Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro

Alternative Title: Analysis of the challenges faced in establishing and maintaining an information security management system on the Brazilian scene

Rodrigo Valle Fazenda
Universidade do Vale do Rio dos Sinos - Unisinos
51-9991-3275
fazendarodrigov@gmail.com

Leonardo Lemes Fagundes
Universidade do Vale do Rio dos Sinos - Unisinos
llemes@unisinos.br

RESUMO

A adesão a norma ISO 27001 cresce em todo o mundo motivada, principalmente, pela necessidade de conformidade e como uma forma de melhoria da gestão dos ativos e dos riscos das organizações. Muitos são os desafios enfrentados para estabelecer e manter um Sistema de Gestão de Segurança da Informanção (SGSI) eficaz e que de fato agregue valor. Entretanto, no que diz respeito as organizações brasileiras os estudos sobre tais desafios são escassos. O artigo em questão identifica e analisa alguns dos desafios enfrentados para estabelecer e manter um SGSI no cenário nacional utilizando-se do método de estudo de caso múltiplo. Obstáculos como falta de apoio da direção, falta de capacitação da área de segurança da informação, influência da cultura local, falhas na análise de riscos e resistência à mudança foram sistematicamente identificados.

Palavras-chave

Segurança, Padronização e Conformidade.

ABSTRACT

The ISO 27001 adoption grows worldwide motivated primarily by the need for compliance and as a way of improving the management of assets and risks of organizations. Many are the challenges to establish and maintain a Information Security Management System (ISMS) effective and adds value. However, the Brazilian organizations studies about these challenges are scarce. This article identifies and analyzes some of the challenges faced in establishing and maintaining an ISMS on the national scene using the multiple case study method. Obstacles such as lack of management support, lack of training of information security area, influence of local culture, failures in risk analysis and resistance to change were systematically identified.

Categories and Subject Descriptors

K.6.M [Management of Computing and Information Systms]: Miscellaneous – *security*.

General Terms

Information Security Management System, Information Security Management, and Information Security.

Keywords

Security, Standard and Compliance.

1. INTRODUÇÃO

As informações desempenham papéis estratégicos fundamentais dentro das organizações, dessa forma, elas acabam sendo cobiçadas tornando-se alvo de ataques que buscam comprometer sua confidencialidade, integridade e disponibilidade. Elas precisam ser protegidas para preservar o capital das organizações. Especialistas como Solms [1] acreditam que a adesão a normas internacionais de segurança da informação é um ponto de partida essencial para proteger as informações de uma organização.

O gerenciamento da segurança da informação exige uma visão bastante abrangente e integrada de vários domínios de conhecimento, englobando aspectos de gestão de riscos, de tecnologias da informação, de processos de negócios, de recursos humanos, da segurança física e patrimonial, de auditoria, de controle interno e também de requisitos legais e jurídicos [2].

Para proteger os seus ativos de forma eficaz as organizações (independete do porte e do segmento de atuação) contam com um sistema de gestão específico, denominado Sistema de Gestão de Segurança da Informação (SGSI). Este sistema de gestão é baseado na análise de riscos, na identificação e aplicação de controles e todos os seus requisitos estão descritos na norma ISO/IEC 27001:2013 [3] e [4].

Ao longo do estabelecimento de um SGSI muitas são as barreiras encontradas pelas organizações. Essas barreiras variam de acordo com diversos aspectos, por exemplo, locais e culturais e podem comprometer a eficácia do SGSI [5], [8] e [9].

A maior parte do conhecimento disponível sobre possíveis obstáculos no estabelecimento de um SGSI em empresas brasileiras é empírico, ou seja, conhecimento do dia a dia, que se obtém pela experiência cotidiana e, portanto, incompleto e carente de objetividade, segundo a metodologia de pesquisa para trabalhos dessa natureza [16].

Frente à escassez de pesquisa científica sobre o tema e considerando a sua relevância para a gestão das organizações, este trabalho procura responder a seguinte pergunta: quais são alguns dos principais desafios, no cenário nacional, a fim de estabelecer e manter um SGSI?

Para responder a questão supracitada, o seguinte objetivo geral foi definido: identificar e analisar de forma sistemática os principais desafios encontrados por empresas brasileiras ao estabelecer e manter um Sistema de Gestão de Segurança da Informação. A

coletada de dados foi restrita a empresas inseridas nos segmentos de mercado que mais possuem certificação na norma ISO 27001. Foram ainda definidos dois objetivos específicos: desenvolver um instrumento de coleta de dados adequado ao propósito do trabalho e organizar e analisar os dados coletados a partir de procedimentos reproduzíveis.

Para atingir os objetivos propostos e, consequentemente, obter a resposta da questão de pesquisa, este artigo foi estruturado da seguinte forma: a seção 2 busca apresentar a definição e informar dados de pesquisa *survey* sobre a ISO 27001; a seção 3 relaciona os trabalhos relacionados que já foram feitos sobre este mesmo tema; a seção 4 descreve a metodologia que foi aplicada nesta pesquisa e suas características; já a seção 5 apresenta a análise dos resultados obtidos durante a coleta de dados. Por fim, na seção 6 encontra-se a conclusão da pesquisa e os trabalhos futuros que poderão ser iniciados com base nos resultados deste trabalho.

2. FUNDAMENTAÇÃO TEÓRICA

Em novembro de 2005 foi publicada a ISO/IEC 27001 que tem como objetivo especificar os requisitos para estabelecer, operar, monitorar, revisar, manter e melhorar um SGSI dentro do contexto geral da organização e riscos ao negócio [15].

Esta norma é o padrão normativo para certificação de um SGSI. É a única norma certificadora de gestão de segurança da informação, e pode ser utilizada por empresas de qualquer segmento, independente do tipo ou tamanho [15].

A ISO 27001 está para a segurança da informação como a ISO 9001 está para a qualidade. Ela é escrita pelos melhores especialistas de todo o mundo em segurança da informação. Sua finalidade é fornecer uma metodologia para estabelecer a segurança da informação em uma organização. Ela também permite que uma organização obtenha a certificação, o que significa que um organismo de certificação independente comprova que a segurança da informação está sendo estabelecida da melhor maneira possível na organização [4].

A ISO 27001 tem relação direta com outras normas de gestão como, por exemplo, a ISO 9001 (Gestão de Qualidade) e a ISO 14001 (Meio Ambiente). Esta norma é projetada para permitir a uma organização alinhar ou integrar seu SGSI com requisitos de sistemas de gestão relacionados [3].

Os dados da pesquisa survey publicadas pela ISO [11], em comparação com os dados da pesquisa de 2010, revelam um crescimento global de 12% de empresas que possuem a certificação na norma ISO/IEC 27001. Fazendo-se uma breve análise da região da América do Sul, somente 185 certificados foram emitidos, fazendo com que a América do Sul seja apenas a antepenúltima região que mais certifica nesta norma, conforme informado na Figura 1.

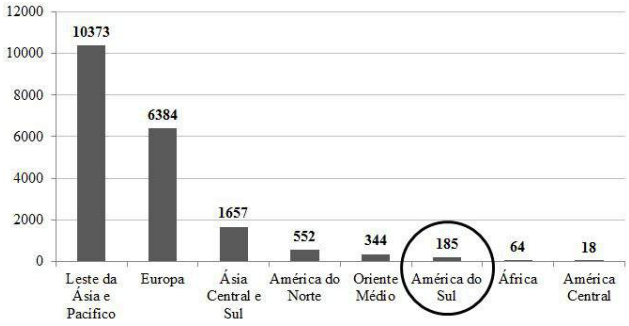

Figura 1. Total mundial de empresas certificadas.

Fazendo uma abordagem mais detalhada na América do Sul, de acordo com informações publicadas pela ISO[11], é possível perceber que o Brasil encontra-se em segundo lugar no ranking de países que mais certificam na norma ISO/IEC 27001, ficando atrás da Colômbia e à frente de Argentina e Chile, conforme representado na Figura 2. Porém, este não é um resultado a ser comemorado, uma vez que o Brasil certificou somente 3 (três) empresas entre 2011 e 2012, enquanto a Colômbia certificou 31 (trinta e uma) organizações, a Argentina 9 (nove) e o Chile 5 (cinco) neste mesmo período, ou seja, o Brasil com uma dimensão geográfica e número de empresas exponencialmente maiores que os países citados, teve um crescimento muito tímido no cenário da América Latina. Estes resultados e o escasso número de estudos mais abrangentes para a região do Brasil sobre os principais desafios que levam a uma baixa taxa de adesão à ISO/IEC 27001, além de motivar, justificam a realização desta presente pesquisa.

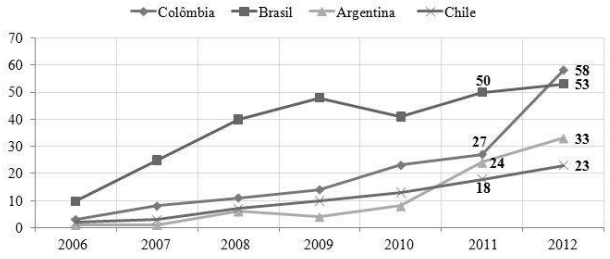

Figura 2. *Top Five* anual do número de empresas certificadas.

3. TRABALHOS RELACIONADOS

Os principais trabalhos identificados durante a etapa de revisão bibliográfica estão listados na Tabela 1 juntamente com o respectivo escopo e as dificuldades identificadas pelos autores.

Tabela 1. Trabalhos relacionados

Autor	Escopo	Dificuldades Identificadas
Martins e Santos [5]	Estudo de caso único	Falta de conhecimento na área de segurança da informação, falta de *budget*, falta de interesse da direção.
Al-Awadi e Renaud [6]	Organizações governamentais em Omã.	Falta de treinamento dos colaboradores, falta de entendimento dos valores de segurança por parte de TI, problemas de *budget*.
Waluyan et al. [7]	Empresas multinacionais no Brasil	Diferenças culturais entre os colaboradores, dificuldade em gerenciar informações

		confidenciais, baixa flexibilidade da norma ISO 27001.
Abusaad et al. [8]	Organizações da Arábia Saudita	Dificuldade em identificar corretamento os ativos das empresas, falta de experiência das equipes para implementação dos requisitos da norma, resistência à mudança, fraco envolvimento da direção, influência da cultura local.
Singh et al. [9]	Organizações da Índia	Falta de avaliação precisa dos ativos das empresas, baixo comprometimento da direção, resistência à mudança, falta de experiência da equipe, não entendimento da norma.

Esta etapa da pesquisa teve o objetivo de buscar trabalhos semelhantes que tivessem abrangido o mesmo escopo definido nesta pesquisa, ou seja, empresas brasileiras de diferentes áreas de atuação localizadas no Brasil. Porém, o número de trabalhos encontrados com este escopo é extremamente reduzido no nosso País, dessa forma, foi realizada uma busca por semelhantes em outros países.

Os trabalhos identificados no Brasil apresentaram escopos reduzidos [5] de estudo de caso único, dificultando a possibilidade de obter uma visão mais abrangente sobre outros tipos de empresas. Foi encontrado, também, um trabalho onde o escopo foram empresas multinacionais que possuem filiais no Brasil [7]. Este trabalho foi o que mais assemelhou-se com esta pesquisa, porém, o objetivo sempre foi buscar empresas essencialmente brasileiras, ou seja, empresas fundadas no Brasil e que a ISO 27001 ou o Sistema de Gestão de Segurança da Informação tivessem sido implementados por brasileiros para fosse possível identificar a visão dos mesmos perante aos desafios enfrentados.

Já, os trabalhos identificados em outros países [6], [8] e [9], possuem escopos interessantes, onde abrangem diversas empresas de setores diferentes. Estes trabalhos foram importantes para esta presente pesquisa pois permitiu obter uma visão abrangente sobre como os desafios impactaram na implantação do Sistema de Gestão de Segurança da Informação, e se eles também possuiriam relação com os desafios identificados no Brasil, ao final desta pesquisa.

Esta presente pesquisa, além de ser um trabalho local pioneiro pelo fato de buscar empresas de diferentes ramos de atuação no Brasil, acaba também trazendo informações adicionais que não foram especificadas nos trabalhos relacionados encontrados como, por exemplo, a categorização dos desafios em relação às etapas do ciclo PDCA aplicado ao SGSI e, também, os benefícios que a implantação trouxe para estas empresas a partir de um ano de estabelecimento deste sistema de gestão. Além disso, esta pesquisa traz o roteiro de entrevistas que pode ser facilmente adaptado para empresas de outros países com o objetivo de coletar informações para expandir o número de pesquisas semelhantes e tornar a implantação de um SGSI cada vez mais eficiente.

4. METODOLOGIA

Nesta pesquisa, um estudo de caso múltiplo foi desenvolvido para analisar o estabelecimento e manutenção do Sistema de Gestão de Segurança da Informação de organizações brasileiras de diferentes ramos de atuação. Entrevistas de abordagem qualitativa com os responsáveis por segurança da informação foram realizadas nestas organizações, baseando-se em um roteiro específico previamente elaborado. Este é um estudo exploratório, pois possibilita desenvolver hipóteses sobre o tema que está sendo estudado. Ao final da pesquisa, hipóteses foram levantadas sobre os possíveis desafios identificados e analisados sobre as empresas selecionadas [10].

A amostragem das empresas foi classificada como não probabilística, ela não utiliza seleção aleatória, confia no julgamento pessoal do pesquisador. Utilizou-se a técnica de amostragem por conveniência devido às limitações de buscar uma relação de todas as empresas brasileiras certificadas na ISO 27001, ou que possuam um Sistema de Gestão de Segurança da Informação estabelecido. Esta técnica mostra-se adequada a este tipo de pesquisa, uma vez que a seleção das unidades amostrais é deixada a cargo do entrevistador [10]. A Tabela 2 apresenta os perfis das empresas selecionadas para as entrevistas.

Tabela 2. Perfis das empresas selecionadas

Ramo	Colaboradores	Tempo de Mercado	SGSI / Período
e-commerce	1000	14 anos	Estabelecido há 4 anos
Indústria	780	12 anos	Estabelecido há 7 anos
TI	174	10 anos	Estabelecido há 2 anos
Financeiro	160	7 anos	Estabelecido há 4 anos
TI	80	20 anos	Estabelecido há 3 anos
Segurança da Informação	60	12 anos	Certificado há 3 anos

Foram selecionadas empresas brasileiras sabidamente certificadas na norma ISO 27001 ou que já possuem o Sistema de Gestão de Segurança da Informação estabelecido. Para que uma empresa estabeleça este sistema de gestão, ela precisará definir um escopo, ou seja, sobre quais os processos da empresa que o Sistema de Gestão de Segurança da Informação será implementado. A empresa de Tecnologia de Informação com 80 colaboradores possui como escopo Data Center e os escopos das demais empresas são todos os processos de negócio, de acordo com suas respectivas áreas de atuação.

Para assegurar a relevância das empresas selecionadas como representação do cenário nacional, os ramos de atuação fazem parte do *Top Five* mundial de seguimentos que mais possuem certificação na norma ISO 27001 e também do *Top Three* de ramos de atuação de empresas brasileiras que mais possuem certificação nesta norma, segundo levantamento realizado pela *International Organization for Standardization* em 2013 [11]. Estes dados publicados pela ISO em 2013 não representam o número total de empresas certificadas a nível nacional ou

mundial, pois não existe uma base única que mantenha estes dados atualizados.

4.1 Coleta dos dados

As entrevistas presenciais e remotas foram realizadas utilizando um roteiro de entrevistas como base. A ideia do roteiro foi questionar os entrevistados sobre o ambiente organizacional e sua relação com o Sistema de Gestão de Segurança da Informação.

4.1.2 Características do roteiro

Para estruturar o roteiro, as questões abrangem todas as etapas do ciclo PDCA aplicado à norma ISO 27001 (Figura 3). Cada questão possui objetivos para avaliar se a organização está seguindo o PDCA que a norma exige, identificando os principais problemas e desafios enfrentados para estabelecer e manter o Sistema de Gestão de Segurança da Informação. As perguntas foram divididas em duas categorias: estabelecer e manter, uma vez que o ciclo PDCA da norma visa estabelecer e manter um SGSI, de um modo geral.

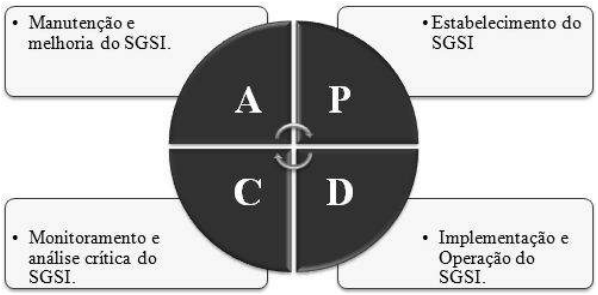

Figura 3. Ciclo PDCA aplicado ao Sistema de Gestão de Segurança da Informação.

O PDCA é um modelo que busca tornar os processos da gestão de uma empresa mais ágeis, claros e objetivos. O roteiro de entrevistas foi estruturado com 13 questões que são correlacionadas, com o objetivo de identificar inconsistências nas respostas coletadas dos entrevistados. Além disso, o roteiro possui outras características que foram utilizadas para sua estruturação, conforme representadas na Tabela 3:

Tabela 3. Estruturação do roteiro de entrevistas

Característica	Descrição	Referência
Abordagem	Tipo funil: perguntas genéricas progredindo para específicas	[10]
Estrutura	Perguntas abertas. Objetivo de buscar detalhes das respostas dos entrevistados, devido a complexidade do tema.	[12]
Enunciado	Utilizadas palavras comuns conhecidas por quem atua na área. Ausência de palavras ambíguas, com alternativas ou suposições implícitas, generalizações e estimativas.	[10]
Objetivos	Cada questão possui um objetivo que descreve o que de fato está sendo buscado como resposta no enunciado das perguntas.	[10]

Depois de estruturado, o roteiro foi previamente avaliado e aprovado por especialistas em segurança da informação que possuem o seguinte currículo, conforme apresentado na tabela 4:

Tabela 4. Perfis dos especialistas

Especialistas	Experiência	Certificações
Especialista 1	Auditor líder *British Standard Institute* (BSI), mais de 5 anos auditando SGSI.	ISO 27001 Lead Auditor; ISO 2000 Lead Auditor; ISO 9001 Lead Auditor; TL 9000 Lead Auditor.
Especialista 2	CEO e Diretor em uma empresa de Segurança da Informação; Mais 15 anos atuando em segurança da informação com empresas de diferentes ramos de atuação.	ISO 27001 Lead Auditor; CISM (Certified Information Security Manager) pela ISACA; CRISC (Certified in Risk and Information Systems Control) pela ISACA.

As perguntas do roteiro de entrevistas foram elaboradas baseando-se nas características supracitadas nesta seção. As perguntas que compõem o roteiro de entrevistas estão listadas na Tabela 5.

Tabela 5. Perguntas do roteiro de entrevistas

Enunciado	Objetivo
1. O que levou a empresa estabelecer o SGSI e de quem partiu a iniciativa?	• Identificar, ao menos, 3 motivos que levaram a estabelecer o SGSI na empresa; • Identificar as partes interessadas *(stakeholders).*
2. De que forma você percebe que o SGSI está contribuindo para o negócio da empresa?	• Identificar evidências da contribuição do SGSI para a empresa; (ao menos 3) • Verificar o que, de fato, o SGSI está trazendo de benefícios para a organização; • Motivar o entrevistado a citar os benefícios trazidos pelo estabelecimento do SGSI.
3. Você considera a gestão de riscos da empresa suficientemente consistente para alinhamento do SGSI? Comente.	• Verificar se a gestão de riscos foi planejada e elaborada de forma concisa; • Identificar o quanto a direção e demais áreas participaram da elaboração da gestão de riscos; • Buscar informações breves sobre a metodologia utilizada.
4. Na sua opinião, os treinamentos de conscientização atingem aos objetivos propostos? Como é feita a avaliação de eficácia	• Fazer uma identificação inicial sobre a cultura de segurança da informação na empresa; • Identificar os principais tópicos abordados no

dos treinamentos?	treinamento; • Identificar possíveis falhas de conteúdo do treinamento e se existe avaliação de eficácia do mesmo. • Citar exemplos de que os treinamentos de conscientização estão surtindo efeito ou não; • Identificar o resultado dos treinamentos está relacionado com os benefícios trazidos pelo SGSI. (questão 2)
5. Na sua visão, quais foram as principais dificuldades enfrentadas no estabelecimento do SGSI na empresa?	• Citar as principais dificuldades que foram enfrentadas na fase de estabelecimento do SGSI na empresa; • Apontar a dificuldade mais importante, na sua visão, enfrentada pela empresa.
6. O que você acha que poderia ter sido feito para evitar ou reduzir estas dificuldades mencionadas?	• Identificar ações que pudessem ser utilizadas para evitar ou reduzir as dificuldades citadas na questão anterior; • Identificar outros problemas não citados na questão 5.
7. Como você vê o alinhamento da política de segurança da informação em relação à gestão de riscos?	• Verificar se a política de segurança da informação está alinhada com a gestão de risco para, dessa forma, verificar se a resposta da questão 3 está coerente.
8. Na sua opinião, os colaboradores estão imbuídos na cultura de segurança? Por quê?	• Identificar se há incoerência na resposta da questão 4; • Buscar exemplos de como os colaboradores exercem a prática de segurança da informação; • Verificar se os colaboradores exercem seus papéis abrindo incidentes de segurança; • Identificar se os treinamentos de conscientização estão fomentando a segurança da informação.
9. O processo de gestão de incidentes da empresa é eficaz? Por quê?	• Identificar os fatores que levam a eficácia ou não do processo de gestão de incidentes. • Identificar possíveis contradições na resposta da questão 8 em relação a abertura de incidentes.
10. Como a direção está comprometida em exercer a segurança da informação?	• Identificar o papel da direção no SGSI; • Verificar se as análises críticas periódicas estão sendo feitas regularmente; • Verificar se existe inconsistência com a resposta da questão 8, uma vez que o corpo diretivo também são usuários que estão cobertos pelo SGSI.
11. Existe medição de eficácia dos controles de segurança aplicados ao escopo do SGSI? Cite exemplos.	• Identificar se controles estão sendo medidos; • Verificar se a resposta da questão 12 está coerente, pois as ações que devem ser tomadas para melhorar o cenário atual do SGSI devem ter sido baseadas na medição de eficácia de controles de segurança.
12. Quais são as principais ações que devem ser tomadas para melhorar o cenário atual do SGSI na empresa?	• Obter exemplos do entrevistado de ações que devem ser aplicadas para melhorar a situação atual do SGSI da empresa; • Verificar se as ações citadas contradizem respostas obtidas nas questões anteriores como um todo.
13. Partindo do ponto de vista da situação atual, como você vê o futuro do SGSI na organização daqui a cinco anos?	• Buscar visão em longo prazo da situação do SGSI na empresa; • Identificar o nível de motivação do gestor de segurança da informação perante a situação atual do SGSI, se o mesmo irá demonstrar uma visão otimista ou não; • Identificar o nível de comprometimento do gestor de segurança em relação ao SGSI.

4.2 Análise dos dados

A técnica de Análise de Conteúdo foi utilizada para a análise de dados desta pesquisa. Esta técnica mostra-se mais adequada para descrição e interpretação de conteúdos de qualquer classe de documentos. Esta técnica permite uma melhor compreensão dos significados dos textos [14].

A técnica de Análise de Conteúdo dos dados foi dividida em cinco etapas, baseando-se nas sugestões literárias [13]: preparação, unitarização, categorização, descrição e, por fim, interpretação, conforme representado na figura 2.

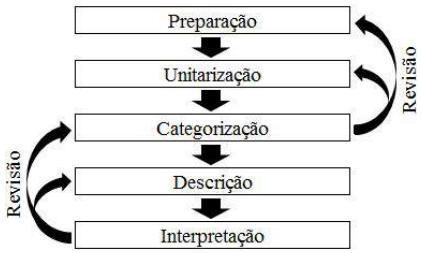

Figura 2. Fluxo da técnica de Análise de Conteúdo.

Na etapa de preparação, foi feita a leitura dos dados coletados e definido quais deles estão de acordo com os objetivos da pesquisa. Nesta fase, o processo de codificação dos dados é

iniciado. Os códigos são utilizados para identificar de forma rápida cada elemento da amostragem de dados.

Na etapa de unitarização, os dados são novamente verificados de forma cuidadosa, com o objetivo de definir a "unidade de registro". Esta unidade é o elemento a ser submetido à categorização. Toda categorização necessita deste elemento para ser classificado. Nesta pesquisa, foram utilizados os temas como a natureza das unidades de registros. Nesta fase, a revisão constante do material é de suma importância para que dados não sejam perdidos, uma vez que os dados são reescritos de forma reduzida e seus conteúdos devem permanecer vinculados aos objetivos da pesquisa.

Na etapa de categorização, os dados foram agrupados considerando partes comuns entre eles. Os dados foram classificados por semelhança, de acordo com os assuntos discutidos identificados pelas unidades de registro. Esta etapa exige que os materiais da fase de unitarização e preparação sejam constantemente revisitados, uma vez que os dados possuem diversos sentidos e podem ser interpretados de formas diferentes. Para que fosse possível obter categorias consistentes, as mesmas obedeceram a critérios de exaustividade, homogeneidade e de exclusão mútua.

A quarta etapa refere-se à descrição, onde o resultado do trabalho alavancado nas etapas anteriores são comunicados na pesquisa. Porém, a descrição é somente o primeiro momento desta comunicação, uma vez que ainda é necessário que os dados sejam interpretados. A descrição consta na seção 5 deste artigo, onde, para cada uma das categorias elaboradas a partir da análise de dados, foi produzido um texto síntese para expressar os significados das diferentes unidades de registros incluídas em cada uma delas.

Para que uma análise de conteúdo seja completa, é necessária a etapa de interpretação. O objetivo desta etapa foi compreender de forma mais aprofundada o conteúdo dos dados gerados. A interpretação dos dados está descrita de forma detalhada na seção 5 desta pesquisa, onde, com base na descrição dos resultados, a teoria foi constituída para responder a questão de pesquisa deste artigo.

5. RESULTADOS OBTIDOS

As hipóteses identificadas resultantes da técnica de análise de foram: Falta de apoio da alta direção, Falta de capacitação da equipe de Segurança da Informação, Influência da cultura local, Falhas na elaboração da Análise de Risco e Resistência à mudança.

5.1 Falta de apoio da alta direção

Fatores que caracterizam esta falta de comprometimento foram identificados nas respostas coletadas como: não provimento de recursos para realização de programas que visam expandir a cultura de segurança da informação dentro das organizações, pouco envolvimento nas ações de segurança da informação com o intuito de demonstrar aos colaboradores que a segurança da informação é uma preocupação oriunda do negócio da organização, falta de análises críticas do sistema de gestão para assegurar a melhoria contínua nos processos e alinhamento dos objetivos da empresa para, não somente permanecer em conformidade com a norma ISO 27001, mas também garantir que todos os processos estejam alinhados e com os mesmos objetivos dentro da organização.

A partir deste desafio, outros poderão ser reduzidos consideravelmente. Um exemplo disso é o provimento de recursos para capacitação das equipes de Segurança da Informação. Uma direção fortemente comprometida com a segurança dispõe de recursos para que sua equipe esteja sempre capacitada a orientar seus colaboradores e utilizar-se das melhores práticas no mercado, incluindo a aplicação dos controles da norma ISO 27001 de forma mais consistente e de acordo com a realidade da organização.

5.2 Falta de capacitação da equipe de segurança da informação

Alguns entrevistados demonstraram sólidos conhecimentos da área de segurança da informação de suas empresas, porém, determinados problemas estavam sendo causados pela própria área de segurança da informação, não por má fé da equipe, mas puramente pela falta de capacitação e experiência.

Exemplos disso são a não necessidade de medição de determinados controles de segurança da informação e orientações específicas para especialistas de Tecnologia da Informação. Dentre as respostas coletadas, houve casos em que a área de segurança da informação sequer sabia responder o que de benefício para a organização o Sistema de Gestão de Segurança da Informação trouxera.

Além disso, existem áreas de segurança da informação que não possuem um entendimento completo da norma ISO 27001. Elas possuem uma visão deturpada do que é de fato um Sistema de Gestão de Segurança da Informação estabelecido. Um exemplo é a aplicação somente dos controles de segurança da informação no ambiente da empresa, sendo que, para que este sistema de gestão seja adequadamente estabelecido deve ter as etapas correspondentes ao ciclo do PDCA implantadas, executadas, medidas e melhoradas.

Entrevistados apontaram, também, que a mão-de-obra não capacitada estava impactando no processo do sistema de gestão como um todo, de tal forma que os incidentes de segurança da informação não estavam sendo solucionados devido a este despreparo.

5.3 Influência da cultura local

É de senso comum que a cultura local do Brasil referente à segurança da informação precisa evoluir. Segundo informações obtidas dos entrevistados, grande parte dos usuários ainda tem a ideia de que segurança da informação é somente "proteger o computador" e, dessa forma, acabam não valorizando as informações confidenciais que são trocadas por outros meios como, por exemplo, informações faladas em locais inadequados, materiais com informações confidenciais descartados de forma incorreta.

Colaboradores atribuindo acessos confidenciais sem um estudo prévio do que realmente é necessário atribuir de acessos, compartilhamento de senhas pessoais em situações de ausência de colaboradores ou para divisão de atividades, falta de apoio dos gestores das áreas de negócio na expansão da cultura de segurança para seus subordinados, excesso de confiança nos colegas de trabalho fazendo com que informações confidenciais sejam expostas em locais indevidos. Ou seja, a cultura de que as

situações devem ser tratadas e resolvidas de forma rápida, fazendo com que a segurança fique em segundo plano.

Um fato interessante observado nas respostas dos entrevistados aponta para a falta de interesse dos colaboradores em abrir incidentes de segurança da informação. Alguns entrevistados acabaram relatando que muitos colaboradores ainda têm o pensamento de que a abertura de incidentes é somente tarefa da área de Segurança da Informação.

5.4 Falhas na elaboração da análise de risco

Uma análise de riscos mal feita é um dano estrutural no Sistema de Gestão de Segurança da Informação, pois é a base do processo como um todo. É da análise de riscos que os ativos do escopo deste sistema de gestão são identificados e, a partir destes ativos, as políticas de segurança da informação e toda uma cadeia de processos serão elaboradas.

Segundo os dados coletados nas entrevistas, a ineficiência em identificar os ativos das organizações para definição dos escopos que serão abrangidos pelo Sistema de Gestão de Segurança da Informação acaba fazendo com que a análise de risco não cubra todas as arestas necessárias. Além disso, os fatores motivadores para estabelecimento deste sistema de gestão também acabam impactando a elaboração da análise de riscos.

Alguns entrevistados relataram que a análise de riscos já estava definida de acordo com outros padrões de segurança mais técnicos, diferentes da norma ISO 27001, e que a partir desta análise de riscos, o Sistema de Gestão de Segurança da Informação foi estabelecido. Exemplo disso é uma análise de riscos feita para atender aos requisitos da norma internacional PCI-DSS (utilizado em empresas com grande volume de transações de cartão de crédito). Os requisitos para a análise de riscos desta norma, por mais que também estejam ligados fortemente à segurança da informação, não atendem a determinados requisitos da norma ISO 27001 e, mesmo assim, foram utilizados como base para estabelecer o Sistema de Gestão de Segurança da Informação.

5.5 Resistência à mudança

O fato de grande parte dos colaboradores ainda terem o pensamento de que segurança da informação é responsabilidade somente de uma área específica, acaba fazendo com que os mesmos resistam a seguir as políticas de segurança da informação e as boas práticas divulgadas pela empresa.

Boa parte das atividades e controles gerados pelas políticas de segurança da informação, por exemplo, são vistos como um "atraso" nos processos de negócio, segundo relatos dos entrevistados. Muitas dessas ideias deturpadas em relação à segurança da informação são fomentadas pelo não conhecimento ou não valorização que as informações exercem sobre o negócio como um todo.

Implantação de novas tecnologias, a inclusão de mais controles de segurança, em geral tudo que gera mais esforço por parte dos colaboradores acaba sendo encarado como atividade burocrática, sem resultados mensuráveis. Cabe aí, portanto, reiniciando o ciclo dos desafios identificados nesta pesquisa, um maior apoio da direção para proporcionar subsídios humanos e técnicos para demonstrar no que, de fato, esses "esforços extras" dos colaboradores estão contribuindo para o ambiente organizacional da empresa para assim, quem sabe, a resistência à mudança acabe dando lugar à conscientização à segurança da informação.

5.6 Outras considerações

Durante a fase de análise de dados, foi possível identificar outras constatações importantes que este trabalho contribuiu, como: os desafios enfrentados por cada etapa do ciclo PDCA, fatores motivadores para o estabelecimento do Sistema de Gestão de Segurança da Informação e os principais benefícios identificados pelas empresas pesquisadas.

Apesar do objetivo deste trabalho ser identificar os desafios de forma geral para estabelecimento e manutenção do Sistema de Gestão de Segurança da Informação, este trabalho também acabou contribuindo para apresentar os obstáculos relacionados a cada etapa do PDCA (Tabela 6). Com base na identificação dos desafios, após a análise, foi possível categorizá-los e indicar em quais etapas do PDCA ele corresponde.

Tabela 6. Desafios enfrentados por cada etapa do ciclo PDCA

Desafios	Etapas
Falta de apoio da alta direção	*Plan, Do, Check, Act*
Falta de capacitação da equipe de segurança da informação	*Plan, Do, Check, Act*
Influência da cultura local	*Do, Act*
Falhas na elaboração da análise de riscos	*Plan*
Resistência à mudança	*Do, Act*

Alguns dos principais fatores motivadores identificados nas respostas foram: exigência por parte da matriz, vantagem competitiva de mercado, busca por um ambiente processual padronizado e controlado, almejar um ambiente seguro culminando em uma certificação na ISO 27001 e proteção das informações confidenciais das organizações.

Além disso, foi possível identificar os principais benefícios que o estabelecimento deste sistema de gestão está trazendo para as organizações: melhorias de imagem e marketing das empresas, aumento da disponibilidade dos ambientes de infraestrutura de Tecnologia da Informação, diminuição nos custos com infraestrutura de Tecnologia da Informação, apoio importante no processo de Governança de TI, mapeamento das falhas de segurança dos ambientes organizacionais e credibilidade perante aos clientes.

Ao final desta pesquisa, também foi possível fazer uma comparação dos resultados obtidos com os desafios identificados pelos trabalhos relacionados, onde ficou evidente a semelhança dos resultados do cenário nacional com os estudos realizados na Índia, Omã e Arábia Saudita.

6. CONCLUSÃO

O presente artigo buscou responder a seguinte questão de pequisa: quais são os principais desafios, no cenário nacional, a fim de estabelecer e manter um SGSI. Esta questão foi respondida com sucesso tendo em vista as restrições do estudo realizado.

Os dados coletados nas entrevistas foram analisados chegando-se a identificação destes desafios através de cinco hipóteses

representadas por categorias. São elas: falta de apoio da alta direção, falta de capacitação da equipe de segurança da informação, influência da cultura local, falhas na elaboração da análise de risco e resistência à mudança. Cada uma destas categorias descreve a síntese dos problemas/desafios citados pelos entrevistados que são responsáveis pelos Sistema de Gestão de Segurança da Informação das organizações participantes desse estudo.

Como resultado de uma análise de dados criteriosa, foi possível obter outras constatações que não estavam entre os objetivos desta pesquisa. Além de identificar os desafios que impedem a adesão em massa de empresas brasileiras à norma ISO 27001 de forma geral, esta pesquisa contribuiu para identificar estes obstáculos através de cada etapa do ciclo PDCA, os principais fatores motivadores e os principais benefícios que estas empresas brasileiras estão obtendo com o estabelecimento do Sistema de Gestão de Segurança da Informação.

Na comparação dos resultados desta pesquisa com os trabalhos relacionados, percebe-se que os desafios identificados neste artigo assemelham-se com os desafios dos estudos realizados na Índia, Omã e Arábia Saudita. Estes dados são interessantes, pois existe uma forte diferença cultural entre o Brasil e os países mencionados e, mesmo assim, os desafios acabaram convergindo-se. Esse resultado acaba motivando a busca por soluções destes desafios, pois, além de auxiliar no processo de implementação da ISO 27001 nas empresas brasileiras, acaba abrindo a possibilidade de expandir estas sugestões de soluções para empresas em outros países.

Sendo assim, os resultados obtidos nesta pesquisa reforçam a ideia de que esse artigo possa ser utilizado como um guia para contribuir de forma preventiva, antecipando para os especialistas em Segurança da Informação, os principais desafios que poderão ser enfrentados para o estabelecimento e manutenção do Sistema de Gestão de Segurança da Informação.

6.1 Trabalhos futuros

Considerando os desafios que foram identificados e analisados nesse artigo como hipóteses em futuros trabalhos de pesquisa será possível realizar análises ainda mais aprofundadas sobre as suas causas. Uma vez que as causas estejam mapeadas, medidas preventivas poderão ser propostas e aplicadas para evitar ou minimizar o impacto no SGSI.

Ampliar o escopo do estudo apresentado nesse artigo para outros segmentos de mercado, por exemplo, financeiro ou governo permitirá não apenas o melhor entendimento dos desafios já identificados, como também a descoberta de novas situações que podem impactar, por exemplo, na eficácia do SGSI.

Por fim, com base no trabalho em questão é possível desenvolver uma pesquisa com objetivo de descrever as causas do grupo de desafios identificados e estabelecer relações entre as diversas variáveis.

7. REFERÊNCIAS

[1] Solms, R. 1999. *Information Security Systems: Why Standards are Important?* Information Management & Computer Security vol. 46, nº 8, p. 91-95.

[2] Rigon, E. e Westphall, C. 2011. *Modelo de Avaliação da Maturidade da Segurança da Informação.* Biblioteca Digital Brasileira de Computação. VII Simpósio Brasileiro de Sistemas de Informação. http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2011/modelodeavalicao.pdf

[3] ABNT NBR ISO/IEC 27001. 2013. *Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos".*

[4] Kosutic, D. 2013. *We have implemented ISO 9001, can something be used for ISO 27001 / ISO 22301 / BS 25999-2?* IS & BCA. http://support.epps.eu/customer/portal/articles/787939-we-have-implemented-iso-9001-can- something-be-used-for-iso-27001-iso-22301-bs-25999-2-

[5] Martins, A. e Santos, C. 2005. *Uma Metodologia para Implementação de um Sistema de Gestão de Segurança da Informação.* Journal of Information Systems and Technology Management, vol 2, nº 2, p. 121-136. Salvador – BA.

[6] Al-Awadi, M. e Renaud, K. 2008. *Success Factors in Information Security Implementation in Organizations.* University of Glascow.

[7] Waluyan, L., Blos, M., Nogueira, S. e Asai, T. 2010. *Potential Problems in People Management concerning Information Security in Cross-cultural Environment – The Case of Brazil*. Journal of Information Processing. Vol 18, p. 38-42, Fevereiro.

[8] Abusaad, B., Saeed, F., Alghathbar, K. e Bilal, K. 2011. *Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes and Lessons Learned.* 9th Australian Information Security Management Conference, Edith Cowan University. Dezembro.

[9] Singh, A., Sharma, S., Pandey, M., Chaurasia, S. e Vaish, A. 2012. *Implementation of ISO 27001 in Indian Scenario: Key Challenges.* International Conference on Recent Trends of Computer Technology in Academy.

[10] Malhotra, N. 2006. *Pesquisa de Marketing: Uma Orientação Aplicada.* Bookman. Porto Alegre.

[11] ISO, International Organization for Standardization. 2013. *ISO Survey 2012.* http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF, Setembro.

[12] Trivinos, A. 1990. *Introdução à Pesquisa em Ciências Sociais: A Pesquisa Qualitativa em Educação.* Atlas. São Paulo, p. 146.

[13] Siqueira, J. 2011. *A Arte das Perguntas Criativas e Desafiadoras.* http://criatividadeaplicada.com/2011/07/28/a-arte-das-perguntas-criativas-edesafiadoras, Julho.

[14] Moraes, R. 1999. *Análise de Conteúdo*. Revista Educação, Porto Alegre, vol. 22, nº 37, p. 7-32.

[15] ISO/IEC 27000. 2012. "*Information technology – Security Techniques – Information security management systems – Overview and vocabulary*".

[16] Gerhardt, T. e Silveira, D. 2009. *Métodos de Pesquisa.* ISBN 978-85-386-0071-8. Editora UFRGS.