

ANA PAULA ALVES FIORE

**Os fatores que influenciam a integração dos sistemas de gestão de segurança da
informação e da qualidade em uma instituição de concursos, vestibulares e avaliações**

Ana Paula Alves Fiore

Os fatores que influenciam a integração dos sistemas de gestão de segurança da informação e da qualidade em uma instituição de concursos, vestibulares e avaliações

Dissertação apresentada ao programa de Mestrado Profissional em Engenharia de Produção da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, para obtenção do título de Mestre em Engenharia de Produção.

Orientador: Prof. Dr. Jorge Muniz Jr.
Co-orientadora: Prof^a. Dr^a. Ana Lúcia Figueiredo Facin

Guaratinguetá - SP
2020

	Fiore, Ana Paula Alves
F518f	Os Fatores que influenciam a integração dos sistemas de gestão de
	segurança da informação e da qualidade em uma instituição de concursos,
	vestibulares e avaliações / Ana Paula Alves Fiore – Guaratinguetá, 2020.
	75 f : il.
	Bibliografia: f. 56-63
	Dissertação (Mestrado) – Universidade Estadual Paulista, Faculdade de
	Engenharia de Guaratinguetá, 2020.
	Orientador: Prof. Dr. Jorge Muniz Júnior
	Coorientadora: Profª Drª Ana Lúcia Figueiredo Facin
	1. Sistemas de informação gerencial. 2. Processo decisório por
	critério múltiplo. 3. Gestão da qualidade total. 4. Cultura
	organizacional. I. Título.
	CDU 658:681.3(043)

ANA PAULA ALVES FIORE

**ESTA TESE FOI JULGADA ADEQUADA PARA A OBTENÇÃO DO TÍTULO DE
! MESTRE EM ENGENHARIA DE PRODUÇÃO"**

**PROGRAMA: ENGENHARIA DE PRODUÇÃO
CURSO: MESTRADO**

APROVADA EM SUA FORMA FINAL PELO PROGRAMA DE PÓS-GRADUAÇÃO


Prof. Dr. Jorge Muniz Junior
Coordenador

BANCA EXAMINADORA:


Prof. Dr. JORGE MUNIZ JUNIOR
Orientador - UNESP/FEG
participou por videoconferência


Prof. Dr. ROBERTO ANTONIO MARTINS
UFSCAR
participou por videoconferência


Prof. Dr. HENRIQUE LUIZ MONTEIRO
UNESP/FC
participou por videoconferência

DADOS CURRICULARES

ANA PAULA ALVES FIORE

NASCIMENTO	25.09.1976 – São Paulo / SP
FILIAÇÃO	Nicola Fiore Neto Clausis Alves da Silva Fiore
2006/2007	Especialista em Gestão da Qualidade e Produtividade Faculdade de Engenharia de Sorocaba
1996/1999	Bacharel em Ciência da Computação Universidade Metodista de São Paulo

Dedico este trabalho à minha família.

AGRADECIMENTOS

Agradeço aos colegas de sala e da Engenharia de Produção pela troca de conhecimento, em especial à Goreth de Carvalho Gonçalves, ao Eduardo de Souza Serrano Filho Serrano e ao Vagner Batista Ribeiro.

Aos colegas da instituição objeto de estudo e aos consultores que participaram das pesquisas, sem os quais esta pesquisa não teria sido concluída.

À instituição objeto de estudo e à sua diretoria executiva, pela confiança depositada em mim e pela contribuição para a realização deste trabalho.

Aos professores Prof. Dr. Roberto Antonio Martins, Prof. Dr. Claudemir Leif Tramarico e Prof. Dr. Henrique Luiz Monteiro pelas contribuições durante as fases de qualificação e defesa desta dissertação.

Ao meu orientador Prof. Dr. Jorge Muniz Jr. e à minha co-orientadora Prof. Dra. Ana Lúcia Figueiredo Facin pela orientação, por me incentivarem e estarem comprometidos com o meu desenvolvimento.

O presente trabalho foi realizado com apoio financeiro da Fundação para o Vestibular da Universidade Estadual Paulista “Júlio De Mesquita Filho” – VUNESP.

RESUMO

A implantação de sistemas de gestão certificados visa melhorar continuamente os resultados das empresas. Em organizações que, eventualmente, já possuam um sistema de gestão certificado, como foi o caso da empresa objeto do presente estudo, pode ser um desafio implantar um novo sistema de gestão. Esta pesquisa identificou e priorizou os fatores que influenciam a integração de um sistema de gestão da segurança da informação certificado de acordo com a norma ISO 27001 com um sistema de gestão da qualidade certificado de acordo com a norma ISO 9001, para guiar a alocação de recursos. A maioria dos artigos pesquisados nas bases Scopus e Web of Science focou nos fatores que impactaram a integração de sistemas de gestão e não foram encontrados artigos sobre a prioridade destes fatores. Foi realizada revisão da literatura e foram identificados cinco fatores como base da presente pesquisa: Modelo de Implantação, Recursos Humanos, Disponibilidade de Recursos, Questões Relativas às Normas e Integração das Normas. Como resultado da pesquisa qualitativa realizada com consultores especialistas em implantação e integração das referidas normas, quatro fatores foram validados e o fator Modelo de Implantação não foi mencionado. Em seguida, para priorização destes fatores, por meio da aplicação do método *Analytic Hierarchy Process* (AHP), verificou-se que para os gestores da instituição objeto de estudo o critério mais relevante é o Apoio, que está relacionado ao provimento de recursos, competência e conscientização para implementação e melhoria contínua dos sistemas de gestão e o fator mais relevante é a Integração das Normas que refere-se à efetiva realização das tarefas necessárias para o processo de integração dos sistemas de gestão. Para os consultores especialistas, o critério mais relevante é o Planejamento, em relação à consideração de questões internas e externas que são relevantes para o propósito da instituição, às necessidades e as expectativas das partes interessadas, à determinação de riscos e oportunidades e ao estabelecimento dos objetivos para as funções e níveis relevantes e o fator mais relevante são os Recursos Humanos, pois a existência de competência interna para lidar com sistemas de gestão integrados é um aspecto facilitador durante o processo.

PALAVRAS-CHAVE: Sistemas de gestão certificados integrados. ISO 27001. ISO 9001. *Analytic hierarchy process*.

ABSTRACT

The implementation of certified management systems aims to continuously improve business results. In organizations that, eventually, already have a certified management system, as was the case of the company object of this study, it can be a challenge to implement a new management system. This research identified and prioritized the factors that influence the integration of an information security management system certified in accordance with ISO 27001 with a quality management system certified in accordance with ISO 9001, to guide resources allocation. Most of the articles researched in Scopus and Web of Science databases focused on factors that impacted management systems integration and there were no articles on the priority of these factors. A literature review was conducted, and five factors were identified as the basis of this research: Implementation Model, Human Resources, Resources Availability, Issues Related to Standards and Standards Integration. As a result of the qualitative research carried out with consultants specialized in the implementation and integration of these standards, four factors were validated, and Implementation Model factor was not mentioned. Then, to prioritize these factors, through the application of the Analytic Hierarchy Process (AHP) method, it was found that for the managers of the institution object of study, the most relevant criterion is Support, which is related to the resources provision, competence and awareness for the implementation and continuous improvement of management systems and the most relevant factor is the Standards Integration, which refers to the effective accomplishment of the necessary tasks for the process of integration of management systems. For specialist consultants, the most relevant criterion is Planning, in relation to the consideration of internal and external issues that are relevant to the purpose of the institution, the needs and expectations of interested parties, the determination of risks and opportunities and the establishment of objectives for the relevant functions and levels and the most relevant factor are Human Resources, as the existence of internal competence to deal with integrated management systems is a facilitating aspect during the process.

KEYWORDS: Integrated certified management systems. ISO 27001. ISO 9001. Analytic hierarchy process.

LISTA DE ILUSTRAÇÕES

Figura 1 – Método de pesquisa.....	32
Figura 2 – Processo de elaboração de questionários	33
Figura 3 – Hierarquia para priorização de fatores que influenciam a integração das normas ISO 27001 e ISO 9001	38
Figura 4 – Exemplo de estrutura hierárquica.....	70
Figura 5 – Modelo de Matriz de Decisão Incompleta	72
Quadro 1 – Fatores comuns entre a norma ISO 27001 e a norma ISO 9001	22
Quadro 2 – Fatores percebidos na integração de sistemas de gestão certificados.....	26
Quadro 3 – Sugestões de atividades para facilitar a integração de sistemas de gestão	30
Quadro 4 – Perfil dos consultores que responderam à pesquisa qualitativa.....	35
Quadro 5 – Perfil dos gestores que responderam à pesquisa quantitativa.....	39
Quadro 6 – Respostas sobre a integração das normas ISO 27001 e ISO 9001	41
Quadro 7 – Resultado da pesquisa: agrupamento das respostas dos consultores para cada fator identificado na literatura.....	66

LISTA DE TABELAS

Tabela 1 – Resumo dos Julgamentos dos Gestores e dos Consultores	44
Tabela 2– Escala Fundamental de Saaty	71

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AHP	<i>Analytic Hierarchy Process</i>
AIJ	<i>Aggregation of Individual Judgments</i>
AIP	<i>Aggregation of Individual Priorities</i>
IC	Índice de Consistência
IEC	<i>International Electrotechnical Commission</i>
IoT	<i>Internet of Things</i>
IPC	<i>Incomplete Pairwise Comparison</i>
ISO	<i>International Organization for Standardization</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
MCDM	<i>Multiple Criteria Decision Making</i>
NBR	Normas Brasileiras
PDCA	Ciclo <i>Plan-Do-Check-Act</i>
TI	Tecnologia da Informação

SUMÁRIO

1	INTRODUÇÃO	13
1.1	CONTEXTUALIZAÇÃO DO PROBLEMA E QUESTÕES DE PESQUISA	13
1.2	JUSTIFICATIVAS	16
1.3	OBJETIVO	16
1.4	ESTRUTURA DO TRABALHO	17
2	REVISÃO DA LITERATURA	19
2.1	SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO	20
2.2	INTEGRAÇÃO DE SISTEMAS DE GESTÃO CERTIFICADOS	25
2.3	ATIVIDADES PARA A INTEGRAÇÃO DE SISTEMAS DE GESTÃO CERTIFICADOS	30
3	MÉTODO DE PESQUISA	32
4	DISCUSSÃO DE RESULTADOS	41
4.1	ANÁLISE QUALITATIVA	41
4.2	ANÁLISE QUANTITATIVA	43
4.3	ANÁLISE FINAL	48
4.4	IMPLICAÇÕES PRÁTICAS	50
5	CONCLUSÃO	53
	REFERÊNCIAS	54
	APÊNDICE A: Questionário estruturado sobre a integração das normas ISO 27001 e ISO 9001	62
	APÊNDICE B: Questionário de coleta de dados	63
	APÊNDICE C: Tratamento de dados sobre a implantação da norma ISO 27001	66
	APÊNDICE D: Método <i>Analytic Hierarchy Process</i> (AHP) combinado com a técnica <i>Incomplete Pairwise Comparison</i> (IPC)	70

1 INTRODUÇÃO

Considerando a temática central desta dissertação, neste capítulo será apresentada a contextualização do problema, bem como serão dispostas: as questões de pesquisa, as justificativas para a relevância do tema, o objetivo e a estrutura que pautaram o presente trabalho acadêmico.

1.1 CONTEXTUALIZAÇÃO DO PROBLEMA E QUESTÕES DE PESQUISA

A implantação de sistemas de gestão certificados visa melhorar os resultados das empresas, com profissionalização e ganho de eficiência, visto que para que os produtos e/ou serviços oferecidos transmitam credibilidade e confiança, é importante que sejam projetados de acordo com normas e padrões apropriados. O sucesso do negócio depende da satisfação e superação da expectativa dos clientes em quesitos como qualidade do serviço prestado, atendimento dos prazos acordados, confiabilidade das informações. A adequação a sistemas certificados torna os processos mais eficazes, gera melhoria nas especificações e proporciona maior controle. A padronização dos processos e a definição de responsabilidades tornam as empresas mais organizadas, com menos retrabalhos e desperdícios, gerando aumento da eficiência e da qualidade dos produtos e serviços (MAEKAWA; CARVALHO; OLIVEIRA, 2013).

Além dos clientes, é importante também considerar as necessidades das partes interessadas (ROSA; TOLEDO, 2015). O grau em que o sistema de gestão da qualidade é implantado é diferente de organização para organização, devido a diferenças existentes entre as condições de mercado, tamanho da organização, cultura social e estilo de gestão (BRITVIC; KOVACEVIC; CINGEL, 2013). Neste sentido, para o atendimento dos requisitos de maneira sistemática, as organizações certificam o sistema de gestão da qualidade de acordo com a norma ABNT NBR ISO 9001:2015 - Sistemas de Gestão da Qualidade (ABNT, 2015), que promove a adoção de uma abordagem de processos ao desenvolver, implementar e melhorar a eficácia de um sistema de gestão da qualidade, visando aumentar a satisfação do cliente, atendendo aos seus requisitos (MESQUIDA; MAS, 2015). Além disso, a implementação também inclui documentação clara e auditorias internas regulares, que funcionam como uma base para a melhoria do gerenciamento do fluxo dos produtos e serviços (HUO; HAN; PRAJOGO; 2014).

Em uma sociedade baseada no conhecimento, a informação e suas repercussões são os principais fatores de crescimento econômico (GASPAR; POPESCU, 2018). Em um mundo competitivo, apenas organizações que aproveitam os benefícios que as melhores informações podem fornecer para a tomada de decisões são capazes de prosperar (GASPAR; POPESCU, 2018; PROENÇA; BORBINHA, 2018; FOMIN; VRIES; BARLETTE, 2008). Com o avanço tecnológico, o acesso às informações privilegiadas pode tornar-se um diferencial, então as empresas estão sujeitas a tentativas de invasão de pessoas ou organizações mal-intencionadas. O vazamento de informações pode prejudicar a reputação e a competitividade das empresas (PROENÇA; BORBINHA, 2018; RIENZO *et al.*, 2018; TATIARA *et al.*, 2018; FAZENDA; FAGUNDES, 2015).

Assim, a segurança da informação afeta partes externas às organizações. As demandas das várias partes interessadas devem ser atendidas e têm influência cada vez maior sobre a tomada de decisões. A oportunidade que as empresas têm para demonstrar a confiabilidade de sua gestão está intimamente ligada à certificação de seus sistemas (SALOMONE, 2008).

A adequação à norma ABNT NBR ISO/IEC 27001:2013 - Sistemas de Gestão da Segurança da Informação (ABNT, 2013) permite às organizações conduzir e proteger efetivamente as informações críticas, reflete a avaliação dos processos de informação, uma atitude proativa da empresa em relação à segurança da informação e mostra que cumprindo um padrão internacional a instituição pode ser mais digna de confiança. Reafirma-se que, em um mercado competitivo, a ISO 27001 pode ser um ponto de diferenciação dos concorrentes, podendo propiciar à empresa destaque em um momento de decisão por um cliente interessado na contratação de seus serviços (LONGRAS *et al.*, 2018; HSU; WANG; LU, 2016; FOMIN; VRIES; BARLETTE, 2008).

Não raro, detectou-se que, diversas empresas optam pela implantação de mais de um sistema de gestão certificado para garantir a eficácia e confiabilidade dos seus processos. A necessidade de ter uma visão global desses sistemas, de maneira a alinhar os objetivos e facilitar a tomada de decisões provoca o desejo de integrar os sistemas (MESQUIDA *et al.*, 2010). A integração de sistemas de gestão certificados pode ser entendida como a junção de diferentes sistemas em um único mais eficaz (BERNARDO *et al.*, 2008; BECKMERHAGEN *et al.*, 2003).

A integração das normas ISO 27001 e ISO 9001 foi estudada por diversos autores, como por exemplo, a integração de auditorias para promoção de eficiência organizacional (HOY; FOLEY, 2015); a possibilidade da integração na prática (BRITVIC; KOVACEVIC; CINGEL,

2013); a relação entre os requisitos compartilhados pelas normas (MESQUIDA *et al.*, 2010) e a introdução de um modelo para a integração das referidas normas (WANG; TSAI, 2009).

Outros artigos tratavam da integração de sistemas de gestão certificados de maneira mais ampla, sem mencionar somente as normas ISO 27001 e ISO 9001, como por exemplo, a introdução de um modelo para integração de sistemas de gestão certificados (MAJERNIK *et al.*, 2017; OLIVEIRA, 2013); as dificuldades percebidas na integração (ABAD; CABRERA; MEDINA-LEÓN, 2016); como a ordem de implementação e o nível de integração mudam durante o tempo (KAFEL; CASADESÚS, 2016); as vantagens e desvantagens da integração (REBELO; SANTOS; SILVA, 2015; SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008); a comparação de modelos de integração (OLARU *et al.*, 2014); os benefícios da integração (BERNARDO *et al.*, 2015; SANTOS *et al.*, 2013; TARÍ; MOLINA-AZORÍN; HERAS, 2012); a frequência de integração e qual é o sistema de gestão mais implantado nas empresas da Croácia (BRITVIC; BLAZEVIC; VLAINIC, 2014); a relação entre as dificuldades, os benefícios e o nível de integração (SIMON; KARAPETROVIC; CASADESÚS, 2012); a verificação do nível de implantação dos sistemas (Bernardo *et al.*, 2008); a investigação dos fatores externos e internos que afetam a integração (ZENG; SHI; LOU, 2007) e o impacto do novo sistema implantado para o sistema de gestão já existente (BECKMERHAGEN *et al.*, 2003).

Sendo assim, em conformidade com a revisão da literatura, esta dissertação foi desenvolvida tendo como referência sua aplicação em uma instituição que tem seu sistema de gestão da qualidade certificado de acordo com a norma ISO 9001 e que pretende certificar seu sistema de segurança da informação de acordo com a norma ISO 27001, de maneira integrada, respondendo as seguintes questões:

- i. Quais são os fatores que influenciam a integração do sistema de gestão de segurança da informação com o sistema de gestão da qualidade?
- ii. Quais são os fatores mais relevantes?

Para responder a estas questões, foi realizada uma revisão de literatura e uma pesquisa qualitativa para a identificação dos fatores. Para a priorização e definição dos fatores mais relevantes foi aplicado o método *Analytic Hierarchy Process* (AHP) desenvolvido por Saaty (2013), para tomar decisão sobre problemas complexos, dividindo problemas com vários julgamentos em diferentes níveis em subproblemas com níveis hierárquicos (ALMEIDA, PRADHAN; MUNIZ Jr., 2017). Uma análise do método é apresentada no Apêndice D.

1.2 JUSTIFICATIVAS

Esta pesquisa pode contribuir para mitigar as dificuldades na integração dos sistemas de gestão certificados tais como falta de competência interna para lidar com sistemas integrados (REBELO; SANTOS; SILVA, 2015; SIMON; KARAPETROVIC; CASADESÚS, 2012) e dificuldades com as normas de implementação e certificação (OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008).

Rebelo, Santos e Silva (2015) indicam que, uma das dificuldades que as empresas enfrentam é não ter um modelo que guie a integração dos sistemas de gestão, portanto, a avaliação da situação real, motivações, vantagens, desvantagens, limitações e modelos de implantação é uma área de pesquisa necessária. Bernardo *et al.* (2008), Nunhes, Motta e Oliveira (2013) sugerem que sejam pesquisadas as dificuldades enfrentadas no processo de integração de sistemas de gestão certificados.

Abad, Cabrera e Medina-León (2016) pesquisaram sobre as dificuldades na integração de sistemas de gestão certificados (qualidade, ambiental e saúde e segurança ocupacional) em empresas espanholas e sugerem novos estudos em diferentes setores e em diferentes contextos geográficos. Adicionalmente, além das dificuldades de integração de sistemas de gestão certificados, Wiengarten *et al.* (2017) pesquisaram sobre como a adoção de sistemas de gestão integrados (qualidade, ambiental e saúde e segurança ocupacional) afetaram o desempenho de empresas situadas na Irlanda e, ao final de sua pesquisa, sugerem que tais dificuldades sejam objeto de pesquisa, versando sobre o mesmo tema, abordando diferentes sistemas e em outros países, propiciando, assim, uma avaliação mais diversificada de dados.

Considerando o mercado de atuação da instituição objeto de estudo e a detecção de forte concorrência, um dos desafios é conseguir que o cliente não escolha o serviço pelo valor, mas veja o custo-benefício de escolher uma instituição com sistema de gestão da qualidade certificado e em busca da certificação de seu sistema de gestão da segurança da informação, com forte empenho em ética, transparência e confidencialidade.

1.3 OBJETIVO

Esta pesquisa tem como objetivo identificar e priorizar os fatores que influenciam a integração do sistema de gestão da segurança da informação certificado de acordo com a norma ISO 27001 com o sistema de gestão da qualidade já certificado de acordo com a ISO

9001, para guiar a alocação de recursos, em uma instituição prestadora de serviços de concursos, vestibulares e avaliações educacionais, de mais de 40 anos de experiência no mercado para o qual atua.

A instituição conta com mais de 200 funcionários, que trabalham anualmente em mais de 120 projetos, avaliando cerca de 3 milhões de pessoas que buscam colocação ou recolocação profissional por meio de seleção pública ou que se submetem à realização de provas que avaliam sua capacidade intelectual, habilidades etc. quando da seleção em vestibulares ou participam de provas para avaliação da qualidade do ensino. Desta maneira, a instituição lida com informações sigilosas na aplicação de provas e com dados confidenciais dos candidatos.

Assim, reiterando a informação de que o mercado de concursos e vestibulares é concorrido, movimenta um grande volume de recursos e impacta diretamente na expectativa de aprovação por muitas pessoas, quando da seleção a que se submetem, constatou-se durante a pesquisa que o sistema de segurança da informação da instituição é alvo constante de tentativas de invasão.

Neste sentido, considerando que o foco da prestação de serviços da organização objeto de estudo é alicerçada no rigor acadêmico, na qualidade e na segurança, com a certificação ISO 27001, a instituição pretende obter um diferencial em relação aos seus concorrentes, demonstrando aos seus clientes e demais partes interessadas o seu empenho em desenvolver sua prestação de serviços pautada nos seguintes atributos: ética, transparência, sigilo e confidencialidade.

1.4 ESTRUTURA DO TRABALHO

Esta dissertação está estruturada conforme descrito a seguir.

O Capítulo 2 contém uma revisão da literatura sobre sistemas de gestão certificados, sistemas de gestão da qualidade, sistemas de gestão de segurança da informação, integração de sistemas de gestão certificados e atividades para a integração de sistemas de gestão certificados.

O Capítulo 3 apresenta o método utilizado nesta dissertação, com apresentação das três etapas: a proposição do modelo de trabalho, o delineamento do trabalho de campo e a realização do trabalho de campo.

O Capítulo 4 é dedicado à apresentação e discussão dos resultados das pesquisas qualitativa e quantitativa.

O Capítulo 5 apresenta a conclusão, com as contribuições desta pesquisa e as recomendações para pesquisas futuras, seguido pelas referências bibliográficas.

Por fim, o Apêndice A exibe o questionário estruturado sobre a integração das normas ISO 27001 e ISO 9001, que foi utilizado na pesquisa qualitativa com os consultores especialistas, o Apêndice B apresenta o questionário de coleta de dados que foi utilizado na pesquisa quantitativa com os gestores da instituição objeto de estudo e com os consultores, o Apêndice C contém o tratamento de dados sobre a implantação da norma ISO 27001, que foram coletados a partir da pesquisa qualitativa e o Apêndice D exibe uma análise do método *Analytic Hierarchy Process* (AHP) combinado com a técnica *Incomplete Pairwise Comparison* (IPC).

2 REVISÃO DA LITERATURA

Neste capítulo será apresentada uma revisão da literatura acerca dos sistemas de gestão certificados, sistemas de gestão da qualidade, sistemas de gestão de segurança da informação, integração de sistemas de gestão certificados e atividades para a integração de sistemas de gestão certificados.

A adoção por uma organização de sistemas de gestão certificados de acordo com as normas da Organização Internacional de Normalização (ISO), que são aceitas mundialmente, é uma realidade justificada por fatores competitivos ou por requisitos formais dos clientes e/ou de outras partes interessadas. Assim, de acordo com as referências estudadas, é importante registrar que a certificação deixa os procedimentos mais exatos e claros e ajuda a competição em mercados globalizados (LONGRAS *et al.*, 2018; MAJERNIK *et al.*, 2017; REBELO; SANTOS; SILVA, 2015; BRITVIC; BLAZEVIC; VLAINIC, 2014; NUNHES; MOTTA; OLIVEIRA, 2013; OLIVEIRA, 2013; TARÍ; MOLINA-AZORÍN; HERAS, 2012).

De acordo com o relatório publicado pela ISO referente ao ano 2018, no Brasil foram emitidos 16.351 certificados ISO 9001 e 110 certificados ISO 27001, com 0,7% de certificados ISO 27001 em relação ao total. No mundo foram emitidos 878.664 certificados ISO 9001 e 31.910 certificados ISO 27001, com 3,5% de certificados ISO 27001 em relação ao total. (The ISO Survey, 2018).

Neste sentido, as empresas que optam pela implementação de um sistema de gestão da qualidade, se concentram em fornecer mais valor para seus clientes e em melhorar a eficiência dos seus processos. A melhoria contínua dos processos e da qualidade do produto leva ao aumento das receitas por meio da confiabilidade do produto e de custos reduzidos (TARÍ; MOLINA-AZORÍN; HERAS, 2012). São diversos os benefícios percebidos com a implantação da norma ISO 9001, tais como: melhoria na organização interna, melhoria no fluxo de informações e na habilidade dos funcionários em desenvolver novos produtos, progresso na comunicação e na rotina da empresa, maior clareza dos objetivos com orientações estratégicas e metas de negócios e confiabilidade na marca da empresa perante consumidores (ALMEIDA; PRADHAN; MUNIZ Jr., 2017; MAEKAWA; CARVALHO; OLIVEIRA, 2013; SANTOS; MENDES; BARBOSA, 2011). A ISO 9001 aperfeiçoa diretamente a gestão do fluxo de decisões ao melhorar procedimentos e políticas e pode ser um catalisador de mudanças em todos os níveis hierárquicos e de processos (ALMEIDA; PRADHAN; MUNIZ Jr., 2017).

2.1 SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

As empresas atuam em mercados competitivos em cada segmento para o qual atuam e, impulsionadas pela concorrência, pela melhoria dos serviços e pela eficiência do trabalho, a maioria das organizações trabalha cada vez mais com a tecnologia de informação. Neste sentido, com o aumento de ataques cibernéticos e de vírus é necessária a adoção de procedimentos de segurança rigorosos (TU; YUAN, 2014; ABUSAAD *et al.*, 2011).

De acordo com Boehmer (2009), as empresas mais suscetíveis à perda de lucro por um ataque cibernético bem-sucedido são aquelas que teriam interesse na proteção dos ativos de tecnologia da informação. Sendo assim, seria possível pensar que somente as empresas de tecnologia da informação ou que lidam com informações críticas e confidenciais como bancos, financeiras ou do ramo de telecomunicações, poderiam se beneficiar da certificação ISO 27001, afirmação esta que não se confirma dada a constante migração dos níveis corporativos dos controles manuais para os controles tecnológicos.

Atualmente um dos aspectos mais importantes das organizações é a segurança da informação. Gerir e proteger as informações se tornou um desafio porque os ativos das empresas estão cada vez mais digitalizados, gradativamente o trabalho é mais baseado em tecnologia da informação e há maior interação entre as instituições (PROENÇA; BORBINHA, 2018; KHAJOUEI; KAZEMI; MOOSAVIRAD, 2017; FOMIN; VRIES; BARLETTE, 2008). Neste sentido, a maior integração entre as instituições permite que novos riscos possam ser apontados, haja visto as notícias recorrentes acerca de violações de dados organizacionais, as mídias sociais e a Internet das Coisas - IoT (LOPES; GUARDA; OLIVEIRA, 2019).

Além do que já foi descrito, em sua pesquisa, Longras *et al.* (2018) divulgaram dados de um relatório que analisou 53 mil incidentes de segurança de informação e 2.216 violações de dados. De acordo com o parecer constante desta pesquisa, apontou-se que parte dos ataques é cometido por agentes internos das organizações, o que demonstra que o fator humano é um dos pontos de vulnerabilidade, aumentando a dificuldade de prevenir incidentes.

Adicionalmente, devido ao estabelecimento da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n. 13.709, de 14 de agosto de 2018) a respeito dos direitos de liberdade e privacidade, a ISO 27001 se torna mais importante, por ser uma ferramenta que poderá ajudar as empresas no atendimento desses regulamentos.

Carvalho e Marques (2019) estudaram a adaptação da ISO 27001 em uma instituição pública de Portugal e afirmam que apesar do orçamento limitado, da falta de profissionais qualificados de tecnologia da informação e da resistência à mudança, o processo foi

importante, pois o número de dispositivos conectados à rede pública é crescente, representando muitos ataques, para os quais a resposta humana não é suficiente, o que exige soluções capazes de impedir, tanto quanto possível, interrupções nas atividades.

Diversas organizações estão buscando a ISO 27001 para cumprir regras de segurança da informação, visando se sentir mais seguras, ao mesmo tempo demonstrando credibilidade a seus clientes. A certificação possibilita que as empresas atendam demandas de auditorias de segurança, promove confiança às partes interessadas da organização ao estabelecer processos apropriados de controle para gerenciar e proteger informações confidenciais. O monitoramento é necessário para verificar se o desempenho do sistema está de acordo com o esperado (LONGRAS *et al.*, 2018).

É importante que não se considere a segurança somente como um assunto de tecnologia. A gestão da segurança da informação exige uma visão integrada e ampla de tecnologias da informação, de gestão de riscos e de negócios, de segurança física e patrimonial, de requisitos legais e de recursos humanos (RIGON; WESTPHALL, 2011).

O estabelecimento de um sistema de gestão de segurança da informação pode não reduzir os riscos imediatamente, mas é uma ferramenta que permite que a organização controle sistematicamente o nível de segurança e de desempenho da informação (LONGRAS *et al.*, 2018; BRITVIC; KOVACEVIC; CINGEL, 2013). O objetivo da norma ISO 27001 é fazer a gestão do sistema para evitar perdas. É necessário identificar, controlar e tratar os riscos existentes no ambiente da organização, minimizando seus efeitos (LONGRAS *et al.*, 2018; HSU; WANG; LU, 2016).

Fazenda e Fagundes (2015) realizaram entrevistas de abordagem qualitativa em empresas certificadas ISO 27001 ou com o sistema de gestão estabelecido e identificaram os principais benefícios que o estabelecimento deste sistema de gestão estava 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, apoio importante no processo de governança, mapeamento das falhas de segurança dos ambientes organizacionais e credibilidade perante aos clientes.

Longras *et al.* (2018) realizaram uma pesquisa em 25 empresas portuguesas e constataram como benefícios da implementação da ISO 27001 a gestão efetiva e a proteção das informações críticas, a posição preventiva em relação às ameaças diárias, maior eficiência nos investimentos, mais confiança das partes interessadas, aumento da competência técnica e implementação de políticas de controle (*backup*, senhas, classificação de informação, contingência).

No Quadro 1, pode ser observada uma compilação dos fatores que influenciam a implantação das normas ISO 27001 e ISO 9001, pesquisados por diversos autores. O objetivo de apresentar esta compilação é verificar se na implantação das duas normas são percebidos fatores comuns. O quadro foi organizado com palavras ou frases diferentes das apresentadas nos artigos, mas que foram agrupadas devido ao entendimento de que são similares.

Quadro 1 – Fatores comuns entre a norma ISO 27001 e a norma ISO 9001

(continua)

Fator	Norma	Descrição	Autores
Apoio da Alta Direção	ISO 27001	Apoio/envolvimento da alta direção.	ABUSAAD <i>et al.</i> , 2011; FAZENDA; FAGUNDES, 2015
	ISO 9001	Compromisso da alta direção.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
Recursos Humanos	ISO 27001	Capacitação da equipe.	FAZENDA; FAGUNDES, 2015; ABUSAAD <i>et al.</i> , 2011; MUELLER; HAN; SCHNEIDER <i>et al.</i> , 2011
	ISO 27001	Resistência dos funcionários à mudança.	LONGRAS <i>et al.</i> , 2018; FAZENDA; FAGUNDES, 2015; ABUSAAD <i>et al.</i> , 2011
	ISO 9001	Confiabilidade e comprometimento da equipe de qualidade.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
	ISO 9001	Conscientização das pessoas sobre o significado da ISO 9001.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
	ISO 9001	Responsabilidades e autoridades definidas.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017; PINTO; CARVALHO; HO, 2006
	ISO 9001	Resistência dos funcionários à mudança.	MAEKAWA; CARVALHO; OLIVEIRA, 2013
Cultura Organizacional	ISO 27001	Influência da cultura local.	FAZENDA; FAGUNDES, 2015; ABUSAAD <i>et al.</i> , 2011
	ISO 9001	Influência da cultura local.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017

Quadro 1 – Fatores comuns entre a norma ISO 27001 e a norma ISO 9001

(conclusão)

Fator	Norma	Descrição	Autores
Disponibilidade de Recursos	ISO 27001	Custo de implementação e certificação.	LONGRAS <i>et al.</i> , 2018
	ISO 9001	Disponibilidade de recursos.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
	ISO 9001	Apuração dos gastos e ganhos com o programa.	PINTO; CARVALHO; HO, 2006
Atividades para Implantação	ISO 27001	Necessidade de uma de análise de riscos adequada.	FAZENDA; FAGUNDES, 2015
	ISO 27001	Necessidade de suporte para a integração de ferramentas de segurança locais.	MUELLER; HAN; SCHNEIDER <i>et al.</i> , 2011
	ISO 27001	Necessidade do estabelecimento de um vocabulário comum entre os diferentes níveis hierárquicos.	MUELLER; HAN; SCHNEIDER <i>et al.</i> , 2011
	ISO 27001	Necessidade de identificação dos ativos da organização.	ABUSAAD <i>et al.</i> , 2011
	ISO 27001	Importância da definição do escopo.	LONGRAS <i>et al.</i> , 2018
	ISO 27001	Importância da interpretação da norma.	LONGRAS <i>et al.</i> , 2018; ABUSAAD <i>et al.</i> , 2011
	ISO 27001	Importância da correta alocação de funções ou tarefas a diferentes funcionários	LONGRAS <i>et al.</i> , 2018
	ISO 9001	Programação para implementação, processo de abordagem e análise do sistema de medição.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
	ISO 9001	Confecção dos documentos necessários para a certificação.	PINTO; CARVALHO; HO, 2006
	ISO 9001	Integração entre departamentos.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017
	ISO 9001	Complexidade das operações realizadas pelas organizações.	ALMEIDA; PRADHAN; MUNIZ Jr., 2017; PINTO; CARVALHO; HO, 2006

Fonte: Elaborado pela própria autora.

Em uma análise do quadro, pode-se perceber a semelhança entre os fatores que influenciaram a implantação dos sistemas de gestão baseados nas duas normas, tais como a

importância do apoio da alta direção, o envolvimento dos recursos humanos, a influência da cultura local, a relevância da disponibilização de recursos e a necessidade da realização efetiva das atividades para o sucesso da implantação.

A partir dos dados obtidos no Quadro 1, observou-se que os fatores identificados em semelhança entre as duas normas, tendo como base a revisão da literatura, foram os descritos a seguir:

- Apoio da Alta Direção: este fator está relacionado ao suporte que a alta direção dá aos funcionários durante o processo de implantação, garantindo orientação e comunicação eficientes para que o objetivo final seja atingido (ALMEIDA; PRADHAN; MUNIZ Jr., 2017; TU; YUAN, 2014), bem como o aporte necessário de recursos (FAZENDA; FAGUNDES, 2015; TU; YUAN, 2014);
- Recursos Humanos: a capacitação da equipe e o conhecimento da norma a ser implantada são facilitadores durante o processo (FAZENDA; FAGUNDES, 2015; ABUSAAD *et al.*, 2011); a resistência à mudança ocorre devido à implantação de mais controles, tarefas vistas como burocráticas, maior esforço para os colaboradores (FAZENDA; FAGUNDES, 2015);
- Cultura Organizacional: crenças que caracterizam o comportamento organizacional (ALMEIDA; PRADHAN; MUNIZ Jr., 2017). Em relação à segurança da informação precisa evoluir, pois em alguns casos, os funcionários tendem a proteger somente os computadores. Existe um excesso de confiança nos colegas de trabalho e não há o registro adequado dos incidentes de segurança da informação (FAZENDA; FAGUNDES, 2015);
- Disponibilidade de Recursos: a implantação de um sistema de gestão certificado depende de suporte, estrutura e de capacidades técnicas (ALMEIDA; PRADHAN; MUNIZ Jr., 2017);
- Atividades para Implantação: importância de suporte e/ou de conhecimento para realizar as tarefas de implantação de uma norma, como por exemplo, a elaboração da análise de riscos (no caso da ISO 27001), que impacta o projeto como um todo, pois é a partir deste processo que as políticas são geradas (FAZENDA; FAGUNDES, 2015).

2.2 INTEGRAÇÃO DE SISTEMAS DE GESTÃO CERTIFICADOS

A manutenção de sistemas de gestão certificados separados demandaria a realização de tarefas duplicadas, o que poderia causar complexidade no gerenciamento interno aumentando a probabilidade de falhas, baixa eficiência, incompatibilidade cultural, aumento de custos e, em um impacto negativo na maioria das partes interessadas, incluindo funcionários e clientes (NUNHES; MOTTA; OLIVEIRA, 2013; HESTON; PHIFER, 2011; ZENG; SHI; LOU, 2007;

BECKMERHAGEN *et al.*, 2003). Em uma pesquisa realizada na Catalunha com 176 empresas, Karapetrovic e Casadesús (2009) concluíram que 85% delas decidiram implantar sistemas de gestão certificados de maneira integrada. Conclusão similar foi obtida por Britvic, Blazevic e Vlainic (2014) em uma pesquisa feita com 210 empresas na Croácia.

Com a integração dos sistemas de gestão certificados pode-se perceber vantagens como: eliminação de conflitos entre sistemas de gestão individuais, otimização de recursos, benefícios estratégicos organizacionais, redução do número de auditorias, bem como o tempo gasto em relação aos custos associados (REBELO; SANTOS; SILVA, 2015; OLARU *et al.*, 2014; OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; TARÍ; MOLINA-AZORÍN; HERAS, 2012; SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008). Neste sentido, são recomendadas ações para a gestão eficiente dos recursos e o estabelecimento de um plano, especificando os objetivos. Foi observado pelos autores que a motivação das pessoas envolvidas é um fator importante para o sucesso da integração.

É importante registrar que as edições atuais das normas ISO são organizadas em uma estrutura de alto nível e permitem maior efetividade na integração dos sistemas de gestão, sendo assim, se torna difícil a tentativa de manter diversos sistemas de gestão atuando de maneira independente (MAJERNIK *et al.*, 2017; BERNARDO *et al.*, 2015; MESQUIDA *et al.*, 2010; FOMIN; VRIES; BARLETTE, 2008; ZENG; SHI; LOU, 2006).

Em uma pesquisa realizada com 81 organizações na Polônia com pelo menos dois sistemas de gestão certificados, Kafel e Casadesús (2016) observaram que o tempo médio para implantação da primeira norma é de 12 meses e da segunda norma é de 7 meses, o que é compreensível pois a maior parte do trabalho é executada na implantação do primeiro sistema de gestão. Abad, Cabrera e Medina-León (2016) realizaram uma pesquisa com 102 empresas espanholas e perceberam uma relação negativa entre o tamanho da empresa e as dificuldades enfrentadas: as pequenas empresas percebem mais dificuldades, principalmente em relação ao envolvimento das pessoas e dos gerentes. Salomone (2008) realizou uma pesquisa com 103 empresas italianas e concluiu que a estrutura, o tamanho e o setor econômico podem

desempenhar um papel decisivo para influenciar se uma organização decide integrar os sistemas de gestão, sendo que o tamanho da empresa é o fator predominante.

O Quadro 2 sumariza os fatores identificados na revisão de literatura que influenciaram a integração dos sistemas de gestão certificados. O quadro foi organizado com frases diferentes das apresentadas nos artigos, mas que foram agrupadas devido ao entendimento de que são similares.

Quadro 2 - Fatores percebidos na integração de sistemas de gestão certificados

(continua)

Fator	Descrição	Autores
Modelo de Implantação	É importante ter um modelo para dar suporte ao processo de integração.	REBELO; SANTOS; SILVA, 2015
	É importante contar com orientação técnica.	ZENG; SHI; LOU, 2007
Recursos Humanos	Competência interna para lidar com sistemas integrados.	REBELO; SANTOS; SILVA, 2015; SIMON; KARAPETROVIC; CASADESÚS, 2012
	Treinamento e mudanças nos métodos e cultura da organização.	SANTOS; MENDES; BARBOSA, 2011
	Segurança da manutenção do emprego, apesar da junção de atividades e de prováveis desalinhamentos de metas operacionais.	BECKMERHAGEN <i>et al.</i> , 2003
	Resistência dos funcionários à mudança.	ABAD; CABRERA; MEDINA-LEÓN, 2016; REBELO; SANTOS; SILVA, 2015; ZENG; SHI; LOU, 2007
Disponibilidade de Recursos	Disponibilização de recursos para a integração.	REBELO; SANTOS; SILVA, 2015; OLARU <i>et al.</i> , 2014; SIMON; KARAPETROVIC; CASADESÚS, 2012
	Maiores custos para implantar simultaneamente do que individualmente; longo tempo de implementação.	SANTOS; MENDES; BARBOSA, 2011
Questões Relativas às Normas	Importância do conhecimento sobre as normas de implementação e certificação.	OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008; ZENG; SHI; LOU, 2007
	Suporte dos organismos de certificação.	SALOMONE, 2008; ZENG; SHI; LOU, 2007

Quadro 2 - Fatores percebidos na integração de sistemas de gestão certificados

(conclusão)

Fator	Descrição	Autores
Questões Relativas às Normas	Percepção de que os sistemas de gestão são revolucionários e burocráticos.	OLARU <i>et al.</i> , 2014
	Necessidade de uma norma internacional para sistemas integrados.	REBELO; SANTOS; SILVA, 2015
Integração das Normas	Importância de se encontrar denominadores comuns para muitas funções do negócio.	REBELO; SANTOS; SILVA, 2015; OLARU <i>et al.</i> , 2014; OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; ZENG; SHI; LOU, 2007; BECKMERHAGEN <i>et al.</i> , 2003
	Percepção de que ocorre perda de identidade dos sistemas de função específica.	BECKMERHAGEN <i>et al.</i> , 2003
	Importância de deixar explícito que a integração dos sistemas é um objetivo.	REBELO; SANTOS; SILVA, 2015
	Importância de auditorias integradas.	ZENG; SHI; LOU, 2007
	Relevância de atribuir níveis de importância a cada sistema.	SALOMONE, 2008
	Necessidade de organizar adequadamente o sistema integrado.	SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008
	Alterações no sistema de gerenciamento devido a mudanças operacionais.	SANTOS; MENDES; BARBOSA, 2011

Fonte: Elaborado pela própria autora.

Somente Rebelo, Santos e Silva (2015) e Zeng, Shi e Lou (2007) indicam a necessidade de um modelo para guiar a integração e a importância da orientação técnica. Os demais fatores são citados por mais autores na literatura pesquisada, como por exemplo a importância do envolvimento dos recursos humanos e a realização adequada das atividades para a integração das normas.

A partir dos dados obtidos no Quadro 2, observou-se que os fatores identificados, tendo como base a revisão da literatura, foram os descritos a seguir:

- Modelo de Implantação: refere-se a importância de as empresas terem um modelo que guie a integração dos sistemas de gestão (REBELO; SANTOS; SILVA, 2015). A existência de uma orientação técnica e de material adaptado para os diferentes

sistemas de gestão de empresas grandes e pequenas é visto como um fator relevante (ZENG; SHI; LOU, 2007);

- Recursos Humanos: a existência de competência interna para lidar com sistemas de gestão integrados pode ser um aspecto facilitador durante o processo (REBELO; SANTOS; SILVA, 2015; SIMON; KARAPETROVIC; CASADESÚS, 2012); a resistência à mudança ocorre, pois é comum que as pessoas não queiram mudar o jeito de fazer as coisas. Mudar exige trabalho extra e novos procedimentos (ZENG; SHI; LOU, 2007);
- Disponibilidade de Recursos: a disponibilidade adequada de recursos para o processo de integração dos sistemas de gestão é relatada por diversos autores como um fator relevante (REBELO; SANTOS; SILVA, 2015; OLARU *et al.*, 2014; SIMON; KARAPETROVIC; CASADESÚS, 2012);
- Questões Relativas às Normas: o aspecto mais relatado pelos autores foi a importância do conhecimento sobre as normas (OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; SANTOS; MENDES; BARBOSA, 2011; SALOMONE, 2008; ZENG; SHI; LOU, 2007); também foi evidenciada a necessidade de suporte dos organismos de certificação (SALOMONE, 2008; ZENG; SHI; LOU, 2007);
- Integração das Normas: refere-se à efetiva realização das tarefas necessárias para o processo de integração dos sistemas de gestão, como por exemplo, a identificação de denominadores comuns para muitas funções do negócio (REBELO; SANTOS; SILVA, 2015; OLARU *et al.*, 2014; OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; ZENG; SHI; LOU, 2007; BECKMERHAGEN *et al.*, 2003).

As normas ISO 27001 e ISO 9001 apresentam uma estrutura de alto nível, o que significa que elas possuem títulos de requisitos idênticos, a mesma redação para o texto central e partilham os termos comuns e as definições principais. Os requisitos específicos de cada norma são inseridos em capítulos apropriados. Esta padronização visa promover a compatibilidade entre as normas, facilitando a integração dos sistemas de gestão certificados (ISO/IEC Directives, Part 1, 2020), sendo que os requisitos comuns das normas podem ser resumidos da seguinte maneira:

- Liderança: a alta direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão;
- Planejamento: quando do planejamento do sistema de gestão, a organização deve considerar questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos, as necessidades e as expectativas das partes interessadas, determinar os riscos e oportunidades e estabelecer os objetivos para as funções e níveis relevantes;
- Apoio: a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão, bem como determinar a competência das pessoas, promover a conscientização e a comunicação e controlar a informação documentada pertinente;
- Operação: a organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos para a provisão de produtos e serviços e implementar planos para alcançar os objetivos, avaliando e tratando os riscos dos processos e da segurança da informação, bem como as saídas não conformes;
- Avaliação de Desempenho: a organização deve avaliar o desempenho e a eficácia do sistema de gestão, bem como realizar auditorias internas e análises críticas pela direção;
- Melhoria: a organização deve ter controles para tratamento de não conformidades, ação corretivas e melhoria contínua.

Em relação ao processo de auditoria dos sistemas de gestão certificados, Hoy e Foley (2015) conduziram uma pesquisa em uma empresa situada na Inglaterra e observaram alguns benefícios de auditar conjuntamente os sistemas de gestão certificados tais como a redução dos esforços, dos custos e da burocracia, considerando os possíveis obstáculos, a seguir destacados:

- falta de verificação de alguns requisitos, caso seja dado mais foco a um dos sistemas de gestão em detrimento dos outros;
- problemas com o nível de competência dos auditores;
- falta de tempo para conduzir adequadamente o processo;
- risco de conflito na documentação e nos processos.

Neste caso, os auditores precisam ser treinados para saber identificar e gerenciar os possíveis conflitos.

2.3 ATIVIDADES PARA A INTEGRAÇÃO DE SISTEMAS DE GESTÃO CERTIFICADOS

Durante a realização desta pesquisa, foi possível encontrar sugestões de atividades que poderiam facilitar a integração dos sistemas de gestão certificados. Wang e Tsai (2009) realizaram uma pesquisa exploratória e um estudo de caso em uma empresa de Taiwan e propuseram um modelo para a integração da ISO 27001 com a ISO 9001. Tatiara *et al.* (2018) realizaram uma pesquisa com 182 usuários de um Data Center na Indonésia e concluíram que algumas atividades devem ser seguidas para apoiar a implementação de sistemas de gestão integrados. Com base em uma pesquisa com 104 empresas na China, Zeng, Shi e Lou (2007) propõem um modelo sinérgico multinível para uma abordagem de implementação eficaz. As sugestões de Abad, Cabrera e Medina-León (2016) foram feitas após uma pesquisa realizada com 102 empresas espanholas.

As atividades sugeridas estão descritas no Quadro 3, organizadas com frases diferentes das apresentadas nos artigos, mas que foram agrupadas devido ao entendimento de que são similares.

Quadro 3 – Sugestões de atividades para facilitar a integração de sistemas de gestão

(continua)

Atividade	Descrição	Autores
Envolvimento da liderança	Conduzir análises, se envolver, comunicar objetivos e planos, motivar e recompensar funcionários.	TATIARA <i>et al.</i> , 2018; ZENG; SHI; LOU, 2007
Envolvimento dos participantes	Formar um comitê de revisão administrativa.	WANG; TSAI, 2009
	Treinar os envolvidos.	WANG; TSAI, 2009
	Comunicar aos funcionários: responsabilidades e autoridades, políticas, procedimentos e objetivos e solicitar que façam melhorias.	TATIARA <i>et al.</i> , 2018
	Cultivar a cultura comum, com regras, procedimentos, programas e sistemas da organização.	ZENG; SHI; LOU, 2007
	Implementar planos de comunicação durante o processo, procurando explicar aos funcionários os incentivos para integrar seus sistemas de gerenciamento, os benefícios esperados e o papel deles no processo de integração.	ABAD; CABRERA; MEDINA-LEÓN, 2016
Integração de documentos	Integrar o sistema de controle de documentos.	WANG; TSAI, 2009

Quadro 3 – Sugestões de atividades para facilitar a integração de sistemas de gestão

(conclusão)

Atividade	Descrição	Autores
Integração de atividades	Integrar atividades para manter a estrutura comum e criar um conjunto de políticas para orientar a implementação do sistema de gestão.	TATIARA <i>et al.</i> , 2018; WANG; TSAI, 2009; ZENG; SHI; LOU, 2007
	Criar um departamento unificado liderado por um único gerente que lida com todos os aspectos do novo sistema integrado, enfatizando a importância de interligar os aspectos organizacionais e técnicos.	ABAD; CABRERA; MEDINA-LEÓN, 2016
Verificação da conformidade	Verificar o atendimento às normas e fazer ajustes, se necessário.	TATIARA <i>et al.</i> , 2018; WANG; TSAI, 2009

Fonte: Elaborado pela própria autora.

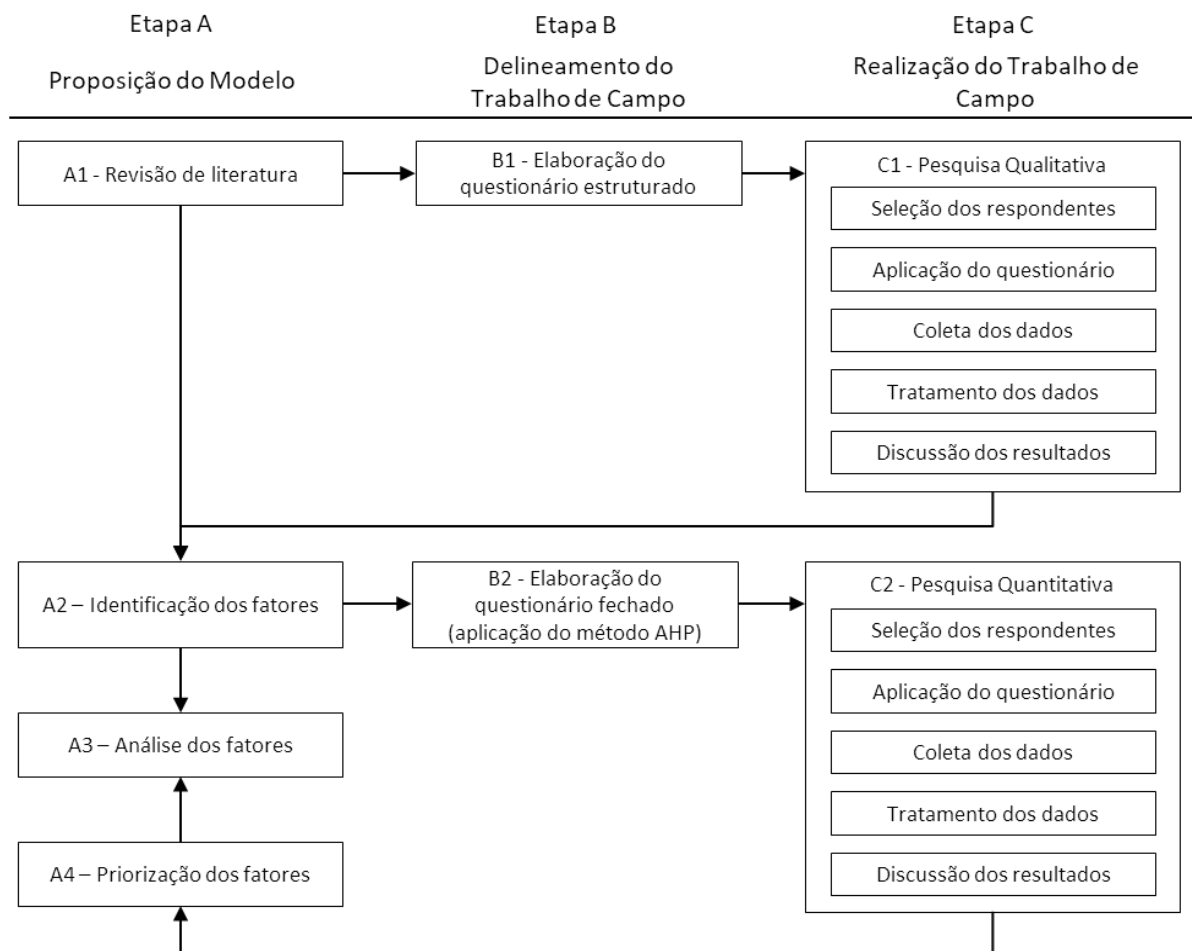
É possível perceber que o foco de Tatiara *et al.* (2018) é maior no envolvimento dos participantes do processo e da liderança, enquanto que para Wang e Tsai (2009) há um reforço acerca da necessidade de verificar se as alterações efetuadas para a implantação da segunda norma atendem os requisitos de ambas as normas e, para Zeng, Shi e Lou (2007) e Abad, Cabrera e Medina-León (2016) detecta-se o enfoque na sinergia das atividades.

3 MÉTODO DE PESQUISA

Neste capítulo será apresentado o método utilizado nesta dissertação. Quanto à natureza, essa pesquisa é classificada como aplicada, pois pretende-se que os resultados sejam aplicados em uma instituição específica para a certificação integrada de seu sistema de gestão de segurança da informação com o sistema de gestão da qualidade.

Na Figura 1, a seguir disposta, ilustra-se as três etapas adotadas para a pesquisa: a Etapa A é a proposição do modelo de trabalho que diz respeito à revisão da literatura e ao resultado gerado após o trabalho de campo, ao passo que a Etapa B trata do delineamento do trabalho de campo com a elaboração dos questionários e aplicação do método AHP; por fim, a Etapa C refere-se à realização do trabalho de campo, ou seja, à aplicação dos questionários elaborados. Cada etapa será detalhada neste capítulo.

Figura 1 – Método de pesquisa



Fonte: Adaptado de Miguel *et al.* (2009).

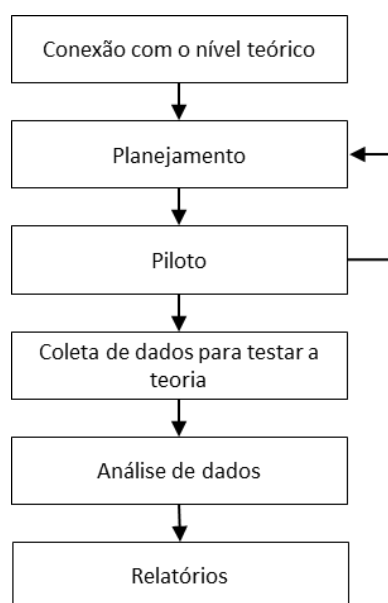
A revisão de literatura (Etapa A1) teve o objetivo de identificar os fatores que influenciam na integração do sistema de gestão de segurança da informação (ISO 27001) com o sistema de gestão da qualidade (ISO 9001).

Foram utilizados artigos das bases Scopus e Web of Science (2003-2019), usando chaves de busca (*strings*) “ISO 9001” and “ISO 27001”, “desafios ISO 27001”, “challenges ISO 27001”, “barriers ISO 27001”, “critical factors ISO 27001”, “desafios ISO 9001”, “challenges ISO 9001” “sistemas integrados”, “integrated systems” e “implementing ISO 27001 after ISO 9001”. Foram identificados e lidos 76 artigos para a análise crítica da literatura. Após este levantamento, selecionou-se 49 artigos, 1 relatório emitido pela ISO e 2 normas da ISO, considerando que estes documentos tratavam diretamente da questão da implantação da ISO 27001 ou de maneira indireta tratando sobre a implantação de outras normas ISO, assim como a integração entre as normas implantadas (ISO 27001 e ISO 9001).

Paralelamente à revisão da literatura, o delineamento do trabalho em campo se deu por meio da elaboração de um questionário estruturado (Etapa B1), direcionado a consultores especialistas na implantação das normas ISO 27001 e ISO 9001, visando a identificação de fatores que influenciam a integração das normas referidas.

As questões foram elaboradas seguindo o método de pesquisa de Forza (2002), ilustrado na Figura 2 e detalhado a seguir.

Figura 2 – Processo de elaboração de questionários



Fonte: Adaptado de Forza (2002).

De acordo com Forza (2002), a conexão com o nível teórico deve guiar a elaboração do questionário. Nesta pesquisa, as perguntas utilizadas nos questionários estão relacionadas aos fatores que influenciam a integração das normas ISO 27001 e ISO 9001 e as atividades para facilitar a integração de sistemas de gestão, que foram levantados a partir dos trabalhos de diversos autores, conforme se pode evidenciar ao observar os Quadros 2 e 3 nesta pesquisa.

Foram elaboradas questões específicas sobre a implantação da norma ISO 27001 (a partir do Quadro 1) e estes dados são tratados no Apêndice C. As questões sobre a integração da norma ISO 27001 com a norma ISO 9001 estão listadas no Apêndice A.

Na elaboração das questões, buscou-se empregar a linguagem mais apropriada ao público de consultores de implantação de sistemas de gestão certificados. Para facilitar o entendimento, não foram feitas perguntas duplas.

A realização do trabalho de campo se deu por meio de uma pesquisa qualitativa, pois a realidade subjetiva dos entrevistados é significativa e contribui para o desenvolvimento da pesquisa. O tratamento dos dados foi realizado por meio de uma abordagem combinada quali-quantitativa. Justifica-se o uso da abordagem qualitativa, devido à ênfase na perspectiva do entrevistado, permitindo a ele a indicação de novas variáveis, caso necessário. A abordagem quantitativa é justificada pela necessidade de mensurar variáveis de pesquisa, neste caso, a priorização dos fatores identificados na literatura (MARTINS, 2012). A combinação das pesquisas qualitativa e quantitativa “possibilita um entendimento melhor dos problemas de pesquisa que cada uma das abordagens permitiria isoladamente.” (MARTINS, 2012, p. 57).

A pesquisa qualitativa (Etapa C1) foi iniciada com a seleção dos respondentes: buscaram-se profissionais em organismos de certificação renomados e em empresas de consultoria com experiência na consultoria de implantação das normas ISO 27001 e ISO 9001.

Em relação à quantidade de respondentes, foi adotada uma abordagem de amostragem por conveniência (REA; PARKER, 2014). Essa opção de amostragem fornece ajuda significativa na coleta de dados e informações úteis que não seriam possíveis usando técnicas de amostragem probabilísticas. Neste caso, os dados encontrados na pesquisa foram usados como base de conhecimento e não generalizados além da própria amostra.

Segundo Forza (2002), na fase de planejamento deve ser feito o ajuste adequado entre o rigor e a viabilidade. Considerando-se as restrições de tempo e de acesso aos consultores, optou-se em encaminhar o questionário a eles por *e-mail*.

Em seguida, foi realizado um piloto para dois consultores (perfis números 1 e 2 detalhados no Quadro 4). A realização do piloto possibilitou o ajuste na questão número 5 do

Apêndice C para maior clareza (as questões apresentadas foram dispostas em seu formato final).

Após o piloto e o ajuste no questionário, a pesquisa qualitativa teve continuidade com o envio dos questionários por *e-mail* para quinze consultores. Foram recebidas respostas de nove consultores que tem experiência superior a 6 anos (perfis número 3 em diante, detalhados no Quadro 4), representando uma taxa de retorno de 60%. Dos nove consultores, todos trabalham com a norma ISO 27001 e seis também trabalham com a norma ISO 9001, mas participaram de processos de integração. A quantidade de respostas foi considerada satisfatória, à medida que se tornaram similares.

Quadro 4 – Perfil dos consultores que responderam à pesquisa qualitativa

(continua)

Consultor	Funções exercidas	Normas abrangidas	Experiência
1	Auditor líder, consultor, e professor de cursos de auditor líder	ISO 27001 ISO 9001 Gestão de projetos	Mais de 30 anos de experiência nas áreas de eletrônica e Tecnologia da Informação. Mais de 15 anos de experiência em implantação de sistemas de gestão.
2	Auditadora líder e consultora	ISO 27001 ISO 9001 ISO 20000	Mais de 12 anos de experiência na atuação em mercados de Telecomunicações e Tecnologia da Informação, em empresas startups, participação em planejamento estratégico e desenvolvimento de mercados e novos produtos e serviços.
3	Auditor líder, consultor e professor de sistemas de gestão	ISO 27001 ISO 9001 ISO 14001 ISO 45001 GEOC 3 OEA	Mais de 10 anos de experiência em sistemas de gestão e 30 anos de experiência atuando no Brasil e Portugal e já tendo auditado na Colômbia, Peru, Equador, Panamá e Costa Rica.
4	Auditor líder e consultor	ISO 27001 ISO 20000-1 ISO 29110-4-1	Experiência de 30 anos na implementação e operacionalização de sistemas de gestão. Experiência de 14 anos na coordenação da área de certificação para programas de certificação.
5	Auditor líder e consultor	ISO 27001 ISO 20000-1 ITIL Manager COBIT	Mais de 13 anos como consultor em projetos de gerenciamento de serviços e governança de Tecnologia da Informação.

Quadro 4 – Perfil dos consultores que responderam à pesquisa qualitativa

(conclusão)

Consultor	Funções exercidas	Normas abrangidas	Experiência
6	Auditor líder e consultor	ISO 27001 ISO 9001 ISO 14001 ISO 45001 ISO 20000-1 TL 9000 Good Privacy OHSAS 18001	16 anos como consultor. 30 anos de experiência da área de telecomunicações.
7	Auditor líder e consultor	ISO 27001 ISO 9001 ISO 14001 ISO 13485 ISO 20000-1	Mais de 25 anos de experiência na atuação em Tecnologia da Informação e Telecomunicações e, atuando em planejamento estratégico e desenvolvimento de sistemas de gestão e controles.
8	Auditor líder e consultor	ISO 27001 ISO 9001 ISO 14001 ISO 20000-1 ISO 29110-4-1	Experiência na área de desenvolvimento de soluções de Tecnologia da Informação e serviços nas áreas governamental e privada. Experiência de 15 anos com implementação e operacionalização de sistemas de gestão.
9	Auditor líder, consultor e professor	ISO 27001 ISO 9001 ISO 14001 ISO 20000-1 ISO 16001 OHSAS 18001 IQNETSR10 Good Privacy	Experiência de 30 anos na área de gestão e 22 anos de experiência em consultoria e treinamento nas normas mencionadas.
10	Auditor líder, consultor e professor	ISO 27001 ISO 9001 ISO 20000-1 PROBARE	Mais de 29 anos de experiência na atuação em Telecomunicações e Tecnologia da Informação. Docente durante 40 anos em universidades em Engenharia de Software, participação em planejamento estratégico e desenvolvimento de mercados e novos produtos e serviços.
11	Auditor e consultor	ISO 27001 ICP-Brasil WebTrust	Mais de 6 anos de experiência em Governança, Riscos e <i>Compliance</i> , Certificação Digital, atuando na implementação das normas e eliminação de riscos nos processos de decisão.

Fonte: Elaborado pela própria autora.

A revisão da literatura, somada à aplicação do questionário estruturado, possibilitou a identificação dos fatores que influenciam a integração da ISO 27001 com a ISO 9001 (Etapa A2). As respostas podem ser observadas no Capítulo 4.

Para a priorização dos fatores (Etapa A4) identificados na literatura foi aplicado o método de tomada de decisão multicritério AHP desenvolvido por Saaty (2013), que divide problemas complexos de tomada de decisão (ou seja, com vários julgamentos em diferentes níveis) em subproblemas com níveis hierárquicos. Uma análise do método é apresentada no Apêndice D.

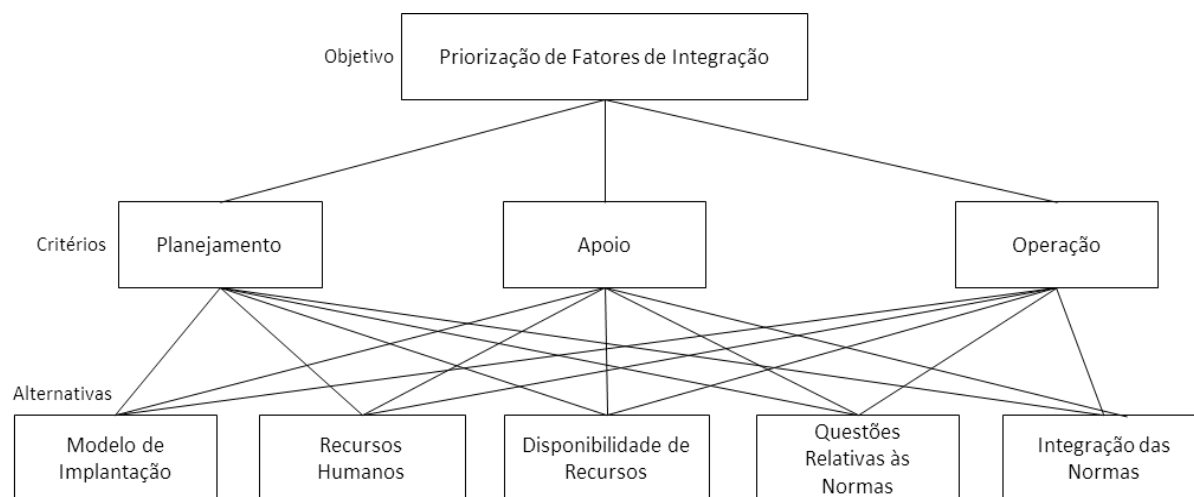
Dentre os métodos de tomada de decisão multicritério existentes, optou-se pelo AHP devido a ser um método conceituado, utilizado mundialmente (TRAMARICO; SALOMON; MARINS, 2017), que pode ser aplicado em uma grande variedade de áreas e é utilizado para estabelecer prioridades (TRAMARICO *et al.* 2015), que é o objetivo desta pesquisa.

Cada nível representa um conjunto de alternativas relacionadas a cada subproblema (MUNIZ Jr. *et al.*, 2019). O nível superior da hierarquia representa o objetivo do problema, que nesta pesquisa é a priorização dos fatores que influenciam a integração de um sistema de gestão da segurança da informação de acordo com a norma ISO 27001 com um sistema de gestão da qualidade certificado de acordo com a norma ISO 9001. É importante estruturar o problema de decisão em níveis hierárquicos e construir um modelo que relacione os fatores em prioridades, identificando, o objetivo geral, os critérios e as alternativas.

Para o estabelecimento dos critérios de integração da ISO 27001 com a ISO 9001, em conjunto com a revisão da literatura, foi feita uma análise dos requisitos das normas ISO 27001 e ISO 9001: Liderança, Planejamento, Apoio, Operação, Avaliação de Desempenho e Melhoria (explanados no Capítulo 2, na página 30). A ordem na qual os requisitos são apresentados na norma não reflete sua importância nem implica a ordem em que devem ser implementados, mas para a utilização nesta pesquisa foram considerados os requisitos que estão mais alinhados em relação aos fatores percebidos por diversos autores como impactantes na integração dos sistemas de gestão certificados: planejamento, apoio e operação.

Para a definição das alternativas, foram utilizados os fatores identificados na literatura (Quadro 2). A estrutura criada para apoiar a priorização dos fatores de integração das normas ISO 27001 e ISO 9001 está representada na Figura 3.

Figura 3 – Hierarquia para priorização de fatores que influenciam a integração das normas ISO 27001 e ISO 9001



Fonte: Elaborado pela própria autora.

Em conjunto com o método AHP, foi utilizada a técnica *Incomplete Pairwise Comparison* (IPC), que permite a redução de julgamentos para seleção de critérios e alternativas (HARKER, 1987). Uma análise da ferramenta é apresentada no Apêndice D.

Os 3 critérios gerariam 3 julgamentos. As 5 alternativas gerariam 10 julgamentos para cada um dos critérios. A técnica IPC possibilitou a redução dos critérios para 2 julgamentos e das alternativas para 4 julgamentos para cada um dos 3 critérios. Sendo assim, o tempo da pesquisa foi otimizado para 20 minutos e obteve-se um questionário mais aderente, pois a utilização do método completo provocaria a repetição de diversas questões.

O método AHP orientou a elaboração do questionário fechado (Etapa B2), que foi adaptado de Muniz Jr. *et al.* (2019) e permitiu que os respondentes avaliassem múltiplos fatores-chave no processo de tomada de decisão hierárquica usando a escala de Saaty (SAATY, 2013). As questões estão apresentadas no Apêndice B e foi utilizada a escala Likert de cinco pontos consistente com Saaty (2013), de acordo com a Tabela 2.

A pesquisa quantitativa (Etapa C2) foi iniciada com a seleção dos respondentes: gestores da instituição objeto de estudo que estarão envolvidos com a integração das normas ISO 27001 e ISO 9001 e os consultores especialistas que foram selecionados para a pesquisa qualitativa.

Em relação à quantidade de respondentes, foi adotada uma abordagem de amostragem por conveniência (REA; PARKER, 2014). Essa opção de amostragem fornece ajuda

significativa na coleta de dados e informações úteis que não seriam possíveis usando técnicas de amostragem probabilísticas. Neste caso, os dados encontrados na pesquisa foram usados como base de conhecimento e não generalizados além da própria amostra.

Foi realizado um piloto com a gestora da área de Logística e que foi responsável pela implantação da norma ISO 9001 na instituição (18 anos de experiência na área de Logística e Representante da Direção no período de 2012 a 2015), que respondeu as questões em um formulário impresso.

A realização do piloto possibilitou a familiarização com a coleta de dados e um ajuste nas questões para maior clareza (as questões apresentadas no Apêndice B já estão em seu formato final).

Após o piloto e o ajuste no questionário, a pesquisa quantitativa teve continuidade com a aplicação do questionário para sete gestores da instituição objeto de estudo (perfis detalhados no Quadro 5). As respostas indicam que o questionário não apresentou problemas no preenchimento. Apenas uma gestora apontou dificuldades, que foram discutidas na entrevista devolutiva que foi executada com cada gestor. Posteriormente, foi realizada uma reunião com os gestores, a fim de apresentar e avaliar os principais resultados da pesquisa quantitativa.

Quadro 5 - Perfil dos gestores que responderam à pesquisa quantitativa

Gestor	Área	Experiência
1	Tecnologia da Informação	21 anos de atuação na área de Tecnologia da Informação, com foco em infraestrutura e segurança da informação.
2	Área Acadêmica	Experiência em atividades acadêmicas relacionadas à elaboração de questões.
3	Área Acadêmica	Experiência em atividades acadêmicas relacionadas à elaboração de questões.
4	Área Acadêmica	26 anos atuando em diagramação de provas e em secretaria acadêmica.
5	Produção	Gestão e supervisão de processos que envolvem manipulação e processamento físico de materiais em grandes volumes.
6	Gerência de Projetos	Gerência de projetos e da equipe.
7	Tecnologia da Informação	Mais de 10 anos como desenvolvedor de sistemas, coordenação do desenvolvimento dos sistemas de tecnologia da informação, de projetos de avaliação, coordenação e gerenciamento do processamento de concursos e vestibulares.

Fonte: Elaborado pela própria autora.

O questionário também foi enviado por *e-mail* para os quinze consultores que foram selecionados para a pesquisa qualitativa, para continuidade do estudo. Foram recebidas respostas de sete consultores (perfis 1, 2, 3, 4, 6, 7 e 10 detalhados no Quadro 4), representando uma taxa de retorno de 47%.

A análise dos fatores (Etapa A3) pode ser observada no Capítulo 4, com os resultados das pesquisas qualitativa e quantitativa.

4 DISCUSSÃO DE RESULTADOS

Neste capítulo será apresentada a discussão dos resultados das análises qualitativa e quantitativa, considerando os dados coletados.

4.1 ANÁLISE QUALITATIVA

Para análise das respostas do questionário (Apêndice A) foi utilizado o método de análise de conteúdo. Segundo Stemler (2001), esta é uma técnica sistemática e replicável para compactar muitas palavras de texto em menos categorias de conteúdo com base em regras explícitas de codificação. Assim, considerando o método adotado, buscou-se cotejar as respostas obtidas com as categorias identificadas na literatura, de modo a identificar o impacto e a relevância delas na visão dos consultores que estavam lidando com a implantação das normas.

O Quadro 6 foi elaborado com as respostas dos consultores às perguntas do questionário apresentado no Apêndice A, associadas a cada fator identificado na literatura.

Quadro 6 – Respostas sobre a integração das normas ISO 27001 e ISO 9001

Fator	Descrição
Modelo de Implantação	Fator não relatado pelos respondentes.
Recursos Humanos	Os funcionários de Tecnologia da Informação sentiram que perderam força e poder no processo de integração. Problemas com a capacitação do pessoal e compreensão da condução dos sistemas integrados. No início do processo foi percebida certa resistência com relação à perda de acesso a informações. Resistência do pessoal de segurança da informação. Resistência devido ao entendimento de que as normas deveriam ser mantidas separadas.
Disponibilidade e de Recursos	No início, a alocação de recursos foi feita de forma inapropriada por falta de conhecimento, porém com a maturidade e as ferramentas do sistema de gestão, a alocação se tornou mais previsível.
Questões Relativas às Normas	Um ponto de atenção destacado foi a necessidade de planejar a implantação do sistema criando regras e métodos que atendessem às normas ao mesmo tempo respeitando a cultura e as diretrizes da organização.
Integração das Normas	A integração não é um processo fácil, pois envolve todas as áreas da empresa.

Fonte: Elaborado pela própria autora.

De acordo com as respostas dos consultores, foi possível analisar que apesar de Rebelo, Santos e Silva (2015), Abad, Dalmau e Vilajosana (2014) e Heston e Phifer (2011) concordarem que as organizações que possuem um modelo estruturado de flexibilização e sistematização da integração, com orientações claras para apoiar o desenvolvimento do alinhamento e integração dos requisitos dos sistemas de gestão e que sejam mais rápidas e mais eficientes no processo de integração terão vantagem competitiva, os entrevistados não relataram a necessidade de um modelo para guiar a implantação dos sistemas de gestão integrados, quando foram questionados sobre as principais dificuldades enfrentadas durante o processo de integração ou o que poderia ter sido feito para reduzir as dificuldades.

Em relação ao envolvimento dos funcionários, os autores pesquisados mencionam problemas com a competência (REBELO; SANTOS; SILVA, 2015; SIMON; KARAPETROVIC; CASADESÚS, 2012) e resistência a mudança (ABAD; CABRERA; MEDINA-LEÓN, 2016; REBELO; SANTOS; SILVA, 2015; ZENG; SHI; LOU, 2007).

Adicionalmente, Simon, Karapetrovic e Casadesús (2012) afirmam que ao implementar um sistema de gestão integrado, as empresas devem administrar a motivação dos funcionários, pois quanto maior a motivação, melhor seria o resultado na redução de conflitos, propiciando melhoria na reação às mudanças trazidas pela integração. Fatores similares foram relatados pelos entrevistados ao citarem problemas com a capacitação do pessoal (Consultor 7) e resistência às mudanças devido à perda de acesso de informações (Consultor 3) ou ao entendimento que as normas deveriam ser mantidas separadas (Consultor 11).

A disponibilidade de recursos para a integração é vista por Rebelo, Santos e Silva (2015) como relevante na etapa de planejamento da integração e deve ser delineada por meio de um trabalho cuidadoso, a fim de responder efetivamente a todos os requisitos normativos. A falta de recursos pode levar a ineficiências e desvios. Um dos benefícios percebidos após a finalização do processo é a redução de custos, no entanto, Santos, Mendes e Barbosa (2011) evidenciaram maiores custos para implantar os sistemas de gestão simultaneamente do que individualmente.

Na pesquisa realizada para esta dissertação com os consultores, a dificuldade com a disponibilidade de recursos foi relatada pelo Consultor 9, que descreveu a alocação inapropriada no início do processo, mas que foi aperfeiçoada com a maturidade do sistema integrado. Os demais entrevistados não informaram tais dificuldades.

Zeng, Shi e Lou (2007) afirmam que o conhecimento sobre as normas de certificação tornou-se cada vez mais importante, não apenas para implementação, mas também para operação e manutenção de um sistema de gestão integrado. Este alicerce de conhecimento se

mostra relevante para minimizar o ponto de atenção destacado pelo Consultor 9, que se refere à necessidade de planejar a integração de forma que a norma seja atendida, mas respeitando a cultura e diretrizes da organização.

Em relação à integração das normas ISO 27001 e ISO 9001, dificuldades em encontrar denominadores comuns para diversas funções de negócios (REBELO; SANTOS; SILVA, 2015; OLARU *et al.*, 2014; OLIVEIRA, 2013; SIMON; KARAPETROVIC; CASADESÚS, 2012; ZENG; SHI; LOU, 2007; BECKMERHAGEN *et al.*, 2003) e o desaparecimento de identidades únicas de sistemas específicos de funções (BECKMERHAGEN *et al.*, 2003) são alguns obstáculos no caminho para a integração dos sistemas de gestão. Estas barreiras também foram apontadas pelo Consultor 11 quando relatou seu entendimento de que a integração não é simples, pois impacta todas as áreas da empresa, mostrando a necessidade de comprometimento em busca do objetivo e uma comunicação eficiente.

Nesta pesquisa, dos nove consultores entrevistados, sete trabalharam com a certificação integrada da ISO 27001 com a ISO 9001 e dois implantaram os dois sistemas de gestão separadamente.

Como medidas para minimizar os fatores percebidos na integração dos sistemas de gestão certificados, a sugestão dos consultores entrevistados seria orientar e conscientizar os funcionários sobre as fases do processo de integração bem como a necessidade de treinamento do pessoal envolvido no processo.

Foram percebidos pelos entrevistados diversos benefícios da integração das normas ISO 27001 e ISO 9001, tais como: aproveitamento dos recursos do sistema de gestão existente, alinhamento de objetivos, menor custo, menor alocação de recursos, otimização do tempo, base única de controle na gestão, permitindo a diminuição dos riscos na tomada de decisões estratégicas, melhor sinergia e comunicação interna, menor dificuldade na participação dos funcionários e redução do impacto do vazamento de informações.

4.2 ANÁLISE QUANTITATIVA

Com as respostas dos gestores da instituição objeto de estudo (perfis detalhados no Quadro 5) e dos consultores (perfis 1, 2, 3, 4, 6, 7 e 10 detalhados no Quadro 4) para o questionário do Apêndice B, foram realizados os cálculos matemáticos previstos no método AHP, por meio do *software* Microsoft Excel. A Tabela 1, a seguir disposta, apresenta o resumo dos julgamentos realizados pelos gestores e pelos consultores.

Tabela 1 – Resumo dos Julgamentos dos Gestores e dos Consultores

Critérios e Alternativas	Aggregation of Individual Judgments - AIJ (1) Agregação de Julgamentos Individuais								Aggregation of Individual Priorities - AIP (2) Agregação de Prioridades Individuais							
	%								%							
	Gestor 1	Gestora 2	Gestora 3	Gestora 4	Gestor 5	Gestora 6	Gestor 7	Prioridade	Consultor 1	Consultora 2	Consultor 3	Consultor 4	Consultor 6	Consultor 7	Consultor 10	Prioridade
Planejamento	14,9	33,3	33,3	86,0	13,0	71,4	13,0	37,0	11,1	8,9	86,0	71,4	89,0	15,3	46,7	55,5
Apoio	74,5	33,3	33,3	12,3	65,2	14,3	65,2	44,4	77,8	79,8	12,3	23,8	9,9	76,3	46,7	39,1
Operação	10,6	33,3	33,3	1,8	21,7	14,3	21,7	18,6	11,1	11,4	1,8	4,8	1,1	8,5	6,7	5,4
Modelo de Implantação	8,4	3,1	20,0	66,3	8,9	11,7	11,6	10,7	5,2	1,4	10,7	7,2	44,8	10,8	1,6	12,7
Recursos Humanos	58,8	27,5	20,0	9,8	9,4	2,3	28,5	18,5	8,1	9,8	74,9	36,2	5,0	34,4	9,5	25,0
Disponibilidade de Recursos	8,9	27,5	20,0	2,6	5,5	11,9	15,3	17,1	44,8	68,9	10,8	12,1	0,6	34,4	9,5	21,6
Questões Relativas às Normas	3,7	15,5	20,0	18,2	31,1	9,3	29,4	24,2	8,1	9,8	3,1	37,1	5,0	15,0	38,7	18,2
Integração das Normas	20,3	26,5	20,0	3,1	45,2	64,9	15,3	29,5	33,7	10,0	0,6	7,4	44,8	5,5	40,8	22,6

Fonte: Elaborado pela própria autora.

(1) A *Aggregation of Individual Judgments* (AIJ) é a abordagem a ser seguida quando especialistas participam de um mesmo grupo, neste caso, os gestores da instituição objeto de estudo, utilizando a média geométrica para sintetizar as matrizes de julgamentos (FORMAM; PENIWATI, 1998).

(2) A *Aggregation of Individual Priorities* (AIP) é a abordagem a ser seguida quando especialistas participam de grupos distintos, neste caso, os consultores especialistas, utilizando a média aritmética para sintetizar as matrizes de julgamentos (FORMAM; PENIWATI, 1998).

No julgamento dos gestores, o critério mais relevante é o Apoio com 44,4%, seguido pelos critérios Planejamento (37,0%) e Operação (18,6%). O critério Apoio está relacionado à determinação e provimento de recursos necessários para a implementação, manutenção e melhoria contínua dos sistemas de gestão, bem como à determinação da competência das pessoas, promoção da conscientização, comunicação e controle da informação documentada pertinente. Neste sentido, as entrevistas com os gestores evidenciam a importância dos critérios escolhidos.

Por exemplo, para o Gestor 1 “o planejamento é um critério importante, porém sem o provimento de recursos e o envolvimento das pessoas a integração dos sistemas de gestão se tornaria inviável ” e para o Gestor 5 “o apoio por meio do provimento de recursos é o critério mais importante, e a instituição deve usar a oportunidade de implantação para agregar melhorias em seu sistema de gestão e para aprimorar seu desempenho”. De acordo com o Gestor 7 “o critério mais relevante é o apoio, pois caso não exista engajamento e competência dos recursos humanos e da alta direção, o planejamento realizado não será concretizado e uma vez que exista comprometimento, o método de execução se torna menos relevante.”

O critério Planejamento refere-se à consideração de questões internas e externas que são relevantes para o propósito da instituição, às necessidades e as expectativas das partes interessadas, à determinação de riscos e oportunidades e ao estabelecimento dos objetivos para as funções e níveis relevantes.

Para a Gestora 4 “seguindo etapas sequenciais, o critério mais relevante é o de planejamento, em seguida o envolvimento das pessoas e provimento de recursos; consequentemente a operação fluirá da maneira desejada” e na análise da Gestora 6 “se o planejamento for feito contemplando todos os quesitos, a integração acontece. Os demais critérios complementam o trabalho e têm igual importância.”

No julgamento da Gestora 2 e da Gestora 3 todos os critérios têm a mesma relevância, pois é “importante planejar e ter o apoio de quem executa” (Gestora 2) e “um não pode acontecer sem a existência do outro.” (Gestora 3)

O Gestor 5 entendeu que é interessante a diferença de visão entre os gestores e os consultores, ao tomar conhecimento de que para os consultores o critério mais relevante é o Planejamento. De acordo com a análise dele “na instituição, para a integração o importante é a prática, ou seja, aplicar o entendimento da norma no processo e com isso perceber o quanto a norma ajuda. É proveitoso ir aprendendo e integrando durante o andamento do projeto.”

Em relação às alternativas, observa-se que para os gestores, o fator Integração das Normas é o que possui maior índice de importância com 29,5%, seguido pelos fatores

Questões Relativas às Normas (24,2%), Recursos Humanos (18,5%), Disponibilidade de Recursos (17,1%) e Modelo de Implantação (10,7%).

O fator Integração das Normas refere-se à efetiva realização das tarefas necessárias para o processo de integração dos sistemas de gestão. Sobre sua prioridade, os gestores fizeram os comentários relatados a seguir.

Para o Gestor 5 “no processo de integração, o fator mais importante é a execução das atividades, com o devido conhecimento das normas pelos envolvidos no processo” e para a Gestora 6 “considerando a equipe já à disposição da instituição objeto de estudo e tendo os recursos necessários, o fator mais importante é a efetiva execução das atividades de integração.”

O fator Questões Relativas às Normas, que está relacionado à importância do conhecimento sobre as normas e ao suporte dos organismos de certificação também teve destaque com 24,2%. Além da devolutiva do Gestor 5 citada anteriormente, podem ser destacadas mais algumas entrevistas a seguir.

Na análise da Gestora 2 “se os recursos humanos forem competentes e tiverem conhecimento das normas, a integração fluirá de maneira natural”, já para o Gestor 7 “seguir um modelo de implantação sem que os recursos humanos sejam competentes ou tenham conhecimento das normas, poderia levar a uma integração equivocada.”

Pontualmente, alguns valores que merecem destaque são o julgamento de 58,8% para o fator de Recursos Humanos pelo Gestor 1, 66,3% para Modelo de Implantação pela Gestora 4 e os valores iguais atribuídos a todas as alternativas pela Gestora 3. A seguir, podem ser observados os parâmetros que eles utilizaram para estas escolhas.

De acordo com o Gestor 1 “o fator mais relevante é o de recursos humanos, com foco no comprometimento das pessoas envolvidas”, para a Gestora 4 “ter o conhecimento da norma pode não ser suficiente. Ter um modelo de implantação norteia o trabalho” e para a Gestora 3 “todas as alternativas apresentadas são interdependentes e têm igual importância, pois uma não pode acontecer sem a existência da outra.”

No julgamento dos consultores, o critério mais relevante é o Planejamento com 55,5%, seguido pelos critérios Apoio (39,1%) e Operação (5,4%). Neste sentido, os consultores fizeram os seguintes comentários que evidenciam a importância dos critérios escolhidos.

Para o Consultor 3 “é fundamental que seja feito um planejamento para a integração e que este seja conhecido em profundidade”, para o Consultor 4 “o planejamento é o item chave de um bom projeto. Se for bem feito e abrangente, podem ser antecipados vários pontos que poderiam impactar negativamente na implantação com sucesso de um projeto” e para o

Consultor 6 “nada caminha se não houver planejamento, apoio, interesse e comprometimento.”

Em relação ao critério Apoio, para o Consultor 1 “um mal planejamento ou alguma falta ou falha de operação podem implicar em retrabalhos ou maior demora na integração. Já a falta de apoio pode implicar no abandono da integração”, para a Consultora 2 “o apoio ao sistema de gestão é fundamental para a integração”, já para o Consultor 7 “no momento do planejamento o apoio seria secundário, porém em relação à operação seria fundamental, pois é necessário ter pessoal competente e treinado para o sucesso da integração.”

No julgamento do Consultor 10 os critérios Planejamento e Apoio têm a mesma importância, pois “o planejamento é essencial para definir objetivos, etapas e prazos a serem gerenciados. Sem o apoio, o planejamento não será cumprido, portanto têm a mesma importância e se complementam.”

Em relação às alternativas, observa-se que para os consultores, o fator Recursos Humanos é o que possui o maior índice de importância com 25,0%, seguido pelos fatores Integração das Normas (22,6%), Disponibilidade de Recursos (21,6%), Questões Relativas às Normas (18,2%) e Modelo de Implantação 12,7%). Sobre esta prioridade, os gestores fizeram os comentários relatados a seguir.

O fator de Recursos Humanos está relacionado à existência de competência interna para lidar com sistemas de gestão integrados como um aspecto facilitador durante o processo.

De acordo com o Consultor 3 “a competência dos recursos humanos é o mais importante, pois é possível operar mesmo com um planejamento não tão bem detalhado.”, na opinião do Consultor 4 “a competência dos recursos humanos e o conhecimento que eles têm dos modelos normativos direciona melhores soluções ao processo organizacional, sem travar a criatividade necessária para agregar valor à integração”, já para o Consultor 7 “a competência dos recursos humanos e a disponibilidade de recursos sempre são importantes quando comparados a outros fatores.”

Pontualmente, alguns valores que merecem destaque com os consultores são o julgamento de 44,8% e 68,9% para o fator de Disponibilidade de Recursos pelo Consultor 1 e pela Consultora 2, 44,8% para Modelo de Implantação pelo Consultor 6 e 40,8% para Integração das Normas pelo Consultor 10. A seguir, podem ser observados os parâmetros que eles utilizaram para estas escolhas.

Para o Consultor 1 “no planejamento, não se espera que os envolvidos já tenham conhecimentos e habilidades específicas, mas que haja plena disponibilidade de recursos e que sejam realizadas atividades de integração. Normalmente há alguém, interno ou contratado,

que conduz o planejamento”, para a Consultora 2 “a disponibilidade dos recursos demonstra o apoio da alta direção ao processo. A partir desse apoio, as demais atividades acontecerão.”

De acordo com o Consultor 6 “planejamento, interesse e capacidade dos envolvidos, são premissas fundamentais. Recursos virão quando demonstrarmos a importância do que pretendemos” e para o Consultor 10 “o planejamento deverá se basear nos requisitos normativos para definir as atividades de integração e a competência dos recursos humanos é fundamental. O apoio é imprescindível para a integração, pois os requisitos devem ser bem entendidos para que não haja conflitos. Para a operação, a realização das atividades dependerá da competência dos recursos humanos. Nesse ponto o conhecimento da norma já foi utilizado no planejamento.”

4.3 ANÁLISE FINAL

Na revisão de literatura foi apontado que, para as empresas que têm um modelo de implantação que permita guiar a integração das normas, o processo apresenta maiores chances de sucesso, porém este fator não foi apontado como relevante na pesquisa qualitativa e, tampouco na pesquisa quantitativa realizada com os gestores e com os consultores. Em ambas, este foi o fator que teve a menor atribuição de importância.

De acordo com o relato dos gestores que participaram da pesquisa, o fluxo de atividades das áreas que eles coordenam é extenso e os requisitos das normas não são de fácil interpretação, consequentemente a implantação de maneira autônoma seria desafiadora, ainda que houvesse um modelo guiando o processo.

Além disto, a figura de um consultor é vista como imprescindível na integração de sistemas de gestão, devido: (i) à sua experiência prática e prévia (muitas vezes como auditor em organismos de certificação), (ii) à sua capacidade de elaborar um diagnóstico da situação atual da organização, buscando alternativas adequadas às diferentes instituições, (iii) e também a sua constante atualização quando da revisão das normas.

Os gestores apontaram como motivadores para a contratação de um consultor a redução do tempo de implantação das normas e um aumento da confiança durante o processo de auditoria e reforçaram que não sentiriam os benefícios, sem o acompanhamento de um consultor, mesmo que estivessem seguindo um modelo de integração.

Para os consultores, ter um modelo de implantação a ser seguido por diversas organizações poderia representar uma diminuição na necessidade da sua *expertise*. Além disso, as empresas ao utilizarem o mesmo modelo, sem a participação de um consultor, poderiam ter

uma implantação inadequada às suas necessidades e desatualizada no que se refere às revisões das normas. Caso houvesse a atuação de um consultor, bem como a utilização de um modelo de implantação, talvez houvesse uma limitação da criatividade dele em explorar as soluções mais adequadas para cada tipo de organização, o poderia influenciar nos resultados almejados pela empresa na implantação e manutenção do sistema de gestão.

Em relação ao fator Integração das Normas, apontado como de maior importância para os gestores, de acordo com Santos *et al.* (2013), a melhor maneira de iniciar a integração dos sistemas de gestão é procurar pontos em comum e assegurar que o maior número possível de processos e procedimentos documentados seja compartilhado entre cada um deles. A identificação de áreas comuns e os requisitos dos sistemas de gestão versus as correspondências e semelhanças entre eles potencializa uma metodologia para desenvolver e estruturar a integração.

Outro fator considerado relevante para os gestores foi o fator Questões Relativas às Normas, que se refere à importância do conhecimento sobre as normas e ao suporte dos organismos de certificação. Considerando o entendimento de Simon, Karapetrovic e Casadesús (2012) dificuldades com as normas expõem um efeito negativo nos recursos de documentação, demonstrando uma forte relação entre o processo de implementação de padrões e o nível de integração da documentação nas empresas.

Adicionalmente, Beckmerhagen *et al.* (2003) também alertam para o fato de que a estrutura de alto nível das normas pode facilitar a integração, mas uma questão complicada é a aplicação real dos requisitos integrados internamente. Dificuldades organizacionais e de comunicação, percepções de diferenças nos requisitos padrão, problemas no alinhamento de objetivos, processos e recursos de gerenciamento, diferentes partes interessadas, bem como percepções de redução de tamanho são alguns obstáculos que as organizações que se propõem à integração de sistemas de gestão certificados estão susceptíveis.

Na pesquisa qualitativa e na pesquisa quantitativa com os consultores foi dado maior destaque para o fator Recursos Humanos. Zeng, Shi e Lou (2007) explicam que os recursos humanos, e não os recursos financeiros, são o principal fator que podem afetar a implementação do sistema de gestão integrado. O conhecimento necessário para os recursos humanos é relevante para a implantação e a manutenção do sistema de gestão integrado.

Em consonância com a afirmação anterior, o fator Disponibilidade de Recursos foi apontado em terceiro lugar na análise dos consultores e em quarto lugar na análise dos gestores, na pesquisa quantitativa.

Para Boon *et al.* (2018) difundir e desenvolver o conhecimento dos recursos humanos aumenta o vínculo entre a equipe e afeta o positivamente a eficiência do negócio. Empresas que buscam uma efetiva implantação dos sistemas de gestão, promovem a qualificação dos funcionários envolvidos por meio de treinamentos (PARRA-LÓPEZ *et al.*, 2016; HUO; HAN; PRAJOGO; 2014).

Após análise dos dados dispostos da Tabela 1 e das justificativas dos entrevistados, notou-se que embora a prioridade global dos critérios tenha obtido valores diferentes para os gestores e para os consultores, no julgamento individual as atribuições foram divididas de maneira similar para os critérios Apoio e Planejamento. Além disso, foi possível perceber a equivalência nos comentários que motivaram as escolhas.

Ainda neste sentido, constatou-se a compatibilidade na análise realizada pelos gestores e pelos consultores em relação à importância do envolvimento das pessoas no processo de integração das normas. Os gestores escolheram o critério Apoio que se refere ao provimento de recursos e competência dos indivíduos e os consultores escolheram o fator Recursos Humanos que está relacionado à existência de competência interna para lidar com sistemas de gestão integrados como um facilitador durante o processo.

Por fim, o fator Integração das Normas, que foi escolhido como o mais relevante na análise dos gestores, foi o fator apontado em segundo lugar como importante para os consultores, demonstrando também seu valor no processo de integração.

4.4 IMPLICAÇÕES PRÁTICAS

Conforme os dados levantados e registrados na presente dissertação, destacam-se os seguintes apontamentos de ordem prática:

Para a Consultora 2, que está orientando o processo de integração na instituição objeto de estudo “é importante saber o resultado da priorização dos gestores para direcionar o trabalho.” O fator Integração das Normas, que foi considerado o mais relevante para os gestores “demonstra o engajamento deles na realização das tarefas necessárias para a integração.”

Para o Gestor 7 “o levantamento dos fatores ajuda a identificar onde colocar os esforços e ter a norma ISO 9001 previamente implantada na organização facilita o trabalho, pois a base das duas normas é a mesma. A identificação dos fatores realizada de acordo com um estudo acadêmico e corroborada com a opinião dos consultores agrega experiência para a instituição.”

Foi verificado que o cronograma para integração da ISO 27001 com a ISO 9001 da instituição objeto de estudo possui 29 atividades englobando diagnóstico inicial, planejamento, treinamentos, auditorias e demais atividades. Tendo como referência o resultado do julgamento dos gestores indicando a relevância de 29,5% para o fator Integração das Normas, foi possível priorizar 6 atividades, sobre as quais merecem destaque a integração do manual de gestão, a definição de responsabilidades e autoridades e a confecção da política e dos objetivos do sistema de gestão integrado.

Uma particularidade da instituição objeto de estudo é que seu estatuto social prevê a rotatividade da alta direção, cujo mandato é de 4 anos (permitindo-se reconduções). Neste sentido, considera-se especialmente importante que a instituição adote sistemas de gestão certificados que contribuam para diminuir esta variabilidade e possibilitem a manutenção do conhecimento organizacional na forma de informação documentada, tais como políticas, procedimentos, manuais e registros e na forma não documentada, tais como conhecimento de posse das pessoas (competências prévias e adquiridas) e conhecimento advindo das relações da instituição com provedores externos e outras partes interessadas.

Durante a reunião realizada para apresentação e análise dos resultados da pesquisa, verificou-se que é consenso entre os gestores que a padronização, os procedimentos e o registro de atividades são fundamentais para apoiar o processo de mudança que a instituição atravessa a cada alteração dos membros da alta direção. Adicionalmente, os gestores relataram fatores positivos identificados com esta mudança sazonal, tais como: renovação, sugestões de melhoria, novas visões e estratégias.

Na experiência do Gestor 7, foi percebido ao longo dos anos que os projetos que contaram com o apoio da alta direção foram os que obtiveram sucesso. Para ele “alguns projetos que abalam o conforto dos funcionários podem gerar resistência e é fundamental o direcionamento promovido pela alta direção para que os projetos prossigam.” Esta opinião é compartilhada pela Gestora 2 e pela Gestora 6.

Esta dissertação apresenta algumas ideias para os gestores sobre as implicações práticas identificadas na revisão da literatura e durante as pesquisas realizadas. Por meio da priorização dos fatores, é possível prover a eles um meio de entenderem o seu papel no processo de integração das normas ISO 27001 e ISO 9001, bem como a visão dos seus colegas. Este trabalho acadêmico também apresenta sugestões para facilitar o projeto, bem como destaca um ponto importante: que os gestores deixem claro para os envolvidos no processo que a integração e a certificação são os objetivos da instituição.

Em seguida, é preciso procurar pontos em comum entre as duas normas, agregar o máximo de atividades possível, criando um conjunto de políticas para orientar o trabalho. Para o sucesso é necessário capacitar os envolvidos e mantê-los engajados e cientes de todas as etapas. Por fim, é fundamental que a alta direção esteja comprometida, provendo recursos, comunicando objetivos e motivando os funcionários.

Segundo o julgamento do Gestor 5 o fator mais relevante foi a Integração das Normas e saber que na prioridade global a observação dos colegas reflete o mesmo resultado reforça esta indicação, pois em sua análise “realizando as atividades, fica mais fácil de compreender e solidificar as principais diretrizes que a norma exige do gestor”. Para ele, “a priorização da atividade de integração do manual de gestão é uma das mais importantes, visto que se ela for feita de maneira bem feita e planejada, a implantação dos demais itens ocorrerá de maneira menos complexa”.

5 CONCLUSÃO

Esta pesquisa identificou (Quadro 2) e priorizou (Tabela 1) os fatores que influenciam a integração do sistema de gestão de segurança da informação com o sistema de gestão da qualidade, tomando como base o julgamento de consultores especialistas na implantação das normas ISO 27001 e ISO 9001 e dos gestores que participam da integração das referidas normas em uma instituição prestadora de serviços de concursos, vestibulares e avaliações educacionais.

Os resultados indicam que os consultores e os gestores pensam de maneira diferente e complementar. A Integração das Normas foi identificada como o fator mais relevante para os gestores da instituição objeto de estudo, pois a efetiva realização das atividades, facilita a compreensão das diretrizes da norma. De acordo com a análise dos consultores, o fator mais relevante foram aqueles ligados aos Recursos Humanos, pois a competência dos envolvidos no processo proporciona mais efetividade na execução das tarefas e é necessário o engajamento para a obtenção de sucesso na integração.

Como contribuição acadêmica, este estudo permite colaborar com a literatura atual, oferecendo mais subsídios para entender e discutir as questões relativas à integração de sistemas de gestão de segurança da informação e gestão da qualidade.

Como contribuição prática para a instituição objeto de estudo, esta pesquisa permitiu entender a relevância dos fatores críticos na opinião dos gestores que participam da integração das normas ISO 27001 e ISO 9001 e com isso prover aos gestores informações adicionais que auxiliem em sua atuação no processo de integração. Além disso, foi possível direcionar o trabalho da consultoria e ajustar o cronograma de integração.

Outras organizações também podem se beneficiar desta priorização, utilizando este trabalho como apoio, de forma preventiva com a antecipação dos principais desafios que poderão ser enfrentados na integração dos sistemas de gestão de segurança da informação e da qualidade.

Considerando os fatores que foram identificados e analisados nesta pesquisa, como hipóteses em trabalhos futuros, sugere-se efetuar o estudo em diferentes segmentos de mercado e em diferentes contextos geográficos, o que pode permitir uma comparação entre os resultados e a identificação de novos desafios que possam impactar a integração de sistemas de gestão certificados. As conclusões desta pesquisa estão limitadas ao grupo de respondentes (gestores e consultores), mas revelam informações que podem ser investigadas estatisticamente no futuro.

REFERÊNCIAS

- ABAD, J.; CABRERA, H. R.; MEDINA-LEÓN, A. An analysis of the perceived difficulties arising during the process of integrating management systems. **Journal of Industrial Engineering and Management**, Barcelona, v. 9, n. 3, p. 860-878, 2016. Disponível em: http://v09-i03-p0860_1989-8955-1-PB.pdf. Acesso em: 07 set. 2019.
- ABAD, J.; DALMAU, I.; VILAJOSANA, J. Taxonomic proposal for integration levels of management systems based on empirical evidence and derived corporate benefit. **Journal of Cleaner Production**, Amsterdam, v. 78, p. 164-173, 2014. Disponível em: <https://doi.org/10.1016/j.jclepro.2014.04.084>. Acesso em: 06 jan. 2019.
- ABUSAAD, B. *et al.* Implementation of ISO 27001 in Saudi Arabia - obstacles, motivations, outcomes and lessons learned. *In: AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE*, 9., 2011, Perth Western Australia. **Proceedings** [...]. Perth Western Australia: Research Online Institutional Repository, 2011. Disponível em: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1104&context=ism>. Acesso em: 18 set. 2019.
- ALMEIDA, D.; PRADHAN, N.; MUNIZ JÚNIOR, J. Assessment of ISO 9001:2015 implementation factors based on AHP: case study in Brazilian automotive sector. **International Journal of Quality & Reliability Management**, Bradford, v. 35, n. 7, 2017. Disponível em: <https://emeraldinsight.com/doi/full/10.1108/IJQRM-12-2016-0228>. Acesso em: 12 jan. 2019.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 9001**: sistemas de gestão da qualidade: requisitos. Rio de Janeiro: ABNT, 2015.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.
- BECKMERHAGEN, I. *et al.* Integration of management systems: focus on safety in the nuclear industry. **International Journal of Quality & Reliability Management**, Bradford, v. 20, n. 2, p. 210-228, 2003. Disponível em: <https://www.emeraldinsight.com/doi/full/10.1108/02656710310456626>. Acesso em: 05 mar. 2019.
- BERNARDO, M. *et al.* Benefits of management systems integration: a literature review. **Journal of Cleaner Production**, Amsterdam, v. 94, p. 260-267, 2015. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0959652615000803?via%3Dihub>. Acesso em: 12 maio 2019.
- BERNARDO, M. *et al.* How integrated are environmental, quality and other standardized management systems? An empirical study. **Journal of Cleaner Production**, Amsterdam, v. 17, n. 8, p. 742-750, 2008. Disponível em: <https://doi.org/10.1016/j.jclepro.2008.11.003>. Acesso em: 06 jan. 2019.
- BOEHMER, W. Cost-benefit trade-off analysis of an ISMS based on ISO 27001. *In: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY*,

2009, Fukuoka. **Proceedings** [...]. Fukuoka: IEEE - Institute of Electrical and Electronics Engineers, 2009. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5066500>. Acesso em: 02 mar. 2019.

BOZÓKI, S.; FÜLÖP, J.; RÓNYAI, L. Incomplete pairwise comparison matrices in multi-attribute decision making. *In*: 2009 IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL ENGINEERING AND ENGINEERING MANAGEMENT, Hong Kong. **Proceedings** [...]. Hong Kong: IEEE - Institute of Electrical and Electronics Engineers, 2009. Disponível em: <https://ieeexplore.ieee.org/document/5373064>. Acesso em: 21 jun. 2020.

BRASÍLIA. **Lei nº 13.709**, de 14 de agosto de 2018: lei geral de proteção de dados pessoais (LGPD). Dispõe sobre a proteção de dados pessoais, cria a Autoridade Nacional de Proteção de Dados e dá outras providências. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: Acesso em 05 out. 2019.

BOON, C. *et al.* Integrating strategic human capital and strategic human resource management. **The International Journal of Human Resource Management**, London, v. 29, n. 1, 2018. Disponível em: <https://doi.org/10.1080/09585192.2017.1380063>. Acesso em: 10 maio 2020.

BRIOZO, R.A.; MUSETTI, M.A. Método multicritério de tomada de decisão: aplicação ao caso da localização espacial de uma unidade de pronto atendimento – UPA 24 h. **Gestão & Produção**, São Carlos, v. 22, n. 4, p. 805-819, 2015. Disponível em: <http://dx.doi.org/10.1590/0104-530X975-13>. Acesso em: 27 jan. 2020.

BRITVIC, J.; BLAZEVIC, Z.; VLAINIC, D. Application of integrated management systems in entrepreneurship. **Economy of Eastern Croatia Yesterday, Today, Tomorrow**, Croatia, v. 3, p. 594-603, 2014. Disponível em: <http://www.efos.unios.hr/repec/osi/eecytt/PDF/EconomyofeasternCroatiaYesterdayTodayTomorrow03/eecytt0359.pdf>. Acesso em: 18 maio 2019.

BRITVIC, J.; KOVACEVIC, A. P.; CINGEL, M. Integration possibilities of ISO 9001:2008 quality management system with ISO 27001:2010 information security management system. **Economy of Eastern Croatia Yesterday, Today, Tomorrow**, Croatia, v. 2, p. 368-373, 2013. Disponível em: <http://www.efos.unios.hr/repec/osi/eecytt/PDF/EconomyofeasternCroatiaYesterdayTodayTomorrow02/eecytt0242.pdf>. Acesso em: 05 maio 2019.

CARVALHO, C.; MARQUES, E. Adapting ISO 27001 to a public institution. *In*: IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES, 14., 2019, Coimbra. **Proceedings** [...]. Coimbra: IEEE - Institute of Electrical and Electronics Engineers, 2019. Disponível em: <https://ieeexplore.ieee.org/document/8760870>. Acesso em: 15 ago. 2019.

FAZENDA, R.; FAGUNDES, L. Análise dos desafios para estabelecer e manter sistema de gestão de segurança da informação no cenário brasileiro. *In*: BRAZILIAN SYMPOSIUM ON INFORMATION SYSTEM, 11., 2015, Goiania. **Anais** [...]. Goiania: Association for Information Systems AIS Electronic Library (AISeL), 2015. Disponível em: <http://aisel.aisnet.org/sbis2015/60>. Acesso em: 03 nov. 2018.

FOMIN, V. V.; VRIES, H. J.; BARLETTE, Y. ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. *In: EUROMOT EUROPEAN CONFERENCE ON MANAGEMENT OF TECHNOLOGY*, 3., 2008, Nice. **Proceedings** [...]. Nice: International Association for Management of Technology, 2008. Disponível em: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption. Acesso em: 09 jun. 2019.

FORMAN, E.; PENIWATI, K. Aggregating individual judgments and priorities with the analytic hierarchy process. **European Journal of Operational Research**, Amsterdam, v. 108, n. 1, p. 165-169, 1998. Disponível em: [https://doi.org/10.1016/S0377-2217\(97\)00244-0](https://doi.org/10.1016/S0377-2217(97)00244-0). Acesso em: 05 abr. 2020.

FORZA, C. Survey research in operations management: a process-based perspective. **International Journal of Operations & Production Management**, Bradford, v. 22, n. 2, p. 152-194, 2002. Disponível em: <http://www.emeraldinsight.com/0144-3577.htm>. Acesso em: 19 ago. 2019.

GASPAR, M. L.; POPESCU, S. G. Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company. **Acta Technica Napocensis**, Cluj-Napoca, v. 61, n. Special, 2018. Disponível em: <https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054>. Acesso em: 22 ago. 2019.

HARKER, P. T. Incomplete pairwise comparisons in the analytic hierarchy process. **Mathematical Modelling**, New York, v. 9, n.11, p. 837-848, 1987. Disponível em: [https://doi.org/10.1016/0270-0255\(87\)90503-3](https://doi.org/10.1016/0270-0255(87)90503-3). Acesso em: 21 jun. 2020.

HESTON, K. M.; PHIFER, W. The multiple quality models paradox: how much 'best practice' is just enough? **Journal of Software Maintenance and Evolution: Research and Practice**, Nova Jersey, v. 23, p. 517-531, 2011. Disponível em: <https://doi.org/10.1002/smr.481>. Acesso em: 16 maio 2019.

HOY, Z.; FOLEY, A. A structured approach to integrating audits to create organizational efficiencies: ISO 9001 and ISO 27001 audits. **Total Quality Management & Business Excellence**, London, v. 26, n. 5-6, p. 690-702, 2015. Disponível em: <https://doi.org/10.1080/14783363.2013.876181>. Acesso em: 05 maio 2019.

HSU, C.; WANG, T.; LU, A. The impact of ISO 27001 certification on firm performance. *In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES*, 49., 2016, Koloa. **Proceedings** [...]. Koloa: IEEE - Institute of Electrical and Electronics Engineers, 2016. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7427787>. Acesso em: 02 mar. 2019.

HUO, B.; HAN, Z.; PRAJOGO, D. The effect of ISO 9000 implementation on flow management. **International Journal of Production Research**, London, v. 52, n. 21, 2014. Disponível em: <https://doi.org/10.1080/00207543.2014.895063>. Acesso em: 10 maio 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **The ISO/IEC directives, part 1**: consolidated ISO supplement - procedures specific to ISO. Disponível em:

https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/Consolidated_ISO-IEC_Part-1_%28E%29_2020.pdf?nodeid=21201080&vernum=-2. Acesso em 18 maio 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **The ISO survey of management system standard certifications**. Disponível em: <https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1>. Acesso em 05 out. 2019.

ISHIZAKA, A.; NEMERY, P. **Multi-criteria decision analysis: methods and software**. Chichester: John Wiley & Sons, Ltd, 2013. 296 p.

KAFEL, P.; CASADESÚS, M. The order and level of management standards implementation: changes during the time. **The TQM Journal**, Spain, v. 28, n. 4, p. 636-647, 2016. Disponível em: <https://www.emeraldinsight.com/doi/full/10.1108/TQM-02-2015-0027>. Acesso em: 02 jan. 2019.

KARAPETROVIC, S.; CASADESÚS, M. Implementing environmental with other standardized management systems: scope, sequence, time and integration. **Journal of Cleaner Production**, Catalonia, v. 17, n. 5, p. 533-540, 2009. Disponível em: <https://doi.org/10.1016/j.jclepro.2008.09.006>. Acesso em: 16 maio 2019.

KHAJOUEI, H.; KAZEMI, M.; MOOSAVIRAD, S. H. Ranking information security controls by using fuzzy analytic hierarchy process. **Information Systems and e-Business Management**, Berlin, v. 15, n. 1, p. 1-19, 2017. Disponível em: <https://link.springer.com/article/10.1007/s10257-016-0306-y>. Acesso em: 16 maio 2019.

LONGRAS, A. *et al.* On the track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations. In: INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS, 2018, Madeira. **Proceedings** [...]. Madeira: IEEE - Institute of Electrical and Electronics Engineers, 2018. Disponível em: DOI: 10.1109/IS.2018.8710558. Acesso em: 11 ago. 2019.

LOPES, I. M.; GUARDA, T.; OLIVEIRA, P. How ISO 27001 can help achieve GDPR compliance. In: IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES, 14., 2019, Coimbra. **Proceedings** [...]. Coimbra: IEEE - Institute of Electrical and Electronics Engineers, 2019. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8760937>. Acesso em: 22 ago. 2019.

MAEKAWA, R.; CARVALHO, M.; OLIVEIRA, O. Um estudo sobre a certificação ISO 9001 no Brasil: mapeamento de motivações, benefícios e dificuldades. **Gestão & Produção**, São Carlos, v. 20, n. 4, p. 763-779, 2013. Disponível em: http://www.scielo.br/pdf/gp/2013nahead/aop_gp0334_ao.pdf. Acesso em: 06 out. 2018.

MAJERNIK, M. *et al.* Design of integrated management systems according to the revised ISO standards. **Polish Journal of Management Studies**, Czestochowa, v. 15, n.1, 2017. Disponível em: <https://pjms.zim.pcz.pl/resources/html/article/details?id=156625>. Acesso em: 02 jan. 2019.

MARTINS, R. A. Abordagens quantitativa e qualitativa. In: MIGUEL, P. A. C. *et al.* (coord.). **Metodologia de pesquisa em engenharia de produção e gestão de operações**. 2. ed. Rio de

Janeiro: Elsevier, 2012. cap. 3, p. 47-63.

MESQUIDA, A. *et al.* Sistema de gestión integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. **Revista Española de Innovación, Calidad e Ingeniería del Software**, Madrid, v. 6, n. 3, p. 25-34, 2010. Disponível em: <https://www.redalyc.org/html/922/92218768002/>. Acesso em: 13 dez. 2018.

MESQUIDA, A.; MAS, A. Integrating IT service management requirements into the organizational management system. **Computer Standards & Interfaces**, Amsterdam, v. 37, p. 80-91, 2015. Disponível em: <https://doi.org/10.1016/j.csi.2014.06.005>. Acesso em: 10 ago. 2019.

MIGUEL, P. A. C. *et al.* Desafios para a metodologia de pesquisa em engenharia de Produção. In: OLIVEIRA, V. F.; CAVENAGHI, V.; MÁSCULO, F. S. (org.). **Tópicos emergentes e desafios metodológicos em engenharia de produção: casos, experiências e proposições**. Rio de Janeiro: Associação Brasileira de Engenharia de Produção, 2009. v. 2, cap.1, p. 17-69.

MUELLER, I.; HAN, J.; SCHNEIDER, J.-G. *et al.* Idea: a reference platform for systematic information security management tool support. In: INTERNATIONAL SYMPOSIUM ON ENGINEERING SECURE SOFTWARE AND SYSTEMS, 3., 2011, Madrid. **Proceedings** [...]. Madrid: Springer-Verlag Berlin Heidelberg, 2011. Disponível em: [https://researchbank.swinburne.edu.au/file/6c554aa4-c49f-4f18-a8fa-37c7d64a333a/1/PDF%20\(Accepted%20manuscript\).pdf](https://researchbank.swinburne.edu.au/file/6c554aa4-c49f-4f18-a8fa-37c7d64a333a/1/PDF%20(Accepted%20manuscript).pdf). Acesso em: 11 maio 2019.

MUNIZ JÚNIOR, J. *et al.* Knowledge sharing in the automotive sector: a comparative study of Chinese and Brazilian firms. **Production = Produção**, São Paulo, v. 29, 2019. Disponível em: <http://dx.doi.org/10.1590/0103-6513.20180084>. Acesso em: 23 set. 2019.

NUNHES, T. V.; MOTTA, L. C. F.; OLIVEIRA, O. J. Evolution of integrated management systems research on the journal of cleaner production: identification of contributions and gaps in the literature. **Journal of Cleaner Production**, Amsterdam, v. 139, p. 1234-1244, 2016. Disponível em: <https://doi.org/10.1016/j.jclepro.2016.08.159>. Acesso em: 06 jan. 2019.

OLARU, M. *et al.* Establishing the basis for development of an organization by adopting the integrated management systems: comparative study of various models and concepts of integration. In: WORLD CONFERENCE ON BUSINESS, ECONOMICS AND MANAGEMENT, 2., 2014, Antalya. **Proceedings** [...]. Antalya: Procedia - Social and Behavioral Sciences, 2014. Disponível em: <https://doi.org/10.1016/j.sbspro.2013.12.531>. Acesso em: 06 jan. 2019.

OLIVEIRA, J. O. Guidelines for the integration of certifiable management systems in industrial companies. **Journal of Cleaner Production**, Amsterdam, v. 57, p. 124-133, 2013. Disponível em: <https://doi.org/10.1016/j.jclepro.2013.06.037>. Acesso em: 20 abr. 2019.

PARRA-LÓPEZ, C. *et al.* ISO 9001 implementation and associated manufacturing and marketing practices in the olive oil industry in southern Spain. **Food Control**, Guildford, v. 62, p. 23-31, 2016. Disponível em: <https://doi.org/10.1016/j.foodcont.2015.09.038>. Acesso em: 10 maio 2020.

PINTO, S.; DE CARVALHO, M.; HO, L. Implementação de programas de qualidade: um

survey em empresas de grande porte no Brasil. **Gestão & Produção**, São Carlos, v. 13, n. 2, p. 191-203, 2006. Disponível em: <https://doi.org/10.1590/S0104-530X2006000200003>. Acesso em: 11 mar. 2019.

PROENÇA, D.; BORBINHA, J. Information security management systems - a maturity model based on ISO/IEC 27001. **Business Information Systems**, Genebra, p.102-114, 2018. Disponível em: http://link-springer-com-443.webvpn.fjmu.edu.cn/chapter/10.1007%2F978-3-319-93931-5_8. Acesso em: 09 jun. 2019

REA, L. M.; PARKER, R. A. **Design and conducting survey research**: a comprehensive guide. 4th ed. San Francisco: Jossey-Bass, 2005. 332p.

REBELO, M. F.; SANTOS, G.; SILVA, R. Integration of standardized management systems: a dilemma? **Systems MDPI**, Basel, p. 46-59, 2015. Disponível em: <https://www.mdpi.com/2079-8954/3/2/45>. Acesso em: 03 nov. 2018.

RIENZO, A. *et al.* Evaluation of the degree of knowledge and implementation of information security management systems, based of the NCh-ISO 27001 standard, in health institutions. *In*: IEEE INTERNATIONAL CONFERENCE ON AUTOMATION, CONGRESS OF THE CHILEAN ASSOCIATION OF AUTOMATIC CONTROL, 23., Concepcion, 2018. **Proceedings** [...]. Concepcion: IEEE - Institute of Electrical and Electronics Engineers, 2018. Disponível em: 10.1109/ICA-ACCA.2018.8609761. Acesso em: 22 ago. 2019.

RIGON, E. A; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. **Revista Eletrônica de Sistemas de Informação**, Campo Largo, v. 12, p. 1-19, 2013. Disponível em: <https://search.proquest.com/docview/1446332954/fulltextPDF/A24C319F028E4D2EPQ/1?acountid=8112>. Acesso em: 09 jun. 2019

ROSA, G. M.; TOLEDO, J. C. Proposta de framework para apoio do processo de integração de sistemas de gestão normalizados. *In*: SIMPÓSIO DE ENGENHARIA DA PRODUÇÃO, 22., Bauru, 2015. **Proceedings** [...]. Bauru: [s.n.], 2015. Disponível em: https://www.researchgate.net/profile/Germano_Rosa/publication/301289783_PROPOSTA_DE_FRAMEWORK_PARA_APOIO_DO_PROCESSO_DE_INTEGRACAO_DE_SISTEMAS_DE_GESTAO_NORMALIZADOS/links/570fa6f808ae38897ba2c9a9.pdf. Acesso em: 23 ago. 2020.

SAATY, T. L. The modern science of multicriteria decision making and its practical applications: the AHP/ANP approach. **Operations Research**, Baltimore, v. 61, n. 5, p. 1101-1118, 2013. Disponível em: <https://doi.org/10.1287/opre.2013.1197>. Acesso em: 25 jan. 2020.

SANTOS, G. *et al.* The main benefits associated with health and safety management systems certification in Portuguese small and medium enterprises post quality management system certification. **Safety Science**, Amsterdam, v. 51, n. 1, 2013. Disponível em: <https://doi.org/10.1016/j.ssci.2012.06.014>. Acesso em: 06 maio 2020.

SANTOS, G.; MENDES, F.; BARBOSA, J. Certification and integration of management systems: the experience of Portuguese small and medium enterprises. **Journal of Cleaner Production**, Amsterdam, v. 19, n. 17-18, p. 1965-1974, 2011. Disponível em: <https://doi.org/10.1016/j.jclepro.2011.06.017>. Acesso em: 07 set. 2019.

SALOMON, V. A. P.; MARINS, F.; DUDUCH, M. Tomada de decisões múltiplas aplicada à seleção de fornecedores de equipamentos de uma linha de montagem em uma fábrica de autopeças. **Pesquisa Operacional para o Desenvolvimento**, Rio de Janeiro, v. 1, n. 3, p. 208-217, 2009. Disponível em: <https://www.researchgate.net/publication/242247071>. Acesso em: 25 jan. 2020.

SALOMONE, R. Integrated management systems: experiences in Italian organizations. **Journal of Cleaner Production**, Amsterdam, v. 16, n. 16, p. 1786-1806, 2008. Disponível em: <https://doi.org/10.1016/j.jclepro.2007.12.003>. Acesso em: 07 set. 2019.

SIMON, A.; KARAPETROVIC, S.; CASADESÚS, M. Difficulties and benefits of integrated management systems. **Industrial Management & Data Systems**, Wembley, v. 112, n. 5, p.828-846, 2012. Disponível em: <https://www.emeraldinsight.com/doi/abs/10.1108/02635571211232406>. Acesso em: 26 fev. 2019.

STEMLER, S. E. An overview of content analysis. **Practical Assessment, Research & Evaluation**, Amherst, 2001. Disponível em https://www.researchgate.net/publication/269037805_An_Overview_of_Content_Analysis. Acesso em: 13 jul. 2019.

TARÍ, J. J.; MOLINA-AZORÍN, J. F.; HERAS, I. Benefits of the ISO 9001 and ISO 14001 standards: a literature review. **Journal of Industrial Engineering and Management**, Novi Sadi, v. 5, n. 2, p. 297-322, 2012. Disponível em: <http://dx.doi.org/10.3926/jiem.488>. Acesso em: 07 set. 2019.

TATIARA, R. *et al.* Analysis of factors that inhibiting implementation of information security management system (ISMS) based on ISO 27001. *In: INTERNATIONAL CONFERENCE ON COMPUTING AND APPLIED INFORMATICS*, 2., 2018, Medan. **Proceedings [...]**. Medan: Journal of Physics, 2018. Disponível em: <http://iopscience.iop.org/article/10.1088/1742-6596/978/1/012039/meta>. Acesso em: 04 nov. 2018.

TRAMARICO, C. L. *et al.* Analytic hierarchy process and supply chain management: a bibliometric study. *In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY AND QUANTITATIVE MANAGEMENT*, 3., 2015, Rio de Janeiro. **Proceedings [...]**. Rio de Janeiro: **Procedia Computer Science**, v. 55, p. 441-450, 2015. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050915014805>. Acesso em: 02 nov. 2019.

TRAMARICO, C. L.; SALOMON, V. A. P.; MARINS, F. A. S. Multi-criteria analysis of advanced planning system implementation. *In: INTERNATIONAL CONFERENCE ON INDUSTRIAL ENGINEERING AND OPERATIONS MANAGEMENT*, 2017, Bogota. **Proceedings [...]**. Bogota: IEOM Society International, 2017. Disponível em: <http://ieomsociety.org/bogota2017/papers/115.pdf>. Acesso em: 02 nov. 2019.

TU, Z.; YUAN, Y. Critical success factors analysis on effective information security management: a literature review. *In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS*, 20., 2014, Savannah. **Proceedings [...]**. Savannah: Information Systems Security, Assurance and Privacy Track (SIGSEC), 2014. Disponível em:

<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1158&context=amcis2014>. Acesso em: 18 set. 2019.

WANG, C.; TSAI, D. Integrated installing ISO 9001 and ISO 27000 management systems on an organization. *In: ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY*, 43., 2009, Zurich. **Proceedings** [...]. Zurich: IEEE - Institute of Electrical and Electronics Engineers, 2009. Disponível em: <https://ieeexplore.ieee.org/abstract/document/5335527>. Acesso em: 06 jan. 2019.

WIENGARTEN, F. *et al.* The adoption of multiple certification standards: perceived performance implications of quality, environmental and health & safety certifications. **Production Planning & Control**, London, v. 28, n. 2, p. 131-141, 2017. Disponível em: <https://doi.org/10.1080/09537287.2016.1239847>. Acesso em: 11 ago. 2019

ZENG, S.; SHI, J.; LOU, G. A synergetic model for implementing an integrated management system: an empirical study in China. **Journal of Cleaner Production**, Amsterdam, v. 15, n. 18, p. 1760-1767, 2007. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0959652606001478>. Acesso em: 05 mar. 2019.

APÊNDICE A: Questionário estruturado sobre a integração das normas ISO 27001 e ISO 9001

Questão	Objetivo
1. Das empresas em que você prestou consultoria, qual a porcentagem das que preferiram manter separados os sistemas de gestão da qualidade e de segurança da informação?	Identificar a porcentagem de integração dos sistemas.
2. A decisão de integrar os sistemas partiu da alta direção ou foi orientação da consultoria?	Identificar o envolvimento da alta direção.
3. Como os funcionários envolvidos reagiram ao processo de integração?	Identificar o papel dos funcionários envolvidos; identificar se houve resistência à mudança e a influência da cultura local.
4. Como você descreve a alocação de recursos humanos e financeiros feita pelas empresas em relação à necessidade do projeto de integração dos sistemas?	Identificar se os recursos foram suficientes.
5. Quais foram as principais dificuldades enfrentadas durante o processo de integração das normas nas empresas?	Identificar os fatores que influenciam na integração dos sistemas.
6. O que poderia ter sido feito para evitar ou reduzir as dificuldades mencionadas?	Identificar atividades que possam contribuir para a eficácia do processo.
7. Quais os benefícios percebidos pelas empresas com a integração dos sistemas?	Identificar os benefícios trazidos pela integração.

Fonte: Elaborado pela própria autora.

APÊNDICE B: Questionário de coleta de dados

Você foi convidado pela Universidade Estadual Paulista (UNESP) para responder este questionário devido a sua experiência de trabalho. O objetivo da pesquisa é avaliar os fatores, que na sua opinião, impactam a integração de um sistema de gestão de segurança da informação certificado de acordo com a norma ISO 27001 com um sistema de gestão da qualidade certificado de acordo com a norma ISO 9001. Serão necessários poucos minutos para as respostas e seu esforço será útil no processo de implantação. As perguntas são simples e não envolvem aspectos confidenciais. Os dados de perfil são sigilosos.

Exemplo: Para que um time de futebol obtenha vitória em uma partida, assinale o grau de importância para a melhor alternativa.

Intensidade de Importância	Definição (...de uma alternativa em relação a outra)
1	Igual importância
3	Pequena importância
5	Média Importância
7	Grande Importância
9	Excepcional Importância

		9	7	5	3	1	3	5	7	9	
A	Habilidade individual dos jogadores						X				Entrosamento entre os jogadores
B	Entrosamento entre os jogadores		X								Número de torcedores em uma partida

- A. Esta resposta indica que Entrosamento entre os jogadores foi considerado ter pequena importância (3) comparado a Habilidade individual dos jogadores para que haja vitória do time.
- B. Esta resposta indica que Entrosamento entre os jogadores foi considerado ter uma grande importância (7) comparado a Número de torcedores em uma partida para que haja vitória do time.

Para que haja a **priorização dos fatores** que impactam a integração da ISO 27001 com a ISO 9001, de acordo com a escala, para cada um dos critérios a seguir, assinale com um “X” o que você considera mais importante:

	9	7	5	3	1	3	5	7	9	
Planejamento dos sistemas de gestão										Apoio dos sistemas de gestão (provimento de recursos, competência e conscientização para implementação e melhoria)
Apoio dos sistemas de gestão (provimento de recursos, competência e conscientização para implementação e melhoria)										Operação dos sistemas de gestão (controle dos processos para atendimento aos requisitos e aos objetivos)

Para que haja um melhor **planejamento dos sistemas de gestão**, para cada uma das alternativas a seguir, assinale com um “X” a que você considera mais importante para a integração da ISO 27001 com a ISO 9001:

	9	7	5	3	1	3	5	7	9	
Ter um passo-a-passo para guiar o processo de integração										A competência dos recursos humanos
A competência dos recursos humanos										A disponibilidade de recursos
A disponibilidade de recursos										O conhecimento da norma pelos envolvidos no processo
O conhecimento da norma pelos envolvidos no processo										A realização das atividades de integração

Para que haja um melhor **apoio dos sistemas de gestão** (provimento de recursos, competência e conscientização para implementação e melhoria), para cada uma das alternativas a seguir, assinale com um “X” a que você considera mais importante para a integração da ISO 27001 com a ISO 9001:

	9	7	5	3	1	3	5	7	9	
Ter um passo-a-passo para guiar o processo de integração										A competência dos recursos humanos
A competência dos recursos humanos										A disponibilidade de recursos
A disponibilidade de recursos										O conhecimento da norma pelos envolvidos no processo
O conhecimento da norma pelos envolvidos no processo										A realização das atividades de integração

Para que haja uma melhor **operação dos sistemas de gestão** (controle dos processos para atendimento aos requisitos e aos objetivos), para cada uma das alternativas a seguir, assinale com um “X” a que você considera mais importante para a integração da ISO 27001 com a ISO 9001:

	9	7	5	3	1	3	5	7	9	
Ter um passo-a-passo para guiar o processo de integração										A competência dos recursos humanos
A competência dos recursos humanos										A disponibilidade de recursos
A disponibilidade de recursos										O conhecimento da norma pelos envolvidos no processo
O conhecimento da norma pelos envolvidos no processo										A realização das atividades de integração

Formação:

Breve descrição da sua experiência de trabalho:

Foi fácil responder o questionário? Sim () Não ()

Se "Não" indique qual foi a dificuldade:

Comentários:

APÊNDICE C: Tratamento de dados sobre a implantação da norma ISO 27001

Questionário estruturado

Questão	Objetivo
1. Quais os motivos que levaram as empresas à certificação do sistema de gestão de segurança da informação?	Identificar os objetivos com a certificação do sistema.
2. Como a alta direção das empresas está comprometida em exercer a segurança da informação?	Identificar o papel da alta direção no sistema.
3. Como os funcionários envolvidos no processo reagiram à implantação do sistema de gestão de segurança da informação nas empresas?	Identificar o papel dos funcionários envolvidos; identificar se houve resistência à mudança e a influência da cultura local.
4. Como você descreve a alocação de recursos humanos e financeiros feita pelas empresas em relação à necessidade do projeto de implantação do sistema de gestão de segurança da informação?	Identificar se os recursos foram suficientes.
5. Enumere as principais dificuldades enfrentadas durante o processo de implantação do sistema de segurança da informação nas empresas.	Identificar os fatores que influenciam na certificação do sistema.
6. O que poderia ter sido feito para evitar ou reduzir as dificuldades mencionadas?	Identificar atividades que possam contribuir para a eficácia do processo.
7. Para empresas certificadas ISO 9001, foram percebidos fatores diferentes na implantação da ISO 27001 dos que influenciaram a certificação do sistema de gestão da qualidade?	Identificar a diferença entre os fatores que influenciam a implantação de cada norma.
8. Quais os benefícios percebidos pelas empresas com a implantação do sistema de segurança da informação?	Identificar os benefícios trazidos pelo sistema.

Fonte: Elaborado pela própria autora.

Quadro 7 - Resultado da pesquisa: agrupamento das respostas dos consultores para cada fator identificado na literatura

(continua)

Fator	Descrição
Apoio da Alta Direção	A alta direção não soube bem como orientar a implantação. Necessidade de conscientização de que a segurança da informação é uma prioridade. Pouco comprometimento da alta direção.

Quadro 7 - Resultado da pesquisa: agrupamento das respostas dos consultores para cada fator identificado na literatura

(conclusão)

Fator	Descrição
Recursos Humanos	Deficiências no processo de comunicação levaram a um envolvimento desigual na organização. Falta de conhecimento da norma. Falta de engajamento do pessoal por comprometimento deficiente da liderança e comunicação inadequada dos resultados obtidos. Falta de informação/entendimento sobre as razões da implantação do sistema. O foco das pessoas estava apenas nos controles de segurança da informação. As empresas focam na implantação de ferramentas automatizadas e pouco na conscientização dos colaboradores. Problemas com comprometimento, treinamento e conscientização. Recusa de participação ou participação efetiva somente após o comando da alta direção. Continuar com a visão direcionada para as atividades do dia a dia. Dificuldade em disciplinar o uso do celular nas organizações. Resistência de gerentes em aceitar mudanças de regras.
Cultura Organizacional	A principal dificuldade na implantação é o ajuste de cultura nas áreas abrangidas. Os funcionários de nível tático e estratégico têm problemas com mudanças culturais.
Disponibilidade de Recursos	Problema quando a empresa entende que o trabalho de implantação deve ser feito pela consultoria e não pela empresa. Problemas com alocação de recursos. Não instituir uma área voltada para a segurança da informação.
Atividades para Implantação	Dificuldades em adotar as práticas recomendadas nos requisitos. Falta de registro das atividades que já eram feitas. Problemas com a implantação efetiva dos controles da norma.

Fonte: Elaborado pela própria autora.

Segundo Fazenda e Fagundes (2015), a falta de apoio da alta direção é um dos desafios que impedem a adesão em massa de empresas brasileiras à norma ISO 27001. Assim, para o sucesso da implantação e manutenção do sistema de gestão, é importante que a alta direção esteja envolvida, com o intuito de demonstrar aos colaboradores que a segurança da informação é uma preocupação para a organização.

Por meio das respostas recebidas dos consultores para esta pesquisa, foi possível verificar que alguns enfrentaram adversidades relacionadas ao apoio da alta direção, tais como: falta de comprometimento da alta direção, falta de orientação das atividades de implantação e falta de conscientização de que a segurança da informação é uma prioridade.

Durante o desenvolvimento da pesquisa qualitativa, registrou-se que o fator Recursos Humanos recebeu a maior quantidade de menções por parte dos entrevistados, como uma dificuldade de implantação da ISO 27001, com indicações de falta de conhecimento da norma, falta de engajamento, entendimento, comprometimento e conscientização, bem como a resistência em aceitar as mudanças de regras. Este fator também é um dos mais relatados pelos autores pesquisados. Fazenda e Fagundes (2015) verificaram em sua pesquisa que a falta de capacitação dos funcionários pode impactar o processo do sistema de gestão como um todo e citam como exemplo a falta de solução de incidentes de segurança da informação e que a resistência à mudança decorre do fato de que os controles implantados pelas políticas de segurança da informação geram maior esforço e são encaradas como burocráticas e sem resultados mensuráveis. AbuSaad *et al.* (2011) afirmam que a falta de experiência pode interromper um projeto, pois equipes inexperientes veem obstáculos menores como problemas insolúveis.

A cultura organizacional precisa evoluir por meio do conhecimento e da valorização das informações confidenciais, para que não haja excesso de confiança entre os colaboradores, compartilhamento de senhas e descarte indevido de informações (FAZENDA; FAGUNDES, 2015). AbuSaad *et al.* (2011) afirmam que diferentes culturas e estilos de vida podem ter efeitos na implementação de um padrão internacional. Alguns entrevistados também relataram o ajuste da cultura organizacional como um fator relevante e que os funcionários de nível tático e estratégico têm problemas com mudanças culturais.

Para Longras *et al.* (2018), os custos financeiros de implantação podem ser um entrave para empresas com baixo orçamento, pois pode haver necessidade de investimento em *hardware*, *software*, capacitação dos colaboradores e consultoria externa. Três entrevistados relataram problemas com alocação de recursos, incluindo a falta de uma área voltada para a segurança da informação e o fato de a empresa entender que todo o trabalho deve ser feito pela consultoria.

Os obstáculos encontrados no processo de implantação estão relacionados à dificuldade de implantar a metodologia adequada para assegurar a conformidade com os requisitos e as políticas e à adequação dos conceitos da consultoria à realidade da empresa. (LONGRAS *et al.*, 2018). Tais obstáculos, também, se refletiram nas dificuldades relatadas por outros autores como a necessidade do estabelecimento de um vocabulário comum entre os diferentes níveis hierárquicos (MUELLER; HAN; SCHNEIDER *et al.*, 2011), necessidade de identificação dos ativos da organização (ABUSAAD *et al.*, 2011). Alguns entrevistados enfrentaram barreiras similares, como a dificuldade em adotar as práticas recomendadas nos requisitos, falta de

registro das atividades que já eram feitas e problemas com a implantação efetiva dos controles da norma.

Além de identificar fatores que impactam na implantação, também foi possível observar alguns motivos que levaram as empresas à certificação, como a busca pela melhoria da segurança da informação, percepção como um atributo diferencial de mercado, marketing, obrigatoriedade regulamentar ou de clientes.

Como medidas para minimizar os fatores percebidos na implantação, a sugestão dos consultores seria ter mais apoio e comprometimento da alta direção, provisionamento de recursos, um prazo maior para implantação do sistema, implantação de um sistema de menor porte, fazendo com que ele evolua posteriormente, a comunicação dos resultados, bem como a capacitação e a conscientização dos envolvidos, com o uso de casos reais de falhas de segurança que causaram impactos aos negócios, de modo a demonstrar que as regras beneficiam o sistema.

Como benefícios da implantação da ISO 27001, os consultores perceberam maior conhecimento dos riscos de maneira a mitigá-los, mais profissionalismo no trato com os dados dos clientes, mais restrições no acesso às informações, aumento na conscientização dos colaboradores, maior controle tecnológico, menores riscos de incidentes, redução do custo de impactos de vazamento de informações, transparência da gestão de Tecnologia da Informação, economia e melhor visão para a alta direção. Externamente, maior confiança e segurança para as partes interessadas e melhoria da imagem da empresa no seu mercado de atuação.

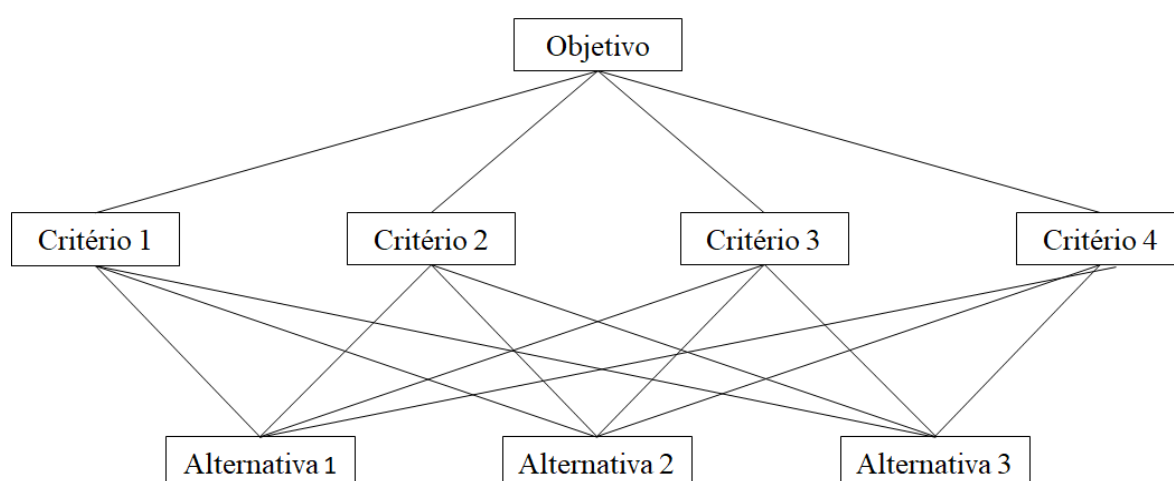
APÊNDICE D: Método *Analytic Hierarchy Process* (AHP) combinado com a técnica *Incomplete Pairwise Comparison* (IPC)

Geralmente, é necessário mais de um critério para chegar a uma decisão, tornando-a mais complexa. Sendo assim, é importante estruturar o problema e avaliar os critérios relevantes antes da tomada de decisão (TRAMARICO *et al.* 2015). A Tomada de Decisão com Múltiplos Critérios (MCDM – *Multiple Criteria Decision Making*) tem sido utilizada com sucesso na solução de problemas (SALOMON; MARINS; DUDUCH, 2009).

O método AHP é aplicado em uma grande variedade de áreas, incluindo planejamento, seleção da melhor alternativa, alocação de recursos e resolução de conflitos. Este método tem o objetivo de estabelecer prioridades a serem atribuídas a diferentes critérios e alternativas, possibilitando a escolha da alternativa mais adequada. Suas etapas são apoiadas na estruturação do problema de acordo com uma hierarquia, no cálculo de prioridades com base na comparação aos pares, na verificação da consistência e na análise de sensibilidade. Os dois últimos passos são opcionais, porém recomenda-se que sejam executados, para atingir credibilidade nos resultados (TRAMARICO *et al.* 2015).

A etapa de estruturação do problema pode ser observada na Figura 4, com o objetivo da tomada de decisão no primeiro nível, os critérios no segundo nível e as alternativas no terceiro nível.

Figura 4 – Exemplo de estrutura hierárquica



Fonte: Adaptado de Saaty (2013).

O cálculo de prioridades é iniciado com o estabelecimento de valores de importância para os critérios, com base na Escala Fundamental de Saaty, conforme Tabela 2.

Tabela 2 – Escala Fundamental de Saaty

Intensidade de Importância	Definição	Explicação
1	Mesma Importância	As duas atividades contribuem igualmente para o objetivo.
3	Importância pequena de uma sobre a outra	A experiência e o julgamento favorecem levemente uma atividade em relação a outra.
5	Importância grande ou essencial	A experiência e o julgamento favorecem fortemente uma atividade em relação a outra.
7	Importância muito grande ou demonstrada	Uma atividade é muito fortemente favorecida em relação a outra; sua dominação de importância é demonstrada na prática.
9	Importância absoluta	A evidência favorece uma atividade em relação a outra com o mais alto grau de certeza.
2, 4, 6, 8	Valores intermediários entre os valores adjacentes	Quando se procura uma condição de compromisso entre duas definições.

Fonte: Briozo; Musetti (2015).

O próximo passo é construir uma matriz de comparação para que seja feita a comparação entre os valores dos critérios.

Segundo Bozóki, Fülöp e Rónyai (2009) uma das desvantagens do método AHP é a quantidade de julgamentos que é necessária para completar a matriz de comparações, em razão do número de alternativas.

O número mínimo de comparações deve estabelecer a premissa estabelecida pela Equação 1, onde n representa o número de fatores estudados e n^2 o número total de comparações possíveis da matriz de decisão (ISHIZAKA; NEMERY, 2013).

$$\frac{n^2 - n}{2} \quad (1)$$

Considerando o número n de fatores, as comparações de fatores entre si representam o preenchimento da diagonal principal na matriz, que é recíproca: os valores das comparações abaixo da diagonal possuem peso inverso aos valores das comparações superiores à mesma diagonal. Sendo assim, em uma matriz recíproca de valor $A = a_{ij}$ de tamanho n , observa-se:

$$a_{ij} > 0, a_{ij} = \frac{1}{a_{ji}} \text{ para } i, j = 1, \dots, n \quad (2)$$

No entanto, de acordo com Harker (1987), pode ser utilizada a técnica *Incomplete Pairwise Comparison* (IPC) para reduzir o número mínimo de comparações necessárias, atendendo a premissa $n - 1$ julgamentos, ao invés da premissa expressa na Equação 1. Esta técnica é utilizada para a dedução dos valores das comparações faltantes (BOZÓKI; FÜLÖP; RÓNYAI, 2009). A dedução pode ser validada pela equação:

$$a_{ij} = a_{ik} \times a_{kj} \quad \forall i, j, k \quad (3)$$

A Figura 5 mostra um modelo de matriz recíproca de juízo de valor com n fatores (F) e julgamentos incompletos. Os julgamentos da diagonal superior à diagonal principal da matriz são definidos com os julgamentos dos respondentes, por representarem $n - 1$ julgamentos e por permitirem a dedução dos demais valores superiores à diagonal. Como um exemplo, a_{13} é deduzido por $a_{12} \times a_{23} = a_{13}$ e a_{14} por $a_{13} \times a_{34} = a_{14}$.

Figura 5 – Modelo de Matriz de Decisão Incompleta

	F1	F2	F3	F4	F5	F6	..	..	..	..	..	Fn
F1	1	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	..	..	..	..	..	..
F2	$1/a_{12}$	1	a_{23}	a_{24}	a_{25}	a_{26}	..	..	..	..	..	..
F3	$1/a_{13}$	$1/a_{23}$	1	a_{34}	a_{35}	a_{36}	..	..	..	..	..	..
F4	$1/a_{14}$	$1/a_{24}$	$1/a_{34}$	1	a_{45}	a_{46}	..	..	..	..	..	..
F5	$1/a_{15}$	$1/a_{25}$	$1/a_{35}$	$1/a_{45}$	1	a_{56}	..	..	..	..	..	..
F6	$1/a_{16}$	$1/a_{26}$	$1/a_{36}$	$1/a_{46}$	$1/a_{56}$	1	..	..	..	..	..	..
..	..	..	..	..	..	..	1	..	..	..	..	..
..	..	..	..	..	..	..	..	1	..	..	..	..
..	..	..	..	..	..	..	..	..	1	..	..	..
..	..	..	..	..	..	..	..	..	..	1	..	..
..	..	..	..	..	..	..	..	..	..	..	1	..
Fn	$1/a_{1n}$	$1/a_{2n}$	$1/a_{3n}$	$1/a_{4n}$	$1/a_{5n}$	..	..	..	..	..	..	1

 Diagonal que representa $n - 1$ julgamentos

Fonte: Baseado na técnica de Hacker (1987).

A verificação da consistência é realizada com base no método de matriz incompleta, onde valores para $\lambda = n$ garantem um Índice de Consistência (IC) igual a 0 na análise dos critérios ou alternativas estudadas (BOZÓKI; FÜLÖP; RÓNYAI, 2009).

Uma tomada de decisão sistêmica é feita posteriormente, exigindo meios de agregação dos julgamentos, para a definição das prioridades globais. A *Aggregation of Individual Judgments* (AIJ) é a abordagem a ser seguida quando especialistas participam de um mesmo grupo ou empresa e utiliza a média geométrica para sintetizar as matrizes de julgamentos. A *Aggregation of Individual Priorities* (AIP) é a abordagem a ser seguida quando especialistas participam de grupos distintos e utiliza a média aritmética para sintetizar as matrizes de julgamentos (FORMAM; PENIWATI. 1998).