GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO: *FRAMEWORKS* DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE PEQUENO E MÉDIO PORTE[1]

Felipe Lain Rizzotto[2]

Resumo: A baixa adesão das pequenas e médias empresas (PME) à implantação de Gestão da Segurança da Informação (GSI) motivou a proposta de um *framework* de GSI aderente aos processos organizacionais de PMEs do ramo de comércio atacadista. O trabalho foi embasado em pesquisa bibliográfica e questionário aplicado a empresas da região de Caxias do Sul. As maiores dificuldades constatadas foram falta de conhecimento das normas e dos riscos aos quais estão expostas, falta de pessoal disponível ou com conhecimento de Segurança da Informação (SI), falta de colaboração dos gestores e complexidade dos modelos conhecidos. Para mitigar as dificuldades percebidas, foi proposto um framework em níveis, que permite sua implantação em etapas. O primeiro nível tem o objetivo de desenvolver a cultura da SI e depois de consolida-la, parte-se para o cumprimento gradual de requisitos normativos nos níveis seguintes. Assim, a organização ganha flexibilidade de implantação e investimento.

Palavras-chave: Segurança, Informação, Gestão, *Framework*.

1 INTRODUÇÃO

A realidade da Gestão da Segurança da Informação (GSI) nas Pequenas e Médias Empresas (PMEs) está muito distante do que sugerem as normas e modelos. Observa-se que há pouca governança e gestão da Segurança da Informação (SI) neste meio, pois o foco das atividades nas PMEs é muito mais operacional, ou seja, concentram-se esforços na realização das tarefas do cotidiano. Apesar disso, não é correto afirmar que a SI não recebe cuidados, a SI é considerada importante, mas os esforços despendidos pelas PMEs não são eficientes e eficazes, pois segundo Neto e Siveira (2007), grande parte das PMEs investem em estrutura tecnológica, mas não investem no fator humano. Desta forma, acabam por não ter conhecimento técnico disponível para implantação de técnicas de governança ou GSI.

Infelizmente, as pequenas e médias organizações têm carências já na estrutura básica de tecnologia da informação. Segundo Thong (2001), as pequenas empresas não

---

[1] Artigo apresentado como trabalho de conclusão de curso de Especialização em Gestão da Segurança da Informação da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Especialista em Gestão de Segurança da Informação. Orientador: Prof. Professor Cláudio César Reiter, Ms. Palhoça - SC, 2018.

[2] **Acadêmico (a) do curso de Especialização em Gestão da Segurança da Informação da Universidade do Sul de Santa Catarina. Felipe.rizzotto@unisul.br

conhecem a importância de fatores-chave em Tecnologia da Informação (TI), além de disporem de recursos reduzidos, podem estar gastando estes recursos e energia em fatores de pouca importância para o sucesso da implantação da TI. Ou seja, apesar de existir o investimento, não é feito de forma eficaz, pois carece de planejamento, conhecimento e treinamento. Segundo Beraldi e Escrivão Filho (2000), devido a essas deficiências, as PMEs não conseguem obter os benefícios desejados no uso da TI que aplicam.

Quando se trata de SI, mais especificamente, a situação não melhora, Begg e Caira (2012) identificaram a dificuldade e escassez de *frameworks* que atendam a realidade das PMEs. Observa-se um cenário em que as PMEs não têm estrutura, equipamentos ou pessoas especializadas e disponíveis e os *frameworks* para GSI não as atendem. Desta forma, a SI fica em segundo plano, na melhor das hipóteses. O problema é que, atualmente, não ter governança e GSI é cada vez mais crítico para as empresas, pois o avanço da tecnologia migrou o valor das organizações dos seus ativos físicos para a informação que possuem.

Diante do cenário de escassez de SI nas PMEs e das dificuldades em aderir aos modelos de mercado é que se chegou ao tema *frameworks* de gestão de segurança da informação em empresas de pequeno e médio porte. Sendo que, o problema foi delimitado sobre a necessidade de levar governança e GSI a ambientes com os recursos limitados e carentes de organização, pois é um requisito essencial para empresas de todos os tamanhos. Assim, a lacuna existente nas PMEs motivou a pergunta que orientou a pesquisa: É possível sugerir um *framework* de Gestão de Segurança da Informação que seja aderente aos processos organizacionais de empresas de pequeno e médio porte do ramo de comércio atacadista? Para responder à questão, foram traçados objetivos específicos de planificar os processos organizacionais de empresas de pequeno e médio porte do ramo de comércio atacadista, avaliar a aderência dos principais *frameworks* de GSI nas PMEs e propor um *framework* de GSI que apresente viabilidade para PMEs do ramo de comércio atacadista.

A pesquisa teve como objetivo a resolução de um problema concreto, da GSI em PMEs, focando o comércio atacadista da região de Caxias do Sul, RS. Desta forma, a pesquisa teve uma abordagem aplicada. Quanto à forma, foi empírica na maior parte, pois foram coletadas informações diretamente sobre fatos e, também indiretamente pela consulta de outras pesquisas correlacionadas, usando essa base teórica para sustentar os conceitos dos *frameworks* existentes que foram comparados. Em relação ao aprofundamento do estudo a pesquisa relacionou a implantação de um modelo de SI (*framework*) em um determinado cenário, as PMEs do ramo de comércio atacadista, enumerou as razões do frequente insucesso

dos métodos convencionais e trouxe métodos alternativos que obtiveram sucesso em práticas semelhantes, com aprofundamento explicativo.

Os dados da pesquisa foram obtidos de questionário próprio e de estudos bibliográficos de referência, ou seja, pesquisa empírica indireta de dados apresentados por outros autores. Para atingir cada um dos objetivos específicos do trabalho, foram necessárias diferentes coletas de dados. Para entender os processos organizacionais de PMEs do ramo de comércio atacadista, usou-se um questionário como método de coleta de dados e a pesquisa teórica. O questionário também foi usado para entender porque os *frameworks* comumente usados não alcançaram os objetivos desejados ou, se alcançaram, como o fizeram. Finalmente, para estudar os *frameworks* dirigidos especificamente as PMEs, o método de coleta de dados foi a pesquisa teórica, em que buscou-se compreender como funcionam, se foram adaptados da ISO/IEC 27000, como foram adaptados e quais resultados obtiveram.

O desenvolvimento do trabalho está organizado na Seção 2, que se divide em outras quatro seções. A Seção 2.1 que apresenta a realidade das pequenas e médias empresas, suas classificações, características, importância econômica, o comércio atacadista e as limitações e as perspectivas das PMEs na Segurança da Informação. Na Seção 2.2 do trabalho são exibidos os frameworks de GSI focados para pequenas e médias empresas. Já na Seção 2.3 apresenta-se o questionário sobre GSI em PMEs atacadistas de Caxias do Sul e Região. Na Seção 2.4 é desenvolvida a proposta do presente estudo: um framework nivelador para PMEs. Finalmente, na Seção 3 estão as considerações finais do trabalho.

2 UM FRAMEWORK PARA GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM PEQUENAS E MÉDIAS EMPRESAS DO COMÉRCIO ATACADISTA

2.1 AS PMES DO RAMO DE COMÉRCIO ATACADISTA

Empresas do comércio atacadista, segundo Camarotto (2009), são empresas que vendem produtos basicamente para outras empresas como varejistas, comerciantes, empreiteiros usuários industriais, usuários institucionais e usuários comerciais. O comércio atacadista é um agente econômico que atua como intermediário entre produtores e varejistas. Trata-se de um agente logístico do mercado que a indústria pode usar como estoque e ponto de entrega e o comércio varejista pode encontrar produtos diversos em um único local. Enquanto o comércio varejista revende produtos para o consumidor final, o comércio atacadista compra os produtos da indústria em grandes quantidades e os revendem aos

varejistas. Conforme Camarotto (2009), os atacadistas estão basicamente relacionados ao comércio de bens físicos e podem vir a fornecer serviços como uma atividade complementar.

2.1.1 Classificação das PMEs

No Brasil, a classificação de uma empresa em pequena ou média é dada por número de funcionários e faturamento. Por número de funcionários, na indústria, uma empresa é pequena tendo de 20 a 99 e média de 100 a 499 funcionários; no comércio, é pequena tendo de 10 a 49 e média de 50 a 99 funcionários. Por faturamento, as pequenas empresas devem faturar de R$ 360 mil a R$ 3,6 milhões anualmente, conforme SEBRAE (2018). Para as médias empresas não há limite de faturamento oficial. Como este estudo cita pesquisas sobre PMEs ao redor do mundo, é importante ao menos, citar outra forma de classificação de empresas. Na União Europeia, por exemplo, para ser PME a empresa deve ter menos de 250 funcionários, um volume de negócios anual que não ultrapasse os 50 milhões de euros ou um balanço total anual que não ultrapasse 43 milhões de euros (Público, 2018).

2.1.2 Características das PME de comércio atacadista

Segundo Camarotto (2009), as funções comumente desempenhadas em um comércio atacadista são vendas, compras, crédito e financiamento, armazenamento, distribuição, informações de marketing (informa à indústria as condições do mercado), transporte e risco (absorver riscos de negócios como manutenção de estoque, por exemplo). Além disso, com a recente terceirização de departamentos, os atacadistas aumentaram seu escopo de atividades prestadas às indústrias, incluindo serviços de logística, como transporte e entregas. Os departamentos chave de uma empresa de comércio atacadista, normalmente, são os que envolvem os serviços comerciais e a logística dos produtos comercializados, pois de fato, são os que tratam diretamente do negócio da organização.

O departamento de vendas é fundamental para uma empresa comercial e deve estar organizado para manter um sólido relacionamento com o cliente, através de políticas empresariais e sistemas específicos como CRM (*Customer Relationship Management*), de acordo com Camarotto (2009). Já os tipos de informação frequentemente encontrados nas PMEs comerciais são: ordens de compra, notas fiscais de entrada, pedidos de vendas, relatórios de separação de materiais, notas fiscais de saída, boletos de pagamento, canhotos de notas, guias de impostos, conhecimentos de frete, romaneio de carga, cartas de correção,

pesquisas de mercado, contratos diversos, listas de preços, cadastros de produtos, fornecedores, clientes e funcionários.

2.1.3 Segurança da Informação nas Pequenas e Médias Empresas

As PMEs, em sua maioria, não têm infraestrutura para implantar segurança da informação (SI) com eficiência, pois não possuem conhecimento técnico suficiente, pessoal com dedicação integral às atividades necessárias ou recursos financeiros para investir, conforme Neto e Silveira (2007). Além disso, Gupta & Hammond (2005) argumentam as PMEs frequentemente retém a tecnologia que já estão familiarizadas, por conveniência e, por dar mais atenção às atividades de negócios, revisam suas necessidades de segurança apenas eventualmente. Soma-se a isso o desconhecimento de normas ou *frameworks* e pode-se compreender porque da carência de projetos em segurança da informação nas PMEs.

2.1.3.1 O contexto e as perspectivas da SI nas PMEs brasileiras

As PMEs representam grande parte dos negócios brasileiros. Segundo estatísticas publicadas em O Povo (2016) e Globo (2017), em 2016 as PMEs do comércio representavam 96,3 % das empresas deste ramo. No comércio atacadista, as PMEs representam 93 % do total de comércios. Apenas os pequenos negócios representam 27 % do PIB nacional, conforme o SEBRAE (2014). Segundo o levantamento PNAD (Pesquisa Nacional por Amostra de Domicílios) do IBGE publicado em Globo (2017), as pequenas empresas estão entre as que mais movimentaram a economia depois da crise de 2014. Os dados indicam migração de trabalhadores das grandes empresas para as pequenas empresas de 2012 a 2016. Além disso, os pequenos e médios negócios são responsáveis pela maioria dos empregos formais no país com 53,5 % dos trabalhadores, conforme Globo (2017). Para a SI há boas perspectiva, segundo a pesquisa *Brazil Small & Medium Business: ICT & Cloud Services Tracker Overview* publicada em CIO (2016), os investimentos em TI nas PMEs brasileiras devem saltar de 48 para 63 bilhões de dólares até 2020. Outros dados desta pesquisa indicam que as soluções de segurança mais usadas nas PMEs brasileiras são serviços de filtro de Web (13 % nas pequenas e 25 % nas médias empresas) e antispams (13 % e 29 % respectivamente). Já quando questionadas sobre quais serviços de segurança pretendem adotar nos próximos 12 meses, a preferência das pequenas é por soluções UTM (*Unified Threat Management*) com 19 %, enquanto 25 % das empresas médias pretendem adotar serviços de VPN (*Virtual*

Private Network). Ainda segundo a pesquisa, várias empresas deverão priorizar soluções contra perda de dados (59 %), gestão de TI (55 %), *data recovery* e *backup* (52 %), segurança de dados em nuvem (55 %) e segurança de dados em *mobile* (23 %).

2.1.3.2 As limitações das Pequenas e Médias Empresas

As limitações das PMEs não influenciam exclusivamente a sua SI, mas todos seus setores, departamentos ou áreas. Assim é o caso da Tecnologia da Informação (TI), que é um setor carente de recursos na maioria das PMEs e impacta diretamente na SI. Thong (2001) analisa a falta de estrutura e conhecimento das pequenas empresas com TI. Em seu estudo com 114 PMEs de Singapura constatou que estas empresas não conhecem a importância de fatores-chave em TI. Além de possuírem recursos reduzidos, podem investir estes recursos em fatores de pouca importância para o sucesso da implantação da TI. Por outro lado, Thong (2001) concluiu que as empresas com maior sucesso na implantação de sistemas de informação tinham suporte externo qualificado, investimento adequado, usuários chave treinados e comprometidos e apoio dos gestores.

O papel dos gestores é um fator fundamental. Casaca (2010), em sua tese de doutorado, propôs uma investigação sobre a eficácia das práticas de GSI nas PMEs de Portugal e a formação da percepção dos riscos da SI pelos seus gestores. Na investigação com 674 respostas, os resultados indicaram que as tecnologias de SI, as pessoas e a percepção do risco de SI pelos gestores são fatores determinantes para a eficácia das práticas de SI. A percepção do gestor, em particular, influencia diretamente na estratégia que a empresa adota para SI. Se o gestor percebe o risco como baixo, os limitados recursos da empresa serão consumidos por outras áreas. Segundo Casaca (2010), a percepção dos gestores tem papel moderador na eficácia da GSI nas PMEs, quanto mais consciente dos riscos que a organização enfrenta, maior será a atenção do gestor e maior a eficácia das práticas de GSI.

Outro fator que deve ser observado é o das influências externas, conforme Dojkovski *et al*. (2007), é preciso perceber o setor como um todo, envolvendo fornecedores, proprietários, empregados, clientes e governos, pois são agentes que podem influenciar o programa de SI. Outros autores constataram a complexidade de implantação das normas de GSI, como Da Silva e Brancher (2016) que identificaram que apesar da ISO/IEC 27001 adaptar-se a qualquer organização, existe uma dificuldade de implantá-la, seja por falta de competência ou indisponibilidade de recursos da empresa. Além disso, existe a falsa percepção das PMEs de que são invisíveis aos olhos dos *cyber* criminosos. Conforme Casaca

(2010), as PMEs que utilizam intensivamente informações não reconhecem o perigo da espionagem e das ameaças a que os seus ativos estão submetidos. Resolver estas deficiências seria um caminho para o desenvolvimento de cultura organizacional da SI. Segundo Dojkovski *et al*. (2007), as organizações que buscam os melhores resultados em SI investem na criação de uma cultura da SI através de políticas, conscientização, treinamento e educação, induzindo os funcionários a ter bons hábitos e cuidar da informação organizacional.

Apesar das limitações, muitas PMEs estão preocupadas com a SI. Neto e Silveira (2007) estudaram quais fatores influenciaram a adoção da GSI nas PMEs. Seu estudo analisou 43 empresas da região do Grande ABC, São Paulo, e classificou as ferramentas e técnicas de GSI usadas nestas empresas em três camadas: física, lógica e humana. Constataram que nas PMEs existe preocupação com a SI, pois em 59 % das pesquisas a GSI pode ser considerada satisfatória em relação à camada física, já que 100 % utilizam antivírus, 97,6 % sistemas de *backup* e 82,9 % *firewall*. Entretanto, as camadas lógica e humana apresentaram índices menos otimistas, pois menos da metade das empresas implementava os controles estudados e era baixa a adequação às seções da norma ISO/IEC 27002:2005, que trata das boas práticas em GSI. Como fatores motivadores para implantar GSI identificou-se evitar perdas financeiras e como fatores inibidores falta de conhecimento, valor do investimento, dificuldade de medir custo/benefício e cultura organizacional.

2.2 *FRAMEWORKS* DE GSI FOCADOS EM PMES

As PMEs, em sua maioria, não têm infraestrutura para implantar SGSI com eficiência. Soma-se a isso o desconhecimento de normas e a complexidade ou baixa aderência destes modelos e o resultado é a existência de poucos projetos de SI nas PMEs. Alguns autores já propuseram trabalhos semelhantes ao que se propõem neste estudo, como Dojkovski *et al*. (2007), Begg e Caira (2012), Da Silva Neto *et al*. (2015) e Da Silva e Brancher (2016), que propuseram *frameworks* simplificados para SGSIs em PMEs. Já Oliveira *et al*. (2016) documentou a implantação da NBR ISO/IEC 27000 em uma PME, falando das dificuldades e das melhorias. A seguir, estes trabalhos serão apresentados.

2.2.1 Um *framework* holístico

A cultura local e a falta de políticas de apoio ao segmento podem ser fatores determinantes para organizações com estruturas enxutas. Dojkovski *et al*. (2007) estudaram os

motivos das PMEs australianas não possuírem uma SI organizacional efetiva e sugeriram um *framework* holístico para promover a cultura da SI nas PMEs. O modelo relaciona as influências externas e internas e obtém como saída o comportamento voltado à GSI. As influências externas devem ser mapeadas e são: cultura nacional e ética, iniciativas do governo e fornecedores. Já as influências internas devem ser avaliadas, revisadas e valoradas e são: análise de risco, orçamento, políticas e procedimentos, responsabilidades, autoavaliação, recursos humanos, aprendizagem individual e organizacional e consciência de segurança organizacional. Os resultados esperados para o sistema são comportamentos de responsabilidade, integridade, confiança, ética, motivação, valorização, orientação e crescimento pessoal. Os autores concluíram que o *framework* pode ser aplicado para ajudar as PMEs a desenvolver sua cultura de SI. Mas, as empresas participantes gostariam de contar com inciativas do governo para ajudar no desenvolvimento. Os autores perceberam que os donos das PMEs não dão suficiente suporte à SI, pois desconhecem sua importância. Além disso, identificaram a dificuldade em promover uma aprendizagem comportamental de GSI que complemente a gestão tradicional de TI. Dojkovski *et al*. (2007) atribuem esta dificuldade à falta de visão de mudança dos gestores das PMEs e propõem que sejam educados sobre o potencial estratégico da SI, para que entendam os benefícios da sua adoção.

2.2.2 *Framewok* para Governança de Dados

Em toda implantação de sistema, ou em todo projeto de forma geral, surgem dilemas que precisam ser resolvidos pela escolha de soluções nem sempre satisfatórias. Os autores Begg e Caira (2012) estudaram dilemas comuns na implantação de sistemas de Governança de Dados (GD) em PMEs. A Governança de Dados é a governança responsável pelo controle e gestão dos dados de uma organização, garantindo que os dados se transformem em informações confiáveis. Na sua pesquisa, propuseram um *framework* que fosse mais adequado às empresas com menor estrutura, onde nem sempre há um departamento ou pessoal dedicado a TI. Para isso buscaram que o modelo fosse adaptável, escalável, simples e sem linguagem técnica. A metodologia usada foram ações de pesquisa, em que os autores atuaram como agentes de mudança em projetos colaborativos com dez PMEs. Begg e Caira (2012) concluíram que os resultados obtidos foram satisfatórios, entretanto não suficientemente adequados para utilização nas PMEs. Os principais dilemas para aplicação da GD neste cenário foram: Primeiro, apesar de perceber os benefícios da GD, o esforço para alcança-los é muito grande, em parte devido aos "*softwares* de pacote" que

não permitem adaptações; Segundo, muitas PMEs são seguidoras de formatos de dados (parceiros, clientes ou fornecedores, por exemplo), dificultando a padronização e criação de uma identidade; Terceiro, os *framewoks* existentes não são facilmente adaptáveis, nem escaláveis, usam linguagem técnica ou precisam ser pagos, o que nem sempre está ao alcance; E, quarto, a comunidade de GD tem a ideia que as PMEs requerem uma governança simples, mas algumas manipulam mais dados e mais complexos do que grandes empresas.

2.2.3 *Framework* a partir de uma simplificação da ISO/IEC 27002

O fato de ser uma PME traz para algumas empresas a falsa impressão de que não são alvos valiosos ou não têm muito a oferecer aos *cyber* criminosos. Da Silva Neto *et al*. (2015) afirmam que a maioria das pequenas empresas subestimam a preferência de bandidos por elas, por desconhecer que todas são possíveis alvos, independentemente do porte. Os autores demonstraram o crescimento do número de ataques às PMEs em 2012 e 2013, quando as ofensivas dirigidas às PMEs, corresponderam a 30 % do total do ano no mundo, com tendência crescente. Da Silva Neto *et al*. (2015) perceberam que por subestimar os riscos, as PME geralmente não adotam um modelo ou norma de SI. Portanto, propuseram uma simplificação dos controles da NBR ISO/IEC 27002 de 133 para 22. A simplificação foi baseada em uma pesquisa com 48 PMEs, onde identificaram a visão destas empresas sobre SI. Vinte controles foram os considerados mais importantes para as PMEs pesquisadas e dois foram acrescentados pelos autores. Os controles definidos para o trabalho podem ser vistos na Tabela 3 e na Tabela 4 na coluna "*Framework* Da Silva Neto". Os autores concluíram que a falta de cultura organizacional sobre SI nas empresas pesquisadas é um fator que as tornam vulneráveis a ameaças que exploram o fator humano. A maioria das PMEs pesquisadas não possuíam uma política de segurança formalizada, o que representa um risco, pois procedimentos informais não são adequadamente comunicados e não proporcionam a formação da cultura de SI. Além disso, identificaram que muitas PMEs não buscam adequação através de normas ou padrões de SI, ou seja, há desconhecimento, desinteresse ou impossibilidade para aderir a um padrão.

2.2.4 O modelo ITMark numa perspectiva para SI

A implantação de uma norma é uma tarefa difícil para qualquer organização, pois requer mudanças culturais, investimento financeiro e tempo. Analogamente, parece um

caminho mais longo e custoso para as organizações menores. Por outro lado, um modelo que traz a possibilidade de implantação em níveis e análise de maturidade pode ser mais atrativo. O modelo analisado por Da Silva e Brancher (2016) traz estas perspectivas. Os autores estudaram um contexto em que as micro e pequenas empresas (MPEs) de *software*, após implantarem modelos de qualidade para o desenvolvimento de *software*, buscaram alternativas para garantir e melhorar outros processos como a SI. O trabalho consistiu em avaliar o desempenho do modelo ITMARK na melhoria da GSI de MPEs de desenvolvimento de *software*. O ITMark é um modelo de qualidade criado pelo ESI (*European Software Institute*) para atender MPEs. O modelo avalia as empresas sob três aspectos: gestão de negócios, gestão de desenvolvimento de software e Gestão de Segurança da Informação baseado nas ISO/IEC 27001 e 27002. Para garantir sua implantação independentemente do tamanho da empresa está agrupado em níveis: *Basic, Premium e Elite*. Para atingir a certificação no nível *Basic*, a organização deve implementar até 27 requisitos, sendo aceita se tiver ao menos 19, dentre eles os obrigatórios. Os requisitos estão na coluna "*Framework* Da Silva e Brancher" das Tabelas 3 e 4. Os autores acompanharam a implantação do *framework* em cinco empresas brasileiras e todas atingiram o nível *Basic*. Da Silva e Brancher (2016) concluíram que o modelo ITMARK é viável para melhorar a GSI das MPEs. Sendo que, uma das vantagens do ITMARK é a nivelação. A análise de maturidade e nivelação possibilitam que a organização visualize onde está e onde pode chegar, assim percebe que pode implantar GSI gradativamente e com a percepção de crescer durante o processo.

2.2.5 A eficiência do modelo ISO/IEC 27001 e 27002

Os autores Oliveira *et al*. (2016) realizaram uma análise da SI em uma média empresa antes e depois da implantação das normas ABNT NBR ISO/IEC 27001 e 27002. O objetivo da análise era verificar a eficácia da implantação das normas em uma PME. Oliveira *et al*. (2016) dividiram a implantação nas seguintes etapas: 1) Alinhamento e planejamento de SI; 2) Levantamento tecnológico; 3) Diagnóstico inicial de conformidade; 4) Criação da Política de SI; 5) Criação de documentos auxiliares; 6) Treinamento em SI; 7) Diagnóstico final de conformidade; 8) Pesquisa de satisfação. Os autores realizaram um diagnóstico de conformidade antes e outro após a implantação. O comparativo dos diagnósticos permitiu identificarem melhorias significativas nos requisitos de SI. Além disso, aplicaram uma pesquisa de satisfação com funcionários e diretores que identificou satisfação positiva dos envolvidos. O trabalho de Oliveira *et al*. (2016) demonstra a possibilidade de implantação das

normas ABNT NBR ISO/IEC 27001 e 27002 com baixo custo e resultados satisfatórios em PMEs. Também é importante o registro da experiência de Oliveira *et al*. (2016), quando falam da necessidade de explicar conceitos e objetivos diversas vezes e como foi necessária a paciência da equipe de implantação para marcar e desmarcar reuniões com a diretoria.

2.3 QUESTIONÁRIO SOBRE GSI EM PMES ATACADISTAS DE CAXIAS DO SUL E REGIÃO

2.3.1 A elaboração do questionário, definição das entrevistas e forma de coleta

O questionário foi estruturado com questões fechadas de simples e múltipla escolha, que foram aplicadas através de entrevista. Portanto, as perguntas elaboradas serviram de orientação ao entrevistador, mas a entrevista foi livre, permitindo a evolução do assunto. O objetivo do questionário era identificar se a organização possuía infraestrutura de SI, se as políticas estão formalizadas, se já implantou um SGSI com a ISO/IEC 27000, quais os resultados da implantação, se não implantou, quais os motivos e de identificar o nível de consciência destas empresas em relação aos riscos que as suas informações correm.

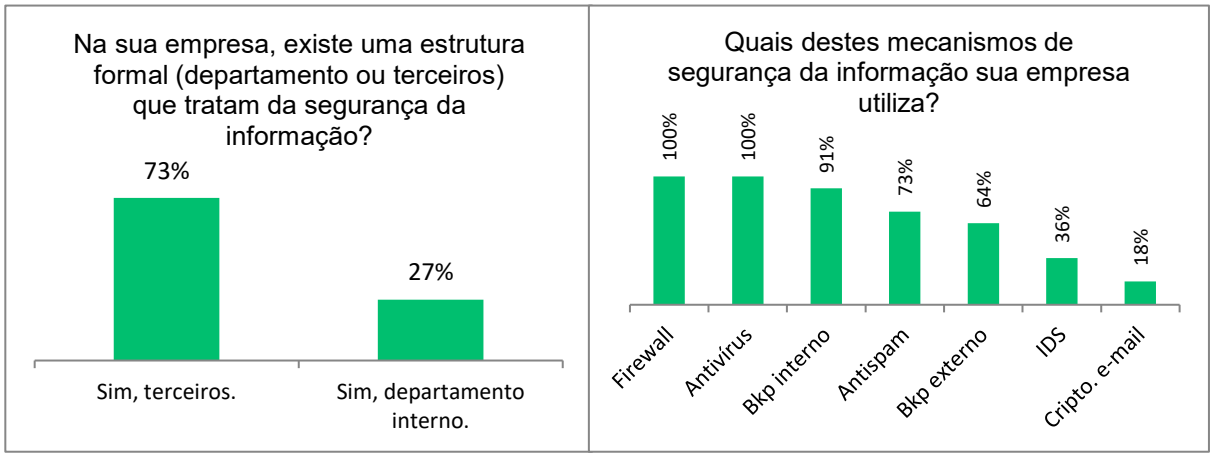
A definição dos entrevistados deu-se por uma lista de PMEs do comércio atacadista de Caxias do Sul requisitada ao CDL (Câmara de Dirigentes Lojistas) do município. Além disso, na empresa onde o autor trabalha, também foi cedida uma lista de empresas do ramo atacadista com autorização da direção para ser aplicada neste estudo. Desta forma, o questionário foi aplicado aos responsáveis por SI, responsáveis pela TI ou ao proprietário da empresa. Para obter o retorno de 11 questionários respondidos, foi necessário o contato com mais de 40 empresas. A grande maioria dos contatos alegaram não poder participar da pesquisa por não terem autorização de fornecer informações. Percebe-se que a obtenção de informações sensíveis às empresas não é tarefa fácil e exige, na maioria das vezes, o estabelecimento de uma relação de confiança através de uma pessoa conhecida ou influente. Todos os questionários foram aplicados por telefone, explicando a importância da participação, evidenciando os possíveis retornos do estudo ao setor envolvido e disponibilizando os contatos do autor e da universidade onde o trabalho está sendo realizado. Assim, procurou-se dar segurança aos entrevistados e abrir um canal para questionamentos, o que é fundamental para uma entrevista, conforme Günther (2003). Como resultado, a maioria das entrevistas foi bastante formal e não permitiu maiores evoluções. No entanto, duas

entrevistas a empresas que, além das vendas ao atacado, forneciam serviços de TI deram suas visões sobre mercado em questão. A seguir serão apresentados os resultados obtidos.

2.3.2 A análise das respostas

Todas organizações entrevistadas possuíam infraestrutura para SI, sendo que em 72,7 % trata-se de um departamento terceirizado, como pode ser visto na Figura 1. Além disso, grande parte das empresas utilizavam antivírus e *firewall*, *backup* interno, *backup* externo, *antispam*, Sistemas de Detecção de Intrusão (IDS) e criptografia nos e-mails (Figura 1). Estas informações consistem com o trabalho realizado por Neto e Silveira (2007), que constatam a preocupação das PMEs com a segurança física e lógica dos dados.

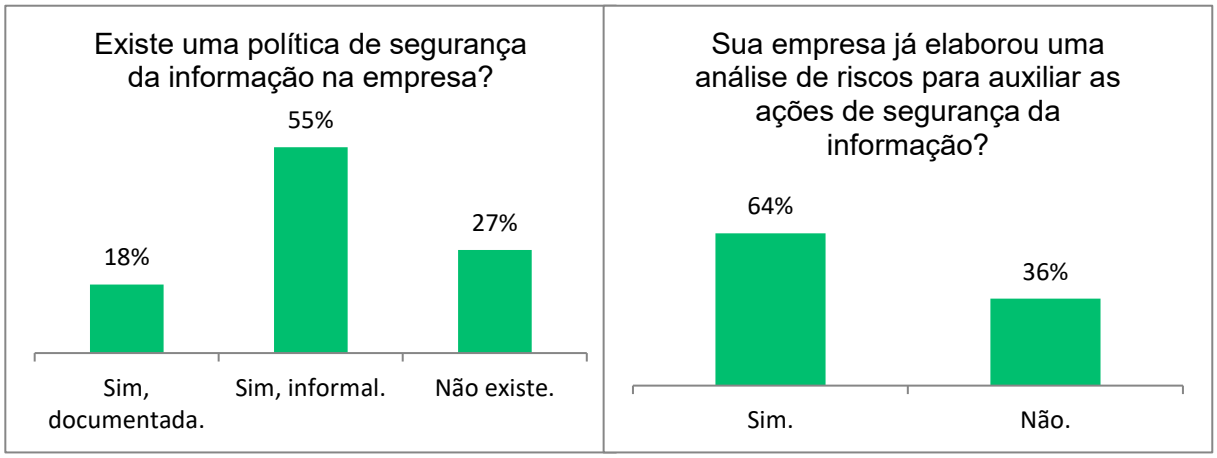
Figura 1 - Infraestrutura das empresas



Fonte: o autor

A grande maioria das empresas entrevistadas, 72,7 %, possuem uma política de SI (Figura 2). O que indica a preocupação dos responsáveis por segurança em elaborar e seguir critérios. No entanto, a política é formal em apenas 18 % delas, o que indica um risco e

Figura 2 - Política e análise de riscos nas empresas



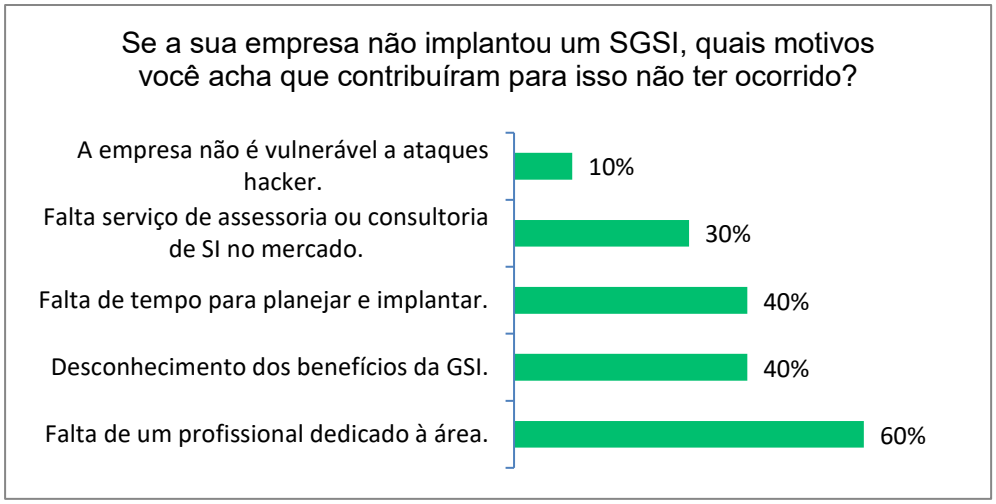
Fonte: o autor

corrobora com o trabalho de Da Silva Neto *et al*. (2015), que alertam para os problemas dos procedimentos informais, pois não são adequadamente comunicados às equipes e dificultam a criação de uma cultura de segurança. Apesar disso, 63,6 %, já elaboraram uma análise de riscos para auxiliar nas ações de segurança (Figura 2), o que significa um norte para orientar as atividades a serem implementadas e controladas.

De todas as empresas entrevistadas, apenas uma delas já implantou um SGSI com base na ISO/IEC 27000. O entrevistado respondeu que as maiores dificuldades encontradas são o *framework* complexo, com muitos requisitos a serem cumpridos, e as dificuldades de colaboração dos demais funcionários e da alta direção da empresa. O principal impacto das dificuldades encontradas foi o atraso nos prazos de implantação e, consequentemente, trabalhar a desmotivação da equipe de implantação. Já o principal fator positivo do processo de implantação, segundo o entrevistado, foi a assessoria externa que colabora com nível de conhecimento e apoio ao pessoal interno. E, apesar dos transtornos enfrentados, o entrevistado considera o nível de satisfação com os resultados obtidos como bom, principalmente devido a organização e orientação para as atividades de segurança.

Por outro lado, apenas cinco das 10 empresas que ainda não implantaram um SGSI têm planos de implantar. Dos principais motivos para não implantar, atribuíram 60 % a falta de um profissional dedicado ao assunto, enquanto que o desconhecimento dos benefícios

Figura 3 - Motivos de não ter implantado um SGSI



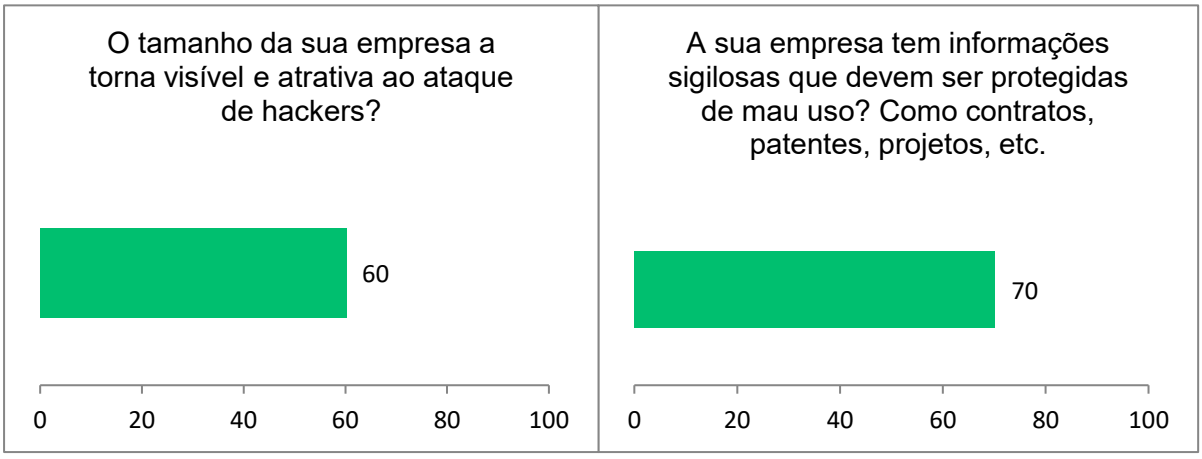
Fonte: o autor

da GSI teve 40 %, assim como a falta de tempo para planejar e implantar, também 40 % (Figura 3). Os dados corroboram com Neto e Siveira (2007) e Thong (2001), para quem a falta de conhecimento e recursos reduzidos foram fatores críticos na implantação de um SGSI. Já a falta de consultoria e assessoria no mercado indicou apenas 30 % e um dos entrevistados

alegou que sua empresa não tem vulnerabilidades. Outro motivo, comum em duas entrevistas em que as empresas forneciam serviços de TI voltados à segurança, foram as dificuldades de obter tempo e dedicação da direção da empresa cliente. Nas conversas foi possível extrair três fatores que impactam neste item. O primeiro fator que aumenta as dificuldades é a linguagem técnica, em que a falta de compreensão de termos e tecnologia distanciam as pessoas menos familiarizadas das necessidades e soluções. O segundo fator é a necessidade de manter as expectativas dos diretores em níveis realistas, ou seja, sempre deixar claro quais serão os ganhos possíveis e as limitações do sistema. Pois, se as expectativas forem muito elevadas e acabarem frustradas, toda a equipe sentirá os efeitos da perda de interesse da alta direção. Por fim, o terceiro fator é a dificuldade de extrair procedimentos e políticas que estão na cabeça de uma pessoa, que representa as normas em si. Conforme os entrevistados, este cenário é comum nas PMEs, principalmente nas familiares. A pessoa centralizadora, frequentemente é o gestor e tem receio de perder o controle da empresa se os funcionários diminuírem a dependência dele. Os fatores citados confirmam a percepção de Casaca (2010), de que os gestores têm um papel moderador na eficácia das práticas de GSI nas PMEs.

Os dados que relacionam o nível de consciência das entrevistadas com os riscos que correm indicam que o nível de consciência está em um patamar médio, mas ainda é preciso melhorar. Percebe-se que em média, os entrevistados deram peso 60 para a questão "se concordavam que o tamanho da sua empresa as tornava atrativas ao ataque de *hackers*" (Figura 4), mas 54,5 % deram muito pouco valor a questão. Já a percepção de valor sobre as informações da empresa foi um pouco melhor e chegou ao peso 70 para a pergunta "A sua empresa tem informações sigilosas que devem ser protegidas de mau uso?" (Figura 4). Mas 36,4 % deram notas baixas e uma delas atribui peso zero para percepção de risco. Este cenário

Figura 4 - Percepção dos riscos nas empresas



Fonte: o autor

confirma a visão de Casaca (2010), quando disse que muitas empresas não reconhecem o perigo da espionagem e das ameaças a que os seus ativos estão submetidos.

Todas as empresas entrevistadas se enquadram como PMEs, de acordo com os critérios do SEBRAE (2018) para empresas do comércio, sendo que 72,7 % eram pequenas e 27,3 % eram médias empresas. Já os atores entrevistados foram administradores, gerentes, diretores ou responsáveis pela TI. Em todas empresas os entrevistados confirmaram envolvimento na elaboração ou aprovação das políticas de SI, mesmo que informalmente. Entretanto, o envolvimento dos entrevistados não refletiu no aumento da consciência em SI das organizações, pois se todos estão envolvidos com SI, por que a consciência destas empresas em relação aos riscos que os seus SI correm é menor que 70 pontos? As hipóteses mais fortes para isso foram lançadas na entrevista, onde cita-se que os motivos mais relevantes para não existir um SGSI formal são a falta de profissional dedicado ao assunto, o desconhecimento dos benefícios da GSI, e a falta de tempo para planejar e implantar.

2.4 UM FRAMEWORK NIVELADOR PARA PMES

Para propor o *framework* nivelador para PMEs serão agrupados e classificados as conclusões e os fatos das seções apresentadas. Os resultados mais representativos indicam as fragilidades e oportunidades de maior consenso entre as pesquisas sobre SGSI em PMEs.

2.4.1 Classificação das conclusões e fatos sobre GSI nas PMEs

As conclusões e fatos apontados na Seção 2.1.3, Segurança da Informação nas PMEs, de a) até o); as conclusões e fatos sobre os *Frameworks* de GSI focados em PMEs da Seção 2.2, de p) até bb); e as conclusões e fatos obtidos no questionário sobre GSI em PMEs atacadistas de Caxias do Sul e região da Seção 2.3, de cc) até ll) podem ser vistos na Tabela 1.

Tabela 1 – Conclusões e fatos sobre GSI nas PMEs

ID	Conclusões e fatos
a	Conhecimento técnico de pessoal insuficiente - Neto e Siveira (2007) e Thong (2001).
b	Recursos financeiros insuficientes - Neto e Siveira (2007) e Thong (2001).
c	Estão preocupadas com segurança física e lógica (antivírus, *backup*, *firewall*) - Neto e Silveira (2007).
d	Retém a tecnologia que já estão familiarizadas e revisam suas necessidades de segurança ocasionalmente - Gupta & Hammond (2005).
e	Os investimentos em TI crescerão até 2020 - CIO (2016).
f	Investem mal seus recursos pois não conhecem a importância de fatores-chave em TI - Thong (2001).
g	Pouca preocupação com recursos humanos e baixa adesão a norma ISO 27000 - Neto e Silveira (2007).
h	Não reconhecem o perigo da espionagem e das ameaças aos seus ativos de informação - Casaca (2010).

ID	Conclusões e fatos
i	Falta de conhecimento, baixo investimento, dificuldade de mensurar custo/benefício e baixa cultura organizacional - Neto e Silveira (2007).
j	As PMEs com sucesso no SI tinham suporte qualificado, investimento, usuários treinados e comprometidos e apoio da alta direção - Thong (2001)
k	As organizações com os melhores resultados investem na cultura da SI - Dojkovski *et al*. (2007).
l	Uma motivação para implantação de um SGSI percebida pelos gestores das PMEs é evitar perdas financeiras - Neto e Silveira (2007).
m	Normas de SI complexas - Da Silva e Brancher (2016) e Begg e Caira (2012).
n	Perceber o setor como um todo - Dojkovski *et al*. (2007).
o	Conscientização dos gestores das PMEs - Casaca (2010).
p	A cultura local e a falta de políticas de apoio ao segmento - Dojkovski *et al*. (2007).
q	Falsa ideia que as PMEs requerem uma governança simples - Begg e Caira (2012).
r	Gestores não proporcionam suficiente suporte à SI - Dojkovski *et al*. (2007).
s	Falta conscientização dos gestores sobre a SI - Oliveira *et al*. (2016).
t	Falta de visão de mudança dos proprietários - Dojkovski *et al*. (2007).
u	O *framework* precisa ser adaptável, escalável, simples e sem linguagem técnica - Begg e Caira (2012).
v	Um *framework* com análise de maturidade e nivelação pode facilitar a implantação da GSI - Da Silva e Brancher (2016).
w	O esforço para implantar GD é muito grande - Begg e Caira (2012).
x	As PMEs são seguidoras de formatos de dados o que dificulta a padronização e criação de uma identidade - Begg e Caira (2012).
y	Por subestimar os riscos não adotam modelos de SI - Da Silva Neto *et al*. (2015).
z	A falta de cultura de SI torna as empresas vulneráveis a ameaças que exploram o fator humano - Da Silva Neto *et al*. (2015).
aa	Não possuíam uma política de segurança formalizada e procedimentos informais não são adequadamente comunicados - Da Silva Neto *et al*. (2015).
bb	Desconhecimento, desinteresse ou impossibilidade em aderir a normas de SI - Da Silva Neto *et al*. (2015).
cc	Possuem infraestrutura de SI e têm preocupação com a segurança física e lógica dos dados.
dd	Possuem uma política de Segurança da Informação.
ee	Em poucas empresas a política de SI está formalizada.
ff	A empresa entrevistada que já implantou um SGSI considerou como dificuldades a complexidade do *framework* e a falta de colaboração de funcionários e alta direção.
gg	Como fator positivo, a entrevistada que implantou um SGSI, destacou a melhora na organização e no foco nas atividades de segurança.
hh	A maioria das entrevistadas não pretende implantar um SGSI, devido à falta de pessoal dedicado, desconhecimentos dos benefícios e falta de tempo para planejar e implantar.
ii	Dificuldades de obter tempo e dedicação da direção da empresa, devido à má compreensão da linguagem técnica, da necessidade de manter as expectativas dos diretores em níveis realistas e da resistência em formalizar procedimentos e políticas de domínio pessoal.
jj	A baixa consciência sobre os riscos que correm as informações críticas destas empresas.
kk	A baixa consciência sobre o valor das informações para a organização.
ll	Os entrevistados confirmaram estar envolvidos na elaboração ou aprovação das políticas de SI, entretanto isso não refletiu em um nível elevado de consciência de SI das suas organizações.

Fonte: o autor.

As conclusões e os fatos apanhados na Tabela 1 foram classificados por assunto. Desta forma, foi possível analisar quais eram os assuntos mais relevantes para serem trabalhados na proposta de *framework*. Em síntese, os assuntos para classificação foram:

Conhecimento, que pode ser sobre investimentos financeiros, funcionários, normatização, percepção de riscos e sobre formação da cultura de SI; *Framework*, que pode ser sobre complexidade de implantá-los, sua característica de nivelação e não conformidade do *framework* implantado; Gestores, que pode ser sobre a conscientização destes gestores, o apoio e suporte dos gestores à GSI e o conhecimento dos gestores em SI; Influências Externas, que pode ser sobre o mercado, a cultura local ou subsídios para o setor; e, por fim Infraestrutura, que pode referir-se a disponibilidade de pessoal, a disponibilidade financeira ou a disponibilidade tecnológica.

Depois de criadas e atribuídas as classificações, pôde-se ponderar as conclusões e os fatos pela sua incidência e identificar quais têm maior impacto na implementação e manutenção de um SGSI em PMEs. Devido ao tempo limitado para elaboração do trabalho, nem todos os itens poderiam ser abordados. Portanto, foi preciso escolher os mais significativos para serem incluídos na análise, que foram: Conhecimento em normatização, Conhecimento dos riscos e Conhecimento para cultura de SI; seguidas de Infraestrutura em tecnologia e Infraestrutura de pessoal; depois a classificação Apoio dos gestores e, por fim, a classificação Complexidade de *framework*.

2.4.2 Classificação das contribuições dos *frameworks* de GSI focados em PMEs

As principais contribuições dos *frameworks* estudados na Seção 2.2 que têm o objetivo de torna-los mais aderentes às PMEs são apresentados na Tabela 2.

Tabela 2 - Contribuições dos *frameworks* de GSI focados em PMEs

ID	Contribuições
i	Mapear as influências externas: a cultura nacional e ética, as iniciativas do governo e os fornecedores. De "Um *framework* holístico", Seção 2.2.1, de Dojkovski *et al*. (2007).
ii	Mapear, avaliar, revisar e valorar as influências internas: assuntos gerencias (análise de risco, orçamento, políticas e procedimentos, responsabilidades, autoavaliação e recursos humanos) e com ênfase na aprendizagem individual e organizacional e consciência de segurança organizacional. De "Um *framework* holístico", Seção 2.2.1, de Dojkovski *et al*. (2007).
iii	Aumentar a consciência da equipe para a cultura de gestão de dados através de ações de pesquisa. Para atingir o objetivo realizaram três ações de pesquisa consecutivas. Na primeira, focaram na importância dos ativos de informação. Na segunda, focaram na governança em cinco domínios: princípios dos dados, qualidade dos dados, metadados, acesso aos dados e ciclo de vida das informações. Por fim, na terceira, em como esses domínios impactam na gestão dos dados e do negócio. De "*Framework* para Governança de Dados, Seção 2.2.2, de Begg e Caira (2012).
iv	Simplificar a implantação de um SGSI aplicando 22 requisitos da ISO 27002 definidos como importantes através de pesquisa pelas empresas alvo do estudo. De "Framework a partir de uma simplificação da ISO/IEC 27002", Seção 2.3.3, de Da Silva Neto *et al*. (2015).

ID	Contribuições
v	Simplificar a implantação de um SGSI com requisitos do ITMARK. A característica de nivelação presente no ITMARK faz deste *framework* uma alternativa muito interessante para empresas de vários tamanhos. Para o nível *Basic*, ideal para empresas iniciantes, há 27 requisitos, sendo que ao menos 19 devem ser implementados, dentre eles alguns são obrigatórios. De "O modelo ITMARK numa perspectiva para SI", Seção 2.2.4, de Da Silva e Brancher (2016).
vi	Implantação da ISO 27001 e 27002 através de equipe qualificada e de um processo bem definido e valorizado por diagnósticos próximos das fases inicial e final. De "A eficiência do modelo ISO/IEC 27001 e 27002", Seção 2.2.5, de Oliveira *et al*. (2016).

Fonte: o autor.

Para as contribuições também foi utilizada a mesma classificação feita em 2.4.1. Desta maneira, foi possível concluir que as contribuições de Dojkovski *et al*. (2007) e Begg e Caira (2012), respectivamente itens ii e iii, seriam as mais eficientes para tratar as dificuldades encontradas nos cenários pesquisados, complementadas pelas contribuições Da Silva Neto *et al*. (2015) e Da Silva e Brancher (2016), respectivamente itens iv e v.

2.4.3 O *Framework* Nivelador

As conclusões e fatos mais relevantes anteriormente analisados e classificados na Seção 2.4.1 e as contribuições classificadas e escolhidas na Seção 2.4.2 foram usados como norteadores para a criação de um *Framework* Nivelador. O modelo proposto foi estruturado em níveis conforme inspiração no trabalho de Da Silva e Brancher (2016). Desta forma, permitirá que as organizações implantem o SGSI de forma gradual e iniciando com baixos custo e complexidade. Todos níveis, exceto o Nível 1, têm como pré-requisito o nível anterior. O Nível 1 tem o objetivo de criar a percepção dos funcionários e gestores para a importância da cultura da SI. A partir do Nível 2, Requisitos Básicos, passa a existir o compromisso de cumprir-se requisitos de forma gradual. No Nível 3 os requisitos aumentam e continuam nos Níveis 4 e 5 até chegarem às normas ISO/IEC 27001 e 27002.

2.4.3.1 O Nível 1 – Cultura de Segurança da Informação

O Nível 1 possui dois objetivos principais, o primeiro é preparar a equipe da organização para desenvolver a cultura da SI, através do aprendizado individual e organizacional, conforme contribuição de Dojkovski *et al*. (2007). O segundo objetivo é ter custo e complexidade de implantação baixos. Para atender os objetivos serão realizados ciclos avaliados de aprendizado, identificação e conscientização de riscos. Todas as análises geradas no Nível 1 da implantação serão utilizadas no Nível 2.

A preparação da equipe de funcionários e gestores para o desenvolvimento de consciência e cultura da SI será inspirado no ciclo de ações de pesquisa de Begg e Caira (2012). Porém, ao invés de ações de pesquisa serão propostos ciclos de aprendizado seguidos de avaliações coletivas e individuais, com objetivo de aumentar o conhecimento dos funcionários e gestores sobre a importância da normatização e criação da cultura da SI. A organização poderá optar pela forma de apresentação do aprendizado com palestras, leituras, vídeos ou apresentações. A forma de avaliação pode ser feita através de pesquisas ou provas que pode ser coletiva ou coletiva e individual. A vantagem da avaliação individual é incentivar o funcionário que se destaca. Para passar ao Nível 2, somente será necessária a avaliação coletiva, com exigência mínima de 80 %.

Além dos ciclos avaliados de aprendizado, para completar o Nível 1 é preciso fazer e divulgar a identificação dos riscos na organização. A identificação dos riscos tem o objetivo de identificar e compreender os riscos aos quais a organização está sujeita, possibilitando decidir se é preciso ou não tomar ações para trata-los. Neste processo serão apurados os eventos que podem causar impactos negativos à organização e deve-se especificar como, onde e por que podem acontecer. No seu final, a organização terá uma lista dos cenários de incidentes com suas consequências associadas aos ativos e processos de negócio, que deverá ser divulgada para gestores e coordenadores de departamentos da organização com o objetivo de conscientizá-los sobre os riscos em potencial. Sugere-se usar a identificação de riscos da ISO/IEC 27005/2011, item 8.2 da norma, de acordo com ABNT (2011). Mas a organização pode adotar outra, desde que a metodologia seja reconhecida.

2.4.3.2 Os Níveis 2 e 3 – Requisitos Básicos

O objetivo principal dos Níveis 2 e 3 é solidificar a cultura da SI iniciada no Nível 1, com o cumprimento de requisitos básicos da norma ISO/IEC 27002/2011. A construção dos Níveis 2 e 3 foi inspirada nos trabalhos e experiências de Da Silva Neto *et al*. (2015) e Da Silva e Brancher (2016), que propuseram *frameworks* simplificados para PMEs. Além dos requisitos citados, a análise de riscos iniciada no Nível 1 deverá ser concluída no Nível 2.

Para se definir os objetivos de cada nível, foram classificadas as experiências de Da Silva Neto *et al*. (2015) e Da Silva e Brancher (2016) de acordo com a norma ISO/IEC 27002/2011, depois foram analisadas criticamente frente aos aspectos que se quer fomentar e frente aos aspectos cujo impacto se quer amenizar nas PMEs. Os resultados desta análise são mostrados na Tabela 3 e na Tabela 4, onde os requisitos do *framework* de Da Silva Neto *et al*.

(2015) estão identificados como "*Framework* Da Silva Neto" e os requisitos do *framework* de Da Silva e Brancher (2016) estão como "*Framework* Da Silva e Brancher". Os requisitos de cada modelo foram classificados em relação ao item da ISO/IEC 27002/2011 na coluna "ISO 27002", conforme (ABNT 2013). Para manter a simplicidade, os requisitos de maior complexidade, em sua maioria ficaram como "não obrigatórios". E, em ambos níveis, exige-se um número mínimo de requisitos maior que o número de obrigatórios, assim a organização pode escolher o que é mais importante implementar durante cada nivelação do *framework*.

Tabela 3 – Requisitos classificados para o Nível 2

***Framework* Da Silva Neto**	***Framework* Da Silva e Brancher**	**ISO 27002**	**Obrig.?**
Alinhamento da segurança da informação ao negócio.		5.1	Sim
Política de segurança da informação.		5.1.1	Sim
Conscientização, educação e treinamento em segurança da informação.		7.2.2	Não
Os responsáveis de segurança receberam treinamento especializado?			
Inventário dos ativos.		8.1.1	Sim
Existe um inventário básico de ativos (hardware e software)?			
Proprietário dos ativos.		8.1.2	Não
Cada ativo tem seu proprietário identificado?			
Há uma política de classificação da informação?		8.2.1	Não
Existem procedimentos de classificação da informação?		8.2.1	Não
Registros de usuários.		9.2.1	Sim
Cada usuário tem um identificador exclusivo?			
Gerenciamento de privilégios.		9.4.1	Não
São definidas permissões em função dos papéis e responsabilidades?			
Perímetro de segurança física.		11.1.1	Não
Existe um perímetro físico de segurança definido?			
Existem equipamentos para alimentação ininterrupta?		11.2.2	Não
Os equipamentos dos usuários são atualizados periodicamente?		11.2.4	Sim
Os servidores são atualizados periodicamente?		11.2.4	Sim
Existem mecanismos de proteção contra malwares?		12.2.1	Sim
Cópias de segurança das informações.		12.3.1	Não
Existem procedimentos de backup e recuperação de dados?			
Um plano de backups é definido e executado?		12.3.1	Sim
As cópias de segurança são etiquetadas e armazenadas em lugares seguros (fora da organização se necessário)?		12.3.1	Não
Os backups são testados periodicamente para verificar sua correta geração e recuperação?		12.3.1	Não
Controles da rede são configurados e implementados?		13.1.1	Sim
Continuidade do negócio e análise/avaliação dos riscos.		17.1.2	Sim
A empresa conhece a legislação que se aplica na sua região e dos parceiros, clientes, fornecedores, etc?		18.1.1	Não
A empresa verifica os direitos de propriedade intelectual (cópias ilegais, etc.)?		18.1.2	Não
A organização cumpre com os requisitos da LOPD (Lei de Proteção de Dados Pessoais)?		18.1.4	Não
Controles de segurança dos SI verificados periodicamente na empresa para garantir o cumprimento das normas vigentes?		18.2.3	Não

Fonte: o autor.

Tabela 4 – Requisitos classificados para o Nível 3

Framework Da Silva Neto	*Framework* Da Silva e Brancher	ISO 27002	Obrig.?
Existem papéis e responsabilidades definidas para a gestão da segurança?		6.1.1	Sim
Foi identificado na empresa um responsável pela gestão da segurança?		6.1.1	Sim
Os funcionários assinam acordos de confidencialidade?		7.1.2	Sim
Uso aceitável dos ativos.		8.1.3	Não
Existem mecanismos para a eliminação segura da informação?		8.3.2	Não
Políticas de controle de acesso.		9.2.2	Sim
Análise crítica dos direitos de acesso dos usuários.		9.2.5	Não
Controles de entrada física.		11.1.2	Não
Acesso do público, áreas de entrega e de carregamento.		11.1.6	Não
Instalação e proteção dos equipamentos.		11.2.1	Não
Documentação dos procedimentos de operação.		12.1.1	Sim
Gestão de mudanças.		12.1.2	Não
Gestão da capacidade.		12.1.3	Não
São assinados acordos de confidencialidade com clientes e fornecedores?		15.1.1	Sim
Incluindo segurança da informação no processo de continuidade do negócio.		17.1.1	Sim
Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.		17.1.2	Não

Fonte: o autor.

Os níveis 2 e 3 foram estruturados a partir dos requisitos exibidos nas Tabelas 3 e 4. O Nível 2 terá 24 requisitos sendo que devem ser implementados no mínimo 18, dos quais 10 são obrigatórios. Por sua vez, o Nível 3 terá 16 requisitos, onde devem ser implementados no mínimo 12, sendo sete obrigatórios. Além disso, no Nível 3, os requisitos do Nível 2 devem ser todos implementados. Já os níveis 4 e 5 não serão implementados neste trabalho, pois exigiriam um cronograma maior que o disponível. Além disso, não seria produtivo evoluir tanto na construção dos níveis antes de realizar-se um teste prático de eficiência do que foi criado até o momento. O teste também será proposto como trabalho futuro.

3 CONCLUSÃO

As Pequenas e Médias Empresas, em sua maioria, não possuem estrutura e conhecimento suficiente ou disponível para investir na implantação e manutenção de sistemas de governança ou GSI. Na maioria dos casos, as PMEs precisam que suas equipes e estruturas enxutas estejam focadas no negócio da empresa. Este cenário, como já foi citado, não é percebido apenas no Brasil, mas também em Singapura, Portugal e Austrália e é, na verdade, uma cena mundial.

No Brasil, as PMEs representam grande parte dos negócios, somando mais de um terço do PIB nacional e são as maiores empregadoras, com mais da metade dos postos de

trabalho. Já, no ramo do comércio, representam mais de 90 % das empresas existentes. O papel das PMEs na economia nacional é, sem dúvidas, muito importante tanto pelos valores que movimenta quanto pela sua função social. Além disso, percebe-se seu potencial de investimentos e preocupação crescente com a tecnologia, mesmo assim, encontram grandes dificuldades quando buscam soluções que não foram pensadas para infraestruturas limitadas.

No questionário aplicado às PMEs do ramo atacadista da região de Caxias do Sul pôde-se perceber pontos positivos como a estruturação dos seus setores de SI, a existência de preocupação com segurança dos dados, mesmo que não devidamente planejada, e a existência de políticas de SI, mesmo que informais. Estas constatações são indicadores de que existe um caminho de SI sendo trilhado pelas PMEs que representam o mercado estudado. Apesar disso, este caminho precisa de melhorias para leva-las ainda mais longe, pois são poucas que pretendem formalizar um SGSI e formalização é muito importante para que um sistema funcione verdadeiramente.

Através dos resultados do questionário e das pesquisas bibliográficas foi possível identificar as maiores dificuldades, que foram a falta de conhecimento sobre os benefícios que a normatização pode trazer para a empresa, a falta de conhecimento dos riscos aos quais estão expostas, a falta de pessoal disponível ou com conhecimento de SI, a falta de colaboração ou visão estratégica dos gestores da empresa e a complexidade dos *frameworks* de SI conhecidos. Torna-se notório que a melhoria necessária deve ser alcançada com medidas facilitadoras para implantação de um *framework* de GSI, que simplifiquem os processos nas PMEs com disseminação do conhecimento aos gestores e funcionários, para que alcancem a consciência necessária em busca de uma cultura da SI. O apoio da gestão, administração ou alta direção são fundamentais para a implantação de qualquer projeto.

Descortina-se a necessidade de ir além da dimensão tecnológica. As PMEs, por falta de conhecimento ou suporte adequado, normalmente investem nos recursos tecnológicos mais comuns, como *firewalls*, antivírus e ferramentas de *backup*, que são muito importantes, mas deixam de lado as dimensões organizacional e humana. Cria-se uma lacuna onde ficam perdidos o planejamento, as análises críticas, o treinamento e a conscientização e, desta forma, cria-se um cenário atrativo aos *cyber* criminosos. Também é importante ressaltar que a falta de conhecimento, os recursos reduzidos e a falta conscientização dos gestores das PMEs com segurança da informação foram fatores comuns a vários autores pesquisados.

Ao observar-se as dificuldades expostas e com a intenção de mitiga-las, questionou-se a possibilidade de propor um *framework* de Gestão de Segurança da Informação aderente aos processos organizacionais de empresas de pequeno e médio porte do

ramo de comércio atacadista. Assim, através das dificuldades observadas e tendo como inspiração modelos e estudos de outros autores, pode-se elaborar um modelo de GSI para PMEs atacadistas, que trabalha em níveis de conformidade, permitindo a empresa subir gradativamente do nível mais fácil até o mais complexo. O modelo propõe um primeiro nível totalmente focado ao aprendizado da organização, para desenvolver a cultura de Segurança da Informação, envolvendo seus funcionários e gestores com conhecimento sem cobrança de requisitos. Também foi possível propor mais níveis básicos que fossem menos complexos, sem deixar de implantar os controles necessários, mesmo que gradativamente. Além disso, a proposta de nivelação em camadas teve o intuito de flexibilizar o *framework* com uma implantação menos impactante.

Obteve-se finalmente um *framework* com grande embasamento teórico e fundamentado em dados de pesquisa, questionário e comparativos que teoricamente é aderente às necessidades das PMEs atacadistas da Região de Caxias do Sul. Pois, apesar destas PMEs possuírem infraestrutura de segurança de TI aplicada, deixam de lado as dimensões organizacional e humana, possuem restrições de tempo e pessoal disponível, carecem de apoio dos seus gestores e também do desenvolvimento de uma cultura empresarial de SI. São justamente nestes fatores que o *framework* nivelador proposto atua, com ênfase nas ideias de simplicidade e flexibilidade para implantação e no desenvolvimento do conhecimento interno para geração de um ambiente com cultura empresarial de Segurança da Informação. No entanto, é necessário observar que o presente trabalho precisa da comprovação prática que não pôde ser concluída nesta fase. Abre-se, portanto oportunidade para trabalhos futuros que tenham interesse em levar adiante esta proposta e realizar a aplicação prática do *framework* desenvolvido e, além disso, a trabalhos que estendam a pesquisa realizada com PMEs do comércio atacadista para outras regiões brasileiras, para compreender se as conclusões obtidas aqui podem ser tomadas como base e generalizadas.

INFORMATION SECURITY GOVERNANCE: INFORMATION SECURITY MANAGEMENT FRAMEWORKS IN SMALL AND MEDIUM-SIZED ENTERPRISES

Abstract: The low adhesion of small and medium enterprises (SMEs) to the implementation of Information Security Management (ISM) motivated the proposal of an ISM framework adhering to the organizational processes of SMEs in the branch of wholesale commerce. The work was based on bibliographical research and questionnaire applied to companies in the region of Caxias do Sul. The main difficulties encountered were lack of knowledge of the norms and risks to which they are exposed, lack of available personnel or knowledge of

Information Security (IS), lack of collaboration of managers and complexity of known models. To mitigate these difficulties, a framework in levels was proposed, which allows its implementation in stages. The first level aims to develop the IS culture and consolidate it, then move towards the gradual achievement of regulatory requirements at the next levels. Thus, the organization gains deployment and investment flexibility.

Keywords: Security, Information, Management, Framework.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002**: Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro. 2013.

ABNT. **NBR ISO/IEC 27005**: Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro. 2011.

BARATA, André Montoia. **Governança de Dados em Organizações Brasileiras:** Uma Avaliação Comparativa entre os Benefícios Previstos na Literatura e Obtidos pelas Organizações. Dissertação (Mestrado em Ciências) - Universidade de São Paulo, São Paulo, 2015.

BEGG, Carolyn e CAIRA, Tom. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. **The Electronic Journal Information Systems Evaluation**, v. 15, art. 1, p. 3-13, 2012. Disponível em: < http://www.ejise.com/ >. Acesso em: 11 fev. 2018.

BERALDI, Larice Castanheira. ESCRIVÃO FILHO, Edmundo. Impacto da Tecnologia de Informação na Gestão de Pequenas Empresas. **Revista Ciência da Informação**, Brasília, v. 29, n. 1, p. 46-50, jan./abr. 2000.

CAMAROTTO, Márcio Roberto. **Gestão de Atacado e Varejo**. Curitiba: IESDE Brasil SA, 2009.

CASACA, Joaquim António Aurélio. **Um Modelo Integrado para a Gestão da Segurança da Informação nas Pequenas e Médias Empresas Portuguesas**. Tese (Doutorado) - Universidade Lusíada, Lisboa, 2010.

CIO. **PMEs: Investimentos em TI devem saltar para US$ 63 bi em 2020.** 2016. Disponível em: <http://cio.com.br/tecnologia/2016/09/28/pmes-investimentos-em-ti-devem-saltar-para-us-63-bi-em-2020/>. Acesso em: 30 mar. 2018.

DOJKOVSKI, Sneza. LICHTENSTEIN, Sharman e WARREN, Matthew J.. Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. In: ECIS 2007 PROCEDINGS, 120., 2007. **Anais eletrônicos...** Disponível em: <http://aisel.aisnet.org/ecis2007/120>. Acesso em: 11 fev. 2018.

GÜNTHER, Hartmut. **Como Elaborar um Questionário** (Série: Planejamento de Pesquisa nas Ciências Sociais, Nº 01). UnB, Laboratório de Psicologia Ambiental. Brasília, DF, 2003. Disponível em < http://www.psiambiental.net/pdf/01Questionario.pdf>. Acesso em: 02 mar. 2018.

GLOBO. **Pequenos negócios já empregam mais da metade dos trabalhadores no país, diz IBGE**. 2017. Disponível em < https://g1.globo.com/economia/noticia/pequenos-negocios-ja-empregam-mais-da-metade-dos-trabalhadores-no-pais-diz-ibge.ghtml>. Acesso em: 30 mar. 2018.

GUPTA, Atul e HAMMOND, Rex. Information systems security issues and decisions for small businesses: an empirical examination. **Information Management & Computer Security**, v. 13, n. 4, p. 297-310, 2005. Disponível em: <https://www.deepdyve.com/lp/emerald-publishing/information-systems-security-issues-and-decisions-for-small-businesses-2QpAwvMYH8?shortRental=true>. Acesso em: 07 fev. 2018.

ISO. **ISO Survey of certifications to management system standards - Full results**: ISO/IEC 27001 - data per country and sector 2006 to 2016. 2017. Disponível em <https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1>. Acesso em: 30 mar. 2018.

NETTO, Abner da Silva. SILVEIRA, Marco Antonio Pinheiro da. Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. **JISTEM: Journal of Information Systems and Technology Management**, São Paulo, v. 4, n. 3, p. 375-397, 2007.

O POVO. **96,3 % das empresas brasileiras são de pequeno e médio porte**. 2016. Disponível em: < https://www.opovo.com.br/noticias/economia/2016/10/96-3-das-empresas-brasileiras-sao-de-pequeno-e-medio-porte.html>. Acesso em: 30 mar. 2018.

PÚBLICO. **Nova definição europeia de PME ameaça empresas portuguesas**. 2018. Disponível em: < https://www.publico.pt/2018/01/30/economia/noticia/mudanca-europeia-do-conceito-de-pme-ameaca-milhares-de-empresas-portuguesas-1801175>. Acesso em: 01 abr. 2018.

SEBRAE. **Micro e pequenas empresas geram 27 % do PIB do Brasil**. 2014. Disponível em: < http://www.sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD>. Acesso em: 30 mar. 2018.

SEBRAE. **Critérios de Classificação de Empresas: MEI - ME – EPP**. Disponível em: <http://www.sebrae-sc.com.br/leis/default.asp?vcdtexto=4154>. Acesso em: 01 abr. 2018.

DA SILVA, Marcelo Pereira. BRANCHER, Jacques Duilio. Avaliação de Segurança da Informação Usando o Modelo ITMark. **Jounal on Advances in Theoretical and Applied Informatics**, Marília, v. 2, ed. 1, p. 7-11, 2016.

DA SILVA NETO, Gonçalo Manuel. ALENCAR, Gliner Dias. QUEIROZ, Anderson Apolonio Lira. Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In: Simpósio Brasileiro de Sistemas da Informação, 11., 2015, Goiânia. **Anais...** Goiânia: Ed. Brazilian Computer Society, 2015.

THONG, James Y. L. Resource Constraints and Information Systems Implementation in Singapoream Small Business. **Omega**, v. 29, art. 2, p. 143-156, 2001. Disponível em: <https://www.deepdyve.com/lp/elsevier/resource-constraints-and-information-systems-implementation-in-iEiMcHG0Zv?key=elsevier >. Acesso em 11 fev. 2018.