uma opinião sobre determinado dado.”. Já ARAÚJO (1998) nos dá uma definição mais completa onde ele exprime que “a auditoria pode ser conceituada como um conjunto de procedimentos aplicados sobre determinadas ações, objetivando verificar se elas foram ou são realizadas em conformidade com normas, regras, orçamentos e objetivos”. Ele ainda completa que a auditoria “é o ato de se confrontar a condição – situação encontrada – com o critério – situação que deve ser.”.

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.

Já sabemos que as Tecnologias da Informação e dentre elas os Sistemas de Informação adquiriram uma importância vital para a sobrevivência da maioria das organizações. É difícil imaginar empresas que num maior ou menor grau não dependa delas.

Mas não podemos partir do princípio que toda informação extraída dos meios tecnológicos como os sistemas são confiáveis, pois é possível que haja erros ou fraudes, ocasionando assim discrepância entre o que está armazenado nos sistemas e a realidade propriamente dita.

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.”.

6 A Segurança da Informação

Já sabemos que informação é um dos maiores bens de uma empresa e que a evolução da tecnologia está permitindo que essa informação esteja disponível em quase todos os lugares. Isso é realmente algo fantástico e permitiu o ser humano ser capaz de coisas maravilhosas. Além dos exemplos citados anteriormente ainda temos a comunicação em tempo real independente das distâncias, o armazenamento de dados na internet (de onde se pode resgatar de qualquer lugar), entre outros.

Agora eis uma pergunta que podemos nos fazer:

Seria preocupante caso essas informações não sejam usadas pelas pessoas corretas?

Imagine 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, pag. 11).

Ainda nesse entendimento ele completa:

“As redes de computadores, e conseqüentemente da Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas do que em sistemas fechados, assim como os riscos à privacidade e à integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e aos dados desses sistemas.” (Laureano 2005, pag. 11).

Com uma pesquisa feita pela Módulo Security Solutions temos uma noção dos potenciais riscos a que a informação pode estar sujeita dentro da organização. A figura 2 a seguir contextualiza bem essa pesquisa:

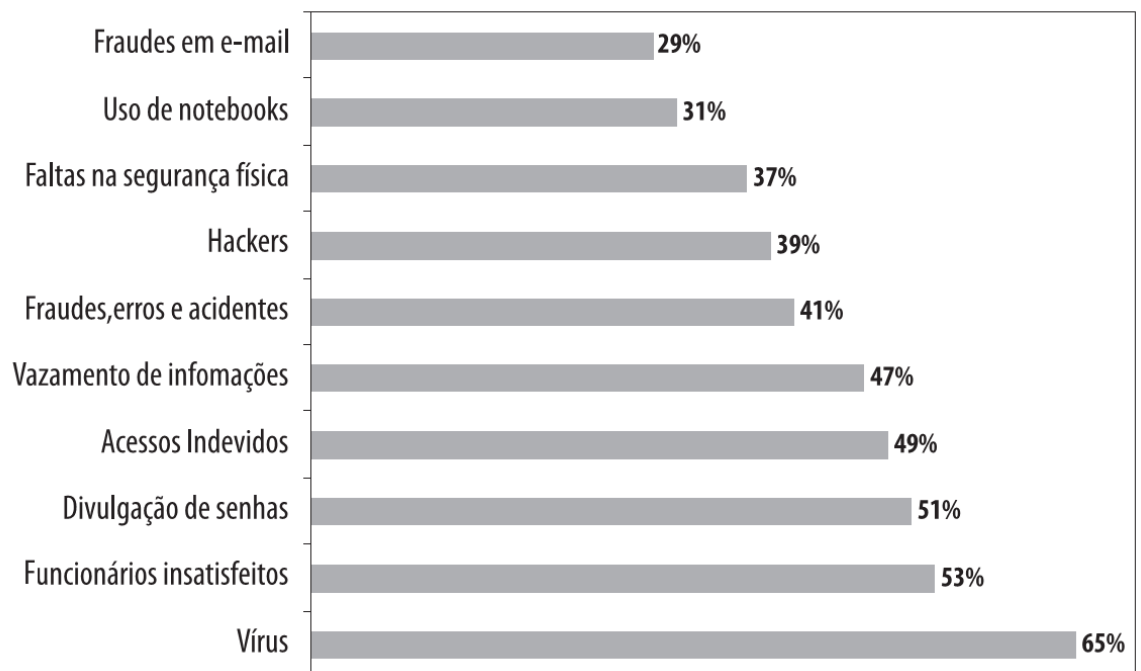


Figura 2 - Principais ameaças às informações nas organizações

Fonte: 9ª Pesquisa Nacional sobre Segurança da Informação – Módulo Security Solutions (2003)

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.

De acordo com SÊMOLA (2003), “podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. Já a ABNT (2003) com a sua norma ISO/IEC 17799:2001, define segurança da informação como “a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos.”. A norma ISO/IEC 17799:2001 ainda complementa que “a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.”.

É importante frisar que a norma ISO/IEC 17799 foi atualizada para numeração ISO/IEC 27002 em julho de 2007, sendo dessa forma designada a partir desse momento.

Temos ainda a definição do governo brasileiro que através do decreto No 3.505, de 13 de junho de 2000 no Art. 2º, paragrafo II conceitua:

“Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.”.

A norma ISO/IEC 27002 fala 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, conseqüentemente 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, é a norma ISO/IEC 27002.

Cuidar da segurança da informação em uma empresa não é algo simples. Somente ler a norma ISO/IEC 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 a norma ISO/IEC 27002, ajudando assim diretamente no seu cumprimento. Dentre elas podemos citar o CobiT (*Control Objectives for Information and related Technology*).

Não é o foco deste artigo, sendo necessário um estudo a parte, mas para entendimento sobre o que é o CobiT, FAGUNDES (2013) responde:

“O CobiT é um guia para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*, www.isaca.org). O CobiT inclui recursos tais como um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do CobiT são recomendadas pelos peritos em gestão de TI que ajudam a otimizar os investimentos de TI e fornecem métricas para avaliação dos resultados. O CobiT independe das plataformas de TI adotadas nas empresas.” (Fagundes, 2013).

7 Considerações Finais

Continuidade do negócio é, 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

CHIAVENATO, Idalberto. **Gestão de Pessoas**. 3ª edição, Editora Elsevier – Campus, 2008.

CHIAVENATO, Idalberto. **Administração nos novos tempos**. São Paulo: Campus, 2000.

REZENDE, D.A.; ABREU, A. F. de. **Tecnologia da informação aplicada a sistemas de informações empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de Informação Gerencial: administrando a empresa digital**. 5 ed. São Paulo: Prentice Hall, 2004.

O'BRIEN, James A. **Sistemas de informação e das decisões gerenciais na era da Internet**. São Paulo: Saraiva, 2004

ATTIE, W. **Auditoria: conceitos e aplicações**. 3. ed. São Paulo: Atlas, 1998.

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

KARAPETROVIC, S.; WILLBORN, W. **Generic audit of management systems: fundamentals**. *Managerial Auditing Journal*. 15-06-2000. Disponível em: <http://www.emerald-library.com/10.1108/02686900010344287>. Acesso em: 30/01/2013.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT)– **Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2001**. Rio de Janeiro: ABNT, 2003.

DECRETO No 3.505, DE 13 DE JUNHO DE 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm . Acesso em: 02/02/2013.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. 01/06/2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf . Acesso em: 02/02/2013.

MÓDULO SECURITY SOLUTIONS. **9ª Pesquisa Nacional sobre Segurança da Informação**. Disponível em http://www.modulo.com.br/media/9a_pesquisa_nacional.pdf . Acesso em: 02/02/2013.

FAGUNDES, Eduardo Mayer. **COBIT - Um kit de ferramentas para a excelência de TI**. Disponível em <http://www.efagundes.com/artigos/COBIT.htm> . Acesso em: 07/02/2013.