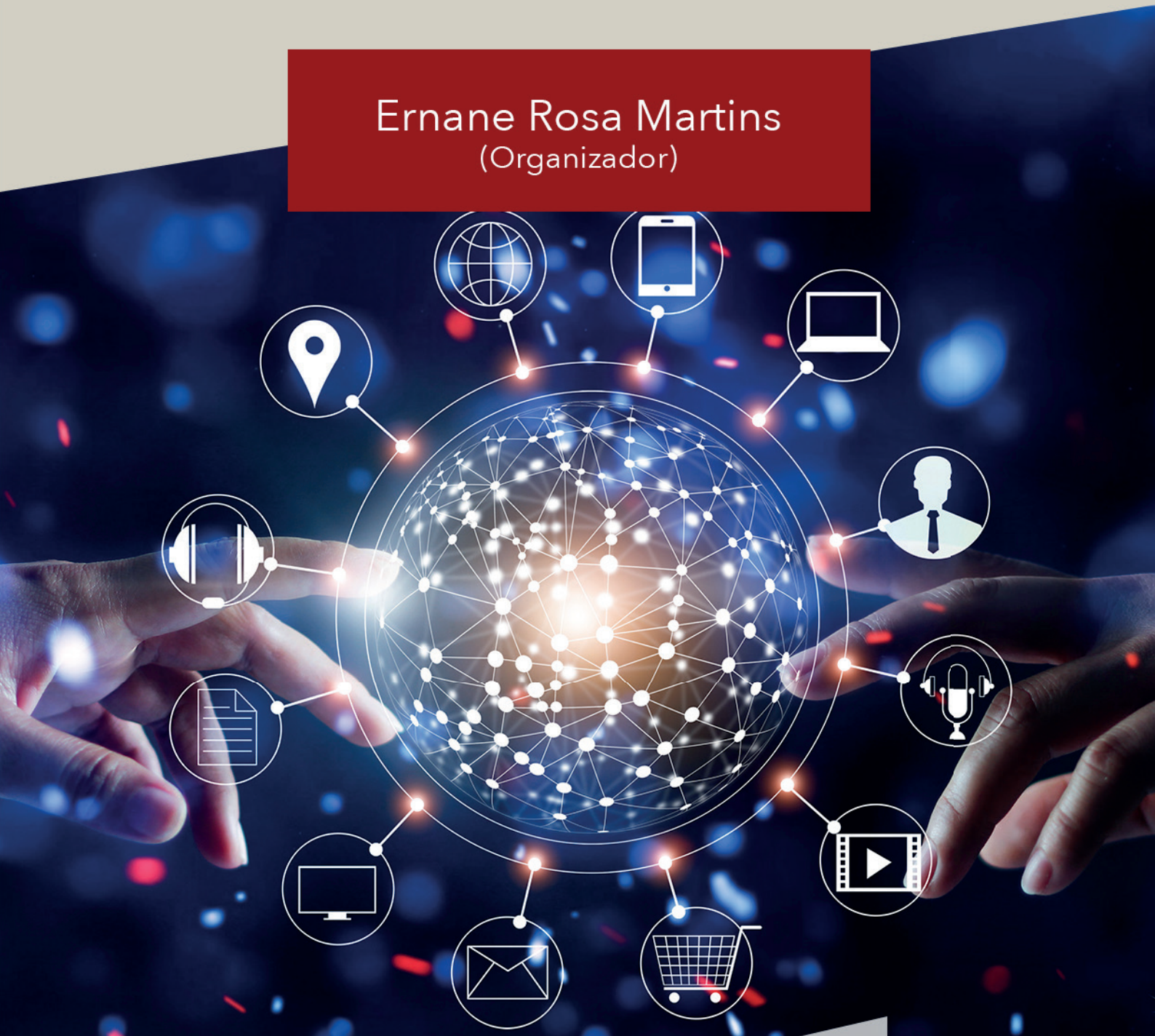
Princípios e Aplicações da Computação no Brasil 2

Ernane Rosa Martins
(Organizador)



Atena Editora
Ano 2019

Ernane Rosa Martins
(Organizador)

Princípios e Aplicações da Computação no Brasil
2

Atena Editora
2019

2019 *by Atena Editora*
Copyright © da Atena Editora
Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação e Edição de Arte: Geraldo Alves e Natália Sandrini
Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

P957 Princípios e aplicações da computação no brasil 2 [recurso eletrônico] / Organizador Ernane Rosa Martins. – Ponta Grossa (PR): Atena Editora, 2019. – (Princípios e aplicações da computação no brasil; v. 2)

Formato: PDF
Requisito de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-85-7247-048-3
DOI 10.22533/at.ed.483191601

1. Computação. 2. Informática. 3. Programação de computador. I. Martins, Ernane Rosa. II. Título. III. Série.

CDD 004

Elaborado por Maurício Amormino Júnior – CRB6/2422

APRESENTAÇÃO

O volume 2 desta obra aborda mais 16 capítulos sobre o panorama atual da computação no Brasil. Tendo como alguns dos assuntos abordados nos capítulos: ensino de raciocínio lógico, desenvolvimento de sistema computacional, micromobilidade em redes sem fio, usabilidade e acessibilidade de sistemas, qualidade da informação, tecnologias de análise de aprendizagem, redes neurais artificiais, analise de vibração, algoritmos evolucionários, sistemas inteligentes e acessibilidade móvel.

Deste modo, esta obra reúne debates e análises acerca de questões relevantes, tais como: Como está o estado da arte da análise de aprendizagem preditiva, nova proposta de um framework para previsão de desempenhos em programação e quais os caminhos para avançar nessas pesquisas? É possível realizar uma modelagem computacional, analisando os parâmetros espaciais relevantes na tomada de decisão, utilizando técnicas de redes neurais artificiais? Quais são os principais desafios, no cenário nacional, a fim de estabelecer e manter um Sistema de Gestão de Segurança da Informação? Uma proposta de um agente testador que realiza busca local no espaço de estados de casos de teste orientado por utilidade e que utiliza os algoritmos evolucionários multiobjetivos, NSGAII, SPEA2, PAES e MOCell pode identificar quais deles são mais eficientes na geração de casos de testes para agentes racionais? Como realizar uma pesquisa científica que identifique os requisitos desejáveis para desenvolver uma aplicação móvel touch screen, que vise auxiliar a alfabetização de deficientes visuais?

Nesse sentido, este material tem grande relevância por constituir-se numa coletânea de referência para pesquisas e estudos da computação, tendo como objetivo reunir trabalhos acadêmicos que permitam contribuir com análises e discussões sobre assuntos pertinentes à área. Os organizadores da Atena Editora, agradecem especialmente aos autores dos diversos capítulos apresentados, parabenizam a dedicação e esforço de cada um, os quais viabilizaram a construção dessa obra no viés da temática apresentada. Por fim, desejamos aos leitores que esta obra, seja de extrema importância para todos que vierem a utilizá-la.

Ernane Rosa Martins

SUMÁRIO

CAPÍTULO 1 1

ENSINO DE RACIOCÍNIO LÓGICO E COMPUTAÇÃO PARA CRIANÇAS: EXPERIÊNCIAS, DESAFIOS E POSSIBILIDADES (XXXVII CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO | 25O WEI - *WORKSHOP* SOBRE EDUCAÇÃO EM COMPUTAÇÃO)

Thâmillys Marques de Oliveira
Willmara Marques Monteiro
Fábio Cristiano Souza Oliveira
Danielle Juliana Silva Martins
Alessandra da Silva Luengo Latorre

DOI 10.22533/at.ed.4831916011

CAPÍTULO 2 12

DESENVOLVIMENTO DE SISTEMA COMPUTACIONAL PARA AQUISIÇÃO E ANÁLISE DE DADOS AMBIENTAIS REMOTAMENTE.

Jucivaldo Araujo Ferreira Junior
Rardiles Branches Ferreira
Rodrigo Da Silva
Julio Tota da Silva
Samuel Alves de Souza

DOI 10.22533/at.ed.4831916012

CAPÍTULO 3 19

CARACTERIZAÇÃO DA MICROMOBILIDADE EM REDES SEM FIO INFRAESTRUTURADAS PELA VARIAÇÃO DA RELAÇÃO SINAL-RUÍDO

Kerlla Souza Luz Prates
Priscila América Solís Mendez
Barreto Henrique Domingues Garcia
Mylène Christine Queiroz de Farias

DOI 10.22533/at.ed.4831916013

CAPÍTULO 4 30

AVALIAÇÃO DE USABILIDADE E ACESSIBILIDADE DO SISTEMA DE GERENCIAMENTO DE REFEITÓRIOS DO IFPI – CAMPUS FLORIANO

Samuel de Araújo Fonseca
Antonio Rodrigues de Araújo Costa
Neto Carlos Eduardo Moreira Borges
Hugo Araújo Gonçalves
Paulo Miranda e Silva Sousa
Rennê Stephany Ferreira dos Santos

DOI 10.22533/at.ed.4831916014

CAPÍTULO 5 39

AVALIAÇÃO DA APREENSIBILIDADE E DA QUALIDADE DA INFORMAÇÃO EM SAÚDE COM O SOFTWARE SPINEFIND

Carine Geltrudes Webber
Asdrubal Falavigna
Caio Rodrigues da Silva
Marco Antonio Koff
Natália Lisboa

DOI 10.22533/at.ed.4831916015

CAPÍTULO 6 54

AS TECNOLOGIAS DE ANÁLISE DE APRENDIZAGEM E OS DESAFIOS DE PREVER DESEMPENHOS DE ESTUDANTES DE PROGRAMAÇÃO

Márcia Gonçalves de Oliveira

DOI 10.22533/at.ed.4831916016

CAPÍTULO 7 67

ANÁLISE E MODELAGEM DA RELAÇÃO INTERPESSOAL EM ESPORTES COLETIVOS UTILIZANDO REDES NEURAIS ARTIFICIAIS

Tadeu Nogueira Costa de Andrade
Marcos Rodrigo Trindade Pinheiro
Menuchi Paulo Eduardo Ambrósio

DOI 10.22533/at.ed.4831916017

CAPÍTULO 8 75

ANÁLISE DOS DESAFIOS PARA ESTABELECER E MANTER SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CENÁRIO BRASILEIRO

Rodrigo Valle Fazenda
Leonardo Lemes Fagundes

DOI 10.22533/at.ed.4831916018

CAPÍTULO 9 87

ANALISE DE VIBRAÇÃO COM CONTROLE DE MEDIÇÃO UTILIZANDO O FILTROS ESTATÍSTICOS

Karla Melissa dos Santos Leandro
Iago Ferreira Lima
Werley Rafael da Silva
Marco Paulo Guimarães
Marcos Napoleão Rabelo

DOI 10.22533/at.ed.4831916019

CAPÍTULO 10 96

ANÁLISE DE REDE COLABORAÇÃO CIENTÍFICA COMO FERRAMENTA NA GESTÃO DE PROGRAMAS DE PÓS-GRADUAÇÃO

Aurelio R. Costa
Celia Ghedini Ralha

DOI 10.22533/at.ed.48319160110

CAPÍTULO 11 109

ALGORITMOS EVOLUCIONÁRIOS MULTIOBJETIVOS PARA A SELEÇÃO DE CASOS DE TESTE PARA SISTEMAS INTELIGENTES

Daniel Victor Saraiva
Francisca Raquel de Vasconcelos Silveira

DOI 10.22533/at.ed.48319160111

CAPÍTULO 12 124

ACESSIBILIDADE MÓVEL PARA ALFABETIZAÇÃO DE DEFICIENTES VISUAIS: PROPOSTA INICIAL DE UM PROTÓTIPO

Jenifer Melissa de Paula
José Valter Amaral de Freitas
Thatiane de Oliveira Rosa

DOI 10.22533/at.ed.48319160112

CAPÍTULO 13 129

AÇÃO PARA INCENTIVAR MENINAS DO ENSINO MÉDIO A CURSAR CARREIRAS TECNOLÓGICAS DA UNIVERSIDADE FEDERAL DE RIO GRANDE DO NORTE

Idalmis Milián Sardina
Cristiano Maciel
Midori Hijioka Camelo
Hortensia Sardina Miranda

DOI 10.22533/at.ed.48319160113

CAPÍTULO 14 137

A TÉCNICA OC2-RD2 COMO UMA PRÁTICA METODOLÓGICA PARA O ENSINO DE PROGRAMAÇÃO DE COMPUTADORES

Karina Buttignon
Ítalo Santiago Vega
Jonhson de Tarso Silva
Adriano Carlos Moraes Rosa

DOI 10.22533/at.ed.48319160114

CAPÍTULO 15 149

A DECADE OF SOFTWARE ENGINEERING BEST PRACTICES ADOPTION IN SMALL COMPANIES:
A QUASI-SYSTEMATIC MAPPING

Alex Juvêncio Costa
Juliana De Albuquerque Gonçalves
Saraiva Yuska Paola Costa Aguiar

DOI 10.22533/at.ed.48319160115

CAPÍTULO 16 162

INVENTORYIOT I²OT: UMA PLATAFORMA DE GERENCIAMENTO AUTOMATIZADO DE INVENTÁRIO

Jauberth Weyll Abijaude
Péricles de Lima Sobreira
Aprígio Augusto Lopes Bezerra
Fabíola Greve

DOI 10.22533/at.ed.48319160116

SOBRE O ORGANIZADOR 177

CAPÍTULO 8

ANÁLISE DOS DESAFIOS PARA ESTABELECER E MANTER SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CENÁRIO BRASILEIRO

Rodrigo Valle Fazenda
Instituto de Informática – Universidade do Vale do Rio dos Sinos (UNISINOS)
São Leopoldo – Rio Grande do Sul

Leonardo Lemes Fagundes
Instituto de Informática – Universidade do Vale do Rio dos Sinos (UNISINOS)
São Leopoldo – Rio Grande do Sul

RESUMO: O estabelecimento da norma ISO 27001 cresce entre as organizações em todo o mundo. Porém, desafios são enfrentados pelas empresas para implementar esta norma. É escassa a quantidade de estudos sobre os desafios que empresas brasileiras enfrentam para estabelecer e manter o Sistema de Gestão de Segurança da Informação. Este artigo tem como objetivo identificar e analisar os desafios enfrentados para estabelecer e manter este sistema de gestão no cenário nacional. Através do método de estudo de caso múltiplo que fatores 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 identificados como obstáculos.

ABSTRACT: The adoption of the ISO 27001 standard grows among organizations worldwide. However, many challenges are faced by companies to implement this standard. There are few studies on the challenges facing Brazilian companies to establish and maintain the Information Security Management System. This article aims to identify and analyze the challenges faced in establishing and maintaining this management system on the national scene. Through the multiple case study method that factors such as lack of management support, lack of training in the Information Security area, influence of local culture, failures in risk analysis and resistance to change were identified as obstacles.

1 | INTRODUÇÃO

As informações desempenham papéis estratégicos fundamentais dentro das organizações, dessa forma, elas acabam sendo cobiçadas tornando-se alvo de ataques que buscam infringir sua confidencialidade, integridade e disponibilidade. As informações precisam ser protegidas para ajudar a garantir o capital das organizações.

Especialistas como Solms (1999) acreditam que o estabelecimento de normas internacionais de segurança da informação é um ponto de partida essencial para melhorar a segurança da informação de uma organização.

Para garantir esta proteção de forma eficaz, existe um sistema de gestão específico que oferece uma estrutura de controles que pode ser aplicada pelas empresas de diferentes ramos de atuação, denominado Sistema de Gestão de Segurança da Informação (SGSI).

Este sistema de gestão provê um modelo internacionalmente comprovado para, segundo a ISO 27001 (2005), estabelecer, operar, monitorar e analisar criticamente ambientes organizacionais sob o aspecto de segurança da informação. Como ferramenta utilizada para aplicar controles de segurança da informação e obter o nível seguro de proteção existe a norma internacional de segurança da informação ISO 27001. É uma norma 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 [Kosutic 2013].

A ISO 27001 tem como abordagem a gestão de riscos para alcançar a segurança da informação eficaz através do uso contínuo de métodos de risco, incorporadas ao modelo de processo PDCA, para monitorar, manter e melhorar a eficácia dos controles de segurança [ISO 27001 2005].

Desafios para estabelecimento e manutenção da ISO 27001 foram identificados em âmbito global. A publicação feita pela The British Assessement Bureau (2013) cita como desafios: o medo ou constrangimento de não conseguir a certificação depois de ser auditado, os custos iniciais e de manutenção que a certificação exige e também o fato de ser mais fácil reivindicar o cumprimento da norma do que realmente demonstrar como cumpri-la.

O estudo supracitado realizado pelo The British Assement Bureau (2013) possui abrangência mundial. É escassa a quantidade de estudos no cenário nacional que abordam as dificuldades enfrentadas pelas empresas brasileiras para estabelecer e manter um Sistema de Gestão de Segurança da Informação. Com base no levantamento bibliográfico de pesquisas sobre este tema, houve forte dificuldade em buscar estudos de empresas brasileiras de ramos diferentes de atuação, foram encontrados estudos de caso único sobre implementação da norma ISO 27001. Estudos de caso múltiplos foram possíveis de localizar somente em empresas estrangeiras. Por mais que os estudos destas empresas contribuam para identificar os desafios, é importante obter uma visão holística para perceber a realidade enfrentada pelas empresas brasileiras ao estabelecer e manter um Sistema de Gestão de Segurança da Informação.

Sendo assim, este trabalho procura responder a questão de pesquisa: quais são os principais desafios , no cenário nacional, a fim de estabelecer e manter um Sistema de Gestão de Segurança da Informação?

Para responder esta questão de pesquisa, o seguinte objetivo geral foi definido: identificar e analisar os principais desafios ao estabelecer e manter um Sistema de Gestão de Segurança da Informação através de um número limitado de empresas brasileiras que representam os principais ramos de atuação que mais possuem certificação na norma ISSO 27001. Para atingir este objetivo geral, os objetivos

específicos estabelecidos foram: desenvolver um instrumento de coleta de dados adequado ao propósito do trabalho e organizar o descrever os dados coletados

Para atingir os objetivos propostos e, consequentemente, obter a resposta da questão de pesquisa, este artigo foi estruturado da seguinte forma: a seção 2 relaciona as pesquisas que já foram feitas sobre este mesmo tema; a seção 3 descreve a metodologia que foi aplicada nesta pesquisa e suas características; a seção 4 descreve os resultados obtidos interpretados da análise dos dados coletados nas entrevistas com as empresas. Por fim, na seção 5 encontra-se a conclusão da pesquisa e os trabalhos futuros que poderão ser iniciados com base nos resultados deste trabalho.

2 I TRABALHOS RELACIONADOS

Os trabalhos pesquisados sobre o tema deste artigo foram organizados conforme representa a Tabela 1.

Autor	Escopo	Dificuldades Identificadas
Singh et al. (2012)	Organizações da Índia.	Falta de avaliação precisa dos ativos das empresas; baixo comprometimento da direção; resitência à mudança; falta de experiência da equipe; não entendimento claro da norma ISO 27001.
Waluyan et al. (2010)	Multinacionais no Brasil.	Diferenças culturais entre os colaboradores; dificuldade em gerenciar informações confidenciais; baixa flexibilidade da norma ISO 27001.
Martins e Santos (2005)	Estudo de caso único de uma empresa brasileira.	Falta de conhecimento na área de segurança da informação; falta de *budget;* falta de interesse da direção.
Al-Awadi e Renaud (2008)	Organizações governamentais em Omã, na Arábia.	Falta de treinamento dos colaboradores; falta de entendimento dos valores de segurança por parte da área de TI; problemas de *budget*; falta de adaptação dos colaboradores aos requisitos da norma.
Abusaad et al. (2011)	Organizações na Arábia Saudita.	Dificuldade em identificar corretamente os ativos das organizações; falta de experiência das equipes para implementação dos requisitos da norma; resistência à mudança; fraco envolvimento da direção; influência da cultura local.

Tabela 1. Trabalhos relacionados

3 I 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. Segundo Malhotra (2006), 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.

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, segundo Malhotra (2006), a seleção das unidades amostrais é deixada a cargo do entrevistador (Tabela 2).

Ramo	Colaboradores	Tempo de Mercado	SGSI	Período
Indústria	780	12 anos	Estabelecido	07 anos
Financeiro	160	07 anos	Estabelecido	04 anos
T.I.	174	10 anos	Estabelecido	02 anos
T.I.	80	20 anos	Estabelecido	03 anos
e-commerce	1	14 anos	Estabelecido	04 anos
Segurança Informação	60	12 anos	Certificado	03 anos

Tabela 2. Perfis das empresas selecionadas

Foram selecionadas empresas brasileiras sabidamente certificadas na norma ISSO 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 do Top Three de ramos de atuação de empresas brasileiras que mais possuem certificação nesta norma, segundo levantamento realizado pela ISO (2013).

3.1. 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.

3.1.2. Características do Roteiro

Para estruturar o roteiro, as questões abrangem todas as etapas do ciclo PDCA aplicado à norma ISO 27001 (Figura 1). 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.

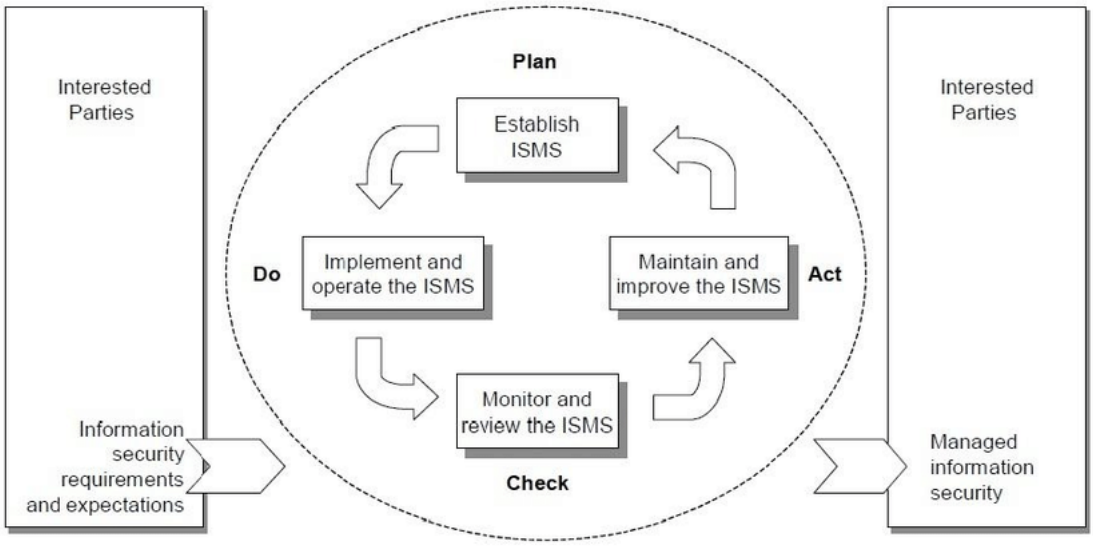


Figura 1. Ciclo PDCA aplicado à ISO 27001

O PDCA é um modelo que busca tornar os processos da gestão de uma empresa mais ágeis, claros e objetivos. Pode ser utilizado em qualquer tipo de empresa e é divido em quatro etapas: PLAN (planejar), DO (fazer), CHECK (verificar) e ACT (agir). 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:

Característica	Descrição	Referência
Abordagem	Tipo funil: perguntas genéricas progredindo para específicas.	Malhotra (2006)
Estrutura	Perguntas abertas. Objetivo de buscar os maiores detalhes possíveis das respostas dos entrevistados, devido a complexidade do tema.	Trivinos (1990)
Enunciado	Utilizadas palavras comuns conhecidas por quem atua nesta área. Não foram uilizadas palavras ambíguas, com alternativas implícitas, suposições implícitas, generalizações e estimativas.	Malhotra (2006)
Objetivos	Cada questão possui um objetivo que descreve o que de fato está sendo buscado como resposta no enunciado das perguntas.	Malhotra (2006)
Nível	Divididas nas categorias "mais vigorosas" e "menos vigorosas". As questões "mais vigorosas" provocam pensamentos mais profundos, já as "menos vigorosas" constituem-se em respostas mais objetivas	Siqueira (2011)

Tabela 3. Estruturação do roteiro de entrevistas

Depois de estruturado, o roteiro foi previamente avaliado e aprovado por

especialistas em segurança da informação que possuem certificações como, por exemplo, CISSP, CISM, auditor líder em ISO 27001, entre outras capacitações.

3.2. Análise dos Dados

A técnica de Análise de Conteúdo foi utilizada para a análise de dados desta pesquisa. Segundo Moraes (199), 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.

A técnica de Análise de Conteúdo dos dados foi dividida em cinco etapas, baseando-se nas sugestões de Moraes (1999): preparação, onde os dados foram transcritos para preparação; unitarização, onde foram identificadas as unidades de registro; categorização, onde os dados resultantes das unidades de registros foram separados de acordo com os termos comuns; descrição, onde um texto síntese por categoria foi elaborado de acordo com as respostas dos entrevistados e, por fim, interpretação, quando os dados descritos nas categorias foram interpretados.

4 I 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.

4.1. Falta de Apoio da Alta Direção

O comprometimento da direção e todos os níveis gerenciais é primordial no estabelecimento e manutenção do Sistema de Gestão de Segurança da Informação, conforme mencionado na ISO 27001. 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.

4.2. Falta de Capacitação da Equipe de Segurança da Informação

A identificação deste desafio partiu não somente das respostas explícitas dos entrevistados, mas, também, das respostas implícitas. 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.

4.3. Influência da Cultura Local

Este desafio acaba aparecendo de forma onipresente entre as respostas dos entrevistados. A influência da cultura local, segundo as respostas obtidas, acaba aparecendo como fator que origina outros desafios como, por exemplo, a falta de comprometimento dos colaboradores para com a cultura de segurança da informação das empresas.

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.

4.4. Falhas na Elaboração da Análise de Risco

As falhas na elaboração da análise de risco desencadeiam outros desafios, assim como a falta de apoio da alta direção. 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.

4.5. Resistência à Mudança

Qualquer norma de gestão enfrenta este desafio antes mesmo da norma ser estabelecida no ambiente. 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.

4.6. 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 4).

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 Risco	Plan
Resistência à mudança	Do, Act

Tabela 4. Desafios enfrentados por cada etapa do ciclo PDCA

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.

5 I CONCLUSÃO

O presente artigo buscou responder a questão de pequisa: quais são os principais desafios no cenário nacional, a fim de estabelecer e manter um Sistema de Gestão de Segurança da Informação? Esta questão foi respondida com sucesso, respeitando a amostra selecionada que representa o cenário brasileiro.

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 citados pelos entrevistados do Sistema de Gestão de Segurança da Informação da organização.

Dificuldades tiveram que ser superadas ao longo desta pesquisa para obtenção dos objetivos propostos. Exaustivos testes na elaboração e aprovação do roteiro de entrevista, dificuldades em conseguir flexibilidade das empresas selecionadas para realização das entrevistas, as frustrações momentâneas enfrentadas nos cancelamentos de entrevistas por motivos diversos, a seleção de outras empresas que atendessem aos requisitos desta pesquisa e, por fim, a própria análise de dados que foi realizada com a paciência e os cuidados que esta fase requer.

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 consideravelmente

com os desafios dos estudos realizados na Índia, Omã e Arábia Saudita. Estes dados são interessantes, pois existe uma diferença cultural forte entre o Brasil e os países mencionados e, mesmo assim, os desafios acabaram convergindo-se.

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 aos 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.

5.1. Trabalhos Futuros

Análises aprofundadas sobre as causas dos desafios mencionados neste artigo poderão ser realizadas. Com as causas mapeadas, medidas preventivas poderão ser elaboradas e aplicadas para evitar ou minimizar a ocorrência dos desafios citados. Como consequência desta pesquisa, também poderá ser conduzido um estudo focado em sugerir e aplicar possíveis soluções aos desafios detectados neste trabalho.

Adaptação do roteiro de entrevistas para utilização em pesquisas que tenham como foco outros escopos, ramos de atuação específicos ou determinadas regiões geográficas.

E, por fim, realizar um estudo mais específico que possa levantar hipóteses para explicar os motivos dos desafios citados neste artigo assemelharem-se com os estudos realizados em outras regiões geográficas com culturas diferentes.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2005, (2005) “Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos”.

Abusaad, Belal, Saeed Fahad A., Alghathbar, Khaled, Bilal, Khan. (2011) “Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes and Lessons Learned”, 9th Australian Information Security Management Conference, Edith Cowan University. December.

Al-Awadi, Maryam, Renaud Karen. (2008) “Success Factors in Information Security Implementation in Organizations”, University of Glasgow.

British Assessment Bureau, (2013) “Survey Shows Fear of ISO 27001”, http://www.britishassessment.co.uk/news/survey-shows-fear-of-iso-27001, Julho.

ISO, International Organization for Standardization, (2013), “ISO Survey 2012”, http://www.iso.org/iso/home/standards/certification/isosurvey.htm?certificate=ISO%209001&countrycode=AF, Setembro.

Kosutic, Dejan (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-, Outubro.

Malhotra, N. K. (2006) “Pesquisa de marketing: uma orientação aplicada”, Porto Alegre: Bookman.

Moraes, Roque (1999) “Análise de conteúdo”, Revista Educação, Porto Alegre, Vol. 22, Nº. 37, pp.

7-32.

Martins, Alaíde, Santos, Celso (2005) “Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação”, Journal of Information Systems and Technology Management, vol 2, Nº 2, pp. 121-136. Salvador.

Singh, Abhay, Sharma, Sammarth, Pandey, Manish, Chaurasia, Sandarbh, Vaish, Anaurika.

Venkatesan S. (2012) “Implementation of ISO 27001 in Indian Scenario: Key Challenges”, International Conference on Recent Trends of Computer Technology in Academia.

Siqueira, Jairo, (2011) “A Arte das Perguntas Criativas e Desafiadoras”, http://criatividadeaplicada.com/2011/07/28/a-arte-das-perguntas- criativasedesafiadoras/, Julho.

Solms, Von R. (1999) “Information Security Management: Why Standards are Important”, Information Management & Computer Security. vol. 46, n° 8, p. 91-95.

The British Assessment Bureau, (2013) “Key Survey Illustrates the Importance of ISO 27001”, http://www.british-assessment.co.uk/news/key-survey-illustrates-theimportance-of-iso-27001, Agosto.

The British Assessment Bureau, (2013) “Survey Shows Fear of ISO 27001”, http://www.british-assessment.co.uk/news/survey-shows-fear-of-iso-27001, Julho.

The Trivinos, Augusto Nibaldo Silva (1990) “Introdução à Pesquisa em Ciências Sociais: A Pesquisa Qualitativa em Educação”, São Paulo, Atlas, 1990. p. 146.

Waluyan, Liska, Blos, Mauricio, Nogueira, Stephanie, Asai, Tatuso. (2010) “Potential Problems in People Management concerning Information Security in Cross-cultural Environment – The Case of Brazil”, Journal of Information Processing, Vol. 18, pp. 38-42. February.

Agência Brasileira do ISBN
ISBN 978-85-7247-048-3