A AUDITORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO COMO INSTRUMENTO DE APOIO À TOMADA DE DECISÕES, PELA ALTA ADMINISTRAÇÃO DE ORGANIZAÇÕES MODERNAS [1]

Gibson Batista Gomes[2]

Resumo: Este artigo tem como objetivo principal analisar a importância da auditoria de sistemas da informação, como instrumento de apoio à tomada de decisões, pela alta administração de organizações modernas. Um mundo cada vez mais virtual, exige de todo grande administrador uma maior preparação para enfrentar os novos desafios e uma adaptação continua a mudanças cada vez mais frequentes. A necessidade de manter a competitividade da organização à qual pertence, com liberdade para crescer, inovar e ampliar os negócios, exige que as informações sejam confiáveis, íntegras, estejam disponíveis, mantenham propriedades de confidencialidade, auditabilidade e privacidade, o que é um grande desafio nos dias atuais. Neste contexto, a auditoria de segurança da informação, mostra-se uma valiosa e eficaz ferramenta para a orientação das decisões. Para este artigo foi utilizada metodologia de ordem teórica, de modo explicativo e a obtenção dos dados se deu a partir de pesquisa junto a administradores e análise de relatórios de auditoria.

Palavras-chave: Auditoria. Apoio à tomada de decisões. Informações confiáveis. Segurança da Informação.

1 INTRODUÇÃO

Vivemos na era da informação, onde todos estão conectados e a globalização é um fato. A segurança das informações tornou-se um elemento essencial ao desenvolvimento e a manutenção desta conectividade. Segundo a CISCO Systems, inc. em 2016, foi ultrapassada a marca de 1,7 exabyte de informações por segundo, transitando pelas redes, sistemas e aplicativos no Brasil, e a previsão é de que em 2020 serão 4,4 exabytes.

---

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Pós-Graduação da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação. Orientador: Prof. Luiz Otávio Botelho Lento, Mestrado. Campinas, 1995.

[2] Acadêmico do Curso de Pós-Graduação em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina. gibsonbgomes@gmail.com

Toda essa revolução da era digital, na transmissão, recepção, guarda e descarte de dados e informações, traz consigo uma série de desafios para a segurança da informação. Segundo Manotti (2010), proteger sua tecnologia, mesmo que esta seja apenas um meio para viabilizar seu negócio, é proteger o seu negócio.

Garantir que as informações sejam confiáveis, íntegras, estejam disponíveis, mantenham propriedades de confidencialidade, auditabilidade e privacidade é um grande desafio. A auditoria é importante para garantir a aderência aos preceitos de segurança tanto da organização quanto do mercado, e assim contribuir para que a tecnologia esteja sempre disponível e confiável para atender ao negócio, de maneira econômica (MANOTTI, 2010, p.XXIII).

Na contramão de toda essa evolução e como um desafio de segurança, vem o cibercrime, que é uma atividade cada dia mais presente e desafiadora para governos, organizações, empresas e pessoas. Tracy (2005), lembra que é bom ter na consciência que o inimigo pode estar dentro da empresa.

Outras questões naturais, de recursos humanos e de infraestrutura, são também, muitas vezes, fatores de preocupação para a área de segurança e limitadoras da evolução de muitos negócios em empresas modernas e com potencial de sucesso.

Segundo Tracy (2005), para todas as empresas em desenvolvimento, a segurança é uma ciência complexa, que precisa encontrar seu caminho, inserindo-se na direção do empreendimento. Sendo assim, uma das funções da Auditoria é de orientar a direção da empresa, abordando esta questão de maneira simplificada, de modo a permitir um melhor entendimento do assunto e assim facilitar a tomada de decisões com oportunidade.

Confiar nos sistemas de informações e sua infraestrutura é uma necessidade, para que uma empresa moderna possa se desenvolver e atingir padrões elevados de qualidade e confiança. A tomada de decisão pelo administrador/gestor de uma empresa informatizada necessita de embasamento técnico apropriado para que ela seja eficaz, efetiva e principalmente que ela seja tomada com oportunidade, para evitar o comprometimento dos seus ativos. Segundo Sêmola (2014), a segurança da informação não é uma ciência exata e se fôssemos classifica-la, ela estaria no campo da gestão de riscos.

Nem todo administrador possui conhecimento técnico suficiente, na área de segurança da informação, que lhe permita tomar decisões estratégicas para proteção de seus ativos de

tecnologia da informação e comunicação (TIC). Sêmola (2014), afirma que muitas pessoas pensam que segurança da informação se resume a compra de equipamentos e sistemas caros. Sendo assim, existe a necessidade da utilização de uma ferramenta de apoio, que preencha essa lacuna, de maneira confiável e oportuna, a auditoria.

A auditoria de segurança da informação, executada de maneira responsável, por profissionais capacitados é uma ferramenta reconhecidamente importante para subsidiar a tomada de decisão pelos administradores, uma vez que ela busca elencar deficiências e necessidades, verificar pontos fortes e oportunidades de melhoria, com base em elementos e evidências coletadas in loco, provendo assim relatórios com informações devidamente fundamentadas e com elevado grau de confiança, para dar o suporte necessário ao negócio e a tomada de decisão.

> Com o advento tecnológico e o processo de disseminação do conhecimento, os sistemas de informação assumiram um papel significativo nas organizações gerando informações integras e confiáveis para a operacionalização dos processos, produtos, serviços e também para o auxílio no processo de tomada de decisão. Assim sendo, é dever do auditor garantir que os sistemas estejam alinhados aos requisitos de segurança, bem como verificar se a adoção de controles está em consonância com a criticidade do negócio. (GOMES, 2010 apud MANOTTI, 2010 p.)

Para garantir que os sistemas estejam alinhados aos requisitos de segurança, Manotti (2010) sugere que devem ser utilizados frameworks de boas práticas notadamente reconhecidos pelo mercado, tais como:

- COBIT (Control Objectives for Information and Related Technologies), que tem como um dos os objetivos otimizar os investimentos de TI, melhorando o retorno sobre o investimento;

- ITIL (Information Technology Infrastructure Library), que é um conjunto de boas práticas para serem aplicadas na infraestrutura, operação e gerenciamento de serviços de tecnologia da informação; e

- ISO/IEC 27001:2013 (International Organization for Standardization e pelo International Electrotechnical Commission), que tem a finalidade de prover um modelo que estabeleça, implemente, opere, monitore, analise criticamente, e mantenha um Sistema de Gestão de Segurança da Informação (SGSI).

As considerações iniciais aqui apresentadas, tem por finalidade orientar o leitor sobre o escopo deste artigo, direcionando o leitor para a fundamentação teórica que tem a função de relativizar a importância e justiçar a necessidade de investimento em auditoria de segurança da

informação, identificando efetivamente sua importância para o aprimoramento da Governança Corporativa e para o fortalecimento e continuidade do negócio, bem como avaliar qual tipo de negócio pode utilizar a função auditoria, como ferramenta de apoio a decisão.

Para a fundamentação do presente artigo, foi realiza uma pesquisa, com perguntas objetivas e subjetivas, com finalidade de verificar a visão dos administradores, bem como sua percepção sobre o tema. Foi verificada ainda, a aceitação pelos usuários, e por fim, foi realizada uma análise sobre alguns relatórios de auditoria de segurança de sistemas de informações. O público alvo, foram administradores de organizações publicas e privadas, bem como seus gestores de TI e seus colaboradores (funcionários).

A questão que orienta essa pesquisa é: A auditoria de segurança de sistemas da informação é um instrumento de apoio à tomada de decisões, útil a administração de organizações modernas?

Para responder a esse questionamento, além da pesquisa de campo, foi realizada uma fundamentação teórica, com objetivo de demonstrar a importância da Auditoria de Segurança de Sistemas da Informação, no processo de tomada de decisão, por administradores de empresas e organizações em um ambiente cada vez mais competitivo e globalizado.

Esse trabalho é composto de cinco seções. A primeira seção é a introdução, a segunda seção apresenta o referencial teórico que fundamenta esse trabalho e está dividida em 3 subseções, tratando da evolução das tecnologias, o uso da auditoria para a tomada de decisões e a agregação de valor ao negócio. Em seguida, na terceira seção encontra-se a apresentação da pesquisa de campo realizada e na quarta seção uma breve apreciação dos dados. Por fim a quinta seção, que contém a apresentação das conclusões finais e o encerramento do artigo.

2 AUDITORIA SEGURANÇA DA INFORMAÇÃO COMO PROCESSO PARA GARANTIR OS OBJETIVOS DO NEGÓCIO

Empresas, organizações, entidades governamentais e privadas, independentemente de seu porte ou ramo de atividade, dependem cada vez mais de Tecnologia da Informação (TI) e seus sistemas. Empresas de alta tecnologia que trabalham com as mais recentes inovações tecnológicas, empresas que operam no sistema financeiro, tais como Bolsas de Valores, Bancos, Exchanges para compra/venda de Bitcoin, entre tantas outras, são exemplos de empresas que necessitam de sistemas seguros, confiáveis e com disponibilidade continuada (24x7x365).

Segundo Sêmola (2014), notadamente, essas novas e modernas condições elevam o risco das empresas a níveis nunca antes vividos, fazendo-as perceber a necessidade de ações corporativas integradas em busca de mecanismos de controle que permitam reduzi-lo e torná-lo administrável e viável.

Conforme Manotti (2010), os sistemas de informação estão expostos a ameaças e riscos de todo tipo, seja por falha ou ação humana intencional ou não-intencional, acidentes, desastres naturais e ocorrências inesperadas. Deste modo, necessitamos de segurança para dar suporte ao negócio, garantindo a integridade, confiabilidade e disponibilidade das informações. Neste quesito entra a auditoria de segurança da informação, que trabalha justamente para que a organização/empresa possa garantir que todos estes pilares da segurança sejam mantidos, de maneira satisfatória.

De acordo com Manotti (2010), a auditoria de sistemas é de vital importância para o bom desempenho dos sistemas de informação, pois possibilita avaliar os controles necessários para que os sistemas sejam confiáveis e seu nível de segurança seja adequado. Manotti (2010) lembra ainda, que a auditoria engloba todo o ambiente: Equipamentos, Centro de Processamento de Dados e Software.

Segundo Albanese (1981), controle é o processo destinado a assegurar que as ações estejam de acordo com os resultados desejados. Sendo assim, a auditoria pode ser um método utilizado para ampliar o controle sobre os processos.

Na mesma linha de raciocínio, Megginson (1986), define controle como o processo de garantir que os objetivos organizacionais e gerenciais estejam sendo cumpridos, ou seja, a maneira de fazer com que as coisas aconteçam do modo planejado.

Conforme Gertners de Magalhães (2013, p.4), a auditoria nas organizações é um instrumento da direção da entidade, dos acionistas, do ambiente externo à organização, do povo para validar e avaliar a qualidade em termos de segurança e eficiência os trabalhos desenvolvidos com a tecnologia computacional.

Os sistemas de informação adquiriram uma importância vital para a sobrevivência de qualquer organização moderna, uma vez que, computadores, sistemas e redes de comunicação, tornaram-se imprescindíveis para a prestação de seus serviços. Conforme Gertners de Magalhães (2013), hoje em dia não existem mais empresas que não dependam da tecnologia da informação, num maior ou menor grau. Sendo assim, manter níveis adequados de segurança é

fundamental para que os ativos estejam protegidos de ações hostis, sejam elas advindas do ambiente interno ou externo.

2.1 EVOLUÇÃO TECNOLÓGICA E A NECESSIDADE DE GARANTIR A SEGURANÇA DAS INFORMAÇÕES

Com a evolução dos computadores, dispositivos móveis, sistemas e das redes que conectam o mundo inteiro, os aspectos de segurança da informação atingiram uma complexidade que exige a necessidade do desenvolvimento de equipes cada vez mais especializadas e com capacidade técnica, para a sua implementação e gerência. Para Sêmola (2014), o melhor a fazer, então, é preparar-se para essa realidade da melhor forma possível e começar a trabalhar na implementação dos controles necessários o quanto antes.

A expansão do uso de soluções informatizadas dentro das empresas e organizações, cresceu muito nos últimos anos. Gertners de Magalhães (2013), afirma que este ambiente em pleno desenvolvimento, trouxe um novo mundo de oportunidades, que veio acompanhado do uso descontrolado dos sistemas de informação, o que gera a necessidade iminente de controle, por parte de empresas, através de um plano de auditoria.

Segundo Sêmola (2014), o nível de segurança de uma empresa está diretamente associado a segurança oferecida pela “porta” mais fraca. Esta é uma frase muito conhecida no ambiente de TI e reforça a importância do assessoramento a tomada de decisões, oferecido pela função auditoria. Nos tempos modernos, um administrador não pode basear suas ações, para proteção de ativos de TI em demandas reativas de caráter emergencial, o administrador necessita sim, de um plano diretor, bem estruturado, baseado em uma análise confiável (auditoria) dos seus sistemas e ativos, para ações de curto, médio e longo prazo. Para Sêmola (2014), a falta deste plano, pode colocar os ativos da empresa em um terreno de alto risco, dando ao administrador uma falsa sensação de segurança e confiabilidade. Sêmola (2014), diz ainda, que não adianta trancar as portas, mas deixar as janelas abertas.

Por outro lado, segundo Manotti (2010), o trabalho da auditoria é um processo continuo, e deve-se compreender que não há motivo para sua realização caso as gerências auditáveis responsáveis pelos controles não cumprem as recomendações emitidas. Ou seja, existe a necessidade de estabelecer um programa de acompanhamento de implantações das recomendações da auditoria.

Quando da execução de uma auditoria, a mesma tem a finalidade de verificar a situação atual de segurança dos sistemas de uma empresa ou organização, e indicar soluções, para tornar o ambiente de TI mais seguro. Segundo Ibraim (2013), o auditor tem dois objetivos a serem atingidos: primeiro, relatar à administração superior todos os seus achados e segundo, deixar todo o lugar que ele audita, melhor do que encontrou.

2.2 A AUDITORIA DE SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA DE APOIO A TOMADA DE DECISÕES

Informação, segundo Oliveira (2008), é o dado trabalhado que permite ao executivo tomar decisões. Quando trata-se de segurança da informação, a gerência de qualquer empresa ou organização necessita de subsídios (informações) para a correta tomada de decisões. Estes subsídios necessitam ser confiáveis, melhorar a eficiência e oferecer soluções que permitam reduzir riscos ao negócio. Neste contexto, a auditoria se apresenta como uma função importante para a empresa, pois tem o papel de fornecer informações sobre a segurança de seus ativos da informação à alta administração. Conforme Imoniana (2016, p.3), a filosofia de auditoria em tecnologia de informação está calcada em confiança e em controles internos, indo de encontro a esta necessidade da alta administração.

A auditoria exige o envolvimento da alta direção, que é a responsável por fazer com que as políticas de segurança da empresa sejam cumpridas pelos seus funcionários. Conforme Manotti (2010), a auditoria é a ferramenta que tem a função de dar subsídios para a tomada de decisões por parte da alta administração.

A auditoria de segurança visa a prevenção, a detecção e a correção de problemas, objetivando minimizar o impacto causado por falhas ou omissões. A NBR ISSO/IEC 27001, define a auditoria como um processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente de modo a determinar a extensão na qual os critérios de auditoria são atendidos.

A auditoria de segurança pode ser considerada um mal/bem necessário a qualquer organização. Avaliar os processos de negócio, para saber se é eficiente, ou mesmo, até quanto o seu sistema de informações é seguro, é uma necessidade estratégica. Logo, se for perguntado por que auditar, uma resposta bastante plausível, pode ser: a necessidade estratégica da segurança das informações, para o subsídio da tomada de decisões pela alta administração, na correta gestão da continuidade do negócio. Segundo Sêmola (2014), somente com apoio

executivo as ações de segurança ganharão autonomia e abrangência capaz de incidir corporativamente sobre as falhas de segurança.

O COBIT apresenta 7(sete) objetivos a serem atingidos com a auditoria de sistemas: eficiência, efetividade, confidencialidade, integridade, disponibilidade, *compliance* e confiança. Sendo assim, o auditor ao adotar esta metodologia para seus trabalhos, pode garantir um assessoramento de qualidade ao decisor, elencando necessidades imediatas e futuras, através de relatórios de auditoria.

> O fato é que a garantia de continuidade dos negócios não se consiste em apenas recomendar e realizar controles internos, com base no histórico organizacional, a fim de tratar os riscos como era no passado. Atualmente, a capacidade de uma organização sobreviver em meio à competitividade imposta diariamente pela acelerada globalização de mercado, exige que a auditoria não se limite a controles, mas que mantenha o diferencial de agregar, ao conhecimento do histórico organizacional, um eficiente gerenciamento de riscos, que atenda todo o universo dos processos das áreas de negócios da companhia.(MARZANO, 2014, p.44).

2.3 A AUDITORIA DE SEGURANÇA DA INFORMAÇÃO SÓ É VALIDA PARA O NEGÓCIO, QUANDO AGREGA VALOR

A TI é um mundo amplo e em permanente desenvolvimento, adventos como a inteligência artificial, a *cloud computing* e a *IoT* estão em plena expansão. Um administrador de empresa ou organização que trabalha com o ativo informação, com a alta tecnologia, com negócios, com mercado financeiro, entre tantos outros, necessita tomar diariamente uma série de decisões, as quais tem impacto direto sobre os negócios, podendo estas serem positivas ou negativas.

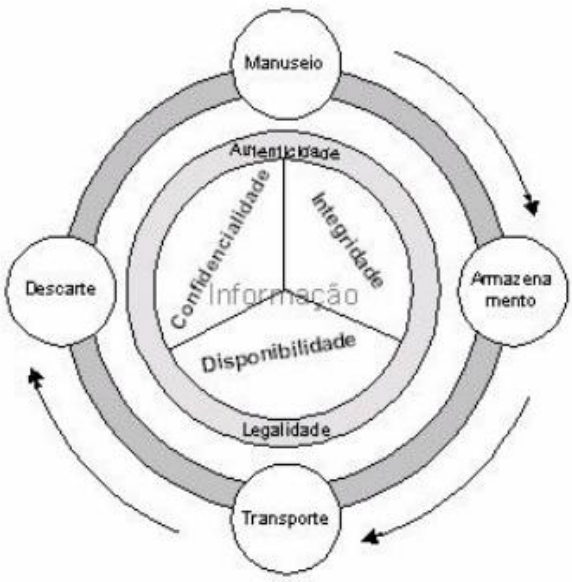
A salvaguarda dos ativos da informação, a integridade, a correção e confiabilidade dos registros, assim como sua eficiência, estão diretamente ligados as políticas de segurança da empresa e são importantes objetivos da auditoria de segurança. Segundo Imoniana (2016), em organizações cujas responsabilidades são impropriamente delineadas, a fraude é perpetrada facilmente, devido ao conhecimento de que niguém será responsabilizado. Ou seja, as políticas de segurança, são parte fundamental para a segurança do ativos, através da atribuição de responsabilidades e deste modo, a auditoria de segurança pode dar contribuição em seu aperfeiçoamento.

É fato que muitas dessas empresas possuem especialistas em TI, capacitados a desenvolverem suas atividades de maneira muito satisfatória. Porém, devemos lembrar que

sempre existe a possibilidade de falhas intencionais ou não e até mesmo desvios de conduta. Existem ainda usuários descuidados que podem cometer erros, sistemas que podem apresentar falhas em processamento ou saída de dados, condições adversas (variação de tensão, umidade, poeira, etc.) que podem influenciar no desempenho dos sistemas.

Ao adotarmos a auditoria de segurança (interna ou externa) como uma ferramenta de apoio a decisão, diminui-se a chance desses erros e problemas ocorrerem. Além disso, uma visão externa é muito importante para evitar vícios que venham a comprometer a segurança das informações e dos sistemas. É importante também, lembrar que a informação possui um ciclo de vida (Figura 1) e que muitas das vezes elas acabam passando por setores diferentes da organização, que não possuem comunicação direta, muitas vezes em virtude da segregação de funções, mas que necessitam manter seus princípios de confidencialidade, integridade e disponibilidade, bem como autenticidade e legalidade. A auditoria de segurança serve neste contexto, para identificar eventuais falhas no processo como um todo, ou em parte dele, que permitirão ao administrador adotar medidas corretivas apropriadas e com oportunidade, se necessário.

Figura 1 – Quatro momentos do Ciclo de Vida da Informação



Fonte: Sêmola (2014, p.11)

> A empresa virou uma grande teia de comunicação integrada, dependendo do fluxo de informações que por ela são distribuídas e compartilhadas. Essas mesmas informações, agora sujeitas a vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e humanos. (SÊMOLA, 2014, P.13)

Outro aspecto, cada vez mais importante e preocupante, são as ações de crackers que tem potencial de causar danos irreparáveis aos sistemas, aos projetos e a imagem da organização. A auditoria de segurança da informação também neste quesito, se mostra eficiente e cada vez mais necessária.

Com todas estas considerações é fácil afirmar que nenhum administrador, por mais que se empenhe, tem condições técnicas de acompanhar, identificar e tomar decisões, de modo a corrigir as falhas e problemas, com oportunidade e eficiência. No entanto, a alta administração de muitas empresas, ainda possui uma deficiência de percepção do problema e conforme Sêmola (2014), possuem uma visão do *Iceberg* (a porção que está fora da água e que eles veem, corresponde a apenas 1/7 de todo o bloco de gelo, permanecendo o resto submerso e, portanto, escondido dos seus olhos).

3 VISAO DA FUNÇÃO AUDITORIA SEGURANÇA DA INFORMAÇÃO POR ADMINISTRADORES E USUÁRIOS DE ORGANIZAÇÕES E EMPRESAS – AMOSTRA

Para o desenvolvimento do presente artigo, foi realizada uma pesquisa de campo com uma pequena amostra de administradores de organizações responsáveis por bancos de dados, sistemas e informações críticas.

A finalidade da pesquisa realizada, foi a de identificar qual a visão e opinião de administradores sobre a validade, a exequibilidade e a importância da auditoria de segurança da informação, bem como se seu custo é compatível com os benefícios para os negócios. Outra finalidade da pesquisa, foi identificar quais os óbices para o uso da auditoria segurança de modo eficaz. Por fim, a pesquisa buscou levantar dados, sobre a visão sobre o processo da auditoria, do ponto de vista geral de uma empresa/organização. As respostas estão concatenadas na Tabela 1, abaixo. Cabe ressaltar que nenhuma das organizações/empresas participantes da pesquisa são especializadas em TI.

Tabela 1: Auditoria – uma visão do administrador

Questionamento realizado	Sim	Não
O Sr. julga que possui conhecimento técnico suficiente para a tomada de decisões sobre assuntos de segurança da informação, de maneira acertada?	----	100%
O Sr. julga que a auditoria de segurança facilitaria a tomada de decisões, na área de TI?	77,78%	22,22%

A organização possui um sistema de auditoria interna de segurança da informação?	22,22%	77,78%
A organização possui um sistema de auditoria externa de segurança da informação?	55,56%	44,44%
O Sr. Julga que o custo x benefício de uma auditoria é compensatório para a empresa?	77,78%	22,22%

Fonte: Autor (entrevista)

Complementando os dados apresentados na Tabela 1, foi possível perceber que a auditoria de segurança da informação é julgada importante para a tomada de decisões, no entanto, a falta de recursos e até mesmo a falta de pessoal habilitado para a solução do problema, compromete sua eficiência para a tomada de decisões e solução de problemas. Conforme Sêmola (2014), é relevante destacar a necessidade de processos contínuos de sensibilização e capacitação das pessoas, sob pena de ter a equipe estagnada e brevemente, despreparada.

Visando ainda, obter um melhor entendimento e fundamentação sobre a visão da função auditoria de segurança, foi realizada também uma pesquisa com uma amostra de integrantes das empresas (Organizações) envolvidas na pesquisa, com a finalidade de obter uma visão geral e de diversos pontos de vista, sobre o tema.

A grande maioria das empresas (organizações) envolvidas possui política de segurança das informações e de uso dos meios de TI, mas em algumas elas não são divulgadas adequadamente e alguns funcionários podem não ter conhecimento (Gráfico 1).

Gráfico 1: A empresa possui política de uso dos meios de TI

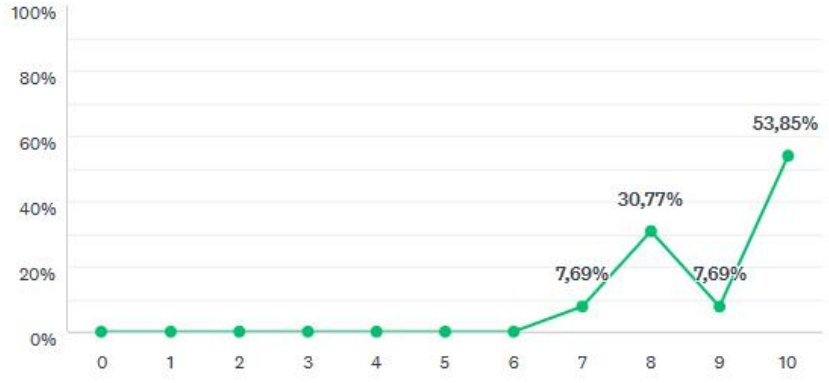
Fonte: Autor (pesquisa)

Na amostra, foi identificado que mais de 95% dos participantes, entende que a auditoria de segurança é uma ferramenta útil para a administração da empresa, para a detecção de

vulnerabilidades, identificação de falhas de segurança e verificação de problemas em geral. Não foi levado em conta o fator custo.

Dentro da amostra em questão, foi perguntado: No seu entendimento qual seria a importância de uma auditoria de segurança, para a tomada de decisões? Atribua uma nota de 0 a 10, onde zero significa que a auditoria não tem importância nenhuma e 10 significando que a auditoria é indispensável para uma empresa (Gráfico 2).

Gráfico 2: A empresa possui política de uso dos meios de TI



Fonte: Autor (pesquisa)

Com finalidade de melhor embasar o artigo, foi realizado um estudo sobre relatórios de auditoria de segurança da informação realizadas nas empresas (organizações) hora analisados.

Os relatórios examinados deixam clara sua importância, uma vez que elas levantaram uma série de vulnerabilidades e erros de execução, que poderiam comprometer os ativos auditados.

Alguns exemplos merecem ser citados:

- Uma das organizações, denominada organização A, não tomou nenhuma atitude após receber o relatório de auditoria de segurança, pois estava certa que não corria risco eminente e 6 meses depois sofreu um ataque cracker em seus sistemas. Como consequência teve que retirá-los do ar por quase 2 meses, para realizar atualizações e reorganizar a segurança dos meios de TI (conforme sugerido no relatório de auditoria). Não houve prejuízo financeiro, mas alguns dados foram expostos e usuários perderam acesso aos dados por algum tempo.

- Uma segunda organização, denominada organização B, achou por bem implementar as atualizações de software e programar para o futuro as atualizações de equipamentos.

- Uma terceira empresa, denominada organização C, do ramo financeiro, implementou as atualizações na integra e já tem prevista uma nova auditoria de segurança para verificar se todas as recomendações foram cumpridas. No relatório foi constatada ainda a necessidade de investimento em atualização de pessoal, que está sendo executada em etapas.

4 APRECIAÇÃO CRÍTICA E VALIDAÇÃO DO ESTUDO

Ao analisar os dados coletados através da pesquisa de campo é possível inferir que a auditoria de segurança da informação é uma função importante para uma boa administração, dando suporte a tomada de decisões. No entanto, observados os documentos de auditoria, verifica-se que ela só tem validade, se seu relatório for utilizado corretamente e não se torne só mais um documento de arquivo, para referência futura. O custo de uma auditoria, só se justifica se a intenção do administrador, for de utilizar suas informações, para a tomada de decisões, de forma efetiva e com oportunidade. Ser auditado externamente ou realizar auditoria interna, com finalidade única de ter um relatório, não se justifica.

Ao administrador não adianta saber dos problemas de segurança a que seus ativos estão expostos, se não for para embasar planejamento, previsão de investimentos e qualificação de pessoal. A auditoria de segurança deve ser adotada como parte da política de segurança da organização ou empresa, para garantir uma maior qualidade para os negócios, inclusive para garantir que funcionários tenham maior cuidado com seu trabalho, pois estarão cientes que atividades ou ações, incompatíveis com sua função, poderão ser detectadas, gerando assim responsabilidade.

Ao analisar o exemplo da organização A, acima citada, fica claro que: se o administrador tivesse adotado os procedimentos contidos no relatório de auditoria de segurança, teria sido evitada a paralização dos serviços e a exposição de dados ocorrida. Neste caso, o administrador possuía um documento produzido pela equipe de auditoria, com a finalidade de apoiar e orientar suas decisões, o qual não foi utilizado em tempo hábil, por rações diversas, resultando em vulnerabilidade para os ativos da informação da organização.

5 CONCLUSÕES

Com o presente estudo demonstrou-se que a auditoria de segurança da informação é peça importante para a manutenção do negócio, mas seu custo, ainda é um fator de preocupação

e fator restritivo para muitas organizações e empresas. Ao adotar a função auditoria de segurança, é necessário que o administrador esteja ciente de que o resultado advindo, não é a solução do problema, mas sim uma orientação de como planejar ações de curto, médio e longo prazo, e que estas ações, quando adotadas corretamente é que trarão resultados positivos ao negócio.

O estudo desnvolvido para a elaboração deste artigo, permite chegar a conclusão de que a auditoria de segurança da informação é uma ferramenta extremamente util, mostra-se eficaz e eficiente, quando os resultados apresentados são utilizados para orientar a tomada de decisão pela alta administração.

O reltório de auditoria de segurança indica ao administrador quais ações devem ser tomadas para a manutenção de níveis de segurança adequados aos seus ativos, indicando a necessidade de ações próativas, indicando necessidades de investimento, atualização de softwares, substituição de hardware e até mesmo a necessidade de treinamento de pessoal, para a execução das correções necessárias.

Assim, é possível concluir que a auditoria de segurança é peça fundamental na tomada de decisões para os administradores de empresas e organizações modernas, por permitir uma visão holística dos ativos da informação que compõe o ambiente tecnológico sob sua responsablidade, e suas possíveis vulnerabilidades. O resultado da auditoria de segurança permite que sejam adotadas ações preventivas e corretivas para a proteção dos sistemas e uma consequente melhora na proteção dos ativos da empresa auditada.

“O que não se conhece não se pode controlar. O que não se controla não se pode mensurar. O que não se mensura não se pode gerenciar. O que não se gerência não se pode aprimorar.” (SÊMOLA, 2014)

Por fim, conclui-se que a auditoria de segurança da informação é uma função importante e necessária para qualquer empresa que possua sistemas para gerenciamento dos seus negócios, não tratando-se no entanto de uma solução, mas sim um meio para sua consecução. Ao adotar a auditoria de segurança da informação como meio de apoio a decisão é necessário o entendimento de que o que fará a diferença para o negócio, não será seu relatório, mas sim as ações adotadas a partir dele.

REFERÊNCIAS

ALBANESE, R. **Managing: toward accountability for performance.** 1981. 3ª edição. Editora Homewood, Illinois.

CARNEIRO, Alberto. **Auditoria de Sistemas de Informação**. 2004. 2ª edição. Editora FCA, Lisboa – Portugal.

GERTNERS DE MAGALHÃES, Carlos Eduardo. **Auditoria em Sistemas de Informação.** Disponível em: <https://siunibanosasco.files.wordpress.com/2013/08/audit-01-apostila-auditoria-em-si.pdf>. Acesso em 18 jul. 2017.

IBRAIM, Lisboa. **Por que Tenho Medo de Ser Auditado?** Disponível em: < https://auditoriaoperacional.com.br/comentarios-finais-para-reflexao/>. Acesso em 20 nov. 2017

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação**. 2016. 3ª edição. Editora Atlas, São Paulo – SP

ISO/IEC 27001*:2013* - Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, necessidades, ISO/IEC, 2013.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008. 253 p.

MANOTTI, Alessandro. **Curso Prático - Auditoria de Sistemas:** compreenda como funciona o processo de auditoria interna e externa em sistemas de informação de uma forma prática. 2010. Editora Ciência Moderna, Rio de janeiro.

MARZANO, Roberta. **Auditoria de Riscos**. 2014. Disponível em: <https://auditoriaoperacional.com.br/auditoria-de-riscos/>. Acesso em 20 nov. 2017.

MASCARENHAS, Flávia Monken. **Avaliação De Riscos Da Administração Pública Como Subsídio Ao Planejamento De Auditoria.** Disponível em: http://*portal.tcu.gov.br.* Acesso em 15/07/2017.

NBR ISO 19011. **Diretrizes para auditorias de sistema de gestão da qualidade**, NBR. 2002.

OLIVEIRA, Djalma de Pinho Rebolças. **Sistemas de Informações Gerenciais**. 2008. 12ª edição. Editora Atlas, São Paulo.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva**.** 2014. 2ª edição. Editora Elsevier, Rio de Janeiro.

TRACY, D. **Segurança da Informação:** Uma questão de sobrevivência. 2005. Editora Scortecci, São Paulo.