CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS PARA A MELHORIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Elson Luciano Weber
Universidade do Vale do Rio dos Sinos

Rosane Machado
Universidade do Vale do Rio dos Sinos

Mônica Cristina Morás
Universidade do Vale do Rio dos Sinos

Adolfo Alberto Vanti
Universidade do Vale do Rio dos Sinos

Marcio Lizardi Lopes
Universidade do Vale do Rio dos Sinos

RESUMO

A TI está inserida nas empresas ocupando diversas funções de forma abrangente ocasionando o aumento do entendimento para seu bom gerenciamento (ALBERTIN E ALBERTIN, 2010). Nesta perspectiva se insere a avaliação da TI por meio do modelo Cobit 4.1 (*Control Objectives for Information and Related Technology*), desenvolvido pela ISACA (*Information Systems Audit and Control Association*). Atualmente é utilizado para auditar a maturidade dos processos de TI (FERNANDES E ABREU, 2012). Para Lunardi (2008) esta auditoria envolve quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte, monitoramento e avaliação, organizados em 34 processos, sendo que este trabalho contemplou apenas aqueles relacionados aos aspectos funcionais (RH). Os funcionários de uma empresa envolvidos no processo de TI devem ter conscientização (BULGURCU; CAVUSOGLU; BENBASAT, 2010) do seu funcionamento e dos riscos operacionais (IBGC, 2009) que eles podem causar. Só assim eles poderão estar atentos para seguir melhor a uma política da informação (ALBERTIN; PINOCHET, 2010) alcançando os resultados almejados (DE SORDI, 2008). O problema de pesquisa foi definido em: Como as empresas estão tratando a conscientização dos funcionários para a melhoria da política de segurança da informação? Para responder a esse problema de pesquisa se estudou a maturidade de processos de TI através do Cobit 4.1 em empresas do RS. Mais operacionalmente se examinou aspectos relacionados prioritariamente aos Planos de TI dentro das empresas e se gerou um Dashboard via Excel com Semáforo para controlar os processos e os diferentes níveis de maturidade de TI.

Palavras Chave: Conscientização. Segurança da informação. Cobit.

INTRODUÇÃO

A TI tem proporcionado novas oportunidades e competitividade às empresas, mediante a obtenção de informações de forma rápida e eficiente para tomada de decisão. Isso a torna o ambiente da TI bastante dinâmico e exige uma gestão organizada e orientada para processos. Por ser um dos bem mais valiosos das empresas, a informação deve ser mantida segura, confiável e acessível a todos que a utilizam, já que se trata de uma questão de sobrevivência no mercado.

Falhas nos sistemas de informação aumentam a vulnerabilidade e podem prejudicar confidencialidade, a disponibilidade e a integridade, os três princípios básicos da segurança da informação (SÊMOLA, 2003). E para que isso não ocorra, deve ser realizada uma análise dos riscos relacionados principalmente a tecnologia, como obsolescência de equipamentos e sistemas, vírus e invasões no sistema ou até mesmo por ações humanas, como espionagem e fraudes (SANTOS; SILVA, 2012; IBGC, 2007).

Os riscos mais graves estão relacionados os recursos humanos da empresa e a forma como os informações são tratadas dentro da organização, pois são as pessoas que diariamente integram com elas e muitas vezes geram as vulnerabilidades. Nesse sentido, cada funcionário deve estar ciente do seu papel para a proteção da informação e os riscos que ela enfrenta. Por isso que a conscientização é fundamental para a melhoria da política da segurança da informação e o atingimento dos resultados (CACIATO, 2004; BULGURCU; CAVUSOGLU; BENBASAT, 2010; FERNANDES; ABREU, 2012; DE SORDI, 2008).

As organizações precisam se preocupar com seu alinhamento estratégico e financeiro para a melhor gestão de seus recursos. Na perspectiva da TI, o melhor modelo é o Cobit 4.1 4.1 (Control Objectives for Information and Related Technology), desenvolvido pela ISACA (Information Systems Audit and Control Association). Atualmente é utilizado para auditar a maturidade dos processos de TI, esta auditoria envolve quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte, monitoramento e avaliação, organizados em 34 processos, (FERNANDES E ABREU, 2012). Este trabalho contemplou apenas aqueles domínios e processos relacionados aos aspectos funcionais (RH).

Nesta perspectiva, o objetivo deste estudo é identificar como as empresas estão tratando a conscientização dos funcionários na melhoria da política de segurança da informação. Diversos estudos tratam do assunto e por isso nota-se desta forma o interesse e a relevância que há no avanço do conhecimento mediante a análise da realidade local.

Esta pesquisa justifica-se por ser uma oportunidade de entender como as empresas estudadas estão trabalhando a conscientização dos funcionários para a melhoria da política de segurança da informação, através do estudo da maturidade dos processos de TI com o uso do Cobit 4.1 4.1. É importante, pois contextualiza uma realidade local através de uma ferramenta global, já que muitas empresas admitem não conseguir estabelecer processos adequados para gestão de TI. E também é viável, considerando que o tema abordado é de amplo interesse para comunidade acadêmica e empresarial. Além disso ampara-se nos estudos realizados por Bulgurcu, Cavusoglu e Benbasat (2010), Fernandes e Abreu (2012) , Santos e Silva (2012) e Albertin e Albertin (2010) .

Além da introdução, o artigo é composto por outras quatro seções. A primeira delas apresenta a fundamentação teórica relacionado ao tema do estudo, a segunda apresenta a metodologia da pesquisa, a terceira compreende a apresentação e análise dos dados e a quarta

e última seção traz as considerações finais. Por fim, tem-se a lista das referências pesquisadas para o desenvolvimento do artigo.

FUNDAMENTAÇÃO TEÓRICA

1. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E CONSCIENTIZAÇÃO

Cada vez mais a TI vem ganhando espaço no ambiente empresarial, devido ao papel estratégico que a informação exerce para a tomada de decisão. Neste sentido, o controle de acesso às informações é um requisito indispensável nos sistemas das organizações, visto que atualmente a grande maioria das informações de uma empresa está armazenada e é trocada entre os seus mais variados sistemas (SILVA; SANTOS, 2012, DE SORDI, 2008).

A informação deve ser considerada um ativo da empresa e seu correto gerenciamento, mantendo-a segura, confiável e acessível, é fundamental para o sucesso de qualquer organização e para auxiliar na sua permanência no mercado (CACIATO, 2004). Atualmente a maior parte das organizações trabalha com um sistema informatizado, com alta conectividade de modo que as informações fluem de maneira mais rápida, o que torna viável basear parte de seu plano de negócio e suas decisões nessas informações. Porém, toda essa tecnologia traz algumas vulnerabilidades para a organização, obrigando-a a desenvolver uma política de segurança da informação, que tem como propósito tratar essas informações desde a sua criação até o seu descarte, definindo regras para que as mesmas não sejam roubadas, alteradas ou perdidas (SÊMOLA, 2003; ALVES; MOREIRA, 2012).

A segurança dos dados de uma empresa inclui desde a preservação da integridade dos equipamentos até as informações que estão armazenadas neles. Ela consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade) e é confiável (integridade). Ou seja, a confidencialidade, a disponibilidade e a integridade são os três princípios básicos para a implementação da segurança da informação e é importante estar atento a eles em todos os momentos do ciclo de via da informação: manuseio, armazenamento, transporte e descarte (SÊMOLA, 2003; SANTOS; SILVA, 2012). Caciato (2004) ainda completa que é através desses princípios básicos que é possível preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado.

Conforme Silva (2011) pode dizer-se que os problemas de segurança estão intrinsecamente relacionados com a forma como a segurança é encarada no interior das organizações. É por isso que ela precisa de uma gestão eficiente e segura para que possa gerar valor e tornar a empresa competitiva frente ao mercado.

Para garantir a segurança das informações, análises quanto aos riscos que identifiquem ameaças quanto à integridade das informações podem ser executadas, apontando soluções que os eliminem, minimizem ou os transfiram esses riscos, conforme Santos e Silva (2012). Os riscos relacionados à tecnologia, de acordo com o IBGC (2007), são representados por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais). Desta forma, a segurança da informação geralmente abrange atividades relacionadas à segurança da infra-estrutura de TI, conscientização para a segurança da

informação, gestão de problemas de segurança, elaboração de planos de continuidade do negócio, análises de vulnerabilidade de segurança da informação, entre outras (FERNANDES; ABREU, 2012).

Devido à sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitadas (CACIATO, 2004). As ameaças são todas as situações que colocam em risco a segurança da informação. Ela pode ser qualquer ação, acontecimento ou entidade que age sobre um ativo ou pessoa, através de uma vulnerabilidade e consequentemente gera um determinado impacto. As ameaças atuam sobre os ativos e são classificadas com as mesmas categorias: ameaças físicas (normalmente decorrentes de fenômenos naturais), tecnológicas (normalmente são ataques propositados causados por agentes humanos como hackers, invasores, criadores e disseminadores de vírus, mas também por defeitos técnicos, falhas de hardware e software) e humanas (são consideradas as mais perigosas, podendo ser casos de roubos e fraudes causados por ladrões e espiões), conforme Santos e Silva (2012).

Muitas vezes a origem dos problemas não está nos meios tecnológicos, mas sim na utilização desses mesmos meios, afinal são as pessoas que interagem diariamente com os sistemas, que têm acesso à informação, que processam essa mesma informação. É por isso que as maiores ameaças para segurança da informação são ações de origem humana, que quando são exploradas podem gerar vulnerabilidade e produzir ataques, que por sua vez, causam incidentes que comprometem as informações, provocando perda de confidencialidade, disponibilidade e integridade, causando impactos aos negócios de uma organização. (SÊMOLA, 2003; SANTOS; SILVA, 2012; SILVA, 2011; CACIATO, 2004). Diante deste fato, várias empresas reconhecem que seus funcionários, que são muitas vezes considerados o elo mais fraco da segurança da informação, podem também ser grandes ativos no esforço para reduzir os riscos relacionados a ela (BULGURCU; CAVUSOGLU; BENBASAT, 2010).

Todos os funcionários de uma empresa, envolvidos no processo de TI devem estar conscientes do seu funcionamento e dos riscos envolvidos, pois só assim eles poderão estar atentos para controlar as falhas que podem surgir e observar se os resultados almejados estão sendo atingidos (FERNANDES; ABREU. 2012; DE SORDI, 2008). Nesse sentido as empresas precisam adotar políticas de segurança da informação e inseri-las na cultura organizacional. É por isso que conscientização dos funcionários sobre os riscos envolvidos no processo é fundamental. De acordo com Fernandes e Abreu (2012), a política de segurança da informação consiste na determinação de diretrizes e ações referentes à segurança dos aplicativos, da infra-estrutura, dos dados, pessoas e organizações (fornecedores e parceiros).

Um aspecto importante para o sucesso das políticas de segurança é a comunicação das mesmas a todos os elementos da organização, para que estes as compreendam, estejam sensíveis a elas e, por conseguinte, as cumpram. Deste modo, a política de segurança deve conter diretrizes claras sobre os seguintes aspectos (SILVA, 2011):

- Objetivos de segurança: devem explicar de forma rápida e sucinta a finalidade da política de segurança.
- A quem se destina: deve definir claramente quais as estrutura organizacionais às quais a mesma se aplica.
- Propriedade dos recursos: deve definir de forma clara as regras que irão reger os diversos aspectos relacionados com a propriedade dos recursos da informação.
- Responsabilidade: deve definir claramente qual o tipo de responsabilidades envolvidas com o manuseamento dos recursos da informação.

- Requisitos de acesso: deve indicar de forma clara quais os requisitos a serem atendidos para o acesso aos recursos da informação.
- Responsabilidade: deve indicar as medidas a serem tomadas no caso das normas serem infringidas.
- Generalidades: nesta seção podem ser incluídos aspectos que não caibam nas demais seções, como normas acessórias.

O objetivo da criação da política de segurança da informação é fazer com que os funcionários fiquem cientes dos riscos relacionados à segurança da informação e para educá-los sobre suas responsabilidades relativas a esses riscos. Eles precisam estar cientes das ameaças que a empresa sofre ao ter suas informações expostas. Desta forma, funcionários que usam a informação e recursos tecnológicos de suas organizações são responsáveis pela proteção desses recursos e por isso é importante conscientizar um empregado para executar essas funções e assumir as suas responsabilidades (BULGURCU; CAVUSOGLU; BENBASAT, 2010; CACIATO, 2004).

Em pesquisa realizada, Bulgurcu, Cavusoglu e Benbasat (2010) observaram que fatores motivacionais têm efeitos positivos no cumprimento da segurança da informação. Mas antes de cumprir as políticas, primeiro o empregado avalia os benefícios percebidos de cumprimento, o custo de conformidade percebida, e o custo percebida descumprimento. Ou seja, os funcionários precisam crer que o cumprimento das políticas de segurança da informação da empresa trará resultados positivos para si. Já o uso de recompensas deve ser feito com cuidado, pois muitos podem entender que a segurança está condicionada a recebimento de algo em troca, ou invés de ser obrigatória. Por isso a importância da comunicação interna dos riscos através de treinamentos e programas específicos para esse fim. E neste mesmo sentido, os gestores devem se esforçar para simplificar os procedimentos de segurança que os empregados são obrigados a cumprir, visto que muitos consideram um processo oneroso e desnecessário, como por exemplo, a troca de senha a cada dois meses (BULGURCU; CAVUSOGLU; BENBASAT, 2010; DE SORDI, 2008).

É importante saber que a política de segurança da informação protege a informação das empresas de vários riscos, tanto que Albertin e Pinochet (2010) relatam que empresas estão atribuindo maior importância aos aspectos do relacionamento com clientes, privacidade e segurança e alinhamento estratégico, sendo que o aspecto de privacidade e segurança é considerado um dos itens mais críticos. Para minimizar a vulnerabilidade aos riscos e saber como estão os processos relacionados a TI, existe a ferramenta Cobit 4.1 4.1 que avalia a maturidade dos processos de TI, e que consequentemente auxilia no aumento da conscientização do funcionário, como será apresentado a seguir.

2. MATURIDADE DOS PROCESSOS DE TI

A TI está inserida nas empresas, ocupando diversos papéis e de forma muito abrangente, o que aumenta a necessidade do seu entendimento e bom gerenciamento. A Governança de TI, que tem como principal objetivo atender às necessidades de negócio da organização, pode ser definida como a responsável pelas decisões referentes ao uso da TI e sua administração (ALBERTIN; ALBERTIN, 2010), possui os pilares fundamentais, representadas por cinco áreas: alinhamento estratégico, entrega de valor, gestão de riscos, gestão de recursos e mensuração de desempenho.

De acordo com Albertin e Albertin (2010), a linha condutora de todo o processo é o alinhamento estratégico, pois permite que as estratégias e os objetivos organizacionais sejam repassados para a TI, da mesma maneira que as estratégias de TI sejam avaliadas e aprovadas

pela organização. Esses pilares estão relacionados ao bom desenvolvimento das atividades e da segurança da informação. Desta forma a Governança de TI é um fator essencial para a gestão da empresa, tanto a nível estratégico, como financeiro.

Nas duas últimas décadas vem surgindo e sendo elaborada uma série de modelos de melhores práticas para TI. Um deles é o Cobit 4.1 4.1 (Objectives for Information and Related Technology), um modelo abrangente aplicável para a auditoria e controle de processos de TI, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos (FERNANDES E ABREU, 2012; ALBERTIN; ALBERTIN, 2010). Ele é formulado em framework, recomendado pelo ISACA (Information Systems Audit and Control Foundation) e seu principal objetivo é contribuir para o sucesso da entrega de produtos e serviços de TI, a partir da perspectiva das necessidades do negócio, com foco mais acentuado no controle do que na execução. De acordo com o ITGI, neste sentido, o Cobit 4.1 4.1:

- Estabelece relacionamentos com os requisitos do negócio.
- Organiza as atividades de TI em um modelo de processos genéricos.
- Identifica os principais recursos de TI, nos quais deve haver mais investimento.
- Define os objetivos de controle que devem ser considerados para a gestão.

O modelo Cobit 4.1 4.1 é genérico o bastante para representar todos os processos normalmente encontrados nas funções de TI e compreensíveis tanto para a operação como para os gerentes de negócios, pois cria uma ponte entre o que o pessoal operacional precisa executar e a visão que os executivos desejam ter para administrar, (FERNANDES; ABREU, 2012). Nesse sentido, utilizando como matriz o ciclo tradicional da melhoria continua (planejar, construir, executar, monitorar), o Cobit 4.1 4.1 possui 34 processos de TI baseados em quatro domínios, que Espelham os agrupamentos usuais existentes em uma organização padrão de TI (FERNANDES; ABREU, 2012; ALBERTIN; ALBERTIN, 2010).

A correta gestão e execução desses domínios auxilia no alcance de possíveis resultados positivos, através do alcance dos objetivos. Segundo Fernandes e Abreu (2012), um dos maiores desafios das empresas é observar o nível de profundidade que deve ser adotado pelos mecanismos de controle e medição de desempenho. Por isso que antes da implementação da Governança de TI, é preciso avaliar a organização, identificando os pontos fracos dos processos e controles mais importantes, ou seja, como ela está posicionada em relação a governança de TI e qual o seu grau de maturidade. A identificação desse posicionamento é realizada através do Modelo de Maturidade dos Processos de TI, do Cobit 4.1 4.1, que permite que a organização identifique, de forma clara, o seu perfil atual e estabeleça as metas que pretende alcançar (ITGI, 2007; FERNANDES; ABREU, 2012). Ou seja, o Modelo de Maturidade é composto por critérios de avaliação da maturidade dos processos, que viabilizam a decisão de investimento nos processos considerados mais importantes para a TI, no âmbito da instituição. Desta forma, conforme explicam Fernandes e Abreu (2012), para cada processo de TI, é estabelecido um modelo de maturidade baseado em níveis, através do qual uma organização poderá ser avaliada como:

- Nível 0 (Inexistente): Processos de gestão não são aplicados.
- Nível 1 (Inicial): Processos são esporádicos e desorganizados, com abordagens de gestão aplicadas caso a caso.
- Nível 2 (Repetitivos mas Intuitivo): Processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
- Nível 3 (Definido): Processos são padronizados, documentados e comunicados.

- Nível 4 (Gerenciado e Mensurável): Processos são monitorados e medidos quanto à conformidade como os procedimentos, e ações são tomadas quando os resultados não são efetivos.
- Nível 5 (Otimizado): Boas práticas são seguidas e automatizadas, com base em resultados de melhorias contínuas e de ações de modelagem de maturidade junto a outras empresas.

O Modelo de Maturidade deve ser utilizado constantemente ao longo do processo, a partir da análise dos resultados de cada etapa, correção da trajetória sempre que necessário e auxilio na determinação de prioridades (ITGI, 2007). Isso porque é a partir deles que é possível mapear a situação atual da organização, comparar com a situação das melhores organizações no segmento (benchmarking), comparar com padrões internacionais e estabelecer e monitorar passo a passo as melhorias dos processos rumo à estratégia da organização.

Fernandes e Abreu (2012) ainda ressaltam que é de extrema importância o entendimento dos estágios de maturidade em que se encontra a organização de TI, de forma que se possa realizar um planejamento adequado do programa de Governança de TI e identificar aquelas vulnerabilidades mais gritantes, que merecem uma atenção imediata, já que nenhum empreendimento de longo prazo sobrevive sem resultados de curto prazo.

3. MÉTODO

Realizou-se uma pesquisa com característica quantitativa, coletada mediante questionário disponibilizado via formulário eletrônico (*Google doc's*) junto a funcionários de diversas empresas escolhidos aleatoriamente por acessibilidade junto a estudantes de uma grande universidade situada no Vale do Rio dos Sinos.

O instrumento foi construído por meio dos 34 processos do Cobit 4.1 4.1, considerando os seis níveis de maturidade. Destes processos, seis foram selecionados em razão de sua relação aos aspectos funcionais (RH) da TI.

Posteriormente foram analisados e tabulados no software SPSS (*Statistical Package for the Social Scienses*), gerando gráficos, relatórios, estatísticas descritivas a partir dos dados lançados. Estes dados foram trabalhados de uma maneira exclusivamente acadêmica.

Destaca-se que o uso da estatística descritiva permitiu a análise de forma cruzada entre os Processos de TI e com os níveis de importância (alta, média e baixa), possibilitando a construção de um *dashboard.*

4 ANÁLISE DOS DADOS

Os dados evidenciados através da realização desta pesquisa foram analisados por meio de tabulações, onde foram cruzadas as respostas fornecidas pelos participantes da pesquisa com o objetivo de examinar o nível de maturidade dos Planos de TI adotados pelas empresas, e também como as empresas estão lidando com a conscientização dos funcionários perante o risco de uma política da informação.

4.1 TABULAÇÕES CRUZADAS

As tabulações que estão descritas ao longo deste capítulo foram baseadas em cruzamentos de dados realizados no software SPSS.

4.1.1 INÍCIO DAS TABULAÇÕES

A primeira tabulação realizada foi com o cruzamento dos dados da questão PO1 (Define o planejamento estratégico de TI. A empresa dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio) com a questão PO6 (A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização), pois uma empresa poderá conscientizar seus funcionários perante os riscos somente se houver definido em sua empresa um Plano de TI. Então realizando este cruzamento, classificando as empresas pelos seus portes (Micro, Pequeno, Médio ou Grande), verificou-se que entre as empresas pesquisadas somam-se 12,5% que descreveram a questão PO1 como Inexistente, todas eram de porte Micro ou Pequeno, e a grande maioria também classificou como Inexistente a questão PO6. Esse dado evidencia que a pesquisa apresenta grande coerência, pois uma empresa só poderá comunicar as metas de TI para a equipe se houver um Plano de TI em funcionamento dentro da empresa.

Através desta mesma tabulação verificou-se que a porcentagem de empresas que classificaram sua empresa na questão PO1 como Inicial foi de 21,9%, dentre elas 85% eram de porte Micro e Médio. Considerando estas, apenas uma empresa que não se auto classificou como Inexistente ou Inicial na questão PO6.

As empresas que descreveram a questão PO1 como Repetitivo representam 9,4% do total de entrevistados, onde 8,6% são de porte Pequeno e 4,3% de porte Médio. Todas as empresas de porte Médio se classificaram como Gerenciado na questão PO6, enquanto que as empresas de porte pequeno se dividiram entre Inicial e Inexistente.

Quanto aos 25% das empresas que se denominaram como Definido para a questão PO1, 62,5% delas eram de porte Grande e nenhuma de porte Micro. Entre as empresas de porte Grande, as respostas para a questão PO6 de dividiram entre Definido, Gerenciado e Otimizado.

Somando as empresas que responderam Gerenciado para a questão PO1 obteve-se um total de 18,8%, sendo destes 12,5% de porte Grande e 6,3% de porte Médio. Apenas 33,3% destas empresas também se classificaram como Gerenciado para a questão PO6.

Porte da empresa: * PO1 - Define o planejamento estratégico de TI. * PO6 - Comunica as metas e diretrizes gerenciais. Crosstabulation

PO6 - Comunica as metas e diretrizes gerenciais.			PO1 - Define o planejamento estratégico de TI.						Total
			Definido	Gerenciado	Inexistente	Inicial	Otimizado	Repetitivo	
Definido	Porte da empresa:	Grande	66,7%	33,3%		0,0%			100,0%
		Média	100,0%	0,0%		0,0%			100,0%
		Pequena	0,0%	0,0%		100,0%			100,0%
	Total		60,0%	20,0%		20,0%			100,0%
Gerenciado	Porte da empresa:	Grande	50,0%	50,0%				0,0%	100,0%
		Média	0,0%	0,0%				100,0%	100,0%
	Total		40,0%	40,0%				20,0%	100,0%
Inexistente	Porte da empresa:	Média	0,0%		0,0%	100,0%		0,0%	100,0%
		Micro	0,0%		66,7%	33,3%		0,0%	100,0%
		Pequena	33,3%		33,3%	0,0%		33,3%	100,0%
	Total		12,5%		37,5%	37,5%		12,5%	100,0%
Inicial	Porte da empresa:	Grande		0,0%	0,0%	100,0%		0,0%	100,0%
		Média		100,0%	0,0%	0,0%		0,0%	100,0%
		Micro		0,0%	0,0%	100,0%		0,0%	100,0%
		Pequena		0,0%	50,0%	0,0%		50,0%	100,0%
	Total			28,6%	14,3%	42,9%		14,3%	100,0%
Otimizado	Porte da empresa:	Grande	20,0%	20,0%			60,0%		100,0%
	Total		20,0%	20,0%			60,0%		100,0%
Repetitivo	Porte da empresa:	Média	50,0%				50,0%		100,0%
	Total		50,0%				50,0%		100,0%
Total	Porte da empresa:	Grande	38,5%	30,8%	0,0%	7,7%	23,1%	0,0%	100,0%
		Média	25,0%	25,0%	0,0%	25,0%	12,5%	12,5%	100,0%
		Micro	0,0%	0,0%	40,0%	60,0%	0,0%	0,0%	100,0%
		Pequena	16,7%	0,0%	33,3%	16,7%	0,0%	33,3%	100,0%
	Total		25,0%	18,8%	12,5%	21,9%	12,5%	9,4%	100,0%

Fonte: Dados da Pesquisa (2013).

Em relação às empresas que se classificaram na questão PO1 como Otimizado, 9,4% eram de porte Grande e 3,1% de porte Médio somando um total de 12,5%. Todas as empresas de porte Grande responderam também Otimizado para a questão PO6, enquanto que as empresas de porte Médio se descreveram como Repetitivo para esta questão.

4.1.2 CRUZAMENTO DE DADOS PO1 X PO7

O próximo cruzamento de dados envolveu novamente a questão PO1 (Define o planejamento estratégico de TI. A empresa dispõe de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio) e juntamente com ela os dados da questão PO7 (Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI). Dessa tabulação foram identificados os resultados que seguem.

Entre as empresas que se denominaram Inexistente na questão PO1, metade delas também se denominaram Inexistente para a questão PO7, e a outra metade se classificou como Inicial.

As empresas respondentes que marcaram Inicial na questão PO1 também se denominaram Inicial e Inexistente para a questão PO7. Dentre as empresas que se identificaram como Repetitivo na questão PO1, todas elas alegaram ter um desempenho Inexistente para a questão PO7. Considerando as empresas que responderam Definido para a questão PO1, o maior percentual dentre elas foi também das que se denominaram como Definido para a questão PO7.

PO7 - Gerencia os recursos humanos de TI. * PO1 - Define o planejamento estratégico de TI. Crosstabulation

		PO1 - Define o planejamento estratégico de TI.						Total
		Definido	Gerenciado	Inexistente	Inicial	Otimizado	Repetitivo	
PO7 - Gerencia os recursos humanos de TI.	Definido	60,0%	40,0%	0,0%	0,0%	0,0%	0,0%	100,0%
	Gerenciado	22,2%	44,4%	0,0%	0,0%	33,3%	0,0%	100,0%
	Inexistente	8,3%	0,0%	25,0%	41,7%	0,0%	25,0%	100,0%
	Inicial	25,0%	0,0%	25,0%	50,0%	0,0%	0,0%	100,0%
	Otimizado	0,0%	0,0%	0,0%	0,0%	100,0%	0,0%	100,0%
	Repetitivo	100,0%	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total		25,0%	18,8%	12,5%	21,9%	12,5%	9,4%	100,0%

Fonte: Dados da Pesquisa (2013).

Percebe-se que a maior parte das empresas que denominaram seu desempenho como Gerenciado na questão PO1, também se denominaram como Gerenciado para a questão PO7.

Por último, entre as empresas que se classificaram como Otimizado na questão PO1, apenas 25% delas se denominaram Otimizado na questão PO7, enquanto que os outros 75% se classificaram como Gerenciado.

4.1.3 PLANO DE TI E A GESTÃO DE RISCOS

Nesta tabulação foram cruzados os dados das questões PO1 e PO9, que enfatizam respectivamente (PO1 - Define o planejamento estratégico de TI. A empresa dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio. PO9 - Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência). Com o objetivo de identificar se as empresas estão tendo uma preocupação com os riscos que o mau uso da TI pode causar dentro da empresa, as empresas foram divididas pelo seu porte, e dessa forma obteve-se os resultados que seguem.

Inicialmente identificou-se um resultado um tanto quanto curioso, pois duas empresas que responderam Inexistente para a questão PO1, o que indica que não possuem um plano de TI efetivo em atividade em sua empresa, alegaram ter um desempenho Inicial para a questão PO9. Ainda entre as empresas que descreveram seu desempenho como Inexistente para a questão PO1, uma empresa descreveu o seu desempenho como Gerenciado para a questão PO9.

Em meio aos 21,9% das empresas que descreveram suas atividades da questão PO1 como Inicial, 57,1% também descreveram como sendo Inicial a gestão de riscos questionada na questão PO9, e as outras 42,9% se denominaram como Inexistente.

Dentre as 9,4% empresas que consideram seu desempenho como Repetitivo na questão PO1, ocorreu uma divisão exata da percentagem na questão PO9, porque entre as empresas pesquisadas identificou-se que: 33,3% marcaram Repetitivo (porte Pequeno), 33,3% marcaram Definido (porte Pequeno), e 33,3% marcaram Gerenciado (porte Médio).

Considerando as empresas que marcaram Definido na questão PO1, o maior índice de frequência dentre elas também foi o das empresas que responderam Definido para a questão PO7.

As empresas que se identificaram como Gerenciado na questão PO1 somaram um total de 18,8%, dentre elas 66,7% também se identificaram como gerenciado na questão PO9.

PO1 - Define o planejamento estratégico de TI. * PO9 - Avalia e gerencia os riscos. Crosstabulation

		PO9 - Avalia e gerencia os riscos.						
		Definido	Gerenciado	Inexistente	Inicial	Otimizado	Repetitivo	Total
PO1 - Define o planejamento estratégico de TI.	Definido	37,5%	0,0%	12,5%	12,5%	25,0%	12,5%	100,0%
		60,0%	0,0%	20,0%	14,3%	28,6%	50,0%	25,0%
	Gerenciado	16,7%	66,7%	0,0%	0,0%	16,7%	0,0%	100,0%
		20,0%	66,7%	0,0%	0,0%	14,3%	0,0%	18,8%
	Inexistente	0,0%	25,0%	25,0%	50,0%	0,0%	0,0%	100,0%
		0,0%	16,7%	20,0%	28,6%	0,0%	0,0%	12,5%
	Inicial	0,0%	0,0%	42,9%	57,1%	0,0%	0,0%	100,0%
		0,0%	0,0%	60,0%	57,1%	0,0%	0,0%	21,9%
	Otimizado	0,0%	0,0%	0,0%	0,0%	100,0%	0,0%	100,0%
		0,0%	0,0%	0,0%	0,0%	57,1%	0,0%	12,5%
	Repetitivo	33,3%	33,3%	0,0%	0,0%	0,0%	33,3%	100,0%
		20,0%	16,7%	0,0%	0,0%	0,0%	50,0%	9,4%
Total		15,6%	18,8%	15,6%	21,9%	21,9%	6,2%	100,0%
		100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fonte: Dados da Pesquisa (2013).

Outro item curioso que esta pesquisa apontou foi que 100% das empresas que caracterizaram seu desempenho como Otimizado na questão PO1, também o fizeram na questão PO9. Sendo que 75% destas empresas eram de porte Grande e 25% de porte Médio. Este dado indica que uma empresa que dispõem de um Plano de TI eficiente baseado em um plano estratégico de negócio, deve estar preocupada com o quadro de gestão de riscos, analisando ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência. Para se alcançar bons resultados, as empresas devem buscar aliar seu Plano de TI com a gestão de riscos.

4.1.4 COMUNICAÇÃO VERSUS TREINAMENTO

Para esta tabulação, foram cruzados os dados referentes à questão PO6 (A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização) e a questão AI4 (Disponibiliza documentação e treinamento para os usuários e profissionais de TI para correta utilização dos sistemas e infraestrutura de TI). Através desse cruzamento de dados foi buscado evidências que possam ser relevantes nesta pesquisa.

Entre os 15,6% das empresas que consideram seu desempenho Inexistente para a questão AI4, 60% destas também se definiram como Inexistente na questão PO6. Dos 18,8% das empresas que consideram seu desempenho como Inicial para a questão AI4, 83,3% delas têm um desempenho Inicial ou Inexistente para a questão PO6, o que evidencia que a maioria das empresas que não estabelecem e comunicam as metas de TI para a equipe também não disponibilizam treinamento para os usuários e profissionais de TI para uma correta utilização dos sistemas e infraestrutura de TI.

AI4 - Desenvolve e mantém procedimentos de TI. * PO6 - Comunica as metas e diretrizes gerenciais. Crosstabulation

		PO6 - Comunica as metas e diretrizes gerenciais.						
		Definido	Gerenciado	Inexistente	Inicial	Otimizado	Repetitivo	Total
AI4 - Desenvolve e mantém procedimentos de TI.	Definido	16,7%	66,7%	16,7%	0,0%	0,0%	0,0%	100,0%
		20,0%	80,0%	12,5%	0,0%	0,0%	0,0%	18,8%
	Gerenciado	33,3%	0,0%	0,0%	16,7%	33,3%	16,7%	100,0%
		40,0%	0,0%	0,0%	14,3%	40,0%	50,0%	18,8%
	Inexistente	20,0%	0,0%	60,0%	20,0%	0,0%	0,0%	100,0%
		20,0%	0,0%	37,5%	14,3%	0,0%	0,0%	15,6%
	Inicial	0,0%	0,0%	50,0%	33,3%	0,0%	16,7%	100,0%
		0,0%	0,0%	37,5%	28,6%	0,0%	50,0%	18,8%
	Otimizado	0,0%	25,0%	0,0%	0,0%	75,0%	0,0%	100,0%
		0,0%	20,0%	0,0%	0,0%	60,0%	0,0%	12,5%
	Repetitivo	20,0%	0,0%	20,0%	60,0%	0,0%	0,0%	100,0%
		20,0%	0,0%	12,5%	42,9%	0,0%	0,0%	15,6%
Total		15,6%	15,6%	25,0%	21,9%	15,6%	6,2%	100,0%
		100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fonte: Dados da Pesquisa (2013).

Destaca-se que dos 18,8% das empresas que responderam Definido para a questão AI4, 66,7% destas responderam Gerenciado para a questão PO6. Dentre os 18,8% das empresas que se descreveram como Gerenciado para a questão AI4, 66,6% delas havia se descrito como Definido ou Otimizado na questão PO6. Esses dados evidenciam que empresas que se preocupam em comunicar as metas de TI para a equipe também se preocupam em proporcionar um treinamento aos usuários e profissionais da TI para uma correta utilização dos sistemas e infraestrutura de TI. Outro dado que vem ao encontro dessa evidência é que 75% das empresas que se denominaram como Otimizado para a questão AI4, também haviam se denominado como Otimizado para a questão PO6, e os outros 25% das empresas se caracterizaram como Gerenciado.

4.1.5 DISPONIBILIZA E MANTÉM O TREINAMENTO DOS USUÁRIOS

Nesta tabulação foram cruzados os dados da questão AI4 (Disponibiliza documentação e treinamento para os usuários e profissionais de TI para correta utilização dos sistemas e infraestrutura de TI) com os dados da questão DS7 (A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação). Essa tabulação veio com o objetivo de buscar evidências que comprovem que as empresas além de treinar sua equipe de funcionários sobre a correta utilização dos sistemas de TI, também mantém treinamentos que desenvolvem a capacidade de aprimorar o uso da TI fazendo com que ela se torne mais eficiente e eficaz. Então através do cruzamento dos dados verificamos as evidências que seguem.

Dos 34,4% das empresas que se caracterizaram como Inexistente ou Inicial na questão AI4, apenas uma empresa que não se caracterizou também como Inexistente ou Inicial na questão DS7.

AI4 - Desenvolve e mantém procedimentos de TI. * DS7 - Educa e treina os usuários. Crosstabulation

		DS7 - Educa e treina os usuários.						
		Definido	Gerenciado	Inexistente	Inicial	Otimizado	Repetitivo	Total
AI4 - Desenvolve e mantém procedimentos de TI.	Definido	33,3%	16,7%	16,7%	0,0%	16,7%	16,7%	100,0%
		40,0%	11,1%	16,7%	0,0%	50,0%	25,0%	18,8%
	Gerenciado	0,0%	83,3%	0,0%	0,0%	16,7%	0,0%	100,0%
		0,0%	55,6%	0,0%	0,0%	50,0%	0,0%	18,8%
	Inexistente	0,0%	0,0%	60,0%	40,0%	0,0%	0,0%	100,0%
		0,0%	0,0%	50,0%	33,3%	0,0%	0,0%	15,6%
	Inicial	0,0%	0,0%	33,3%	50,0%	0,0%	16,7%	100,0%
		0,0%	0,0%	33,3%	50,0%	0,0%	25,0%	18,8%
	Otimizado	50,0%	50,0%	0,0%	0,0%	0,0%	0,0%	100,0%
		40,0%	22,2%	0,0%	0,0%	0,0%	0,0%	12,5%
	Repetitivo	20,0%	20,0%	0,0%	20,0%	0,0%	40,0%	100,0%
		20,0%	11,1%	0,0%	16,7%	0,0%	50,0%	15,6%
Total		15,6%	28,1%	18,8%	18,8%	6,2%	12,5%	100,0%
		100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fonte: (Dados da Pesquisa, 2013).

Entre as empresas que se caracterizaram como Otimizado na questão AI4, 50% delas se definiram como Definido para a questão DS7 e os outros 50% se definiram como Gerenciado. Essa evidência mostra que há uma maior preocupação por parte das empresas de treinar sua equipe de funcionários para uma correta utilização dos sistemas de TI, do que capacitar a equipe de funcionários para tornar o uso da TI mais eficiente e eficaz.

4.1.6 QUESTÃO PO1 E O SEU NÍVEL DE IMPORTÂNCIA DENTRO DA EMPRESA

Realizando o cruzamento dos dados da questão PO1 com o seu nível de importância, evidenciou-se que 25% das empresas que se denominaram como Inexistentes na questão PO1 declararam dar um alto nível de importância para esta questão dentro da empresa. Inicialmente este dado aparenta ser contraditório, mas esta porcentagem é referente as empresas de porte pequeno, que ainda não conseguiram adotar um Plano de TI.

PO1 - Define o planejamento estratégico de TI. * PO1 - Nível de importância Crosstabulation

		PO1 - Nível de importância				
			Alto	Baixo	Médio	Total
PO1 - Define o planejamento estratégico de TI.	Definido	12,5%	75,0%	0,0%	12,5%	100,0%
	Gerenciado	0,0%	33,3%	0,0%	66,7%	100,0%
	Inexistente	0,0%	25,0%	25,0%	50,0%	100,0%
	Inicial	14,3%	28,6%	0,0%	57,1%	100,0%
	Otimizado	0,0%	75,0%	0,0%	25,0%	100,0%
	Repetitivo	0,0%	33,3%	0,0%	66,7%	100,0%

Fonte: (Dados da Pesquisa, 2013).

Entre as empresas que se denominaram como Otimizado para a questão PO1, 75% delas declararam dar um alto nível de importância para esta questão, e os outros 25% declararam dar um nível médio de importância.

4.1.7 NÍVEL DE IMPORTÂNCIA DA QUESTÃO PO6 COM A QUESTÃO PO7

Por meio da realização do cruzamento dos dados dos níveis de importância da questão PO6 e PO7, evidenciou-se que está sendo atribuido um maior grau de importância para a comunicação das metas de TI para a equipe e as políticas de TI para a organização do que para o desenvolvimento de um plano de capacitação e desenvolvimento de pessoal.

PO6 - Nível de importância * PO7 - Nível de importância Crosstabulation

		PO7 - Nível de importância			
		Alto	Baixo	Médio	Total
PO6 - Nível de importância		0,0%	0,0%	100,0%	100,0%
		0,0%	0,0%	7,1%	3,1%
	Alto	33,3%	16,7%	50,0%	100,0%
		57,1%	18,2%	42,9%	37,5%
	Baixo	27,3%	54,5%	18,2%	100,0%
		42,9%	54,5%	14,3%	34,4%
	Médio	0,0%	37,5%	62,5%	100,0%
		0,0%	27,3%	35,7%	25,0%
Total		21,9%	34,4%	43,8%	100,0%
		100,0%	100,0%	100,0%	100,0%

Fonte: Dados da Pesquisa (2013).

Esta evidência esta fundamentada na porcentagem das empresas que atribuíram um alto nível de importância para estas questões, sendo que 37,5% para a questão PO6 e 21,9% para a questão PO7.

CONSIDERAÇÕES FINAIS

O nível de conscientização percebido nas pequenas empresas evidencia que apesar de não existir um plano de TI atribui um alto nível de importância para este aspecto. Isto foi encontrado na análise da relação entre o planejamento estratégico de TI e seu nível de importância.

PO1 - Define o planejamento estratégico de TI. * PO1 - Nível de importância Crosstabulation

		PO1 - Nível de importância				
			Alto	Baixo	Médio	Total
PO1 - Define o planejamento estratégico de TI.	Definido	12,5%	75,0%	0,0%	12,5%	100,0%
	Gerenciado	0,0%	33,3%	0,0%	66,7%	100,0%
	Inexistente	0,0%	25,0%	25,0%	50,0%	100,0%
	Inicial	14,3%	28,6%	0,0%	57,1%	100,0%
	Otimizado	0,0%	75,0%	0,0%	25,0%	100,0%
	Repetitivo	0,0%	33,3%	0,0%	66,7%	100,0%

Outras análises foram realizadas e como produto destas foi construído um sintético Dashboard de controle mediante semáforos para gerenciar os níveis de maturidade dos processos de TI. Após ser gerada uma primeira aplicação de dashboard que não foi validada no grupo de pesquisa, gerou-se uma nova aplicação mais robusta e validada, representada pela figura 2 com maior rigor de extração das informações. Ambas aplicações possuem foco acadêmico e usam dados fornecidos por empresas mas que não são usados para uso comercial fora do ambiente de atuação do grupo de pesquisa Gestão de Tecnologia da Informação Unisinos/CNPQ.

Figura 2: Dashboard de controle dos processos de TI

Nível	Inexistente	Inicial	Repetitivo	Definido	Gerenciado	Otimizado	Total
PO5	3	3	3	7	8	8	32
PO7	12	4	1	5	9	1	32
AI1	3	3	4	7	6	9	32
AI2	5	3	1	10	9	4	32
AI3	3	4	3	7	8	7	32
AI6	4	3	5	8	6	6	32
DS1	3	4	3	8	8	6	32
DS2	3	4	0	6	8	11	32
DS4	2	3	2	4	13	7	31
DS9	6	4	3	7	7	5	32
DS10	7	3	3	6	10	3	32
DS11	5	4	4	5	7	7	32
DS12	6	4	2	9	9	2	32
MO1	7	3	2	8	6	6	32
MO3	5	4	2	5	11	5	32
MO4	5	4	4	6	6	7	32

Fonte: Dados da Pesquisa (2013).

A identificação como as empresas estão tratando a conscientização dos funcionários na melhoria da política de segurança da informação foi contemplada neste trabalho através de análise estatística de dados bem como pela geração de um dashboard desenvolvido via Excel, considerando uma segunda aplicação já que a primeira apresentou problema de extração de informação. Tanto um instrumento quanto o outro permite ao gestor visualizar e gerenciar melhor a conscientização de seus funcionários perante os processos de tecnologia da informação, permitindo assim reduzir riscos operacionais em TI.

Salienta-se aqui que o *dashboard* apresentado não realiza análises estatísticas. Estas foram efetivadas via SPSS com dados exclusivos da pesquisa e do referido grupo de pesquisa Unisinos/CNPQ.

REFERÊNCIAS

ALBERTIN, Alberto Luiz; PINOCHET, Luis Hernan Contreras. **Política de Segurança de Informações.** Rio de Janeiro: Campus, 2010.

ALBERTIN, Rosa Maria de Moura; ALBERTIN, Alberto Luiz. **Estratégias de governança de tecnologia da informação.** São Paulo: Elsevier, 2010.

ALVES, Luiz Cláudio Macena; MOREIRA, Jander. Gerenciamento da Política de Segurança da Informação. T.I.S, São Carlos, V.1, n. 2, p. 130-137, set-dez. 2012, Disponível em http://revistatis.dc.ufscar.br/index.php/revista/about

BULGURCU, Burcu; CAVUSOGLU, Hasan; BENBASAT, Izak. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **MIS Quarterly.** Vol.34, n.3, p.523-548, set, 2010.

CACIATO, Luciano Eduardo. **Gerenciamento da Segurança de Informação em Redes de**

Computadores e a Aplicação da Norma ISO/IEC 17799:2001. Campinas, 2004. Disponível em Disponível em: <http://www.rau-tu.unicamp.br/>.

DE SORDI, José Osvaldo. **Gestão por processos: uma abordagem da moderna administração.** 2.ed. São Paulo: Saraiva, 2008.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. São Paulo: 3ª ed. Brasport, 2012.

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa.** São Paulo, 2009.

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de Orientação para Gerenciamento de Riscos Corporativos. 2007. Disponível em: <http://www.ictsglobal.com/new/arquivos/IBGC-orientacaogerriscoscorporativos.pdf>.

ISACA: Information Systems Audit and Control Association, Disponível em http://www.isaca.org/

ITGI: Information Technology Governance Institute. Cobit 4.1 4.1 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. Disponível em: http:// www.isaca.org/

SANTOS, Diana Luísa Rocha; SILVA, Rita Maria Santos. **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001**. Dissertação (Mestrado) – Mestrado em Ciência da Informação, Faculdade de Engenharia da Universidade do Porto. 2012.

SÊMOLA, M. **Gestão da Segurança da Informação** – Uma visão executiva. 3. Ed. Rio de Janeiro: Elsevier, 2003. 160p.

SILVA, Bruna Patricia Ribeiro Alves da. **Planeamento e Implementação de um Sistema de Gestão da Segurança da Informação**. Dissertação (Mestrado) – Mestrado em Ciência da Informação, Faculdade de Engenharia da Universidade do Porto. 2011.