UNIVERSIDADE PAULISTA

PROGRAMA DE MESTRADO EM ENGENHARIA DE PRODUÇÃO

ANÁLISE DO IMPACTO DA SEGURANÇA DA INFORMAÇÃO NA COMPETITIVIDADE DAS PEQUENAS E MÉDIAS EMPRESAS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

EMERSON JOSÉ BENETON

SÃO PAULO

2015

UNIVERSIDADE PAULISTA

PROGRAMA DE MESTRADO EM ENGENHARIA DE PRODUÇÃO

ANÁLISE DO IMPACTO DA SEGURANÇA DA INFORMAÇÃO NA COMPETITIVIDADE DAS PEQUENAS E MÉDIAS EMPRESAS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

Orientador: Prof. Dr. Rodrigo Franco Gonçalves

Área de Concentração: Gestão de Sistemas de Operação

Linha de Pesquisa: Redes de Empresas e Planejamento da Produção

Projeto de Pesquisa: Gestão da produção de software e mídias interativas.

EMERSON JOSÉ BENETON

SÃO PAULO

2015

FICHA CATALOGRÁFICA

Beneton, Emerson José.
Análise do impacto da segurança da informação na competitividade das pequenas e médias empresas / Emerson José Beneton. - 2015.
85 f.: il. color. + CD-ROM.

Dissertação de Mestrado apresentado ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista, São Paulo, 2015.

Área de concentração: Gestão de Sistema de Operação.
Orientador: Prof. Dr. Rodrigo Franco Gonçalves

1. Segurança da informação. 2. Competitividade. 3. Pequenas e médias empresas. 4. Incidentes de segurança da informação. I. Gonçalves, Rodrigo Franco (orientador). II. Título.

EMERSON JOSÉ BENETON

ANÁLISE DO IMPACTO DA SEGURANÇA DA INFORMAÇÃO NA COMPETITIVIDADE DAS PEQUENAS E MÉDIAS EMPRESAS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

Aprovado em:

BANCA EXAMINADORA

_____/____/_____

Prof. Dr. Rodrigo Franco Gonçalves

Universidade Paulista - Unip

_____/____/_____

Prof. Dr. João Gilberto Mendes dos Reis

Universidade Paulista – Unip

_____/____/_____

Prof. Dr. Getúlio Kazue Akabane (convidado)

Faculdade de Tecnologia, Centro Paula Souza - FATEC

DEDICATÓRIA

Dedico este trabalho a Isabel, minha esposa e Lucca e Victor, meus filhos, que, pelo fato de existirem dão sentido a minha vida.

A minha mãe Irene, pela dedicação e carinho na minha formação.

A meu amigo, meu pai João Luiz, que me ensinou a ser uma pessoa melhor e que está sempre a meu lado.

AGRADECIMENTOS

Agradeço ao Professor Dr. Rodrigo Franco Gonçalves, a quem considero umamigo, pelos ensinamentos e pela paciência e apoio durante toda a orientação.

A todos os professores do programa de pós-graduação da UNIP, por compartilharem seu conhecimento com os alunos e permitirem nosso crescimento.

À Associação Brasileira das Empresas de Tecnologia da Informação (ABRAT), por permitir a realização da pesquisa que foi base deste trabalho e a empresa BRconnection que operacionalizou a pesquisa, e sem a qual não seria possível obter número tão expressivo de respondentes.

À empresa ABCTec que, durante este período, me apoiou, compreendendo a necessidade de minha ausência para executar o trabalho.

Ao Professor Dr. Getúlio Kazue Akabane que sempre me incentivou a percorrer este caminho, que se tornou meu mentor na área acadêmica e que me dá o prazer de ser seu amigo.

RESUMO

A Tecnologia da Informação tem influência importante na condução dos negócios e na vida das pessoas, deve ser trabalhada de forma a preservar as informações. Este trabalho analisou como empresas vem tratando a questão da segurança da informação, como atuam na prevenção de incidentes de segurança da informação, quais os resultados que estão conseguindo com as ações atuais e como estes incidentes tem impactado suas operações.
O desenvolvimento desta avaliação ocorreu por intermédio de levantamentos (*survey*). Foi realizada uma primeira avaliação com 21 empresas, onde foi possível identificar a relevância do assunto. Em segundo momento, realizou-se levantamento com 376 empresas com a possibilidade de identificar a percepção das empresas com relação aos impactos que incidentes de segurança da informação trazem a suas operações. Identificou-se ações executadas por essas empresas com objetivo de reduzir os impactos negativos em suas operações e quais destas ações obtiveram resultado relevante. Das ações identificadas como de prevenção a incidentes de segurança da informação, utilização de treinamentos de equipes para capacitação e conscientização, utilização de recursos tecnológicos e utilização de políticas de segurança da informação.

Palavras-chave: Segurança da informação. Competitividade. PME. Incidentes de segurança da informação.

ABSTRACT

Information technology became an important weapon to conduct business even people's lives then should be crafted to preserve the information's sharply. This study examined how companies have been treating information security issues, how they treat incidents prevention of information security, what kind of results they are achieving under current actions and how such incidents are impacting their operations itself. The assessment operation was conducted through companies' surveys. A first step of evaluation throughout 21 companies identified the relevance of this issue. In a next step survey was conducted with 376 companies to identify the companies' perception regarding how the information security incidents impact their operations. Also was identified actions taken in order to reduce operations negative impacts and which of them encompassed relevant results. The actions such as information security incidents preventions, providing enough team training in order to getting capacity and awareness and use of technological resources and information security policies.

Keywords: Information Security. Competitiveness. SMEs. Information security incidents.

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT	-	Associação Brasileira de Noras Técnicas
ABRAT	-	Associação Brasileira das Empresas de Tecnologia da Informação
ABNT NBR ISO 27001	-	Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos
ABNT NBR ISO 27002	-	Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação
ABNT NBR ISO 27005	-	Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação
ADWARES	-	Programa que age automaticamente exibindo vários anúncios sem a permissão do usuário.
BACK DOOR	-	Recurso utilizado por software malicioso para garantir acesso remoto a um sistema ou rede infectada, explorando falhas críticas de segurança.
BNDES	-	Banco Nacional do Desenvolvimento
BOOT	-	Termo em inglês para identificar o processo de inicialização do computador.
CRACKERS	-	Individuo que pratica a quebra de um sistema de segurança de forma ilegalou sem ética.
DLP	-	Do inglês Data loss prevention, prevenção de perda de dados.
EPS	-	Do inglês Encapsulated postscrip, é um formato digital de imagens.
FIREWALLS	-	Software ou hardware utilizado para proteção de redes locais quando conectadas na internet.
FMI	-	Fundo Monetário Internacional
HACKERS	-	Individuo que se dedica, com intensidade incomum, a conhecer e modificar os aspectosmais internos de dispositivos, programas e redes de computadores.

IBGE	-	Instituto Brasileiro de Geografia e Estatística
IDS	-	Do inglês intrusion detect systems, detecção de intrusões.
IP	-	Internet Protocol (protocolo de internet)
IPS	-	Do inglês intrusion prevention systems, prevenção de intrusões.
MALWARES	-	Proveniente de “malicios software” do inglês, que significa software malicioso, é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita.
MPEs	-	Micro e pequenas empresas
NBR	-	Norma Brasileira
PIB	-	Produto Interno Bruto
PSI	-	Política de Segurança da Informaçaõ
RSE	-	Responsabilidade social empresarial
ROI	-	Return on investment (Retorno sobre investimento)
RONI	-	Return on not investment (Retorno do não investimento)
ROTEADOR	-	Aparelho utilizado em redes de computadores para encaminhamento de informações em pacotes de dados.
SEBRAE	-	Serviço de Apoio às Micro e Pequenas Empresas
SPYWARES	-	Programa que recolhe informações do usuário de forma ilícita e envia a entidade externa.
TI	-	Tecnologia da Informação
TIC	-	Tecnologia da Informação e Telecomunicações
TROJANS	-	Software malicioso que age entrando no computador para criar uma porta para possíveis invasões.
VBR	-	Visão baseada em recursos
VR	-	Vantagem de recursos

SUMÁRIO

1 INTRODUÇÃO

1.1 Considerações iniciais

A tecnologia está em constante evolução. As tecnologias emergentes, por um lado, transformam corporações, mas por outro lado influenciam nos riscos financeiros que os executivos e gestores enfrentam diariamente. Pesquisas da revista Fortune 500, dentre as empresas classificadas na ordem da sua capitalização de mercado em 1980 e 1990, mostravam domínio das empresas de petróleo, automóveis e de transformação. Já a lista das empresas em 2000, mostrava o dominio de empresas de base tecnológica, como a Microsoft, America Online, Intel e Cisco (BRIGHAM & HOUSTON, 2004; FORTUNE MAGAZINE, 1981, 1991, 2001). Outras empresas estabelecidas há muito tempo, como o Citigroup, Pfizer e Wal-Mart, que entraram para a lista em 2000, tiveram crescimento de mercado, por haverem aplicado as tecnologias novas e emergentes na transformação de suas atividades de negócios.

Melhoria em tecnologia cria oportunidades para empresas de formularem e implementarem estratégias para redução de custos, introdução de produtos inovadores e desenvolvolvimento de mercados. Da mesma forma, a tecnologia da informação (TI) pode introduzir concorrência e acrescentar componentes que são susceptíveis de provocarem aumento dos custos e redução das receitas e lucros. Isso, por sua vez, requer a formulação e implementação de novas estratégias (BRIGHAM & HOUSTON, 2004). A TI pode não só fazer uma indústria mais eficiente operacionalmente e produtiva, bem como fazer uma empresa reduzir custos e tornar-se mais rentável (DEHNING & RICHARDSON, 2002;. GUNASEKARAN et al., 2001). No entanto, Dehning e Richardson (2002) e Gorla (2004) observaram que a aquisição de infraestruturas de TI, que incluem gastos com *software* e *hardware* e despesas com equipes de TI, podem inundar os orçamentos com custos.

Aliada à complexidade tecnológica, nos projetos de TI, a utilização dessa tecnologia pode trazer vulnerabilidades à operação, ora por falta de treinamento e especialização do usuário ora por causa da utilização ética dos sistemas. Na sociedade atual poucos argumentam que a ética nos negócios não é importante para líderes empresariais e sociedade. A ética nos negócios reflete padrões da empresa, código de valores e princípios do que é certo ou o que é errado (CARROLL & BUCHHOLTZ, 2006).

No entanto, as normas da empresa são implementadas através de partes interessadas na organização e, especificamente, através do comportamento de cada empregado, e não

simplesmente pela publicação de documentos. A prevenção de mau comportamento muitas vezes provoca a redação de leis usadas para fazer cumprir o comportamento esperado. A ética nos negócios não deve ser encarada como exceção, as leis devem ser usadas para regular as normas éticas. A ética nos negócios, bem como a responsabilidade social intimamente relacionada a ela, deve abranger mais do que a conformidade legal (BERGER, et al., 2007; SIEGEL & VITALIANO, 2007; SCHULER & CORDING, 2006; STUEBS & SUN, 2010). Ela inclui compreender a diferença entre o certo e o errado e agir de forma ética.

A definição do que é certo é complexa e está sujeita a interpretações. Enquanto a maioria das empresas pode ter códigos de ética ou normas de conduta, as palavras escritas são valiosas somente se sua intenção se reflete na cultura da empresa e nas ações dos executivos (BEGG & DEAN, 2007; BROWN, et al., 2005; MINOJA, et al., 2010). Liderança ética pode ser um fator-chave de comportamento ético das empresas (BASU & PALAZZO, 2008).

O impacto financeiro do comportamento ético negativo foi amplamente divulgado em casos como Enron, WorldCom, Bemie Madoff, Tyco International, e Arthur Andersen (NIKOI, 2009). No entanto, mesmo nos casos em que o impacto não é tão negativo, o impacto financeiro é devastador para as empresas (KARPOFF, et al., 2008; KARPOFF & LOU, 2010; MURPHY et al., 2009). Compreender o comportamento concorrencial de uma corporação pode levar a uma melhor compreensão do processo de tomada de decisão ética (CHRISTENSEN, 2010; MARENS, 2010; MINOJA, et al., 2010).

Enquanto a utilização eficaz de recursos na competição, tem sido estudada exaustivamente como parte da teoria beseada em recursos (HUNT, 2007; WEMERFELT, 1984), a ética raramente é descrita como um recurso. A reputação tem sido descrita como uma das principais razões para investir em ética e responsabilidade social (PORTER & KRAMER, 2006). Karpoff, et al. (2008) em estudo, concluiram que as perdas por improbidade ética, impostas pelo mercado, foram 7,5 vezes maiores que todas as penalidades legais aplicadas. Há uma questão que deve ser avaliada: incidentes de segurança da informação podem ocorrer apenas por questões tecnológicas ou o comportamento ético de usuários pode influenciar?

1.2 Problematização e Escopo da Pesquisa

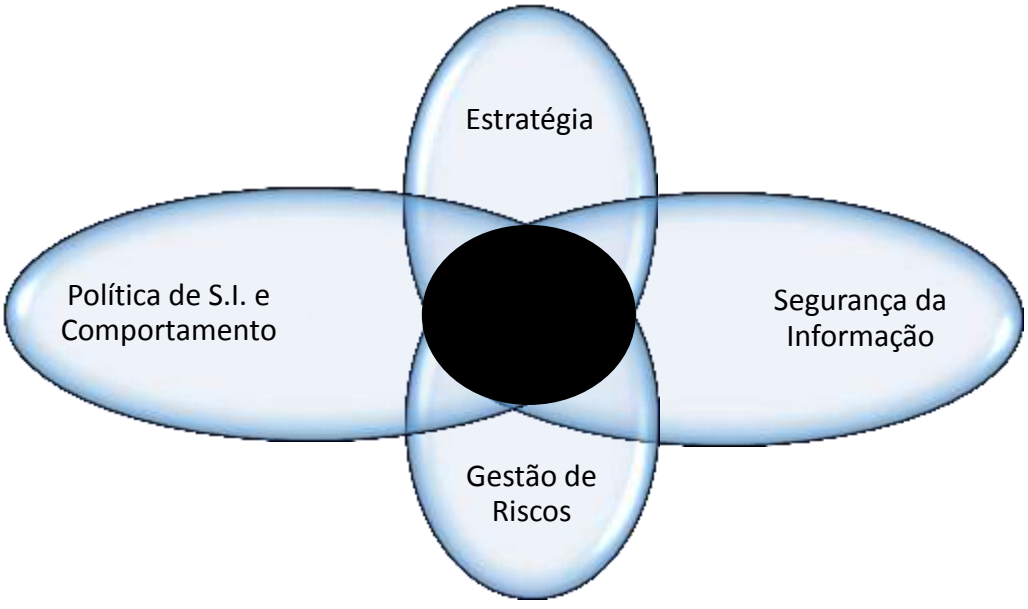
No processo de identificação de estratégias corporativas, a utilização da informação sempre foi de grande importância para as empresas, independente de porte, ramo de atuação ou verticalização. A manutenção da competitividade é preocupação recorrente em mercados

cada vez mais dinâmicos. Nos últimos anos a questão da Segurança da Informação vem ganhando eco, inicialmente em corporações de maior porte, com objetivo de reduzir fraudes, evitar paralisação de operações, reduzir danos à imagem e manter sua posição perante os concorrentes.

Em um mercado pulverizado, como o mercado brasileiro, onde as empesas de menor porte respondem pela grande massa de empregos, torna-se necessário identificar como essa questão está sendo encarada, como o gestor de pequenas e medias empresas trata as questões de perda de dados, vazamento de informações confidenciais que podem trazer prejuízos ao seu negócio. A percepção de que essas ocorrências podem reduzir a competitividade de seus negócios no mercado atual, deve ser melhorada gradativamente.

Uma visão da gestão de riscos, ou pelo menos o mapeamento de riscos para endereçamento de ações preventivas, deve fazer parte da rotina dos gestores de PME. Na identificação de riscos latentes, no tratamento de questões de processo/procedimento, políticas de segurança devem ser implantadas, mas muitas vezes existe uma barreira cultural, essas mudanças podem demorar tempo suficiente para cair em descrédito e com isso aumentar a energia necessária para provocar as mudanças. Uma composição orquestrada, entre a *Estratégia e Competitividade*, os conceitos de *Segurança da informação*, a *Gestão de Riscos* e finalmente *Políticas de Segurança da Informação e Comportamento*, em uma intersecção de ponto ótimo, podem trazer o equilíbrio necessário e a melhora na competitividade da empresa (Figura 1).

Figura 1 – Intersecção de atributos de Segurança e Competitividade (do autor)



Fonte: Elaborado pelo autor.

De acordo com esta ótica, há seguintes questões:

1- Como empresas de pequeno e médio portes percebem a relação da Segurança da informação com a sua competitividade?

2- Pode-se desenvolver um modelo de melhores práticas, que possa auxiliar pequenas e médias empresas no controle de seus ativos, contribuindo assim para o incremento de sua competitividade por melhor controle em segurança da informação?

Nesse contexto adota-se nesta pesquisa a seguinte hipótese: A segurança da informação influencia na competitividade da PME.

1.3 Objetivos

1.3.1 Objetivo geral

Este estudo tem por objetivo analisar os impactos da segurança da informação na competitividade das pequenas e médias empresas.

1.3.2 Objetivos específicos

a. Realizar uma pesquisa exploratória para identificar os aspectos e variáveis-chave no universo da pesquisa.

b. Avaliar quantitativamente as ações das empresas quanto à segurança da informação para redução de incidentes, considerando: a faixa de faturamento anual, além dos impactos percebidos.

c. Apresentar uma análise comparativa ente empresas que possuem recursos tecnológicos na preservação de suas operações e empresas que investem em treinamento de suas equipes, com objetivo de reduzir os incidentes de segurança da informação.

1.4 Justificativa

De acordo com dados do IBGE (2011), as MPEs representam 27% do produto interno bruto (PIB) brasileiro, são responsáveis por mais da metade dos empregos formais no País e constituem 9 milhões de estabelecimentos.

Dessa forma, a manutenção da sustentabilidade dessa parte da economia é fundamental para a evolução do Brasil. O cenário atual tem apresentado um nível de vulnerabilidade aos negócios dessas empresas que, muitas vezes, não estão preparadas, principalmente devido à cultura e falta de conhecimento, quanto às ameaças e aos incidentes de segurança da informação. Tais ameaças e incidentes podem comprometer o armazenamento de dados e a garantia de integridade no tempo, tornando-se cada vez mais grave e sendo o suficiente até para causar o fracasso das empresas (YU-PING et al., 2011).

Considerando-se ainda a mudança de cenário nos próximos anos, com o aumento da concorrência de empresas de outros países, com cultura de negócios mais avançada em relação à tecnologia, levará a uma maior preocupação por parte das empresas brasileiras com relação à segurança de seus sistemas de informação e dos dados sob sua responsabilidade.

1.5 Organização do Trabalho

O trabalho está organizado em 7 capítulos. No primeiro capítulo existe a contextualização identificando o cenário atual, a problematização e o escopo da pesquisa realizada; os objetivos geral e específicos; a justificativa; e a organização do trabalho.

No segundo capítulo foi feita a revisão bibliográfica com o tratamento dos conceitos pertinentes ao objeto de estudo, apresentando as questões de competitividade, segurança da informação, gestão de riscos e política de segurança da informação.

No capítulo três é apresentado o método de pesquisa. Foram utilizados dois survey: o primeiro com 21 respondentes para identificar os aspectos pertinentes do assunto e o segundo com 376 respondentes, com informações para avaliar a percepção dos gestores das empresas com relação à segurança da informação e às ações que trazem controle e redução de incidentes.

No quarto capítulo, apresenta-se o primeiro artigo: “A influência da segurança da informação na competitividade das PMe’s: pesquisa realizada na região da grande São Paulo”. Nesse artigo, identifica-se a pertinência do estudo por completo.

No capítulo 5, apresenta-se o segundo artigo intitulado “Avaliação das empresas com relação à segurança da informação em suas operações”, com amostra bem mais significativa, este trabalho avalia como as empresas percebem a influência dos incidentes de segurança da informação em suas operações.

No sexto capitulo, há o terceiro artigo: “Análise de incidentes e ações para segurança da informação: uma comparação entre o uso de recursos tecnológicos e o investimento em treinamento e capacitação”.

No capítulo sete é realizada a conclusão do trabalho, com nossas considerações sobre os resultados e perspectivas de trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA

2.1 Competitividade

Existem três teorias primárias em vantagem competitiva, incluindo a teoria clássica da empresa (McWILLIAMS & SIEGEL, 2001; PORTER & KRAMER, 2006; SIEGEL & VITALIANO, 2007); visão baseada em recursos (VBR) teoria de Wermerfelt (1984); e da vantagem de recursos (VR) teoria de Hunt (2007).

Na teoria clássica da empresa, a motivação principal da corporação é de maximizar o lucro (McWILLIAMS & SIEGEL, 2001). Com relação as expectativas sociais de uma empresa, denominada responsabilidade social empresarial (RSE), a estratégia da empresa se concentra no uso da perspectiva de escolher uma posição de negócios única e, através dessa vantagem, obter-se a oportunidade necessária para o negócio e alcançar o sucesso financeiro (McWILLIAMS, et al., 2006; PORTER & KRAMER, 2006; SIEGEL & VITALIANO, 2007).

A partir dessa perspectiva, a questão não é se uma causa é digna de investimento, mas se apresenta uma oportunidade para criar valor compartilhado entre a corporação, clientes e sociedade em geral (GRAYSON & HODGES, 2004; MENGUC, et al., 2010). Porter e Kramer (2006) criaram um quadro para priorização das questões sociais e observaram que quanto mais próxima a questão social do objetivo do negócio, maior a oportunidade de usar os recursos da empresa para tornarem-se valor compartilhado, e assim, beneficiar a sociedade.

Uma empresa pode usar as informações da concorrência para identificar forças, fraquezas, oportunidades e ameaças e desenvolver um plano de ação para melhorar sua postura competitiva (PORTER, 1985). Um plano de ação eficaz deve incluir posicionamento da empresa para se defender da competição (PORTER, 1979).

Ormanidhi e Stringa (2008) avaliaram alternativas para as cinco forças do modelo de concorrência, incluindo estrutura-conduta-desempenho; nova organização industrial; teoria dos jogos; perspectiva baseada em recursos; e economia do processo de mercado. De acordo com Ormanidhi e Stringa (2008), a principal limitação do modelo de Porter (1979, 1985) é que ele inclui um enfoque sobre os pontos fortes e fracos de um segmento de mercado ao invés de uma empresa específica, o que torna difícil determinar ações específicas necessárias para uma empresa. O modelo de Porter, apesar de existir há décadas, continua a ser muito

utilizado, principalmente por causa da popularidade, estrutura, clareza, simplicidade e generalidade (ORMANIDHI & STRINGA, 2008).

Entender o comportamento competitivo de uma corporação pode levar a uma melhor compreensão do processo de tomada de decisões éticas (CHRISTENSEN, 2010; MARENS, 2010; MINOJA, et al., 2010). Fundamentalmente, uma vantagem competitiva existe quando uma empresa é capaz de motivar o cliente a selecionar o seu produto em detrimento de seu concorrente, com maior retorno financeiro para os acionistas (CHRISTENSEN, 2010).

Existem dois tipos básicos de vantagem competitiva: custo e diferenciação (PORTER, 1985; PORTER & KRAMER, 2006). A vantagem de custo ocorre quando uma empresa é capaz de oferecer o mesmo produto ou serviço a um cliente a um custo menor. A vantagem na diferenciação ocorre quando uma empresa oferece as características do produto ou serviço, que ultrapassam os de um concorrente (MENGUC, et al., 2010; ORMANIDHI & STRINGA, 2008). Berger, et al. (2007) cunharam a frase "Vantagem diferencial de entregar a virtude" para descrever o comportamento competitivo e mostrar como o trabalho ético pode levar uma vantagem competitiva para a empresa.

Na literatura, os termos criação de valor e vantagem competitiva estão intimamente relacionados, de tal forma que algo só tem valor se um cliente e/ou a sociedade percebe que ele seja importante (ANITSAL & FLINT, 2006; COMITE, 2009; McWILLIAMS, et al., 2006; PELOZA, 2009, STUEBS & SUN, 2010). Há quase um conjunto ilimitado de valores, mas Jin e Drozdenko (2010) definiram como valores fundamentais: colaboração; orientação; criatividade; incentivo; sociabilidade; estimulação organizacional; equidade entre os funcionários; e confiança. Nas corporações mecanicistas, são considerados valores: hierarquia; processos e procedimentos; e orientação estruturada na tomada de decisão; executada por quem detém o poder (JIN & DROZDENKO, 2010).

Isso resulta na compreensão das necessidades e desejos do cliente de forma mais completa, do que a avaliação de valor superior de um comcorrente (PORTER & KRAMER, 2006). Isso também representa uma vantagem competitiva porque não é algo que um concorrente pode facilmente imitar. Por exemplo, Hu e Fátima Wang (2009) estudaram se a Responsabilidade Social das Empresas (RSE) cria uma vantagem competitiva e concluíram que em relação a outros fatores de gestão, tais como posição no mercado, e disposição para inovar, a RSE é de pouca importância a menos que resulte em alto desempenho financeiro. Para Wemerfelt (1984), as barreiras à entrada de Porter (1980) foram substituídas pelas barreiras por recurso, e a matriz de participação no mercado pela matriz de produção por

recuros, definindo um recurso como qualquer coisa que possa ser uma força ou uma fraqueza de uma companhia.

A teoria VBR ajuda os gestores a compreender a vantagem competitiva de uma empresa por estar utilizando de forma eficaz os recursos de apoio às partes interessadas (WERMERFELT, 1984). O VBR é utilizado para analisar as corporações a partir de uma perspectiva de recursos, e não a partir da perspectiva do produto (PORTER 1979, 1985; PORTER & KRAMER, 2006).

Wermerfelt (1984) fornece quatro elementos chave: olhar para as empresas apartir de uma perspectiva de recursos; fornecer novos *insights* sobre a diversidade das empresas, identificando os tipos de recursos que podem resultar em lucros mais elevados; encontrar um equilíbrio entre a exploração dos recursos existentes e o desenvolvimento de novos; e usar uma aquisição como um recurso raro, resultando em aumentos de lucro.

A teoria de Hunt (2007) estendeu a teoria VBR, chamando-a Vantagem de Recursos (VR) e descreveu a natureza de desequilíbrio dinâmico da concorrência. Isso serve para contrastar com a teoria inicial da empresa, que assumiu ser estável e ter informação perfeita sobre uma empresa (McWILLIAMS & SIEGEL, 2001). No modelo VR, o crescimento financeiro das empresas é resultado de capitalização de informação imperfeita que os clientes percebem sobre uma corporação. Hunt (2007) aceitou a definição de recurso de Wemerfelt (1984), mas acrescentou que recursos podem ser tangíveis (mensuráveis) ou intangíveis (indiretamente mensuráveis). Concluiu que os recursos podem ser classificados como financeiros (fluxo de caixa e acesso aos mercados financeiros); físicos (instalações e equipamentos), jurídicos (marcas e licenças); humanos (habilidades e conhecimentos dos colaboradores individuais); ou organizacionais (competências, controles, políticas e cultura). Ambos, Wemerfelt (1984) e Hunt (2007), descreveram o uso eficaz dos recursos na competição, mas não especificamente mencionaram a RSE (Responsabilidade Social Empresarial) ou a ética como um recurso.

Alinhado com valor baseado em recursos e vantagem de recursos, McWilliams, et al. (2006) demonstraram como a responsabilidade social empresarial pode ser um recurso capaz de levar a uma vantagem competitiva sustentável. Uma empresa só ganha uma vantagem competitiva se impede que um concorrente imite essa estratégia. Essa abordagem é consistente com discussões sobre a vantagem de diferenciação (MENGUC, et al., 2010; ORMANIDHI & STRINGA, 2008; PORTER, 1985; PORTER & KRAMER, 2006). Tal fato

pode ser conseguido através da oferta de um produto eticamente responsável ou socialmente responsável sobre o de um concorrente.

Menguc, et al. (2010) analisaram os aspectos de concorrência de forma semelhante a McWilliams, et al. (2006), pesquisando o impacto de um enfoque social pró-ativo e o papel de vantagem de antecipação de Porter (1985). Os autores concluíram que existia ganhos para a corporação e vantagem competitiva por ser pró-ativa, adotando RSE.

No entanto, outros pesquisadores (POMERING & DOLNICAR, 2009) chegaram a uma conclusão contrária, usando experimentos de laboratório, onde foi analisado se clientes estariam dispostos a pagar mais por produtos construídos sobre princípios da responsabilidade social e valores éticos, em relação a produtos mais baratos, sem essas característica. Os pesquisadores concluíram que há um consumidor de baixa compreensão das questões sociais e a RSE não provou ser eficaz na diferenciação de mercado. Grande parte da pesquisa, porém, foi realizada no mercado australiano, e ainda não está claro se outras culturas agiriam da mesma forma.

Vários pesquisadores têm utilizado o foco da criação de valor para abordar a vantagem competitiva e para quantificar o impacto financeiro. Vilanova, et al. (2009) utilizam a teoria de que a relação entre RSE e competitividade ocorre por meio de uma aprendizagem iterativa e processo de inovação, em que os valores corporativos evoluem ao longo do tempo.

Em uma meta-análise, Peloza (2009) analisou como RSE cria valor ao negócio para uma organização, melhorando as medidas financeiras ou contábeis, tais como lucro, preço das ações ou retorno sobre o patrimônio. Embora os resultados tenham mostrado uma relação positiva, houve 39 medidas únicas, com a maioria deles não associadas com a criação de valor ou competição, tornando clara as conclusões a respeito de um vínculo entre vantagem competitiva e RSE claro. Sem dados empíricos, Peloza (2009) concluiu que o desempenho ético claramente resulta na criação de valor para o cliente.

Gilley, et al. (2010) propuseram um modelo destacando a ligação entre o compromisso com o código de ética, a cultura corporativa, os valores da parte interessada e a vantagem competitiva, mas não validaram o modelo. Finalmente, Anitsal e Flint (2006) exploraram as lacunas entre a proposta de valor oferecida fornecida por uma empresa, e as percepções dos clientes no que diz respeito à ética, sem conclusões úteis. Em conclusão, a maioria dos estudos sobre a criação de valor e vantagem competitiva eram multi-indústria, multifacetado, multi-site, e multi-nacionalidade, faltando uma compreensão do subjacente cultura. Isso limita a capacidade de extensão dos resultados para um ambiente de negócios específico.

2.2 Segurança da informação

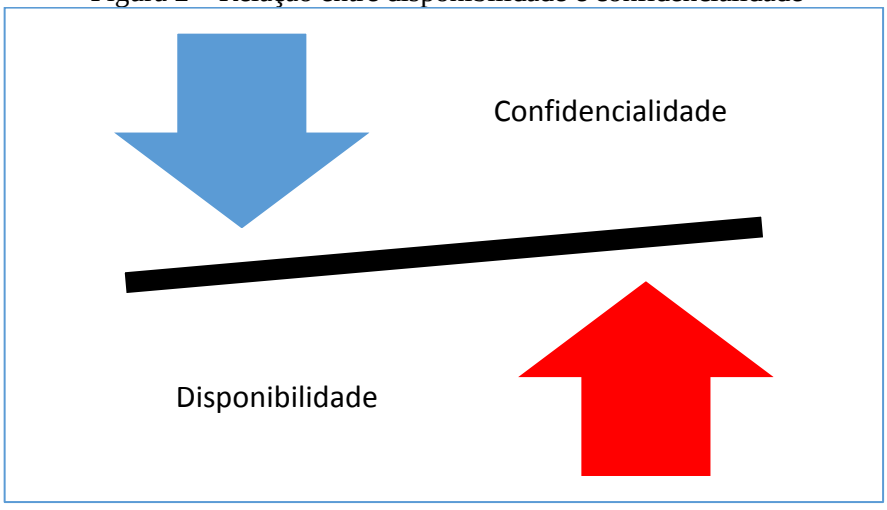
A segurança da informação pode ser alcançada por intermédio da utilização de um conjunto específico de controles, que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. No estabelecimento desses controles é necessário que sejam monitorados, revistos e melhorados, sempre que necessário, com o objetivo de manter a segurança dos sistemas e assim manter os negócios específicos da organização.

O conceito de segurança da informação é tratado, na preservação de variáveis definidas como:

- Confidencialidade - a informação está disponível apenas a quem tem direito de utilizá-la;
- Integridade - a informação está íntegra e correta no momento de sua utilização; e
- Disponibilidade - a informação deve estar disponível sempre que for necessário utilizá-la (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27002:2013).

Analisando esses conceitos, pode-se avaliar que existe uma inter-relação dessas variáveis, como apresentado na figura 2, sendo que sempre é necessário que a informação esteja íntegra, caso contrário deixa de ter valor. Todavia, na questão de confidencialidade e disponibilidade, existe um contraponto, isto é, quanto mais confidencial é a informação menos disponível ela está, e quanto mais disponível, menos confidencial.

Figura 2 – Relação entre disponibilidade e confidencialidade



Fonte: Elaborado pelo autor.

O desafio na manutenção do tripé de segurança da informação, (recursos tecnológicos, processos e pessoas), sem com isso interferir de forma negativa na operação das empresas, está no equilíbrio da proteção dessas três variáveis, tarefa nem sempre fácil já que quando se interfere em uma delas existe um reflexo em outra.

Na utilização da tecnologia da informação, o conceito de Segurança da Informação é mais aliado a sistemas computacionais do que a outros setores da empresa, e com o desenvolvimento das redes de comunicação e dos sistemas computacionais, as ameaças de incidentes de segurança da informação e que podem comprometer as informações armazenadas pelas organizações, estão cada vez mais presentes. Para reduzirem o risco de terem sua operação comprometida as empresas devem proteger seus sistemas (YU-PING et al., 2011).

Segundo Ryan et al. (2012), mesmo com esse cenário, refletindo a necessidade de preservar informações sensíveis ao negócio, é muito difícil convencer as empresas a investir em segurança cibernética. O assunto é árido e o empresário tem dificuldades de quantificar o risco que corre nessa área.

Existe uma verdadeira falta de informação específica nesse setor, além da cultura, muito mais alicerçada em correção do que em prevenção. A mudança cultural ocorre de forma gradativa em uma sociedade, por exemplo, segundo a Associação Brasileira de Empresas de Seguros, o gasto com seguros no Brasil, entre seguros de automóveis, vida entre outros, era de 0,5% do PIB, na década de 70, já 20 anos mais tarde, na década de 90 os brasileiros já gastavam cerca de 2% do PIB com seguros, isso mostra uma mudança de cultura. Vê-se que a questão da prevenção vem ganhando espaço na sociedade brasileira. Da mesma forma a percepção de segurança nas operações das empresas vem ganhando espaço, todavia ainda de forma incipiente.

Existe também uma dificuldade em determinar o valor para a segurança da informação, já que o sucesso é medido ou por meio da não ocorrência de eventos ou da sensível diminuição dessas ocorrências. Mede-se, pois, a chance, ao invés da segurança eficaz (RYAN et al., 2012). Uma forma que pode ser utilizada na identificação da necessidade de investir em segurança da informação é o conceito do RONI, ou retorno do não investimento, que ao contrário do ROI, retorno sobre o investimento, executa uma comparação entre os investimentos necessários para se prover segurança adequada aos sistemas, contapondo essa

informação aos possíveis prejuízos caso exista uma ocorrência de incidente de segurança da informação.

2.3 Gestão de riscos

Nas organizações, atualmente, a utilização de tecnologias e a conexão a um ambiente complexo deixam de ser escolha para ser uma necessidade de sobrevivência, para prosperar e manter sua posição no mercado. Entretanto, para isso, é necessário identificar e mapear os riscos que a empresa está correndo. Inicialmente precisa-se identificar questões importantes como vulnerabilidade, ameaças, impactos ao negócio e medidas de segurança (QIAN et al., 2012).

Vulnerabilidade é o caráter ou qualidade de vulnerável, e vulnerável é do lado fraco de um assunto ou questão, e do ponto onde alguém pode ser atacado ou ofendido; ameaça é o ato delituoso pelo qual alguém, por escrito, por gesto ou por qualquer outro meio simbólico e inequívoco, promete fazer injustamente um mal grave a determinada pessoa. (MICHAELIS, 29/08/2013). Ainda com relação à ameaça, esta pode ser humana ou ambiental. Nesta, estão ocorrências como chuva, terremoto, incêndio, dentre outras; naquela estão as intencionais (provocadas por pessoas mal-intencionadas, que pretendem prejudicar alguém) e as não intencionais (cometidas por falta de conhecimento especifico ou falta de treinamento)

A questão principal da empresa é a saúde de seus negócios Dessa forma, aparece o componente que deverá priorizar as ações, ou seja, o impacto no negócio, pois não faz sentido investir em ações para prevenir ocorrências nocivas às empresas se essas ocorrências significam baixo impacto nas operações. Acaba ocorrendo, então, um desiquilíbrio entre investimento e o que se quer proteger. Utiliza-se a expressão conceitual abaixo:

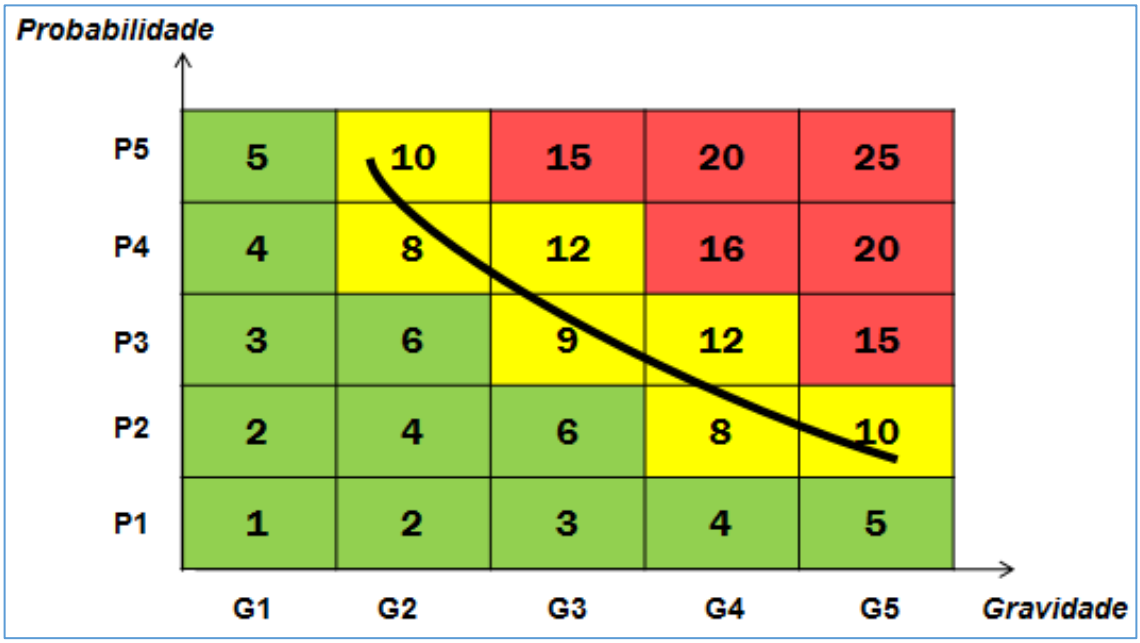
$$\text{Risco} = \frac{\textit{vulnerabilidade x ameaça x impacto ao negócio}}{\textit{Medidas de segurança}}$$

Ainda no que se refere ao risco, é necessário identificar a priorização na implementação das medidas de segurança. Para isso é possível realizar a classificação de risco com a identificação do grau de impacto à operação e a probabilidade de sua ocorrência. Nesse mecanismo, pode-se observar de forma mais clara as ações para redução do risco. Cada análise é feita de forma individual, com a obtenção da percepção, por parte dos envolvidos em

cada operação, da gravidade e da probabilidade da ocorrência de algum incidente de segurança da informação.

Para a classificação de risco, solicita-se que seja atribuída uma nota entre 1 a 5, sendo 5 maior probabilidade e/ou gravidade e 1 menor probabilidade e/ou gravidade. Em seguida, é possível obter quadrantes que podem ser classificados, como risco aceitável para as pontuações entre 1 e 6, risco tolerável entre 8 e 12 e risco inaceitável entre 15 e 25 (ABNT NBR ISO/IEC 27005:2008).

Figura 3 – Gráfico de risco



Fonte: Adaptado de ABNT NBR ISO/IEC 27005:2008

As empresas devem identificar o risco com base em informações pertinentes ao seu negócio, priorizando suas ações motivadas pelo risco identificado. Mesmo a questão da segurança da informação sendouma preocupação constante das empresas, a maioria das organizações controla essa questão de forma reativa. As ações nesse sentido são vistas como despesas e não como uma forma de produzir retorno. A gestão aborda questões de segurança apenas quando os incidentes acontecem e são descobertos (QIAN et al., 2012).

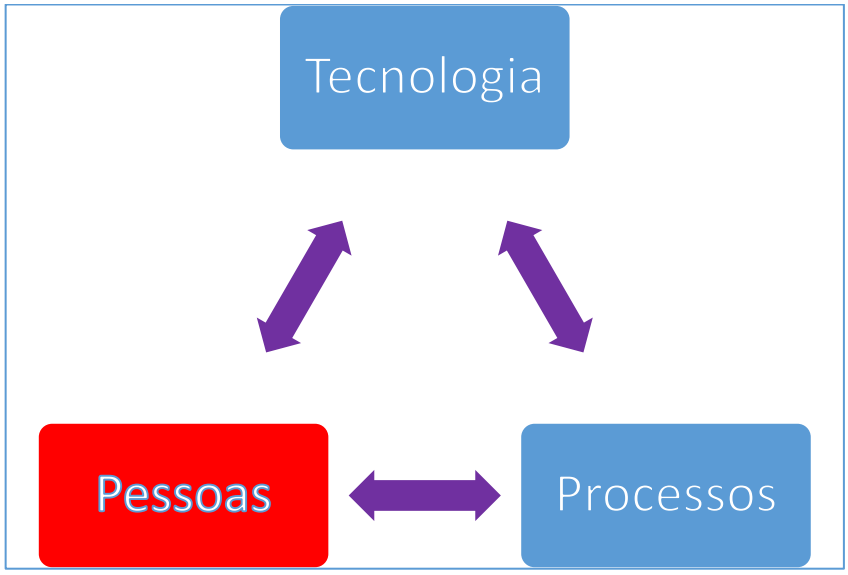
Para a implantação das medidas de segurança, é possível reduzir a gravidade trazendo o risco identificado do quadrante de risco como inaceitável para aceitável ou tolerável. Nesse caso, tais medidas são classificadas como proteção, ou seja, é possível reduzir a probabilidade e assim executar-se a prevenção.

2.4 Políticas de segurança da informação e comportamento

O estabelecimento de uma política de segurança é um dos elementos chave em uma organização no quesito gestão de segurança da informação. Em um ambiente organizacional, existe a possibilidade de se utilizarem, como forma de controle as sanções não apenas limitadas ao formal, como nas políticas de segurança, já que existem outros três níveis de código de ética: controle informal, grupo através dos níveis e de normas sociais, e pessoal, com o autocontrole (GUO & YUAN, 2012).

A maioria das questões estudadas, referentes à forma de implantar as regras de segurança da informação, normalmente está centrada em questões técnicas, mas dentro do tripé de segurança da informação mostrado na figura 4, tecnologia, processos e pessoas, o componente de maior destaque nessa relação são as pessoas (CROSSLER et al., 2013).

Figura 4 – Tripé da Segurança da Informação



Fonte: Elaborado pelo autor.

A implantação de novas regras tem o potencial de introduzir conflitos, deve-se identificar um poder mobilizador para reduzir esses conflitos. De acordo com Kolkowska e Dhillon (2013), com a utilização de comitês de segurança da informação, a responsabilidade em identificar as regras de utilização dos sistemas computacionais é distribuída entre os vários atores da organização. Todavia, para essa formação é necessário identificar colaboradores em posição relevante dentro da organização, pois na definição das regras a interferência na

operação deve ser avaliada e devidamente contornada, para que essas regras possam ser implementadas sem maiores impactos na operação (ABNT NBR ISO/IEC 27002:2013).

Esse procedimento é necessário pois sempre que as regras de segurança são executadas ou modificadas, existe uma estrutura organizacional resultante, gerando mudanças nos processos de negócios. Precisa-se de uma definição de poder e identificação de responsabilidades, já que, devido à falta de conhecimento das vulnerabilidades envolvidas, muitas das ações de relaxamento na regra de controle, são vistas como necessárias sem, contudo, a avaliação do risco potencial ao negócio.

Dessa forma por intermédio do desenvolvimento de uma boa compreensão das dimensões do poder de organização, é possível garantir uma melhor conformidade em relação às regras de segurança. Na maioria dos casos, no processo de implantação das regras de segurança, no sentido de adequar as novas definições aos conceitos arraigados durante muitos anos de trabalho, os colaboradores podem desenvolver não só sua própria visão de segurança como também comportamentos não seguros para lidar com as deficiências. A principal razão para não usar o sistema, porém, está no conflito de valores entre os profissionais na prestação de serviços (KOLKOWSKA & DHILLON, 2013).

Para garantir que funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com suas funções, objetivando a redução de riscos de roubo, fraude ou mau uso dos recursos computacionais, é necessária a conscientização dos mesmos acerca das ameaças e consequências de seus atos, ofertando a eles a coparticipação da implantação e preservação das políticas de segurança da informação (KNORST et al., 2011).

3 MÉTODO DE PESQUISA

O plano geral da pesquisa envolve a elaboração de três artigos de forma a atender aos objetivos específicos traçados.

O primeiro artigo tem o propósito de explorar o tema, através de survey com amostra reduzida (21 empresas) para identificar aspectos pertinentes, problemas, questões e variáveis-chave no universo, de forma a direcionar os artigos seguintes.

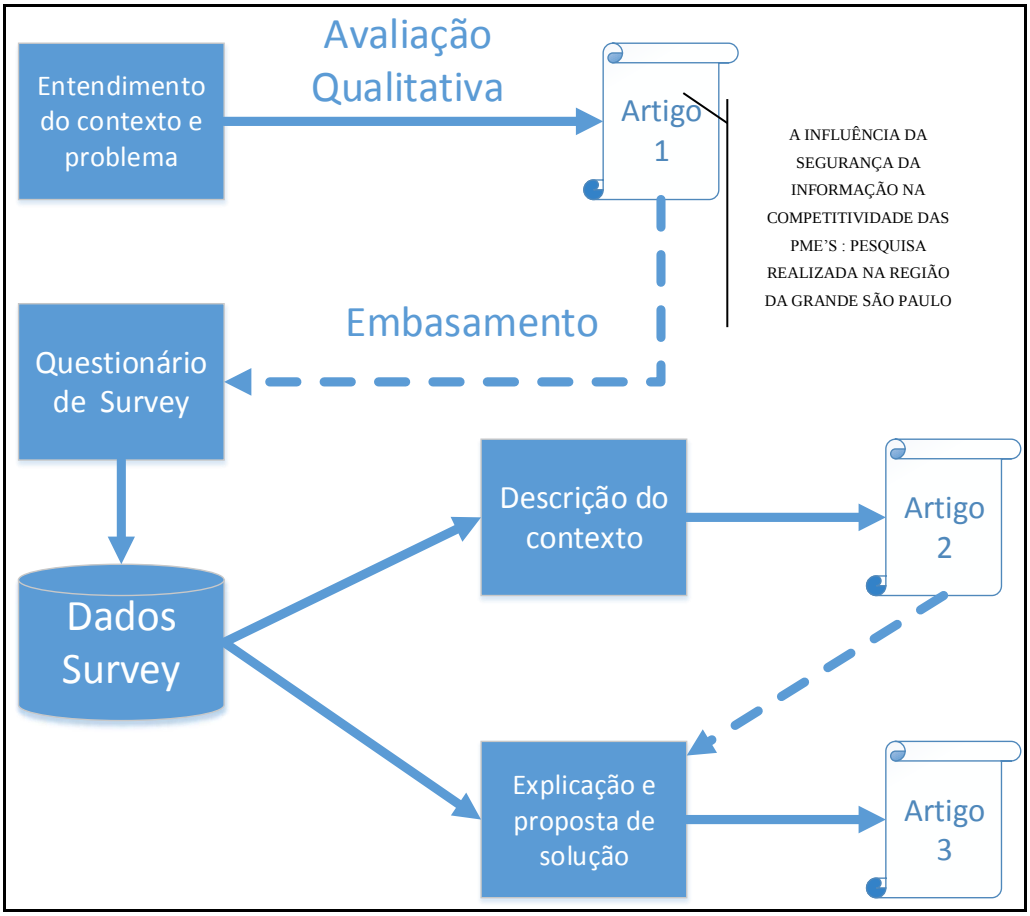
Assim, com o contexto identificado, elabora-se um questionário mais abrangente (Apêndice A) e realiza-se um levantamento com 376 empresas, sendo que de acordo com o método de classificação de porte de empresas pelo BNDES e pelo SEBRAE temos 259 empresas de pequeno e médio portes (faturamento até 90 milhões de reais ao ano e/ou até 499 funcionário) e 117 empresas de médio-grande e grande portes (faturamento acima de 90 milhões de reais ao ano e/ou mais de 500 funcionários) todas elas localizadas no Brasil, no qual obtém-se resultados mais específicos, compondo uma base de dados de respostas.

De posse do Banco de dados da segunda pesquisa, realiza-se a avaliação da percepção que as empresas têm com relação a segurança da informação em suas operações. É possível classificar essas empresas levando em conta seu porte, seus ramos de atividade e a maneira como a percepção do gestor influencia a tomada de decisões para preservar a operação da empresa (tema do Artigo 2).

Completando o método, o artigo 3 explora a utilização da política de segurança da informação, o uso de recursos de tecnologia para preservação das informações e a utilização de treinamentos com as equipes para que seja possível obter a redução de incidentes de segurança da informação.

Este trabalho não tem a pretensão de esgotar o assunto, mas sim proporcionar uma discussão do tema, levantando a possibilidade de, em estudos futuros, identificar um conjunto de regras e ações organizadas, que possam amadurecer os controles das PME’s, melhorando gradativamente a segurança da informação em um mercado cada vez mais competitivo.

Figura 5 – Plano geral de pesquisa



Fonte: Elaborado pelo autor.

4 ARTIGO 1 – A influência da segurança da informação na competitividade das PME's: pesquisa realizada na região da grande São Paulo

4.1. Considerações iniciais

Este artigo foi aprovado e apresentado no XX Simpósio de Engenharia de Produção, Engenharia de Produção & Objetivos de Desenvolvimento do Milênio em Bauru, São Paulo em 4 a 6 de novembro de 2013. Utilizamos este artigo para identificar inicialmente a relevância do assunto e com isso dar continuidade a um trabalho mais completo, realizado nas próximas etapas. A pesquisa realizada em 2013, contou com 21 empresas respondentes. Com os resultados obtidos identificamos viabilidade na continuidade deste trabalho, e elaboramos nova pesquisa que foi realizada em 2013/2014, onde obtivemos 376 respondentes, em vários estados brasileiros.

A INFLUÊNCIA DA SEGURANÇA DA INFORMAÇÃO NA COMPETITIVIDADE DAS PME'S: PESQUISA REALIZADA NA REGIÃO DA GRANDE SÃO PAULO

Emerson José Beneton – Universidade Paulista – UNIP

Atila de Melo Lira – Faculdade Santo Agostinho

Ivanir Costa – Universidade Paulista – UNIP

Rodrigo Franco Gonçalves- Universidade Paulista -UNIP

Resumo

No cenário atual, a competitividade das empresas é definida pela inovação, velocidade de suas decisões, sua gestão e como se não bastasse, ainda é necessário colocar questões mais complexas. Na era da informação, saber como tratar a informação pode definir sua posição no mercado. Este artigo analisa como as empresas na região metropolitana de São Paulo entendem essa questão, como é a sua percepção entre a preservação de suas informações e como isso pode afetar a sua competitividade. Como metodologia de pesquisa foi aplicado um questionário com tratamento estatístico das respostas, sendo possível classificar a dimensão das organizações em relação ao número de funcionários e receitas anuais. Entre as conclusões obtidas, o critério dos investimentos em segurança da informação, mais forte na cultura do gerente da área responsável e menos na receita e no negócio, chamando assim a atenção, já

que esta forma de tratamento pode não trazer a preservação de dados efetiva e consequente competitividade desejada.

Palavras-chave: Competitividade, Segurança da Informação, Planejamento Estratégico de TI.

1. Introdução

As organizações na atualidade contam e dependem das informações para exercerem suas atividades. Atualmente, mais de 99% das informações no mundo moderno são criadas, armazenadas, transmitidas e mantidas digitalmente (ORLOVSKI; KISIELEWICZ & RIBEIRO, 2012). A informação é um bem valioso, de modo que os dados corretos e como eles são usados podem criar ou destruir milhões de reais em receitas em um curto espaço de tempo.

Dessa forma a segurança das informações torna-se a principal preocupação para qualquer gestor de uma empresa. Segurança da marca, fluxos de receita e a eficiência geral de operações são coisas que precisam estar em ordem para uma organização operar de forma rentável e eficiente. Isso garante que todos sejam pagos, que o negócio prospere e que seja protegido de possíveis ameaças.

Muitas empresas pequenas e médias (PMEs) consideram a segurança da informação como preocupação de um “grande negócio” - algo que só os bancos e os governos deveriam se preocupar, porque nesse ponto de vista as PMEs não são susceptíveis de serem alvos de invasores digitais (*hackers e crackers*). Mas a realidade demonstra que as PMEs também possuem riscos de falhas de segurança que podem ameaçar sua organização (DIAS; RODRIGUES &PIRES, 2012).

Muitas empresas consideram-se imunes a problemas de segurança pois acham que "não precisam de segurança da informação", contudo, acabam entrando em contato com especialistas em segurança, depois ou durante um enorme incidente de segurança que acaba ameaçando seriamente a subsistência de seus negócios.

Nesse momento, o controle de danos se torna caro e normalmente existem perdas que não podem ser recuperadas. Se essas organizações não tomaram medidas preventivas antes desses eventos, no entendimento do risco da informação que carregam em seus ativos, então, é improvável que tenham de suportar um evento tão prejudicial.

No mundo digital é praticamente impossível não se preocupar com a segurança da informação e no dia-a-dia, pequenas e médias empresas no mundo são colocadas em sérios riscos, devido principalmente aos eventos de segurança de informação.

Alguns eventos ocorrem por falhas de conformidade, outros por ataques de vírus e softwares maliciosos (*malwares*) e outros surgem a partir de fontes acidentais, tais como incêndio ou inundação. Independente de qual for a fonte da ameaça, uma organização despreparada pode sofrer pesadas perdas na eficiência e na integridade dos negócios, bem como ter um alto custo de recuperação.

1.1. Ameaças à Segurança da Informação em Pequenas Empresas

Ano a ano, são introduzidas novas ameaças à segurança das informações empresariais. Essas ameaças são cada vez mais complexas e tiram o máximo de proveito das vulnerabilidades em aplicações e ativos de infraestrutura de rede. Cada produto, seja software ou hardware, tem vulnerabilidades que, quando exploradas, podem levar a grandes danos (DIAS; RODRIGUES & PIRES, 2012).

Em empresas de médio e grande porte, o total de perdas por danos na segurança ascendem a cada ano, sendo os custos decorrentes de vírus correspondentes a quase 40% desse total. Em anos anteriores, o roubo de informações confidenciais representou a maior quantidade de danos de segurança. As pequenas empresas são menos propensas na capacidade de absorver as perdas financeiras e incidentes graves que podem ser prejudiciais para a sobrevivência do negócio. Já as grandes empresas também são mais propensas a imporem impedimentos ao abuso de segurança do que as pequenas (GORDON et al., 2004).

A primeira geração de ameaças à segurança começou na década de 1980. Normalmente, essas ameaças eram vírus de carga de sistema (*boot*) que afetaram computadores individuais e redes ao longo de semanas. A geração seguinte de ameaças consistia principalmente de vírus que estavam contidos em macros e e-mails. Os vírus são definidos como peças de código de programação que são projetados para se espalharem automaticamente para outros usuários. Eles fornecem resultados indesejados e geralmente desagradáveis e são normalmente disfarçados com algo a mais (AMERICAN EXPRESS, 2002).

Ataques que danificam os serviços oriundos de invasores digitais maldosos (*hackers*) também se tornaram predominantes na década de 1990 e continuam a ser um problema. Hoje,

as empresas enfrentam novos tipos de ameaças que afetam computadores individuais, redes individuais ou múltiplas e até mesmo redes regionais. Os vírus se popularizaram rapidamente e podem se autoreplicar para infectarem rapidamente um grande número de usuários. Eles residem na memória ativa dos computadores e podem atrasar sistemas ou até mesmo levar os processos a pararem (MOREIRA, 2012).

Códigos maliciosos (Trojans) que residem em um programa aparentemente inofensivo podem causar danos ao sistema, uma vez que são abertos ou executados. Eles são muitas vezes utilizados para criar entradas "*back door*" em computadores que comprometem a segurança da rede. Muitos deles são projetados para roubar senhas e são transmitidos por um vírus, o que pode levar a ameaças combinadas (CISCO SYSTEMS, 2013).

A ameaça combinada é um vírus que pode ter múltiplas técnicas de infecção e se propaga através de rotinas de Internet e de rede sem intervenção humana. Eles geralmente exibem *Trojans* como comportamento. No primeiro semestre de 2011, mais de 60% dos pedidos de códigos maliciosos eram na forma de ameaças combinadas (DIAS; RODRIGUES; PIRES, 2012). *CodeRed* e *Nimda* são exemplos de ameaças combinadas avançadas. Estas, ao contrário dos vírus, são destinadas a causarem danos ao invés de serem apenas um incômodo. Outra diferença entre ameaças e vírus combinados é que a ameaça combinada não necessita de intervenção humana (como abrir um anexo de e-mail) para se espalhar. Os vários métodos de propagação de uma ameaça combinada podem fazer a contenção mais difícil do que a de um vírus. Correções de segurança estão disponíveis, que seria mitigar a maior parte do dano de ameaças combinadas, mas infelizmente nem todas as empresas têm feito as atualizações com as últimas correções (MOREIRA, 2012).

No momento as crescentes preocupações são com a expansão de *spywares*, *adwares e malwares*. Esses programas são baixados para máquinas sem o conhecimento ou consentimento do usuário; simplesmente visitando sites, esses programas podem ser descarregados para o computador do usuário sem que o mesmo esteja ciente de que o programa foi instalado. Eles normalmente são executados em segundo plano e são usados para rastrear informações pessoais ou executar comandos indesejados e às vezes prejudiciais.

Webroot Software e Earthlink recentemente escanearam mais de 1,5 milhões de PCs pessoais para *spyware* e descobriram que os computadores contêm uma média de 27,5 pedaços de programas potencialmente maliciosos (FURNELL & THOMSON, 2009). Existem várias ferramentas disponíveis para minimizar os efeitos de tal código malicioso, muitos dos

quais são gratuitos. Alguns programas detectam e removem esses programas maliciosos e outros são mais pró-ativos através da imunização de sistemas para se tornarem infectados novamente.

Frangopoulos, Eloff e Venter (2013) realizaram uma pesquisa e, aos seus entrevistados, pediram que indicassem quais as ferramentas que eles usaram para lidar com tais ameaças. AdAware e Spybot foram os mais populares em 50% e 33,3%, respectivamente, sendo que ambos são distribuídos gratuitamente. Apesar da disponibilidade de ferramentas eficazes que custam pouco ou nada para os empresários, 22,2% das pequenas empresas não usam todas as ferramentas de spyware.

Novas ameaças estão em constante desenvolvimento, podendo ter um impacto global. O Slammer foi um exemplo dessas ameaças, 10 minutos depois de ser liberado, ele havia infectado 90 por cento dos sistemas vulneráveis (FURNELL & THOMSON, 2009).

Os ataques à segurança da informação, que começaram na década de 1990, têm aumentado na rede e na infraestrutura global, isso porque eles normalmente usam um endereço de IP falso, eliminando os rastros. Originalmente, esses ataques foram projetados para desligar um alvo, como um computador individual, servidor ou rede. Hoje, eles se tornaram mais maciços, utilizando vários computadores, sem a permissão ou o conhecimento dos proprietários para atacar um alvo específico.

Eles provocam a distribuição dos serviços na rede e agora são a segunda principal causa de perdas entre empresas de segurança (GORDON et al., 2004), envolvendo pirataria e ataques maliciosos em grande escala. Com o conhecimento de que *hackers* experientes, também conhecidos como "*blackhats*", ganharam ao longo dos anos, eles podem agora voltar sua mira para alvos maiores. Em vez de infectar apenas uma máquina, eles podem agora derrubar uma rede inteira. Um exemplo disso é o lendário vírus MyDoom, cujo alvo derrubou os servidores SCO Group Inc. em 2004. As empresas correm agora o risco de ter seus bens de informática usados como "zumbis" no controle de um hacker externo à execução de comandos especificados no plano de fundo.

Os ataques a flash são outro tipo de ameaça que tem o potencial para dominar os esforços de segurança atuais e futuros em termos de desenvolvimento de aplicações na web. Pequenas empresas muitas vezes dependem de seus sites para uma variedade de funções, incluindo aspectos relativos à movimentação financeira. Muitos sites, no entanto, são vulneráveis a esse tipo de ataque, especialmente sites não estáticos que incorporam a

participação do usuário. Este tipo de ataque viola a confiança entre o proprietário do conteúdo e do espectador (EYE ON SECURITY, 2002).

Ela envolve o uso de *cross-site scripting* (XSS) onde o código JavaScript é injetado em aplicações da web, o que pode demorar mais de uma sessão do usuário e roubar informações pessoais. Embora a abordagem comum para limitar XSS envolve a filtragem de conteúdo, ele é muito ineficiente devido ao fato de que aplicações Web confiam no conteúdo flash por descuido. Isso abre as portas para a injeção de código malicioso (EYE ON SECURITY, 2002). Novas ameaças no horizonte incluem vírus que possuem como alvo mensagens instantâneas, mensagens de voz, aparelhos portáteis, consoles de jogos e celulares (NETTO & SILVEIRA, 2007). O primeiro vírus a infectar telefones celulares foi descoberto em 2004 e infectou telefones da Nokia.

É certo que determinadas plataformas são mais propensas a serem alvos do que outras e que a maioria dos vírus de hoje atacam alvos com sistemas baseados em Windows (FRANGOPOULOS; ELOFF & VENTER, 2013). Embora as vulnerabilidades em sistemas operacionais da Microsoft tenham causado a emissão de vários patches para evitar certas falhas de segurança, os usuários geralmente não instalam esses patches imediatamente. Nesse intervalo de tempo, o sistema é vulnerável. Além disso, o estudo supracitado pediu aos seus entrevistados para indicarem qual (quais) plataforma (s) é (são) empregada (s) em seus pequenos negócios. Como esperado, uma maioria esmagadora utiliza a plataforma Microsoft (83,3%).

1.2. A percepção de pequenos negócios quanto a grandes ameaças

Quintairos, Oliveira e Mendonça (2012) pediram aos entrevistados de seu estudo em pequenas empresas para identificarem as principais ameaças que eles percebiam como suscetíveis de causar prejuízos para a sua empresa ou para os seus dados. Os resultados são que mais da metade dos entrevistados consideraram que as ameaças principais para os dados vêm do pessoal interno (55,6%), além de trojans (27,8%), hackers (22,2%), vírus (22,2%) e controle de senha, vulnerabilidades da Microsoft e spyware/malware (5,6% cada). No entanto, muitos dos entrevistados também indicaram que essa ameaça em grande parte pode ser acidental ou intencional.

Isso é consistente com outra pesquisa referente ao tema em que revelou que 59% das empresas indicaram que tinham tido experiências atuais com problemas internos de acesso à

rede (Gordon et al., 2004). Outros estudos descobriram que o maior número de ataques de segurança foi resultado de erros humanos e foram acidentais (FURNELL & THOMSON, 2009; SMITH, 1989). A ameaça do funcionário também foi citada como a quinta principal causa de perdas financeiras em 2004 devido a violações de segurança (GORDON et al., 2004).

Cerca de apenas um em cada cinco entrevistados (22,2%) considerara que hackers seriam uma ameaça. No entanto, pesquisas anteriores indicaram que as pequenas empresas são alvos cada vez mais frequentes no ambiente de hoje e dizer que só porque a empresa possui um tamanho menor ela está protegida é uma falácia (FURNELL & THOMSON, 2009).

Gestores de pequenas empresas muitas vezes sentem que possuem um risco baixo de ameaças da Internet, vendo-se como muito pequeno para ser de qualquer interesse (QUINTAIROS; OLIVEIRA & MENDONÇA, 2012). Este parece ser o caso das pequenas empresas entrevistadas pelo estudo supracitado, uma vez que 16,7% acreditam que não houve ameaças aos seus dados. Os resultados do estudo são, portanto, consistentes com uma atitude de "baixo risco" em relação a ameaças externas.

Em ambiente de informações globais de hoje, independentemente do tamanho, as empresas podem sofrer igualmente ataques às suas informações. Todo o mundo, todas as empresas e todos aos pequenos pedaços de arquivos, desde números de cartões de crédito pessoais a informações confidenciais das empresas, são de interesse dos que atacam a segurança das informações.

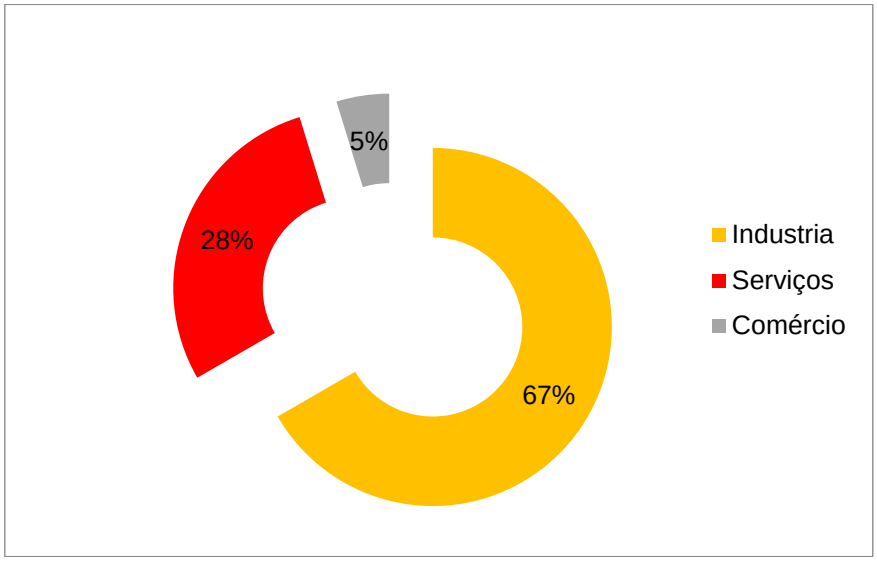
Gordon et al. (2004) indicam que 47% dos entrevistados tiveram entre um e cinco incidentes de segurança no ano passado, 20% passaram por seis a dez e 12% experimentaram mais de dez incidentes. Isso é uma forte divergência a partir do que foi apontado por pesquisas anteriores, em que poucas pequenas empresas admitiram já terem sofridas incidentes de segurança. Ou essas pequenas empresas foram extremamente sortudas, ou as invasões passaram despercebidas.

2. Metodologia

O objetivo deste artigo foi verificar o comportamento das empresas de pequeno e médio portes com relação a sua percepção de como a segurança da informação pode

influenciar na competitividade de seus negócios. Foi desenvolvido um questionário, contendo 6 blocos de perguntas, que foi distribuído para uma amostra de 60 empresas, da região metropolitana de São Paulo, sendo que se obtiveram respostas de 21 questionários. Dentre os respondentes, traçou-se o seguinte perfil apresentados na figura 6:

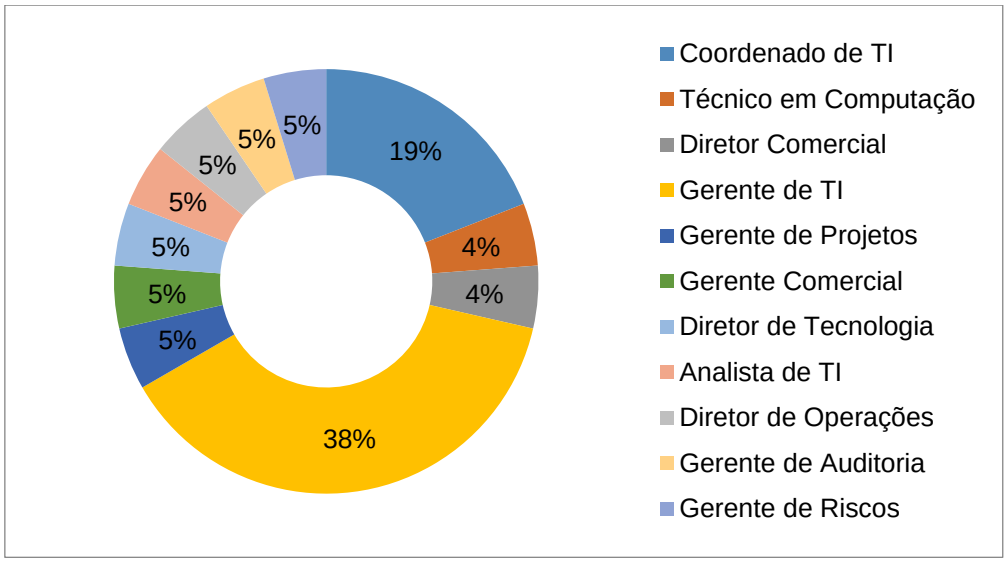
Figura 6 – Distribuição dos respondentes pela vertical econômica



Fonte: Elaborado pelo autor.

A maioria dos respondentes eram indústrias, seguidos pela área de serviços e uma pequena porção de comércio. Com relação à distribuição pela função ocupada pelos respondentes, obtiveram-se os valores apresentados na figura 7.

Figura 7 – Distribuição dos respondentes pela função profissional

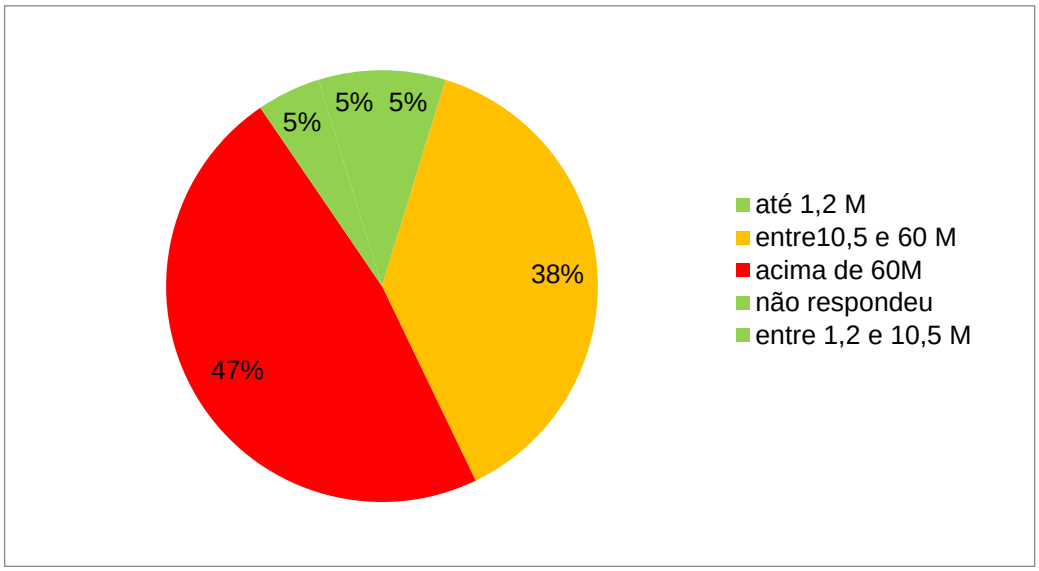


Fonte: Elaborado pelo autor.

Dentre as funções dos respondentes, verificou-se que o maior percentual foi dos Gerentes de TI seguidos pelos coordenadores de TI, perfazendo um total de 57% dos respondentes.

De acordo com o faturamento anual, as empresas foram subdivididas em 4 categorias, ou seja, até 1,2 milhões de dólares, entre1,2 e 10,5 milhões de dólares, entre 10,5 e 60 milhões de dólares e acima de 60 milhões de dólares, conforme apresentado na figura 8.

Figura 8 – Distribuição dos respondentes pelo faturamento anual

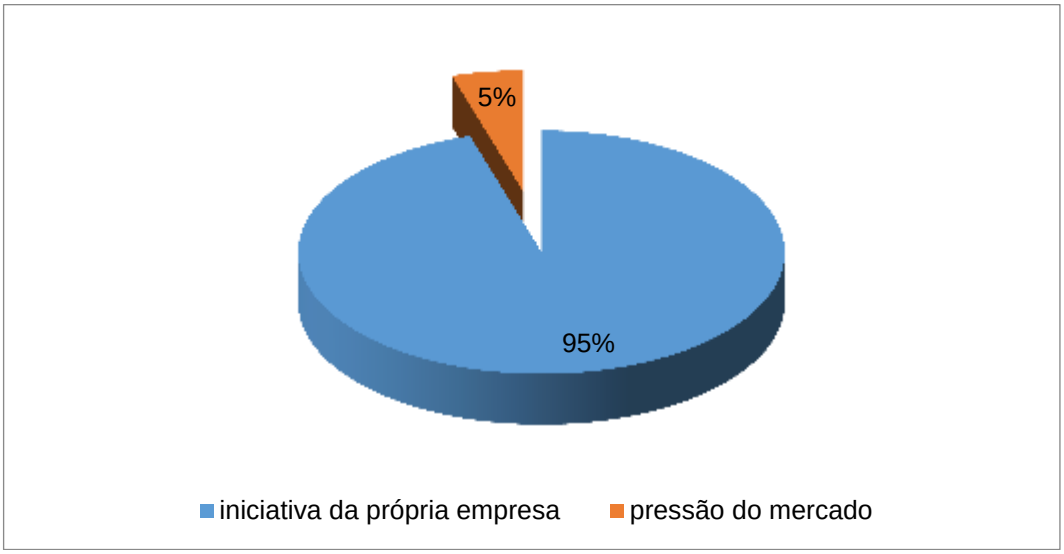


Fonte: Elaborado pelo autor.

3. Resultados e discussões

Quando perguntados sobre a origem de investimentos para modernização da empresa, através de novas tecnologias de informação e/ou processos de fabricação, serviços ou inciativas semelhantes, um percentual de 95% dos entrevistados responderam que têm essa iniciativa pela própria empresa, e apenas 5% responderam que essas ações são motivadas pela pressão dos consumidores, o que demonstra que em sua maioria as empresas já possuem perfil de melhoria tecnológica, como diferencial competitivo de forma proativa, sem esperar a movimentação do mercado, tentando angariar com isso um diferencial competitivo, como mostra a Figura 8.

Figura 9 – Origem do capital investido em Tecnologia de SI



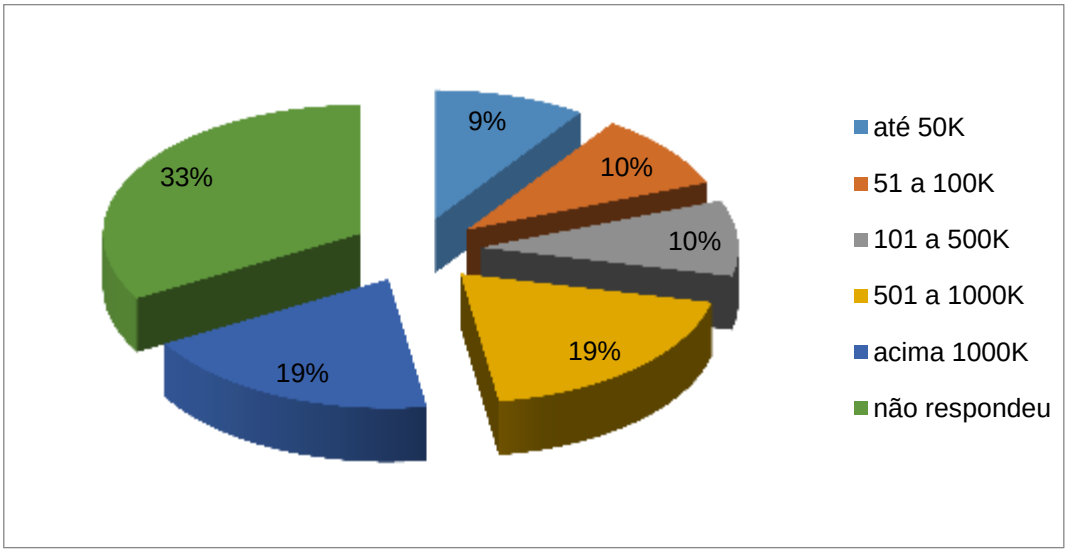
Fonte: Elaborado pelo autor.

Uma constatação de destaque, foi que, apesar de a maioria das empresas realizar investimentos por conta própria, para melhoria de suas operações e melhoria da segurança da informação, nota-se que os valores investidos são distribuídos de forma regular, com relação ao montante investido, ou seja, percebe-se que independente do faturamento da empresa, existe uma preocupação de investir em tecnologia diferente em cada empresa, e isso ficou mais evidente com relação ao foco de diferenciação de mercado que cada empresa atua.

Empresas que estariam competindo por preço, não realizam investimentos altos em tecnologia e redução dos riscos, já que precisam ter preço competitivo para permanecer no mercado, na contrapartida, deixam de realizar a gestão de riscos, o que deixaria essa estratégia mais coesa, pois sendo mapeados os riscos, a empresa estaria menos sensível a incidentes de segurança da informação.

Nota-se que os investimentos estavam mais aliados à cultura do gestor de TI, do que da estratégia corporativa da empresa, colocando em risco o equilíbrio da operação, como apresenta a Figura 10.

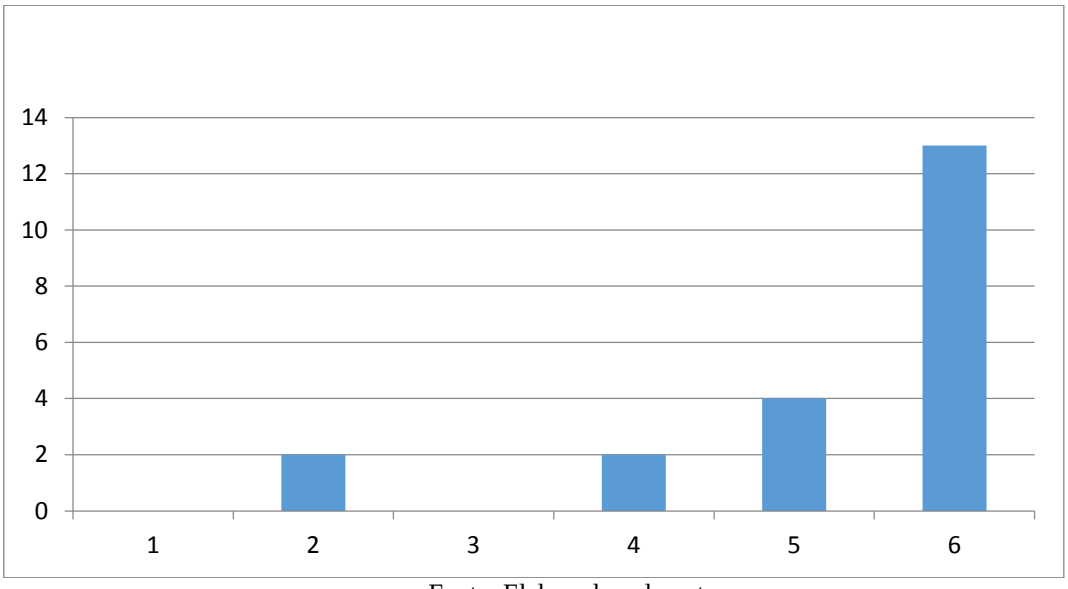
Figura 10 – Distribuição dos Investimentos em Tecnologia para SI



Fonte: Elaborado pelo autor.

Uma das questões feitas na pesquisa foi quanto à importância da segurança da informação na operação da empresa, e para ela o respondente poderia classificar quanto ao grau de importância para este assunto. Em sua maioria este item foi classificado como muito importante com pontuação máxima, mostrado na figura 11.

Figura 11 – Identificação do nível de importância para a empresa com relação aos investimentos em Segurança da Informação



Fonte: Elaborado pelo autor.

Analisando essa questão e verificando o descompasso de investimentos em segurança da informação comparativamente ao faturamento da empresa, conclui-se que esses investimentos, apesar de serem importantes para a operação, podem não dar o devido retorno

na segurança e competitividade da empresa, pois são feitos de forma reativa, com demandas pontuais e na maioria das vezes motivados pela cultura do gestor de TI.

Investimentos feitos dessa forma passam a ter sua avaliação distorcida, já que por falta de conhecimento da gestão da empresa, podem dar uma falsa sensação de segurança. Existe investimento, mas não sendo compatibilizado com a análise de risco e foco da operação, pode cobrir parte das demandas, deixando ainda assim a empresa em situação de vulnerabilidade, reduzindo sua competitividade no mercado.

4. Considerações finais

A maioria das empresas brasileiras, independentemente do tamanho, são sensíveis à necessidade de segurança da informação. Observa-se uma grande demanda nessa área e mais ainda um aumento significativo nos incidentes, anteriormente ocasionados de forma intencional, por pessoas mal-intencionadas e atualmente ocorrendo muitas vezes por falta de preparo das equipes profissionais das empresas.

Os investimentos não estão vinculados à receita potencial e são direcionados por demandas pontuais, na maioria das vezes devido à cultura dos profissionais envolvidos, à falta de uma visão sistêmica da operação. Apesar de reduzirem a vulnerabilidade em pontos específicos das operações, não oferecerem, contudo, a proteção global resultando em um alto grau de vulnerabilidade.

Em face às mudanças culturais em andamento, essas empresas buscam competitividade para operar no novo cenário brasileiro para os próximos anos e a segurança da informação será ainda um árduo caminho a ser trilhado.

REFERÊNCIAS

AMERICAN EXPRESS. OPEN Small Business Network Semi-Annual Monitor, 2002. Disponível em: <http://home3.americanexpress.com/corp/latestnews/osbnm2002.asp>. Acesso em: 29/05/2013.

CISCO SYSTEMS. Security and VPN Solutions for Large Enterprises, 2013. Disponível em: <http://www.cisco.com>. Acesso em: 29/05/2013.

DIAS, J.M.F.; RODRIGUES, R. C. M. C.; PIRES, D. F. *A Segurança de Dados na Computação em Nuvens nas Pequenas e Médias Empresas*. Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica, Franca, v.2, n.1, 2012.

EYE ON SECURITY. By-passing JavaScript Filters — The Flash! Attack**.** Eye on Security, 2002. Disponível em: <http://eyeonsecurity.org/papers/flash-xss.pdf>. Acesso em: 29/05/2013.

FRANGOPOULOS, E. D.; ELOFF, M. M.; VENTER, L. M. Psychosocial risks: Can their effects on the security of information systems really be ignored?,Information Management & Computer Security, v.21, n.1, p.53-65, 2013.

FURNELL, S. & THOMSON, K.L. Recognizing the varying user acceptance of IT security. Computer Fraud & Security, Volume 2009, Issue 2, 5-10. Elsevier, 2009.

GORDON, L. A.; LOEB, M. P.; LUCYSHYN, W.; RICHARDSON, R. 2004 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2004. Disponível em: <http://www.gocsi.com/forms/fbi/pdf.html>. Acesso em: 29/05/2013.

MOREIRA, N. S. *A segurança da informação na pequena e média empresa: Um instrumento alavancador de vantagem competitiva*. **Fasci-Tech**, São Caetano do Sul, v.1, n.6, p.101-115, Mar./Set., 2012.

NETTO, A. S.; SILVEIRA, M. A. P..*Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas*. JISTEM - Journal of Information Systems and Technology Managemen**t**. (Online), São Paulo, vol.4, n.3, 2007.

ORLOVSKI, R.; KISIELEWICZ, L. A.; RIBEIRO, S. R. A. *Segurança de Informação em Sistemas Agrícolas: estudo de caso Fundação ABC*. Revista de Engenharia e Tecnologia, v.4, n.3, Dez, 2012.

QUINTAIROS, P. C. R.; OLIVEIRA, E. A. A. Q.; MENDONÇA, M. G. M. *Impactos dos procedimentos dos usuários na segurança da informação em ambientes de rede de computadore*s. Latin American Journal Of Business Management, Taubaté, v.2, n.2, p.118-144, Jul./Dez., 2011.

SMITH, M. Computer security – threats, vulnerabilities and countermeasures. Information Age(IK), v.11, n.4, p.205-210, Oct., 1989.

5 ARTIGO 2 – Percepção das Empresas com relação à segurança da informação em suas operações

5.1. Considerações iniciais

Este artigo foi apresentado à revista Exacta- Engenharia de produção, revista B5 para engenharias III, aguardando retorno. A pesquisa utilizada neste artigo possui 376 empresas respondentes, foi feita entre 2013 e 2014.

AVALIAÇÃO DAS EMPRESAS COM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO EM SUAS OPERAÇÕES

Emerson José Beneton – Universidade Paulista – UNIP

Rodrigo Franco Gonçalves – Universidade Paulista – UNIP

Getúlio Kazue Akabane – FATEC

Ivanir Costa - UNINOVE

Resumo

No cenário organizacional atual a percepção dos gestores na identificação das vulnerabilidades em suas operações, pode ser o diferencial na competitividade. A evolução nos processos de tratamento e transporte de informações, com a informatização e conectividade, cria um nível de risco às operações, de grau importante. Este trabalho observou, em um universo de 376 empresas pesquisadas, em sua maioria no estado de São Paulo, como as ações na identificação de riscos, relacionados à segurança da informação, foram tratados e de que forma houve percepção dos gestores com relação aos incidentes que ocorreram e os prejuízos na operação.

1. Introdução

A TI Tecnologia da Informação mudou a forma de as organizações fazerem negócios. Os recursos tecnológicos como a interconexão das redes, a velocidade do tráfego dos conteúdos e sua acessibilidade tiveram mudanças profundas neste começo do século XXI.

No sentido da perenidade dos negócios são necessários profissionais qualificados no apoio às operações. Os gestores dependem da TI para acompanhar a dinâmica do mercado, identificar novas necessidades dos clientes, manter os dados estratégicos atualizados e se manterem competitivos nas suas operações.

Nesse novo cenário, os riscos nas operações também se modificam, onde a perda de informações ou a divulgação não autorizada pode ser mais fácil e trazer prejuízos consideráveis. Com a rápida evolução na forma de fazer negócios, a percepção dos gestores, no que se refere aos riscos pela falta de segurança das informações, pode ser um componente prejudicial na competitividade dos negócios, se não houver o devido alinhamento com os objetivos corporativos.

O objetivo deste trabalho é realizar uma avaliação quantitativa das ações de empresas quanto à segurança da informação, considerando: faixa de faturamento anual, ações para redução de incidentes de segurança da informação, implantação de políticas de segurança da informação, estruturação de departamento de TI, controles de incidentes de segurança da informação e impactos percebidos tanto com relação aos incidentes como com relação a perdas financeiras.

2. Revisão bibliográfica

2.1. Segurança da Informação, risco e métodos de medição.

O objetivo da segurança na informação é garantir a confidencialidade, integridade e disponibilidade das informações da empresa e também encontrar uma forma de manter controle para prestação de contas. Confidencialidade garante que os ativos relacionados à informática são acessados apenas por pessoal autorizado, integridade garante que os ativos relacionados a computadores são modificados apenas por pessoal autorizado e disponibilidade assegura que as informações sempre estarão disponíveis quando necessário e seus recursos têm *performance* adequada (BISHOP, 2003; PFLEEGER & PFLEEGER, 2003; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27002:2013). Autenticidade garante prova de origem de mensagem (STACKPOLE, 2004) confidencialidade, integridade, disponibilidade e prestação de contas podem ser asseguradas por processamento de informações com uso de controles eletrônicos e físicos, reforçando políticas de segurança e procedimentos para reduzir o risco de comprometimento do sistema. Uma abordagem que contempla de forma aceitável o controle de segurança da informação é a

gestão de risco. O risco é a probabilidade e o custo de uma ameaça explorando uma vulnerabilidade existente (KAPLAN, 2004). Uma ameaça é a circunstância que tem o potencial de causar perda ou dano ao patrimônio. A vulnerabilidade é um ponto fraco na segurança que pode permitir que uma ameaça cause perda ou dano ao patrimônio. De acordo com Ozier (2004), os seis elementos primitivos da modelagem de risco são:

I. Valor patrimonial: A identificação de ativos tangíveis e intangíveis em risco e o seu valor em termos monetários ou não monetários - valor de custo de reposição como o bem, como o valor da disponibilidade de informações de ativos, integridade e confidencialidade.

II. Frequência da ameaça: Quantas vezes uma ameaça poderia ocorrer em uma base anual.

III. Fator de exposição a ameaça: Medida da magnitude da perda de valor de ativos decorrentes a partir de um evento de ameaça, expressa como uma percentagem que varia de 0 a 100.

IV. Salvaguarda da eficácia: O grau em que a salvaguarda pode ser caracterizada como efetiva para mitigar a vulnerabilidade e reduzir o risco associado de perda, expressa em percentagem de 0 a 100.

V. Custo de salvaguarda: O custo de uma série de medidas de redução de risco que detecta, previne, ou minimiza a perda associada à ocorrência de ameaça ou de categoria especificada de ameaças.

VI. Incerteza: Termo que caracteriza o grau em que há menos confiança no valor de qualquer elemento de avaliação do risco, expresso em percentagem de 0 a 100.

Os métodos quantitativos e qualitativos referem-se fundamentalmente a diferentes regimes e métricas tradicionalmente utilizados para a medição de alguns ou de todos os elementos de risco (OZIER, 2004).

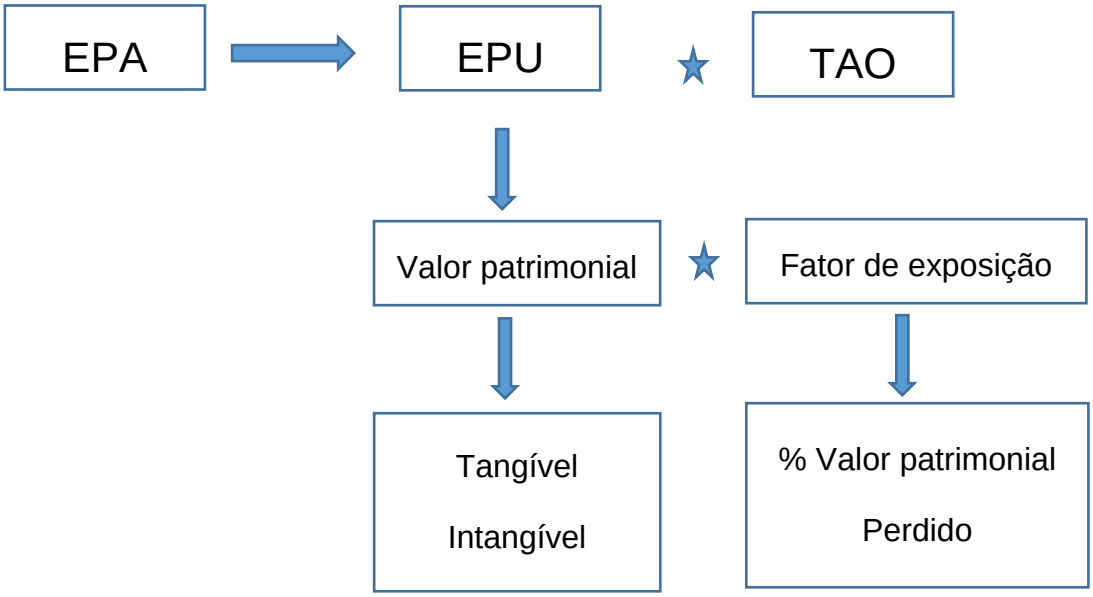
2.2. Medição Quantitativa de Riscos

Se os seis elementos primitivos da modelagem de risco, (1) valor patrimonial, (2) frequência da ameaça, (3) fator de exposição a ameaça, (4) salvaguarda da eficácia, (5) o custo de salvaguarda e (6) a incerteza, são todos quantificados com métricas objetivas de

forma independente, a análise do processo pode ser caracterizada como totalmente quantitativa (OZIER, 2004).

A Expectativa de Perda Anual (EPA) é o valor usado, tradicionalmente, para expressar a perda monetária, para ativos associados com um risco identificado, que ocorre dentro do período de um ano (BELL, 2015; SHIMONSKI, 2015). A EPA é calculada como mostrado na Figura 12, onde EPU é a Expectativa de Perda Única, é a quantidade estimada de dinheiro que seria perdida caso o risco identificado ocorresse, e a TAO é Taxa Anualizada de Ocorrência, é a frequência com que o risco está previsto para ocorrer no prazo de um ano (BELL, 2015; SHIMONSKI, 2015).

Figura 12 – Cálculo da Expectativa de perda anual (EPA)



Fonte: Adaptado de Shimonski, 2015

O cálculo da EPA requer a determinação de um valor em dólares para os ativos, tangíveis e intangíveis, associado a um risco identificado (SHIMONSKI, 2015). Para os ativos tangíveis, o custo para reparação, compra, instalação, configuração, substituição ou recuperação deve ser considerado (OZIER, 2004; SHIMONSKI, 2015). O cálculo do EPA também inclui a determinação do valor de ativos intangíveis de informações:

- **Disponibilidade**: Para um site de e-commerce, quanto dinheiro seria perdido se o local não estiver disponível para os clientes por um determinado período de tempo? Para um sistema crítico de negócios, quanto dinheiro seria perdido se os funcionários fossem incapazes de trabalhar por causa de indisponibilidade do sistema? (SHIMONSKI, 2015).

- **Integridade**: Dependendo da natureza da falha e opções de recuperação disponíveis, a precisão dos dados recuperados pode estar prejudicada, em parte ou na sua totatidade, ou nem ser possível. Que impacto financeiro têm, na empresa, dados imprecisos ou incompletos? (OZIER, 2004) e

- **Confidencialidade**: Que impacto financeiro produziria a revelação de informações confidenciais ou dados secretos de uma entidade pública ou privada? (OZIER, 2004).

Em medidas do fator de exposição, quantos por cento do valor dos ativos é perdido por causa da ocorrência de um risco identificado? (BELL, 2015). Caso um roteador fosse exposto a um risco físico, quantos por cento do valor do roteador seria perdido? Devem ser dados secretos expostos ao público? Qual o valor perdido por causa da exposição? (YOUNG, 2004) Qual seria o custo subjacente associado com a perda da confiança do público em uma empresa com risco identificado?

Para determinar o TAO, gerentes de risco dependem de dados históricos para estimar a frequência com que pode ocorrer um risco identificado dentro de um período de um ano. Estatísticas do Departamento de Polícia sobre a criminalidade, os dados das empresas de seguros com relação às ocorrências de riscos semelhantes, dados de agências de notícias, monitoramento de incidentes de computador com dados de organizações, informações de tempo médio entre falhas em equipamentos podem ser usados para determinar a TAO (SHIMONSKI, 2015). Se uma ameaça ocorre uma vez em 5 anos tem um TAO de 1/5 ou 0,2 (BELL, 2015; OZIER, 2004). A ameaça ocorre 40 vezes em um determinado ano tem uma TAO de 40,0 (OZIER, 2004).

Uma vez que EPU e TAO são determinados para um risco identificado, a EPA pode ser calculada e usada diretamente em uma análise de custo-benefício para determinar se deve aceitar, mitigar ou transferir o risco em questão, com a regra de ouro, não pagar mais para atenuar o risco do que os bens afetados valem (BELL, 2015).

A quantificação de risco de segurança da informação em um prazo razoável é uma difícil tarefa (KAPLAN, 2004; OZIER, 2004). Na verdade, é impossível realizar uma avaliação puramente quantitativa de riscos de segurança da informação (KAPLAN, 2004; OZIER, 2004). Os primeiros esforços para realizar essas avaliações quantitativas de risco, experimentaram considerável dificuldade (OZIER, 2004):

Um conjunto verificável e confiável de métricas de risco e as estatísticas não foram estabelecidos nem mantidos, pois as abordagens eram variadas; a avaliação de risco oferecia dificuldade para ser executada; o mapeamento era denso e complexo; o emparelhamento e o cálculo eram obrigados a construir modelos de risco representativos de grandes quantidades de dados coletados; o trabalho era feito manualmente, não havia disponibilidade de nenhum software nem equipamentos para avaliação de risco; devido à grande quantidade de tempo que era necessária, a concentração de recursos para preparar avaliações era uma grande preocupação; os resultados não eram confiáveis, (OZIER, 2004).

Colocar um valor monetário em todos os ativos de informação tangíveis e intangíveis, incluindo a sua disponibilidade, confidencialidade e integridade; calcular a perda de valor de ativos e identificar a exposição ao risco; estimar a frequência de ocorrência de risco para a aplicação de risco quantitativo. Pode-se facilitar os cálculos de avaliação e fornecer uma base para uma melhor compreensão das perdas esperadas. No entanto, muitas organizações não possuem os recursos adequados para reunir as informações necessárias para acomodar esses cálculos em um tempo razoável, mesmo com o uso de ferramentas automatizadas (WARE, 2005).

De acordo com Young (2004), a análise de risco convencional (quantitativa) é uma poderosa ferramenta para o gerenciamento de risco, mas funciona melhor quando se analisa de forma estática ou evoluindo lentamente em sistemas como, padrões de tráfego, ou fenômenos terrestres. A prática geral de profissionais de gestão de risco é se fortalecer contra as ameaças do passado, bem como a natureza dos criminosos de computador é atacar pontos mais fracos do sistema (YOUNG, 2004).

As organizações não estão dispostas a denunciar as brechas de segurança da informação para criação de uma base de conhecimento por medo de diminuir a confiança do público, tornando-se alvo de ataques futuros, nem de admitir a responsabilidade pela divulgação de informções de clientes, entre outros motivos. Os dados históricos de ameaças são essenciais para cálculos quantitativos de razoável precisão, na medição de risco (BELL, 2015; OZIER, 2004; SHIMONSKI, 2015). Informações voláteis dos ambientes de processamento, ameaças cada vez mais criativas e a falta de histórico de ameaças com dados suficientes para se realizar uma análise e avaliação de riscos de segurança da informação, utilizando métodos quantitativos convencionais, transformam essa tarefa de difícil execução na melhor das hipóteses, com a confiabilidade dos cálculos em constante questionamento (OZIER, 2004; GAO, 1999; YOUNG, 2004).

Um desafio adicional a essa questão é garantir profissionais de segurança da informação qualificados em tempo suficiente para que se dediquem a reunir e analisar as informações necessárias para realizar avaliações válidas (WARE, 2005)

2.3. Medição Qualitativa de Riscos

A abordagem qualitativa para medição de risco, geralmente inclui uma avaliação subjetiva do impacto em uma organização, por exemplo, o que seria afetado, ou qual a extensão do dano, dada a ocorrência de um conjunto de cenários de ameaças breves que envolvem, por exemplo, intrusos, criminosos, funcionários descontentes, terroristas, desastres naturais, com base na melhor estimativa de uma equipe de profissionais experientes (administradores de segurança do sistema e gerentes de aplicativos de negócios) (HENRY, 2004; GAO, 1999).

Abordagens qualitativas para medição de risco não exigem de forma independente métricas objetivas para os seis elementos primitivos da modelagem de risco, conforme identificado por Ozier (2004). São caracterizadas pela aplicação de medidas de risco organizadas, num formato de matriz, para descrever o risco ou gravidade ou extensão da perda de ativo, dada a ocorrência de um cenário de risco identificado (HENRY, 2004; OZIER, 2004). Os *rankings* da matriz são baseados em dados recolhidos através de entrevista e / ou questionários das partes interessadas conhecidas (HENRY, 2004; OZIER, 2004). A figura 13 [a partir de Ozier (2004)] ilustra a avaliação da disponibilidade dos ativos e da informação e escala de risco associados. (ABNT NBR ISO/IEC 27005:2008).

Figura 13 – Valor da disponibilidade da informação e o risco associado

		VALOR		
		BAIXO	***MÉDIO***	***ALTO***
RISCO	***BAIXO***			
	MÉDIO			
	ALTO			

Fonte: Adaptado de Ozier, 2004

A estratégia de usar essa abordagem é das áreas de sombreamento mais forte para áreas de sombreamento menor, ações imediatas, planos de correção ou aceitação do risco

(OZIER, 2004). A figura 14, mostra o conceito aplicado pelo United States General Accounting Office (GAO) (1999).

Figura 14 – Matriz de avaliação de risco

NIVEL DE GRAVIDADE	PROBABILIDADE DE OCORRENCIA				
	(A) FREQUENTE	(B) PROVAVEL	(C) OCASIONALMENTE	(D) REMOTO	(E)IMPROVÁVEL
I(ALTO)					
II					
III					
IV(BAIXO)					

RISCO 1 (indesejável e requer medidas correctivas imediatas)
RISCO 2 (indesejável e requer medidas correctivas, mas é permitido a gestão planejar a execução)
RISCO 3 (aceitável com avaliação pela gerência)
RISCO 4 (aceitável sem avaliação pela gerência)

Fonte: Adaptado de GAO, 1999

Os cenários com níveis de gravidade são definidos, como segue:

- Categoria I: morte, perda de informações críticas proprietárias, interrupção do sistema, ou grave dano ambiental;
- Categoria II: lesão grave, perda de informações confidenciais, doença ocupacional grave, ou grande sistema ou danos ambientais;
- Categoria III: pequenas lesões, doenças ocupacionais menores, ou sistema menor ou danos ambientais;
- Categoria IV: menos que pequenas lesões, doenças ocupacionais, ou menos do que menor sistema ou danos ambientais.

Os cenários com níveis de probabilidades são definidos, como segue:

- Categoria A (freqüente) – Possibilidade de repetidos incidentes;
- Categoria B (provável)– Possibilidade de incidentes isolados;
- Categoria C (ocasional) – Possibilidade de alguma ocorrência;
- Categoria D (remoto) – Não é provável que ocorra;
- Categoria E (improvável) - Praticamente impossível.

Verificando a figura 14, os riscos de 1 a 4 são categorias que descrevem a aplicação de políticas da organização na quais os riscos são inaceitáveis. Tornam-se então, necessárias ações corretivas.

O GAO (1999) realizou um estudo com quatro organizações privadas que passaram por programas de segurança ou estavam perseguindo ativamente a melhoria nas práticas de avaliação de risco com base em métodos de avaliação de risco (GAO,1999). Os organismos foram escolhidos com base na recomendação do governo e fontes do setor privado. O estudo identificou seis fatores-chave para os programas de avaliação de risco de sucesso, sendo que essas organizações não tentaram quantificar com precisão o risco (GAO, 1999). Os métodos de avaliação de risco e ferramentas desenvolvidas eram "simples e, em sua maior parte, de natureza qualitativa" (GAO, 1999).

A análise de risco e avaliação utilizando a abordagem qualitativa não exigem a aquisição de grandes quantidades de dados para o cálculo da frequência de ameaça ou a determinação da disponibilidade de informação, confidencialidade, integridade e valor (OZIER, 2004). No entanto, a qualidade dos resultados da avaliação depende muito do conhecimento e experiência da equipe de condução da avaliação (GAO, 1999). Uma avaliação de risco qualitativa eficaz, vai descobrir áreas de risco inaceitável, caso existam, e em que ponto será necessário proceder-se a uma análise mais profunda, de preferência usando uma combinação dos métodos qualitativos e quantitativos para determinar o curso rentável de ação para mitigar o risco identificado (HENRY, 2004).

3. Metodologia

A pesquisa foi realizada entre 2013/2014, durante 10 meses por intermédio de um questionário estruturado na plataforma SurveyMonkey, cujas respostas foram tabuladas em Excel. A amostra original foi uma lista aleatória de 4000 empresas de todos os setores da economia e de todas as regiões do Brasil. Enviou-se convite para participar da pesquisa a todas as empresas obtendo-se resultado de 376 respondentes.

A ferramenta de avaliação utilizada foi constituída de sistema de respostas simples que acomodavam os dados em planilha de Excel. Essa planilha foi utilizada posteriormente no tratamento das informações. O tratamento das informações foi de forma estatística, com a utilização de filtros da própria ferramenta. As células não possuíam integração correlacional, conforme figura 15.

Figura 15 – Amostra dos dados em Excel utilizados na pesquisa

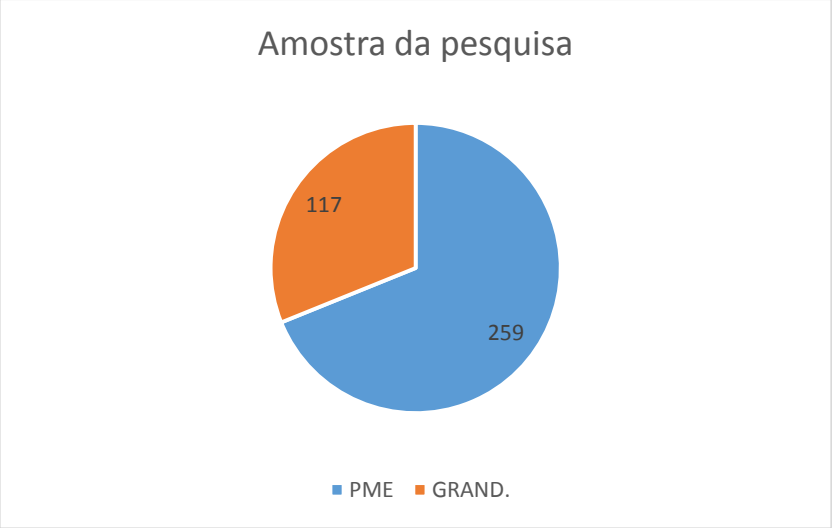
Faturamento médio ou arrecadação média anual:	A empresa	A empresa realiza revisões periódicas na política de				
Entre R$ 2,4 milhões e R$ 16 milhões	Não	Sim				
Entre R$ 90 milhões e R$ 300 milhões	Não	Não				
Não sei informar	Não	Não				
Não sei informar	Não	Sim				
Entre R$ 16 milhões e R$ 90 milhões	Não	Não				
Até R$ 2,4 milhões	Não	Não				
Entre R$ 16 milhões e R$ 90 milhões	Não	Sim				
Não sei informar	Não	Não				
Até R$ 2,4 milhões	Não	Não				

Fonte: Elaborado pelo autor.

O questionário enviado possuía 50 perguntas. Tratava-se de pesquisa abrangente para mapear o mercado de TI nas empresas pesquisadas, parte das questões relacionadas à segurança da informação foi utilizadas para os levantamentos deste trabalho. Dentre cada bloco de informações os dados foram apurados por porte de empresa, para que fosse possível identificar as diferentes condutas, conforme o faturamento anual.

Na identificação das empresas pesquisadas, obtiveram-se 259 empresas de pequeno e médio porte e 117 empresas de grande porte, (Figura 16).

Figura 16 – Gráfico da amostra da pesquisa



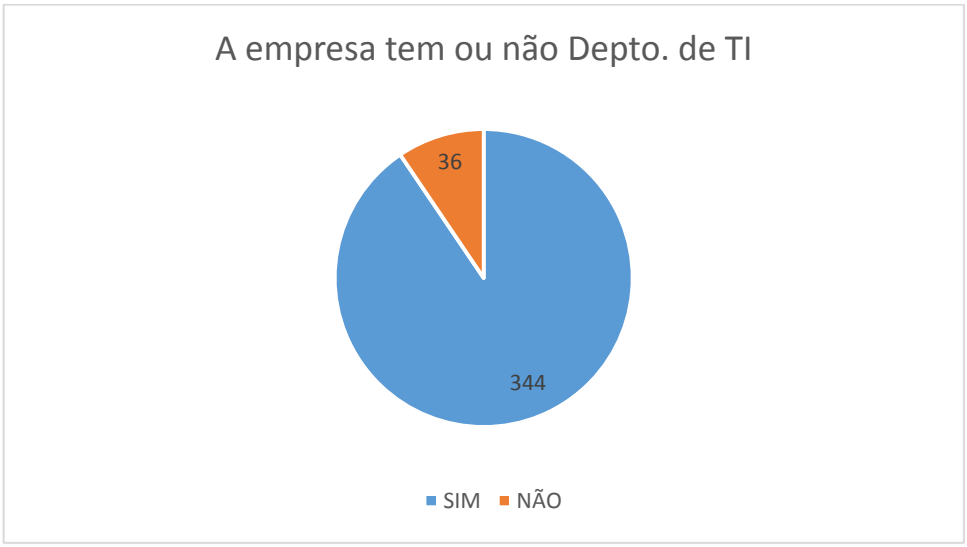
Fonte: Elaborado pelo autor.

3. Resultados e discussões

Dentre as respostas obtidas, um dos itens iniciais foram com relação a se essas empresas tinham ou não departamentos de TI, conforme a figura 17 identificou-se que 344 empresas tinham departamento de TI, devidamente constituído.

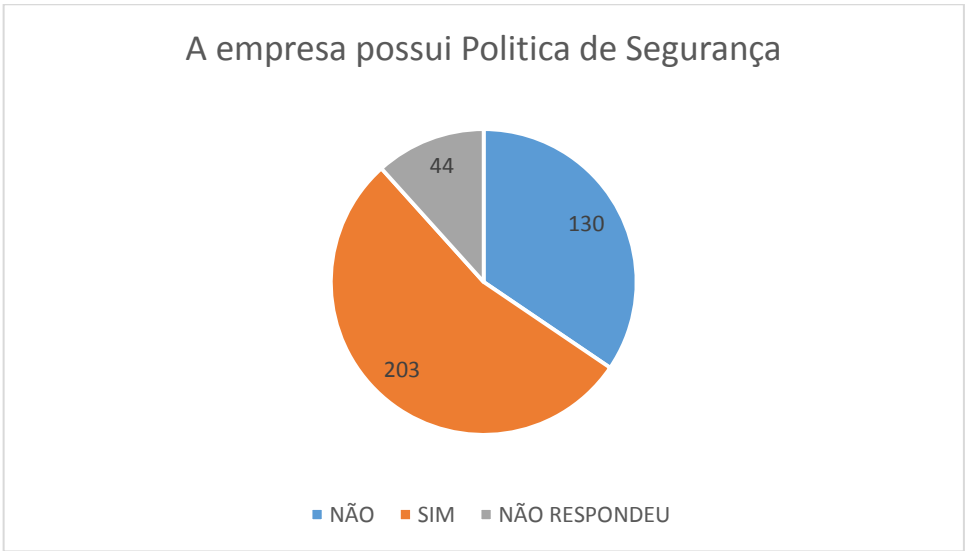
Ainda na identificação inicial, verificou-se se as empresas possuíam ou não política de segurança da informação. Duzentas e três empresas do universo pesquisado possuíam política de segurança da informação devidamente constituída, (Figura 18).

Figura 17 – Identificação da quantidade de empresas que têm ou não depto. de TI



Fonte: Elaborado pelo autor.

Figura 18 – Quantidade de empresas que possuem política de segurança da informação

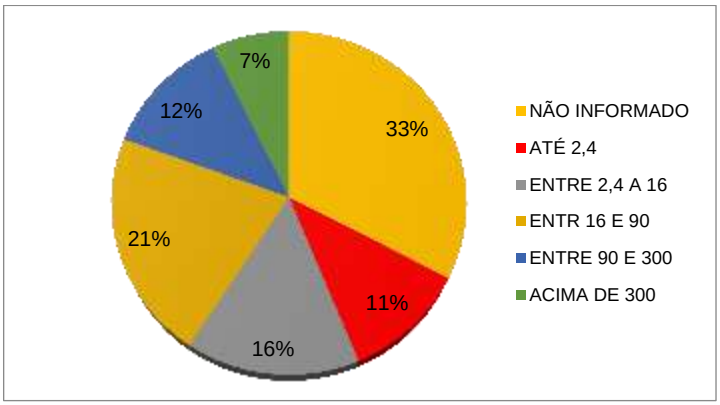


Fonte: Elaborado pelo autor.

Foram levantadas questões com relação a revisões das políticas de segurança, se a empresa teve ou não incidentes de segurança. Havendo a identificação de incidentes se, perguntou-se se foi possível identificar o prejuízo financeiro. Indagou-se, também, sobre quais ferramentas de prevenção/proteção as empresas estão utilizando. Houve muitas questões relacionadas ao controle que essas empresas têm de suas operações e de que forma reagiram a ocorrências de falhas.

Dentre os respondentes, traçou-se o seguinte perfil conforme o faturamento anual em R$, (Figura 19):

Figura 19 – Distribuição dos respondentes pelo faturamento, em milhões de reais

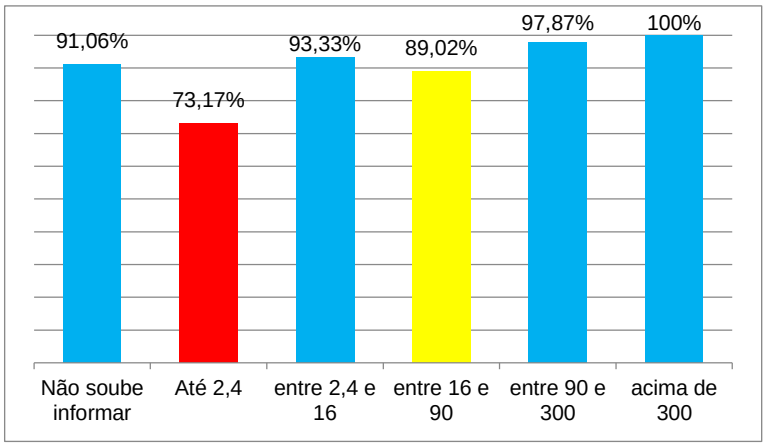


Fonte: Elaborado pelo autor.

Conforme observado na figura 19, 33% dos respondentes não souberam informar o faturamento anual. Dentre os que informaram esse parâmetro, houve maior concentração de empresas com faturamento anual entre 16 e 90 milhões de reais (21%), em seguida empresas que faturam entre 2,4 e 16 milhões (16%), entre 90 e 300 milhões (12%), até 2,4 milhões (11%) e acima de 300 milhões (7%). A concentração de empresas é no estado de São Paulo, com 331 empresas, ou 89 %.

A primeira avaliação feita relaciona-se às empresas que possuíam departamentos de TI, 90% das empresas responderam que sim, possuíam departamentos de TI ou algum outro departamento responsável por essa função. Essa média também foi acompanhada mesmo se avaliado por faturamento das empresas, a não ser as que faturam menos de 2,4 milhões ano, (Figura 20).

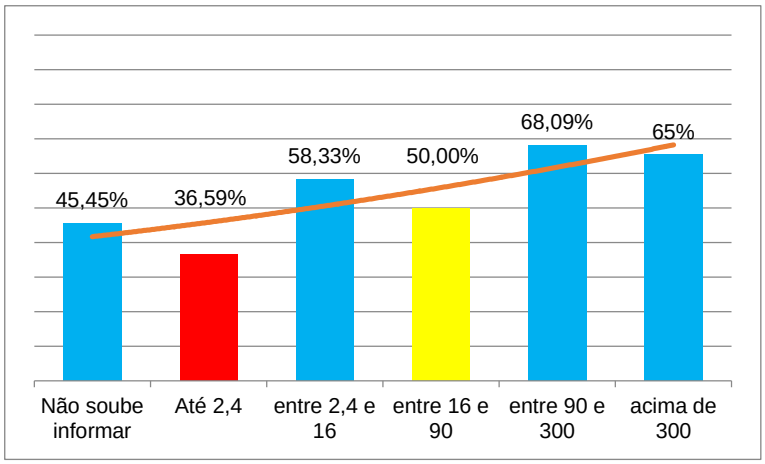
Figura 20 – Empresas que possuem departamento de TI, de acordo com faixa de faturamento anual em milhões de reais



Fonte: Elaborado pelo autor.

Quando foi perguntado à empresa se possuía política de segurança da informação formalmente estabelecida, os resultados foram claros com relação a preocupação das empresas em estabelecer uma política, mas não tão fortes como ter um profissional ou departamento responsável pela área de TI, (Figura 20). Observou-se que, à medida que o faturamento anual das empresas é maior, de forma diretamente proporcional, essas empresas possuem política de segurança formalmente estabelecida. Essa constatação é mais forte ainda quando este faturamento é superior a 90 milhões ano, o que leva a concluir que corporações com faturamento maior são mais sensíveis a fraudes, ataques de violação de segurança e consequentemente se estruturam melhor para evitar essas ocorrências.

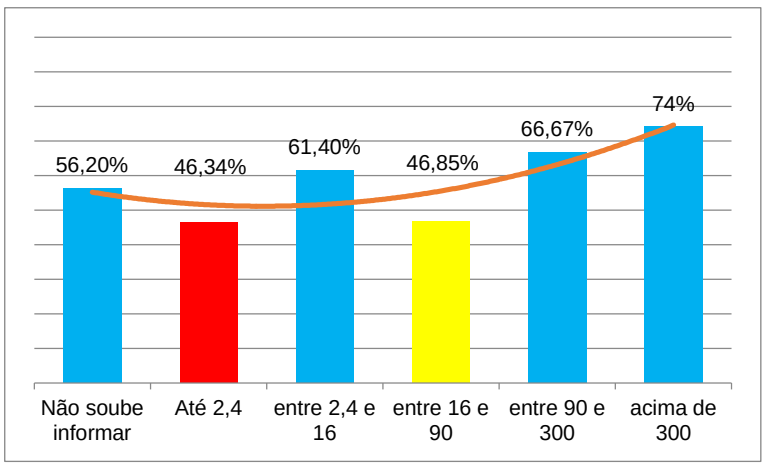
Figura 21 – Empresas que possuem política de segurança formalmente estabelecida, de acordo com faixa de faturamento anual em milhões de reais e curva de tendência



Fonte: Elaborado pelo autor.

A avaliação sistemática da política de segurança da informação também foi avaliada nesta pesquisa, conforme figura 22:

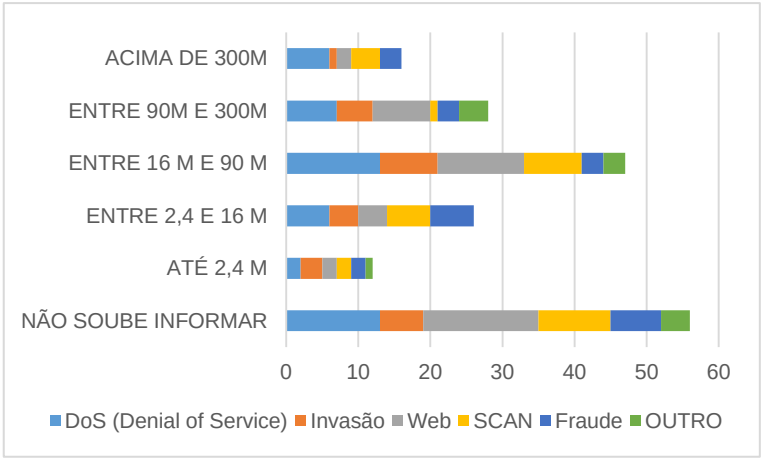
Figura 22 – Empresas que realizam avaliações periódicas da PSI, de acordo com faixa de faturamento anual em milhões de reais e curva de tendência



Fonte: Elaborado pelo autor.

Avaliando todas as faixas de empresas por faturamento, um bloco tem comportamento diferente da tendência constatada, ou seja, nas três questões, empresas que possuem departamento de TI, empresas que têm política de segurança formalmente definida e empresas que revisam sua política periodicamente, à medida que o faturamento anual sobe, sobe também o percentual de empresas que atende essas três questões, apenas o bloco composto por empresas com faturamento anual entre 16 e 90 milhões de reais ao ano, isto não acontece. Observa-se uma ligeira queda nas três questões só nesse bloco.

Figura 23 – Incidentes de segurança relatados, de acordo com faixa de faturamento anual em milhões de reais

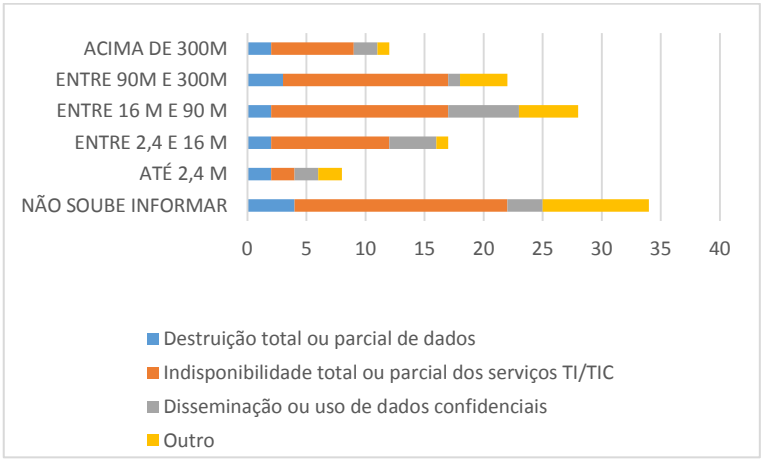


Fonte: Elaborado pelo autor.

Quando se realiza uma comparação entre as ações que as empresas estavam tomando com relação à segurança da informação, ou seja, devida estruturação de um departamento de TI, formalização de política de segurança e revisões periódicas dessa política com as ocorrências de incidentes de segurança da informação, (Figura 23), constata-se que nos extremos, ou seja, empresas com faturamento até 2,4 milhões de reais ao ano e empresas com faturamento superior a 300 milhões de reais ao ano, existe uma menor incidência de ocorrências.

Empresas com menor faturamento têm também menor percepção de incidentes, por falta de indicadores competentes. Já as empresas com maior faturamento, por terem essa questão bem definida em sua estrutura, possuem sistema de avaliação e devido os investimentos para prevenção, passam por menor número de incidentes. Quando se avaliam os outros blocos de empresas, constata-se que, à medida que o faturamento aumenta, devido aos investimentos em prevenção, o número de incidentes diminui, a não ser, novamente, no bloco de empresas com faturamento entre 16 e 90 milhões de reais.

Figura 24 – Impacto percebido pelas empresas, com ocorrências de incidentes de Segurança da Informação, de acordo com faixa de faturamento anual em milhões de reais

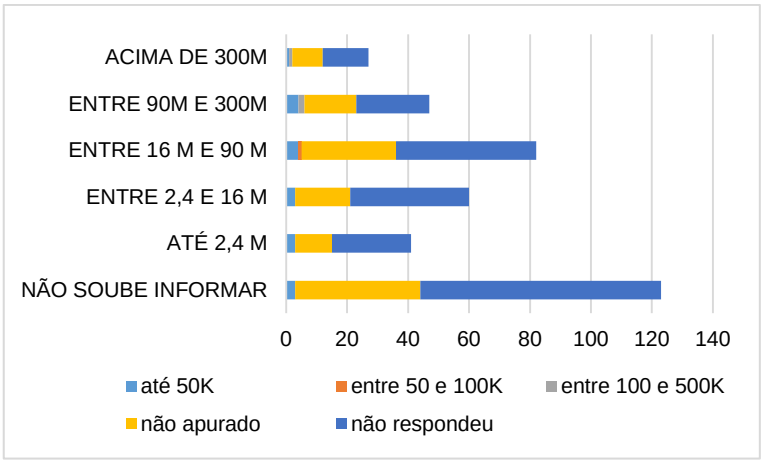


Fonte: Elaborado pelo autor.

Na avaliação do impacto percebido pelas empresas, em todas as faixas de faturamento, a indisponibilidade total ou parcial dos serviços de TI/TIC, foi a maior incidência, (Figura 24).

Dado preocupante constatado na avaliação da percepção de impacto financeiro foi que mesmo percebendo que incidentes prejudicaram a empresa, a percepção de valor em poucos casos foi avaliada, (Figura 25).

Figura 25 – Impacto financeiro percebido pelas empresas, com ocorrências de incidentes de Segurança da Informação, de acordo com faixa de faturamento anual em milhões de reais

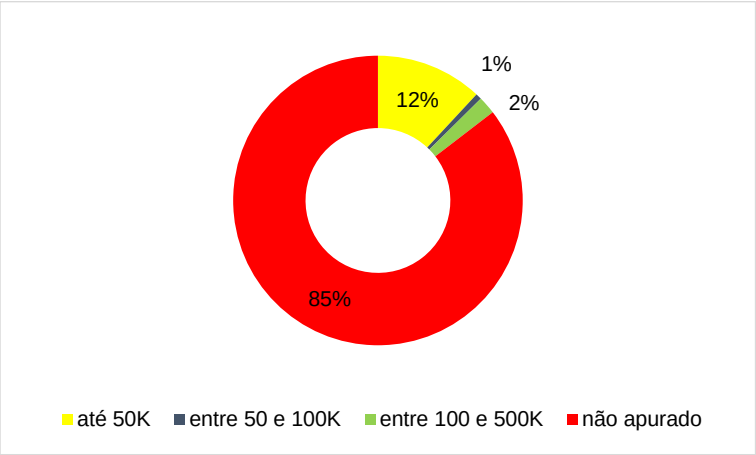


Fonte: Elaborado pelo autor.

Observa-se que em 85% dos casos as empresas não souberam apurar o prejuízo causado por incidentes de segurança da informação, (Figura 26), em demonstração clara da falta de mecanismos de controle e apuração de ocorrências. Esses valores podem reduzir a

competitividade dessas empresas já que suas operações podem estar mais caras sem uma clareza na formação de custos.

Figura 26 – Impacto financeiro percebido pelas empresas, com ocorrências de incidentes de Segurança da Informação



Fonte: Elaborado pelo autor.

5. Conclusão

Em consonância com os objetivos do trabalho, a saber, avaliação quantitativa das ações quanto à segurança da informação, identificou-se que, dentre as empresas que possuem ações para redução de incidentes de segurança da informação, cerca de 92% possuem departamento de TI ou profissional devidamente formalizado; 52% dessas empresas, independentemente da faixa de faturamento, possuem política de segurança da informação.

Particularmente em relação às empresas que possuem política de segurança da informação, 56% realizam revisões periódicas, indicando preocupação com esta ação no sentido de preservar suas operações. Quando se buscou identificar o controle efetivo de incidentes de segurança da informação, verificou-se porção importante de empresas que não tinham esses dados de forma precisa: 51% não souberam informar se sofreram algum incidente, 68% não souberam nem idenificar o impacto percebido na operação e 85%, das empresas que sofreram algum incidente, não tinham a informação dacerca de prejuizos financeiros ocasionados por esses incidentes de segurança da informação. Tais resultados evidenciam uma possível desconexão entre a efetivação de políticas de segurança da informação e demais ações para preservação das operações das empresas. Nesse sentido, verifica-se a necessidade de controle de incidentes de segurança da informação e de ações preventivas.

Outro resultado revelado na pesquisa é uma tendência à melhoria nas ações em direção a redução de incidentes de segurança da informação à medida em que a faixa de faturamento aumenta.

Como continuidade da presente pesquisa, propõe-se a identificação de ações ou melhores práticas no tratamento de incidentes de segurança da informação, com objetivo de redução de perdas e preservação das operações.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002. **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas, 2013.

ABNT NBR ISO/IEC 27005. **Tecnologia da Informação** – Técnicas de segurança – Gestão de riscos de segurança da informação. Associação Brasileira de Normas Técnicas, 2008.

BELL, M. Z.,. Risky Thinking - On Threat Analysis and Business Risk Management, **Albion Research Ltd**., Dunrobin, Ontario, Canada. Http://www.riskythinking.com/glossary/annualized_loss_expectancy.php. (current 17 Maio 2015).

BISHOP, M.. Computer Security: Art and Science. **Addison-Wesley**, Boston, Massachusetts, 2003.

HENRY, K.. Risk Management and Analysis,- **In Information Security Management Handbook**, 5th edition, ed. H.F. Tipton and M. Krause, Auerbach Publications, Boca Raton, Florida, pp. 751-758, 2004.

Information Security Management and Assurance (2000). **A call to action for corporate governance**. Retrieved September8, 2011, from http://www.aicpa.org/assurance/systrust/ press/report_b.htm

KAPLAN, R. . A Matter of Trust, **In Information Security Management Handbook**, 5th edition, ed. H. F. Tipton and M. Krause, Auerbach Publications, Boca Tation, Florida, pp. 727-750, 2004.

OZIER, W. . Risk Analysis and Assement, **In Information Security Management Handbook**, 5th edition, ed. H. F. Tipton and M. Krause, Auerbach Publications, Boca Raton, Florida, pp. 795-820, 2004.

PFLEEGER, C. P.; PFLEEGER, S. L. . **Security in Computing**, 3rd edition, Prentice Hall, Upper Saddle River, New Jersey, 2003.

SHIMONSKI, R. J.. Risk Assessment and Threat Identification,- **TechGenix,** Ltd., St. Julians, Malta. <http://www.windowsecurity.com/articles/Risk_Assessment_and_Threat _Identification.html>. (current 17 Maio 2015).

STACKPOLE, B.. Application-Layer Security Protocols for Networks, **In Information Security Management Handbook**, 5th edition, ed. H.F. Tipton and Krause, Auerbach Publications, Boca Raton, Florida, pp. 435-445, 2004

United States General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, **A Supplement to GAO's May 1998 Executive Guide on Information Security Management**, (GAO/AIMD-99-3), Accounting and Information Management Division,.http://www.gao.gov/special.pubs/ai00033.pdf.,1999.

YOUNG, B. R.. New Trends in Information Risk Management,- **In Information Security Management Handbook**, 5th edition, ed. H.F. Tipton and M. Krause, Auerbach Publications, Boca Raton, Florida, PP. 759-765, 2004.

WARE, L. C.. The State of Information Security 2004: Best Practices; **A Worldwide Study Conducted by CIO Magazine and Pricewaterhouse Coopers**, CIO Research Reports, CXO Media Inc. http://www.csoonline.com/csoresearch /report82.html. (current 03 Jan. 2005).

6 ARTIGO 3 - Análise de incidentes e ações para segurança da informação: uma comparação entre o uso de recursos tecnológicos e o investimento em treinamento e capacitação

6.1. Considerações iniciais

Este artigo será apresentado na RAE, para submissão. Foram utilizadas as respostas de 376 empresas em pesquisa realizada em 2013/2014, com objetivo de mapear o mercado de TI, parte da pesquisa teve foco na área de segurança da informação.

ANÁLISE DE INCIDENTES E AÇÕES PARA SEGURANÇA DA INFORMAÇÃO: UMA COMPARAÇÃO ENTRE O USO DE RECURSOS TECNOLÓGICOS E O INVESTIMENTO EM TREINAMENTO E CAPACITAÇÃO.

Emerson José Beneton – Universidade Paulista – UNIP

Rodrigo Franco Gonçalves – Universidade Paulista – UNIP

Getúlio Kazue Akabane – FATEC

Ivanir Costa - UNINOVE

Resumo

A redução de incidentes, no que se refere à segurança da informação, que podem trazer prejuízos ou paralisação das empresas é de vital importância na competitividade das empresas, em um ambiente de alta interconexão das corporações e vulnerabilidades complexas. A sustentabilidade da empresa pode estar em perigo devido a possibilidade de incidentes de segurança da informação. Em uma análise de 376 empresas, foi possível identificar, de acordo com a faixa de faturamento anual, percepções das empresas com relação a incidentes de segurança da informação, problemas enfrentados, prejuízos nas operações e ações para redução destes incidentes, o uso das políticas de segurança da informação, acesso a recursos tecnológicos e treinamento de equipes para conscientização.

1. Introdução

Em estudo recente da FIESP (2015), identificou-se que os ataques cibernéticos estão sendo realizados tanto com foco em empresas de grande porte como em empresas de menor

porte, democratizando, assim, essa incidência e trazendo prejuizos a todas as empresas, independente de seu tamanho. Com a estruturação da economia, com a competitividade mais forte e com o momento particular que o Brasil enfrenta, a preocupação das empresas em preservar suas operações torna-se ponto focal.

Segundo a pesquisa da FIESP (2015) a maioria das empresas ainda possui falta de conhecimento sobre segurança da informação, na mesma pesquisa 35% das empresas pesquisadas informaram que os ataques que sofreram foram bem sucessidos, numa escala de 1% a 25%, destacando-se que essa resposta teve um percentual de 46% quando o respondente era empresa de medio porte.

Quando se verificou a relação entre utilização de ferramentas tecnológicas e treinamento, a pesquisa da FIESP (2015) apresentou outro dado a ser observado, 96% apresentaram alguma ferramenta tecnológica para sua proteção, por outro lado. A pesquisa também mostrou que, apenas 21% executavam treinamentos para sua proteção.

De acordo com a ABNT NBR ISO/IEC 27002(2013), a segurança que pode ser obtida por intermédio de tecnologia é limitada e deve ser apoiada por procedimentos e formas de gerenciamento apropriados. Dentre as ferramentas para proteção de ativos, existem os softwares de detecção e remoção de softwares mal intencionados, os Firewalls, utilizados para proteção periférica das redes de comunicação (ISO 27000, 2014). Além disso, treinamento e conscientização das equipes devem ocorrer de forma a promover o conhecimento sobre segurança da informação, facilitando, dessa forma a aplicação de normas e condutas estabelecidas nas políticas de segurança da informação (ABNT NBR ISO/IEC 27002, 2013).

O objetivo deste trabalho é apresentar uma análise comparativa entre empresas que possuem recursos tecnológicos na preservação de suas operações e empresas que investem em treinamento de suas equipes, com objetivo de reduzir incidentes de segurança da informação. Para tal utiliza-se um levantamento (survey) com 376 empresas.

2. Revisão bibliográfica

2.1. Segurança da informação

O principal objetivo de qualquer programa de segurança da informação na empresa é apoiar o usuário, fornecendo proteção aos recursos do sistema de informações em níveis adequados de integridade, disponibilidade e confidencialidade, sem afetar a produtividade,

inovação e criatividade no avanço da tecnologia dentro da corporação (Tipton & Krause, 2000). De acordo com o Glossário da Segurança da Informação, a integridade é a garantia de que a informação é autêntica e completa, atestando que ela pode ser utilizada e é suficientemente precisa para a sua finalidade. A integridade do sistema é definida como a capacidade do sistema para proteger-se contra o acesso de usuários não autorizados, evitando que haja comprometimento dos dados (IBM Corporation, 2011). O departamento de Segurança Interna publicada US-Cert (2011) afirma que os dois componentes-chave da integridade do sistema são autenticidade de *software* e certeza da identidade do usuário (US-CERT, 2011).

Os três conceitos básicos de segurança que são importantes para informações na internet são confidencialidade, integridade e disponibilidade. A Figura 27 mostra os três objetivos básicos em segurança da informação e sistemas de informação (NIST, 2004). No contexto de informações seguras, confidencialidade refere-se a limitar o acesso à informação e divulgação a apenas usuários autorizados, impedindo o acesso ou divulgação para àqueles não autorizados (Universidade de Miami, Miller School of Medicine, 2006). O aceso ilegal a informações confidenciais pode causar repercussão prejudicial. Integridade refer-se a proteger as informações para que não sejam modificadas por terceiros não autorizados (CHIA, 2012). Integridade no contexto de segurança da informação não se refere apenas à integridade da informação em si, mas também à garantia com relação à origem da informação (integridade da fonte de informação). Por fim, a disponibilidade de informações refere-se a assegurar que as partes autorizadas são capazes de acessar as informações quando necessário (CHIA, 2012).

Figura 27 – Potencial impacto

Objetivo de segurança	Definição	Impacto de perda
Confidencialidade	Preservar autorizações de acesso à informações e a divulgação, incluindo os meios necessários para proteção da privacidade e informações pessoais.	A perda de confidencialidade é a divulgação não autorizada da informação.
Integridade	Proteção contra modificações ou destruição da informação, inclui a garantia de autenticidade.	A perda da integridade é a modificação ou destruição não autorizada da informação.
Disponibilidade	Garantir o acesso correto e sempre que necessário às informações.	A perda de disponibilidade é o rompimento de acesso ou uso de informações ou sistema de informações.

Fonte: Elaborado pelo autor.

Os conceitos relacionados com pessoas que usam informações são: autenticação, autorização e não repúdio (PESANTE, 2008). Portanto, quando a informação é lida ou copiada por alguém não autorizado, o resultado é conhecido como perda de confidencialidade (PESANTE, 2008). As informações podem ser corrompidas quando estão disponíveis em uma rede insegura. Quando a informação é modificada de maneira inesperada, o resultado é conhecido como perda de integridade (PESANTE, 2008). As informações podem ser apagadas ou tornar-se inacessíveis, resultando em perda de disponibilidade. Isso significa que as pessoas que estão autorizadas a obter informações não podem trabalhar com o que precisam (PESANTE, 2008). A ideia básica é que a integridade é a qualidade da consistência em caráter; a pessoa age como acredita e seus valores coincidem com a sua conduta. Integridade se manifesta como uma insistência em manter um código moral, apesar das circunstâncias ou pressões externas (KHALED, 2010).

2.2. Política de Segurança da Informação

O núcleo de um sistema de gestão de segurança da informação é a política de segurança da informação. A política de segurança da informação é projetada para proteger a confidencialidade, integridade, e disponibilidade dos ativos de informação de propriedade da organização e seus clientes (KNAPP, et al., 2009). A política é o resultado de insumos internos e externos, de diretivas da gestão (WEILL & ROSS, 2004), o conhecimento das ameaças existentes e emergentes (WHITMAN, 2003), as necessidades de segurança da empresa e do controle de acesso> Tudo isso resulta em requisitos de controle (WARD & SMITH, 2002), cenários de impacto, probabilidade de impactos (TIPTON & KRAUSE, 2000), e exposições dos ativos da organização a riscos da informação (KNAPP et al., 2009).

A política de segurança da informação define os papéis dos diversos agentes, as suas responsabilidades e as suas atividades e tomadas de decisão pertencente a integração da segurança da informação nas tarefas do dia-a-dia, nos processos, e procedimentos (FUCHS et al., 2011). Herath e Rao (2009) afirmaram que uma política de segurança da informação é implementada com sucesso se existe uma melhora nos resultados e intenções da conformidade em uma organização. A política de segurança da informação deve prover orientação da direção da empresa e apoio de acordo com requisitos do negócio e leis e regulamentações (ABNT NBR ISO/IEC 27002, 2013).

A formatação de uma política de segurança da informação deve ser trabalhada de forma a atender todos os requisitos do negócio e ainda prover proteção de forma adequada. O

início de formulação de uma política se dá com a formação do comitê de segurança da informação, formado por componentes relevantes de cada área da corporação, para que na identificação dos controles e bloqueios haja validação por todos os setores do negócio, sem correr o risco de se executar a proteção das informações com uma paralisia operacional, onde não é possível desenvolver as atividades de negócio de forma eficaz. Em um nível mais baixo, a política de segurança da informação deve ser apoiada por temas mais específicos, como por exemplo: controle de acesso, classificação e tratamento da informação, segurança física e do ambiente, backup, transferência da informação e gerenciamento de vulnerabilidades técnicas (ABNT NBR ISO/IEC 27002, 2013).

Por mais que se confie em tecnologia, não se pode evitar que o elemento humano que desempenhe um papel significativo para a segurança da informação. Os seres humanos são constantemente identificados como o elo mais fraco da segurança (SCHNEIER, 2000; HUANG,et al., 2007). Portanto, para obter um sistema eficaz de segurança da informação, deve-se confiar em muitos aspectos ou níveis de segurança, como a confiança, integridade e ética que são cruciais em segurança da informação.

2.3. Incidentes de Segurança da Informação

Existem diversos incidentes de segurança da informação que podem prejudicar ou paralisar as operações em uma empresas. Dentres estes, os que têm maior destaque em levantamentos por orgãos de monitoramento são:**dos,** do inglês *Denial of Service*, são notificações de ataques de negação de serviço, onde o atacante utilza um computador ou conjunto de computadores para tirar de operação um serviço, computador ou rede; **invasão**, caracterizado por um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede; **web**, caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na internet; **scan**, que são notificações de varreduras em redes de computadores, com o intuito de identificar computadores que estão ativos e os serviços disponíveis, tipo de ataque que tem ampla utilização principalmente para que seja possível identificar alvos potenciais, pois é possivel associar vulnerabilidades conhecidas a serviços disponíveis nos computadores; **fraude**, isto é, qualquer ato ardiloso, enganoso, de má-fé, com objetivo de lesar ou ludibriar outrem, ou de não cumprir determinado dever, logro (CERT, 2015).

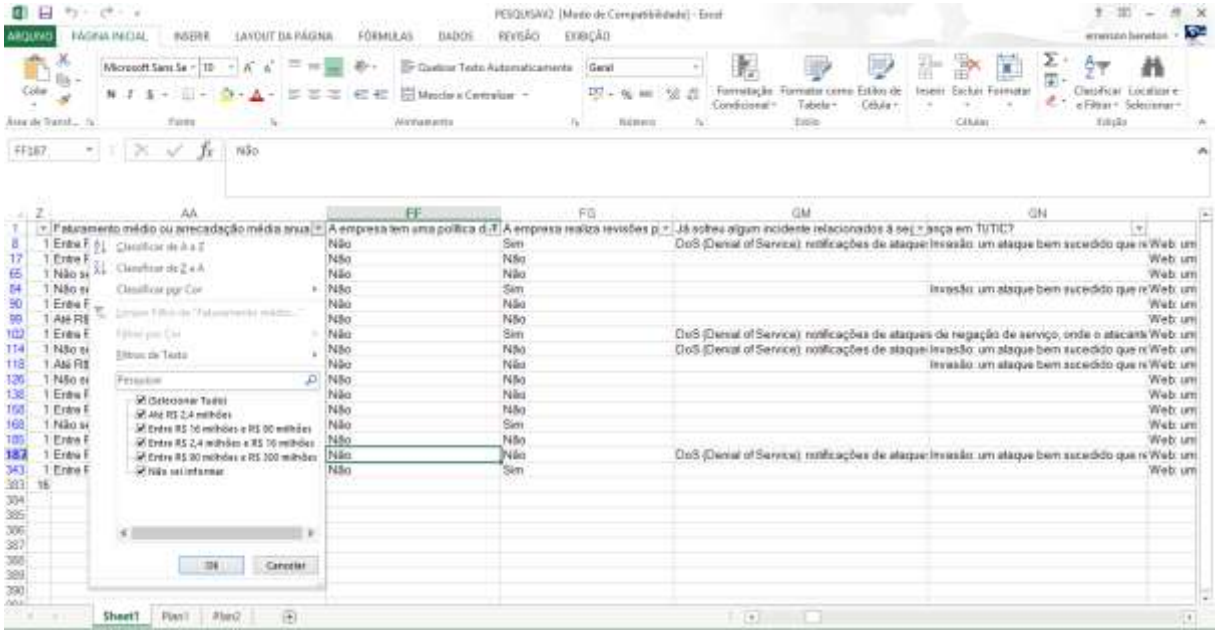
Os incidentes de segurança da informação devem ser evitados, pois uma ruptura nos sistemas de segurança da informação pode ocasionar significativa perda financeira, perda na

reputação prejudicando assim os negócios de uma empresa (GERBER & VON SOLMS, 2008). A conformidade de segurança da informação é necessária para cumprir com requisitos legais, obrigações regulamentares, cláusulas contratuais, exigências de declarações conjuntas além de tratados internacionais e proteção dos interesses dos acionistas (GERBER & VON SOLMS, 2008).

3. Metodologia

Os dados utilizados para esta pesquisa foram obtidos em pesquisa realizada pela ABRAT (Associação Brasileira das Empesas de T.I.) em 2013/2014, duante um período de 10 meses, com a obtenção de 376 respondentes, para um envio de 4000 empresas de todas as verticais de trabalho. Para receber as respostas foi utlizada a plataforma SurveyMonkey, que já estruturava cada resposta em uma planilha de Excell, utilizada no tratamento estatístico das informações por intermédio de filtros, (Figura 28).

Figura 28 – Exemplo do tratamento de dados por filtros



Fonte: Elaborado pelo autor.

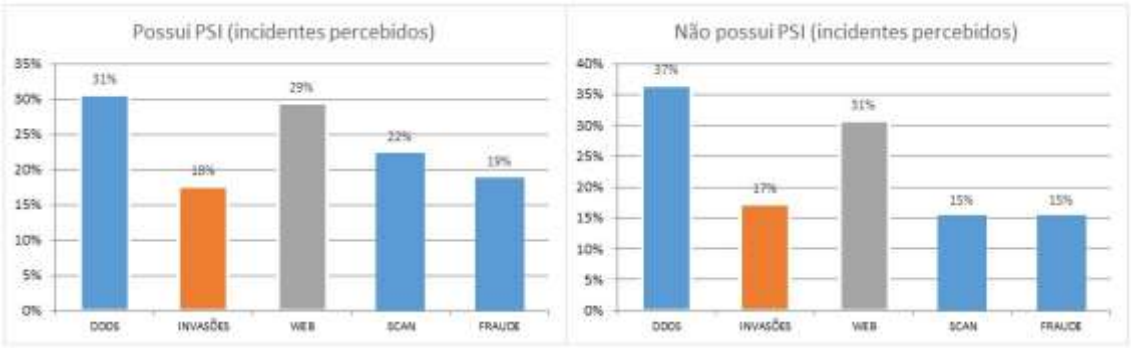
Identificaram-se práticas e procedimentos executados pelas empresas e os resultados efetivos obtidos durante essas execuções, também foi feito um comparativo entre empresas que utilizam recursos tecnológico e treinamento para redução de incidentes de segurança da informação.

4. Resultados e discussões

Na avaliação de resultados, os primeiros dados obtidos foram com relação aos problemas que as empresas tiveram com incidentes de segurança da informação, como perda de dados; Invasões pelo firewall, ou seja, ataques executados por pessoas mal intensionadas, que tentam entrar nos sistemas das empresas de forma ilícita pelas conexões via internet que a empresa possui; ataques web, isto é, os sites das empresas são atacados com objetivo de entrar em banco de dados para obter informações sigilosas; fraudes, caracterizado quando o atacante tenta obter algum benefício financeiro por intermédio de fraudes eletrônicas (CERT, 2015).

Essa avaliação foi feita de forma comparativa entre empresas de todos os portes que tinham políticas de segurança da informação e empresas que não tinham política de segurança da informação, (Figura 29).

Figura 29 – Comparativo entre empresas que possuem e que não possuem política de segurança da informação com relação aos incidentes percebidos



Fonte: Elaborado pelo autor.

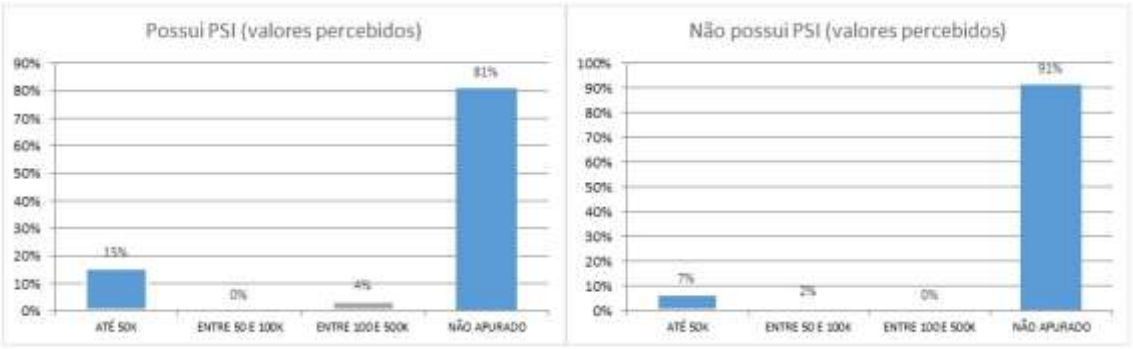
A avaliação feita em seguida foi com relação aos problemas percebidos, como perda total ou parcial de dados, indisponibilidade total ou parcial dos sistemas e disseminação de dados sigilosos, Figura 30.

Figura 30 – Comparativo entre empresas que possuem e que não possuem política de segurança da informação com relação aos problemas percebidos

Fonte: Elaborado pelo autor.

Na avaliação de problemas percebidos, os percentuais avaliados foram em relação ao número de empresas que possuiam ou não políticas de segurança da informação, também os dados relacionados aos valores percebidos foram identificados comparativamente às empesas que possuiam ou não política de segurança da informação.

Figura 31 – Comparativo entre empresas que possuem e que não possuem política de segurança da informação com relação aos valores percebidos



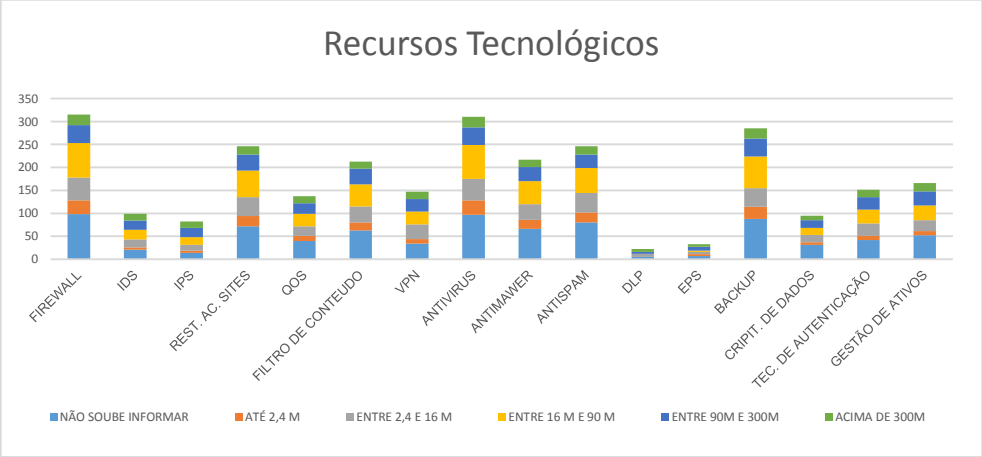
Fonte: Elaborado pelo autor.

Em uma primeira análise, as diferenças entre as empresas que possuem ou não possuem, política de segurança da informação, com relação a percepção de ter sofrido incidenes de segurança da informação, como perda de dados, invasões, ataques web e scan's não parece ter uma diferença significativa.

Analisando ainda a percepção dessas empresas com relação aos problemas percebidos como perda total ou parcial de dados, indisposição total ou parcial das operações ou vazamento de informações e mais ainda valores envolvidos em perdas, tanto para empresas com políticas de segurança da informação como para empresas sem políticas de segurança da informação, as diferenças apuradas não foram relevantes. Levanta-se a questão: Existe influência efetiva em se estabelecer ou não uma política de segurança da informação para preservação de operações em empresas?

No levantamento de informações com relação ao uso de tecnologias de prevenção a incidentes de segurança da informação de acordo com a faixa de faturamento, obteveram-se os seguintes resultados:

Figura 32 – Utilização de recursos tecnológicos na prevenção de incidentes de segurança da informação de acordo com a faixa de faturamento

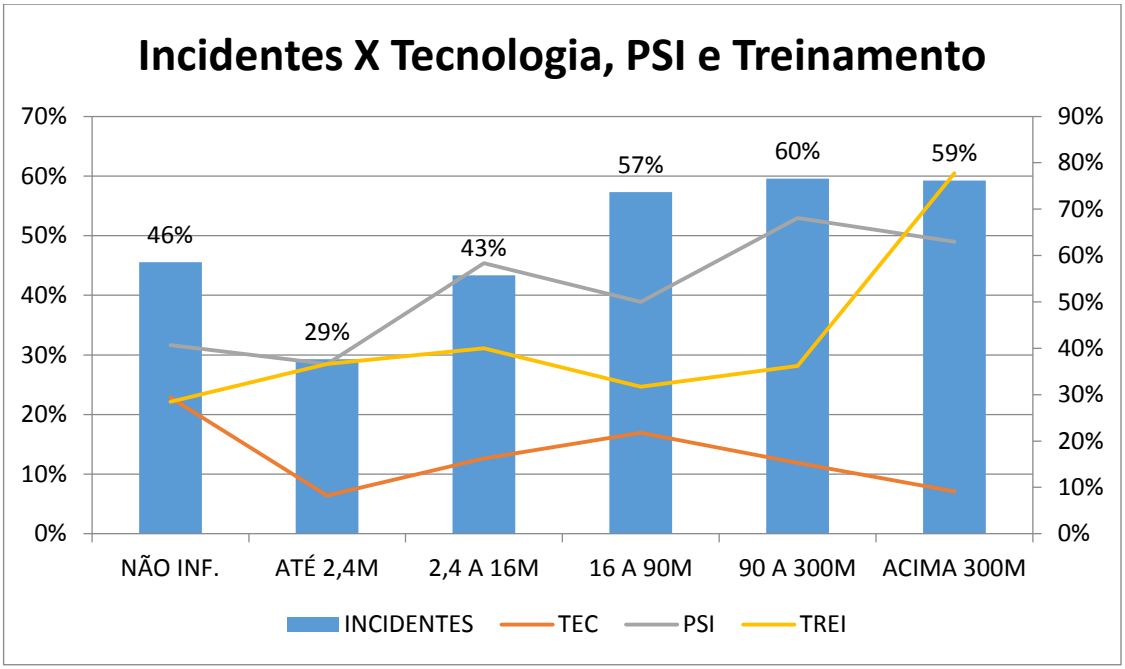


Fonte: Elaborado pelo autor.

Os dados demonstram uma concentração maior na utilização de tecnologias mais difundidas no mercado, como os Firewalls, Antivirus e Backup. Em contrapartida tecnologias com menor divulgação como DLP, EPS, IPS e IDS, são muito menos utilizadas em todas as faixas de faturamento.

A avaliação seguinte foi uma comparação entre o índice de incidentes de segurança da informação relatados por faixa de faturamento, medidas protetivas englobando uso de tecnologias, instituição de política de segurança e treinamentos, (Figura 33).

Figura 33 – Comparativo de incidentes relatados por faixa de faturamento, uso de tecnologia para prevenção, PSI e Treinamento



Fonte: Elaborado pelo autor.

À medida que o faturamento é maior, observa-se que o percentual de relatos de incidentes aumenta gradativamente até a faixa de 16 a 90 milhões de reais/ano, a partir de então existe uma manutenção da média relatada. O gráfico de utilização da política de segurança da informação como medida de proteção contra incidentes de segurança da informação, tem aumento gradativo, também acompanhando o aumento de faturamento das empresas alcançando uma certa estabilidade, a partir da faixa de faturamento de 90 a 300 milhões ano.

Comportamento diferente acontece ao se compararem os gráficos de utilização de recursos tecnológicos com treinamentos. Enquanto a utilização de tecnologia parece ser utilizada na prevenção, de uma forma crescente e gradativa entre as faixas de faturamento de até 2,4 milhões de reais até a faixa de 16 a 90 milhões, tendo queda de 16 a 90 milhões até acima de 300 milhões, a utilização do treinamento como medida preventiva, na proteção contra incidentes de segurança da informação, tem comportamento variando dentro de uma escala de 30% a 40% de utilização, até a faixa de faturameto de 90 a 300 milhões, crescendo em utilização sensivelmente a partir desta faixa atingindo 80% de relatos de utilização na faixa de faturamento acima de 300 milhões.

Observando o comportamento contrário entre as curvas de tecnologia e treinamento e a estabilidade da curva da PSI, conclui-se que a manutenção dos programas de prevenção a incidentes de segurança da informação para empresas de maior faturamento, é formada com o amadurecimento das equipes de trabalho. Melhorando-se os processos, pode-se reduzir os investimentos no uso da tecnologia e prover reforço em treinametos e conscientização.

5. CONCLUSÃO

A presente análise comparativa entre empresas que possuem recursos tecnológicos na preservação de suas operações e empresas que investem em treinamento de suas equipes, para que se obtenha a redução de incidentes de segurança da informação, indicou que à medida que é obtido um amadurecimento das equipes de trabalho, pode-se manter equilíbrio entre tecnologia e treinamento para esse fim.

É possível a redução de investimentos em tecnologia desde que exista investimento em treinamento, para que as equipes de trabalho possam acompanhar os processos estruturados nas políticas de segurança da informação. Todavia, essa equação é utilizada para corporações que possuem faturamento acima de 90 milhões de reais por ano.

Observando-se o comportamento das empresas estudadas, sugere-se estudo futuro que possa identificar um conjunto de boas práticas e que contemple equilibrio entre o uso da tecnologia, estruturação de processos adequados e treinamentos e concientização de equipes para prevenção de incidentes de segurança da informação racionalizando investimento e retorno desejado.

REFERENCIAS

ABNT NBR ISO/IEC 27002. TECNOLOGIA DA INFORMAÇÃO – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas, 2013.

CERT, CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTESDE SEGURANÇA NO BRASIL. http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque-acumulado.html, 22 mai. 2015.

CHIA, TERRY, (2012). Confidentiality, integrity, availability: The three components of the CIA Triad. *IT Security Community Blog*., http://security.blogoverflow.com/2012/08/confidentiality-integrity-availabilitythe-three-components-of-the-cia-triad/, 10 mar.2013.

FEDERAÇÃO DAS INDUSTRIAS DO ESTADO DE SÃO PAULO, DEPARTAMENTO DE PESQUISAS E ESTUDOS ECONÔMICOS. **Projeto Rumos da Indústria Paulista, segurança cibernática**. São Paulo, 2015.

FUCHS, L., PERNUL, G., & SANDHU, R. Roles in information security - A survey and classification of the research area. *Computers & Security*, *30*(8), 748-769, 2011.

GERBER, M., & VON SOLMS, R. Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5), 124-135, 2008.

HERATH, T., & RAO, H.R. . Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165, 2009.

HUANG, D. L., RAU, P. L. P., & SALVENDY, G. A survey of factors influencing people's perception of information security. In *Human-Computer Interaction. HCI Applications and Services (pp. 906-915).* Springer Berlin Heidelberg, 2007.

IBM CORPORATION. Z/OS basic skills information center, http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp?topic=/com.ibm.zcontact.doc/webqs.html, 13 out., 2011

ISO/IEC 27000. INFORMATION TECHNOLOGY – Security techniques – Information security management systems – Overview and vocabular, 2014.

KHALED, (2010). The meaning of integrity: The complete human., http://www.khaledallen.com/warriorspirit/the-meaning-of-integritythe-complete-human/, 13 out. 2011.

KNAPP, K. J., MORRIS JR., R. F., MARSHALL, T. E., & BYRD, T. A. Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508, 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Federal information processing standards publication. Standards for security categorization of federal information and information systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, . 8 set. 2011.

PESANTE, LINDA (2008). Introduction to information security. Carnegie Mellon University.http://www.uscert.gov/sites/default/files/publications/infosecuritybasics.pdf., 10 mar. 2013

SCHNEIER, B.. *Secrets and lies: Digital security in a networked world*. Indianapolis, IN: Wiley Publishing, Inc.,2000

TIPTON, H. F., & KRAUSE, M. *Information security management handbook*, *1*, 3-154. Auerbach Publications, (2000).

UNIVERSITY OF MIAMI, Miller School of Medicine (2006). Privacy/data protection project.,http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm, 10 mar. 2013.

US-CERT TECHNICAL INFORMATION Paper – TIP-11-075-01 March 16, 2011., from http://www.us-cert.gov/reading_room/TIP11-075-01.pdf., 8 set. 2011.

WARD, P., & SMITH, C. L. The development of access control policies for information technology systems. *Computers & Security*, *21*(4), 356-371, 2002.

WEILL, P., & ROSS, J. W. *IT governance: How top performers manage IT decision rights for superior results*. Boston, MA: Harvard Business School Press., 2004.

WHITMAN, M. E. Enemy at the Gate: Threats to information security. *Communications of the ACM*. *46*(8), 91-95, 2003.

7 DISCUSSÃO FINAL

Este trabalho defende a hipótese de que incidentes de segurança da informação podem influenciar na competitividade das empresas, sobretudo em empresas que possam ter dificuldades em implantar processos de prevenção à esses incidentes ou realizar um controle preciso dos prejuízos que venham a prejudicar suas operações.

Com as pesquisas realizadas, constata-se que existe uma preocupação da maioria das empresas com relação a estruturar departamentos de TI, para melhorar suas operações. Muitas das empresas têm políticas de segurança da informação, porêm, constata-se tamém que mesmo com essas ações a identificação precisa de prejuízos não foi possível, em sua maioria, 85% das empresas pesquisada mesmo tendo departamentos de TI e Políticas de Segurança da Informação devidamente estabelecidas, não puderam avaliar o prejuízo causado por incidentes de segurança da informação em suas operações. Esta falta de informações mais precisas, pode trazer aumento de custos nas operações das empresas, muitas vezes de forma aleatória e que dependendo do momento deixam seus produtos mais caros e consequentemente menos competitivos.

Outra constatação, foi com relação aos resultados obtidos pelas empresas quando em direção ao controle de incidentes de segurança da informação. Verifica-se que dentre as ações que as empresas tomam para preservar suas operações, existe uma maior utilização de recursos tecnológicos mais conhecidos, ou seja, os recursos mais difundidos no mercado e que desta forma estão mais acessíveis aos profissionais de tecnologia da informação. Muitas vezes esses recursos podem não ser a melhor escolha, se o responsável da área não tem devidamente mapeados os riscos associados à operação.

Por fim, na última análise, quando realizada comparação dos resultados obtidos com ações na preservação das operações, utilização de recursos tecnológicos, implantação de política de segurança da informação e treinamento de equipes da operação, constata-se que a medida que as empresas possuem maior faturamento, a utilização da política de segurança da informação passa a ter estabilidade na sua utilização. Ou seja, não existe uma maior utilização deste recurso na prevenção dos incidentes. Ainda acompanhando o faturamento anual, existe uma redução de investimentos em recursos tecnológicos e, como compensação passa a existir um maior investimento em treinamentos. Conclui-se nesta situação, que equipes mais treinadas e com maior conscientização de suas responsabilidades, podem contribuir de forma

mais efetiva na preservação das operações das empresas, ajudando na redução dos incidentes de segurança da informação, corroborando Schneier, (2000); por mais que se confie na tecnologia, o fator humano desempenha papel significativo para a segurança da informação.

Como sugestão para trabalhos futuros, propõe-se a identificação de um conjunto de melhores práticas a fim de trazer equilíbrio entre os investimentos feitos em tecnologia, processos e pessoas. Um estudo que possa identificar os caminhos percorridos por empresas bem-sucedidas na implantação de sistemas de segurança da informação, obtendo redução de incidentes com investimentos controlados, pode fornecer um conjunto de ações que replicadas em outras empresas possa trazer o mesmo sucesso, encurtando desta forma o tempo de avaliação, implantação e resultados efetivos às operações

.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002 Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27005 Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

ALVAREZ I.; MARIN R..*FDI and Technology as Levering Factors of Competitiveness in Developing Countries. Journal of International Management*, v.19, p.232-246, 2013.

BOGLIACINO, F.; LUCHESE, M.; PINTA, M.. *Job creation in business services: Innovation, demand, and polarisation. Structural Change and Economic Dynamics*, v.25, p. 95-109, 2013.

BOONS, F. et al. *Sustainable innovation, business models and economic performance: na overview. Journal of Cleaner Production*, v.45, p.1-8, 2012.

COX, J. *Information systems user security: A structured model of the knowing-doing gap. Computers & Human Behavior*, v.28, p.1849-1858, 2012.

CROSSLER, R. E. et al. *Future directions for behavioral information security research. Computers & Security*, v.32, p.90-101, 2013.

DENIZ, M.; SEÇKIN S. N.; CUREOGLU M.. *Mico-economic competitiveness: a research on manufacturing firms operating in TRB 1region, Procedia – Social and Behavioral Sciences*, v.75, p.465-472,2013.

GIANESI, I. G. N.; CORRÊA H. L.. Administração estratégica de serviços, operações para satisfação do cliente. 1. Ed. São Paulo: Atlas, 1994.

GILKINSON, N.; DANGERFIELD, B.. *Some results from a system dynamics modelo of conctruction sector competitiveness. Mathematiacal and Computer Modelling*, v. 57, p.2032-2043, 2013.

GUO, K. H.. *Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security*, v.32, p.242-251, 2013.

GUO, K. H.; YUAN, Y.. *The effects of multilevel sanctions on information security violations: A mediating model. Information & Managenent*, v.49, p.320-326, 2012.

IFINEDO, P.. *Understanding information systems security policy complice: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security*, v.31, p.83-95, 2012.

KNORST, A. M. et al. *Aligning information security with the image of the organization and prioritization based on fuzzy logic for the industrial automation sector.Journal of information systems and techenology management*, v.8, p.555-580, São Paulo, 2011.

KOLKOWSKA, E.; DHILLON, G. *Organizational power and information security rule complince. Computers & Security*, v.33, p.3-11, 2013.

KUMAR, V.; MUDAMBI, R.; GRAY, S..*Internationalization, Innovation and Institutions: The 3 I's Underpinning the Competitiveness of Emerging Market Firms. Journal of International Management*, v.19, p.203-206, 2013.

MAHADEVAN, B.. *Spirituality in business: Sparks from the Anvil In conversation with Suresh Hundre, Char main and MD, Polyhydron Pvt. Ltd. IIMB Management Review*, v.25, p. 91-103, 2013.

PORTER, M. ; KRAMER, M. *Sttrategy and society: The link between competitive advantage and corporate social respopnsibility*. Harvard Business Review, 34(12), 78-92, 2006.

PORTER, M. *Competitive advantage: Creating and sustaining superior performance*, New York, 1985.

PORTER, M. *How competitive forces shape strategy,* Harvard Business Review 57(2), 87-94, 1979.

QIAN, Y.; FANG, Y.; GONZALEZ, J. J. *Managing information security risk during new technology adoption. Computers & Security*, v.31, p. 859-869, 2012.

RHEE, H. S.; RYU, Y. U.; KIM, C. T.. *Unrealistic optimism on information security management. Computers & Security*, v.31, p.221-232, 2012.

RYAN, J. J.C.H. et al. *Quantifying information security risk using expert judgment elicitation. Computers & Operations Research*, v.39, p.774-784, 2012.

STEINBART, P. J.et al. *The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems,* v.13, p.228-243, 2012.

YANG, Y. O.; TZENG, H.. G. *A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences*, v.232, p.482-500, 2013.

APÊNDICE A: Questionário da pesquisa quantitativa

As Tecnologias de Informação e Comunicação TIC são atualmente percebidas como instrumentos fundamentais para o desenvolvimento socioeconômico, especialmente em razão de seu potencial de contribuição para a inclusão social, a criação de empregos, o aumento de produtividade e competitividade, entre outros benefícios. Este estudo tem por objetivo a construção de indicadores nacionais para o desenvolvimento de políticas visando à universalização do uso das TIC nas empresas brasileiras, sendo também de grande utilidade aos tomadores de decisões no setor privado. A ABRAT – Associação Brasileira de Empresas de Tecnologia da Informação – agradece antecipadamente a todas as empresas participantes, particularmente aos entrevistados.

Emerson Beneton
Presidente

1. Identificação da Empresa
CNPJ (só números): _____
Razão Social: _____
2. Localização da Empresa
Tipo (Rua, Avenida, Praça,
Etc.): _____
Endereço: _____
Número: _____
Complemento: _____
Cidade: _____
Estado: _____
CEP: _____
3. Telefone da Empresa
DDD: (2 dígitos) _____
Telefone: (até 9 dígitos) _____
4. Entrevistado:
Nome: _____
Cargo: _____
e-mail_____
(corporativo): _____
5. Faturamento médio anual:
o Até R$ 2,4 milhões
o Entre R$ 2,4 milhões e R$ 16 milhões
o Entre R$ 16 milhões e R$ 90 milhões
o Entre R$ 90 milhões e R$ 300 milhões
o Acima de R$ 300 milhões
o Não sei informar
6. Quantidade de funcionários:

7. Equipamentos:
o Quantidade de servidores
o Quantidade de computadores de mesa
o Quantidade de computadores portáteis
o Quantidade de dispositivos mobile

8. A empresa possui departamento (área) de TI/TIC ou funcionário responsável pela TI/TIC?
o Sim
o Não
9. Há orçamento mensal ou anual destinado a TI/TIC em sua empresa?
o Sim
o Não
10. Qual o nível de prioridade é dado aos investimentos em TI/TIC na empresa?
o Muito alto
o Alto
o Moderado
o Baixo
o Muito baixo
11. Quem aprova os investimentos em TI/TIC?
o CEO (Diretoria Executiva)
o CFO (Diretoria Financeira)
o CTO (Diretoria Técnica)
o Outro (especifique)
12. Utiliza soluções de código aberto?
o Sim
o Não
13. Utiliza soluções de virtualização?
o Sim
o Não
14. A empresa desenvolve softwares para uso específico com mão de obra própria?
o Sim
o Não
15. A empresa desenvolve softwares para uso específico com mão de obra externa?
o Sim
o Não
16. Que tipo de software a empresa utiliza para integrar os dados e processos de seus departamentos?
o Editor de texto / planilha eletrônica / editor de apresentações
o Gestão contábil / fiscal / folha de pagamento
o ERP (compra, venda, estoque, finanças)
o CRM (gestão do relacionamento comercial)
o BPM (processos)
o BI (gestão de conhecimento)
o GED (gestão eletrônica de documentos)
o SGDB (sistema de gerenciamento de base de dados)
o Automação Industrial / Robótica
o Desenvolvimento de Produtos / Serviços (CAD, CAM, CASE)
o Aplicações Multimídia, Gráficos e Geoprocessamento
o Outro (especifique)
17. Quantas operadoras de telefonia fixa atendem a empresa?
o 1
o 2
o 3
o 4
o 5 ou mais

18. Quantas operadoras de telefonia celular atendem a empresa?
o 1
o 2
o 3
o 4
o 5 ou mais
19. Linhas telefônicas
Quantidade de linhas fixas digitais
Quantidade de linhas fixas analógicas
Quantidade de linhas celulares
20. O sistema de telefonia da empresa é:
o Central telefônica convencional
o Central telefônica IP
o Central telefônica convencional + IP
o Não utiliza central telefônica
o Outro (especifique)
21. Quais tecnologias de telefonia a empresa utiliza?
o URA
o Gravação das ligações
o VoIP
o Correio de voz corporativo
o Sistema de tarifação / bilhetagem
o Discagem Direta Ramal (DDR)
o Conferência
o Outro (especifique)
22. Quantas operadoras (ex. Vivo, Embratel, Oi, etc.) provêem acesso a internet a empresa com links de tecnologia fixa?
o Nenhuma
o 1
o 2
o 3
o 4
o 5 ou mais
23. Quantidade de links de acesso à internet contratados pela empresa junto a operadoras (ex. Vivo, Embratel, Oi, etc.), por tipo de tecnologia fixa.
o ISDN
o xDSL
o TV a cabo / cable modem
o Rede elétrica
o Rede sem fio: WiFi, WiMAX, TMAX, Satélite, a rádio (MMDS, LMDS)
o Linha dedicada (fibra, LP de dados, framerealy, etc.)
o Outras tecnologias fixas
24. Qual a soma das velocidades dos links de tecnologia fixa de acesso a internet?
o Até 256 kbps
o Acima de 256 Kbps até 1 Mbps
o Acima de 1 Mbps até 10 Mbps
o Acima de 10 Mbps até 100 Mbps
o Acima de 100 Mbps
o Não sei responder

25. Quantas operadoras (ex. Vivo, Embratel, Oi, etc.) provêem acesso a internet a empresa com links de tecnologia móvel (3G, 4G, etc)?
o 1
o 2
o 3
o 4
o 5 ou mais
26. Quantidade de links de acesso à internet contratados pela empresa junto a operadoras (ex. Vivo, Embratel, Oi, etc.), por tipo de tecnologia móvel
o 2G
o 2,5G
o 3G
o 4G
o Outras tecnologias moveis
27. Quem tem acesso acesso remoto (quando está fora da empresa) por meio da internet ao ambiente computacional da empresa?
o Presidência
o Vice-presidência
o Diretoria
o Gerentes
o Coordenadores
o Supervisores
o Todos os funcionários
o Outro (especifique)
28. Os e-mails da empresa estão hospedados internamente?
o Sim
o Não
29. Oferece rede interna wifi (sem fio) para acesso a internet? Caso ofereça, especifique quem pode usar o recurso.
o Clientes
o Fornecedores
o Visitantes
o Presidência
o Vice-presidência
o Diretoria
o Gerentes
o Coordenadores
o Supervisores
o Todos os funcionários
o Outro (especifique)
30. Caso o uso de dispositivos pessoais (BYOD bring your own device / traga o seu dispositivo pessoal) seja permitido na empresa, especifique quem pode usálos?
o Clientes
o Fornecedores
o Visitantes
o Presidência
o Vice-presidência
o Diretoria
o Gerentes
o Coordenadores

o Supervisores
o Todos os funcionários
o Outro (especifique)

31. Para quais das seguintes atividades a empresa utiliza a Internet?

o Enviar e receber e-mails
o Telefonar usando Internet/VoIP, inclusive para vídeoconferência (VoIP referese a voz sobre IP)
o Buscar informações sobre bens e serviços
o Fazer pagamentos e consultas bancárias online (Inclui as transações eletrônicas com bancos para pagamento, transferências, etc. ou para a busca de informações relativas a contas bancárias.)
o Acessar outros serviços financeiros (Inclui as transações eletrônicas via Internet para outros tipos de serviços financeiros como aquisição de ações, seguros, etc.)
o Fornecer catálogos de produtos ou listas de preços online ou por email (Inclui a possibilidade de customizar o produto.)
o Fornecer produtos online (Compreende o fornecimento de informações de produtos digitalizados entregues através da Internet, por exemplo, relatórios, software, úsica, vídeos, jogos de computador e outros serviços online, tais como: serviços elacionados à informática, serviços de informação, serviços de reservas de viagens, etc.)
o Recrutar pessoal interno ou externo (Compreende o fornecimento de informações sobre postos de trabalho através da Internet ou da página da empresa na Internet permitindo o preenchimento de formulários online para o preenchimento das vagas oferecidas, a pessoas de dentro ou de fora da empresa.)
o Treinar e qualificar pessoal da empresa (Compreende a utilização pela empresa aplicativos de educação a distância (elearning) disponíveis na rede Intranet ou Internet.)
o Outro (especifique)

32. Sua empresa usa a internet para interagir com órgãos do governo e usar alguns dos seguintes serviços eletrônicos?

o Obter informações da Administração Pública (consultas)
o Obter (download) formulários e certidões
o Enviar declaração de imposto de renda (IRPJ e ITR)
o Enviar a declaração da RAIS
o Enviar informações estatísticas às autoridades
o Fazer pagamentos online de impostos, taxas e recolhimentos (IPI, ICMS, ISS, COFINS, FGTS e outros)
o Submeter propostas de licitação/pregão eletrônico e leilões
o Emitir nota fiscal eletrônica
o Outro (especifique)

33. Caso possua website, quais recursos estão disponíveis.

o Informações sobre a empresa (institucional, contato, endereço, mapas)
o Catálogos de produtos
o Suporte pós-venda
o Personalização ou customização de produtos para clientes
o Listas de preços
o Outro (especifique)

34. É frequente fazer compras pela internet?

o Extremamente frequente
o Muito frequente
o Frequente
o Pouco frequente

o Nada frequente

35. Quão seguro se sente de que os dados da empresa são mantidos em confidencialidade quando faz compras pela internet?

o Extremamente seguro
o Muito seguro
o Moderadamente seguro
o Muito inseguro
o Extremamente inseguro

36. Caso não tenha canal de vendas pela internet, especifique um ou mais motivos que justifique(em) tal decisão

o Produtos da empresa não são adequados para venda online
o Preferência pelo modelo comercial atual
o Baixa demanda de compras pela internet
o Carência de pessoas capacitadas para desenvolver e manter o site
o Alto custo de desenvolvimento e manutenção
o Motivos de segurança
o Sistemas dos clientes ou fornecedores não são compatíveis com o da empresa
o Incerteza quanto à legislação
o Outro (especifique)

37. Caso utilize algum tipo de rede social, qual tipo de informação a empresa veicula?

o Postar notícias sobre a empresa
o Responder a comentários e dúvidas de clientes
o Postar notícias sobre temas relacionados à área de atuação da empresa
o Postar conteúdo institucional sobre a empresa
o Lançar produtos ou serviços
o Fazer promoções de produtos ou serviços
o Outro (especifique)

38. Caso utilize algum tipo de rede social, informe a frequência com que atualiza o conteúdo?

o Extremamente frequente
o Muito frequente
o Frequente
o Pouco frequente
o Nada frequente

39. A empresa tem uma política de segurança em TI/TIC formalmente definida?

o Sim
o Não

40. A empresa realiza revisões periódicas na política de segurança?

o Sim
o Não

41. Que tipo de medida(s) e/ou ação(ões) a empresa toma sobre o uso da internet junto aos funcionários?

o Orienta os usuários sobre o uso da internet na empresa
o Monitora sites visitados por alguns ou todos os usuários
o Bloqueia acesso a conteúdo de alguns ou todos os usuários
o Monitora tráfego de dados individual de alguns ou todos usuários
o Outro (especifique)

42. Quais soluções estão implementadas para garantir a disponibilidade de seu ambiente computacional, bem como a segurança das informações?

o Firewall
o IDS (intrusion detection system)
o IPS (intrusion prevention system)
o Restrições de acesso a sites
o QoS (controle de banda)
o Filtro de conteúdo
o VPN (virtual private network)
o Antivírus
o Antimalwares
o Antispam
o DLP (data lost prevention)
o EPS (end point security)
o Backup
o Criptografia de dados
o Tecnologias de autenticação
o Gestão de ativos (equipamentos, impressoras, licenças de software)
o Outro (especifique)

43. O que é restringido pela política de acesso a sites na internet?

o Sites pornográficos
o Jogos
o Instalação de aplicativos / softwares / complementos
o Serviços de comunicação
o Download de arquivos
o Sites de relacionamento
o Portais de entretenimento / notícias / esportes
o Acesso a e-mail pessoal
o Outro (especifique)

44. Já sofreu algum incidente relacionados à segurança em TI/TIC?

o DoS (Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
o Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
o Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na internet.
o SCAN: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
o Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de máfé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro".
o Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
o Outro (especifique)

45. Caso tenha sofrido algum incidente relacionados à segurança em TI/TIC, qual foi o impacto percebido?

o Destruição total ou parcial de dados
o Indisponibilidade total ou parcial dos serviços TI/TIC
o Disseminação ou uso de dados confidenciais
o Outro (especifique)

46. A empresa proporcionou treinamento/qualificação ao seu pessoal de TI/TIC para desenvolver ou aperfeiçoar as habilidades nos últimos 12 meses?
o Sim
o Não
47. Caso a empresa tenha proporcionado treinamento/qualificação, que tipo de treinamento/qualificação foi proporcionado pela empresa?
o Para desenvolvimento de habilidades básicas em TI (ex.: editor de texto, planilha eletrônica, editor de apresentações, uso da internet, etc.)
o Para obtenção de certificações (ex.: Microsoft, Cisco, COBIT, ITIL, PMP, etc.)
o Para aprendizado de domínio de ambientes de desenvolvimento: linguagens, banco de dados,etc. (ex.: Java, Delphi, Visual Basic,
o Outro (especifique)
48. A empresa contratou ou tentou contratar especialistas em TI/TIC nos últimos 12 meses?
o Tentou e conseguiu contratar
o Tentou contratar, mas não conseguiu
o Não precisou contratar
49. Caso tenha tentado contratar especialistas em TI/TIC nos últimos 12 meses, mas não tenha conseguido, especifique um ou mais motivos que justifique(em) a frustração?
o Falta de qualificação específica (estudo e/ou treinamento) em TI
o Falta de candidatos, ou poucos candidatos especialistas em TI
o Falta de experiência profissional no ramo de TI
o Pretensões salariais altas (altos custos de remuneração para especialistas em TI)
o Outro (especifique)
50. Caso tenha utilizado serviços de TI/TIC prestados por fornecedores externos, especifique quais serviços foram terceirizados?
o Suporte técnico para reparo e manutenção dos equipamentos
o Suporte técnico para sistema interno da empresa
o Desenvolvimento de aplicações
o Serviços de hospedagem
o Consultoria especializada em segurança da informação
o Infraestrutura
o Outro (especifique)