UNIVERSIDADE DE CAXIAS DO SUL

PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO – PPGA

CURSO DE MESTRADO

MATEUS BUOGO

SEGURANÇA DA INFORMAÇÃO APLICADA NO MODELO SECI:

DESENVOLVIMENTO DE UM FRAMEWORK DE GESTÃO DO CONHECIMENTO SEGURO

CAXIAS DO SUL

2022

MATEUS BUOGO

SEGURANÇA DA INFORMAÇÃO APLICADA NO MODELO SECI:

DESENVOLVIMENTO DE UM FRAMEWORK DE GESTÃO DO CONHECIMENTO SEGURO

Projeto de Dissertação de Mestrado submetida à Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Administração da Universidade de Caxias do Sul, como parte dos requisitos necessários para obtenção do título de Mestre em Administração.

Orientador: Prof. Dra. Cintia Paese Giacomello

CAXIAS DO SUL

2022

Dados Internacionais de Catalogação na Publicação (CIP)
Universidade de Caxias do Sul
Sistema de Bibliotecas UCS - Processamento Técnico

B943s Buogo, Mateus
Segurança da informação aplicada no modelo SECI [recurso eletrônico] : desenvolvimento de um *framework* de gestão do conhecimento seguro / Mateus Buogo. – 2022.
Dados eletrônicos.

Dissertação (Mestrado) - Universidade de Caxias do Sul, Programa de Pós-Graduação em Administração, 2022.
Orientação: Cintia Paese Giacomello.
Modo de acesso: World Wide Web
Disponível em: https://repositorio.ucs.br

1. Gestão do conhecimento. 2. Sistemas de recuperação da informação - Segurança. 3. *Framework* (Arquivo de computador). I. Giacomello, Cintia Paese, orient. II. Título.

CDU 2. ed.: 005.94

Catalogação na fonte elaborada pela(o) bibliotecária(o)
Ana Guimarães Pereira - CRB 10/1460

MATEUS BUOGO

SEGURANÇA DA INFORMAÇÃO APLICADA NO MODELO SECI:

DESENVOLVIMENTO DE UM FRAMEWORK DE GESTÃO DE CONHECIMENTO SEGURO

Projeto de dissertação de mestrado submetida à Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Administração da Universidade de Caxias do Sul, como parte dos requisitos necessários para obtenção do título de Mestre em Administração.

Aprovado (a) em: ____/____/2022.

Banca Examinadora

_____

Prof. Dra. Ana Cristina Fachinelli Bertolini

Universidade de Caxias do Sul – UCS

_____

Prof. Dr. Ademar Galelli

Universidade de Caxias do Sul – UCS

_____

Prof. Dra. Jamile Sabatini Marques

Universidade de São Paulo – USP

Dedico este trabalho à comunidade de Segurança da Informação e profissionais da área.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me fazer capaz de chegar à conclusão do Mestrado em Administração executando esse trabalho e dessa forma poder assimilar o conhecimento necessário para meu crescimento pessoal e profissional. Sou grato pelo apoio que minha esposa me deu durante todos os anos que estamos juntos, que foi de fundamental importância para meu sucesso pessoal, acadêmico e profissional. Agradeço também ao meu pai e minha mãe pela forma como me criaram e me apoiaram durante todos os instantes da minha vida. Gostaria de agradecer à minha professora orientadora Dra. Cintia Paese Giacomello que sempre se demonstrou disponível para auxílios e esclarecimentos, proporcionando uma maior maturidade para o trabalho.

Em segurança da informação, tudo é uma questão de tempo, dinheiro e oportunidade.

José Ricardo Longatto

RESUMO

Devido à importância estratégica do conhecimento, faz-se necessário nas organizações a adoção de metodologias de gestão que facilitem a criação e disseminação do conhecimento mas que também considerem boas práticas de segurança e adequação dos processos às leis como a Lei Geral de Proteção de Dados Pessoais (LGPD) e a *General Data Protection Regulation* (GDPR). Dessa forma, a proposta deste estudo foi desenvolver um *framework* de Gestão do Conhecimento Seguro, considerando os pontos de consenso entre a espiral do conhecimento do modelo SECI (Socialização, Externalização, Combinação, Internalização) e os controles de segurança propostos pela ISO27001. Para isso foi realizada uma pesquisa utilizando a metodologia Delphi com a consulta de 20 especialistas, dez de cada área. Ao finalizar três rodadas, obteve-se um framework que evidencia os controles de segurança propostos em cada fase do modelo SECI. O controle de Conscientização, educação e treinamento em Segurança da Informação aparece nas etapas de Socialização, Externalização e Internalização do SECI com 80% ou mais de escolhas. Na etapa de Combinação o controle mais consenso é Rótulos e tratamento da informação, que chegou a 75% de consenso de escolhas. A implantação desse framework pode ser realizada através de sistematização e periodização de capacitações dos colaboradores das empresas sobre o tema de Segurança da Informação aplicada na Gestão do Conhecimento, sendo apoiado pelos rótulos das informações e conhecimentos. Observou-se, ainda, que existe uma lacuna de conhecimento sobre os temas opostos à especialidade de cada especialista envolvido na pesquisa.

Palavras-chave: Gestão do Conhecimento. Segurança da Informação. Framework. Conhecimento Seguro. Controles.

ABSTRACT

Due to the strategic importance of knowledge, it is necessary for organizations to adopt management methodologies that facilitate the creation and dissemination of knowledge but that also consider good security practices and suitability of processes to laws such as the General Law for the Protection of Personal Data (LGPD) and the General Data Protection Regulation (GDPR). Thus, the purpose of this study was to develop a Secure Knowledge Management framework, considering the points of consensus between the knowledge spiral of the SECI (Socialization, Externalization, Combination, Internalization) model and the security controls proposed by ISO27001. In order to do so, a survey was carried out using the Delphi methodology with the consultation of 20 specialists, 10 from each area. At the end of three rounds, a framework that highlights the security controls proposed in each phase of the SECI model was obtained. The control of Awareness, education and training in Information Security appears in the stages of Socialization, Externalization and Internalization of the SECI with 80% of votes or more. In the Combination stage, the most consensus control is Labels and information handling, which reached 75% of vote consensus. The implementation of this framework can be carried out through systematization and periodization of training of company employees on the topic of Information Security applied in Knowledge Management, supported by information and knowledge labels. It was also observed that there is a knowledge gap on topics that are opposite to the specialty of each specialist involved in the research.

Keywords: Knowledge management. Information security. Framework. Secure Knowledge. Controls.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CISSP	*Certified Information System Security Professional (Certificação Profissional de Sistemas de Segurança da Informação)*
DCPT	*Desec Certified Penetration Tester (Pentester Certificado Desec)*
GC	Gestão do Conhecimento
GDPR	*General Data Protection Regulation (Regulamento Geral de Proteção de Dados)*
IEC	*International Electrotechnical Commission (Comissão Eletrotécnica Internacional)*
ISO	*International Organization for Standardization (Organização Internacional para Padronização)*
LGPD	Lei Geral de Proteção de Dados Pessoais
NBR	Norma técnica brasileira
SECI	Socialização, Externalização, Combinação e Internalização
SI	Segurança da Informação

SUMÁRIO

1 INTRODUÇÃO

A Segurança da informação é preponderante para as empresas, pois diariamente enfrentam ameaças e riscos em suas operações. Um dos principais desafios é como avaliar o nível de segurança para se proteger. As empresas precisam definir abordagens e habilidades para que seja possível implementar segurança em seus processos (AL-MATARI *et al*., 2020).

Com o advento de legislações de proteção de dados como a lei europeia *General Data Protection Regulation* (GDPR) e a lei brasileira, Lei Geral de Proteção de Dados Pessoais (LGPD), a responsabilidade das empresas, no que tange à proteção de dados, aumentou exponencialmente. O grande desafio lançado pela LGPD e pela GDPR é como criar oportunidades de compartilhamento de conhecimento e ideias, visando atender a proteção dos dados pessoais (AMRAM, 2020).

As premissas da LGPD visam a proteção dos ativos de informação e conhecimento, visando a proteção dos dados pessoais que circundam os ambientes. O gerenciamento organizacional das empresas tem como função a proteção desses ativos através de atividades de gerenciamento de riscos de segurança eficientes e eficazes (ELLIS; HERTIG; METSCHER, 2020).

A manipulação, por parte das empresas, de conhecimento e informação é necessária para sua subsistência. Kaplan e Norton (2004) e Baranes (2020) explanam que os ativos intangíveis, como informação e conhecimento, desempenham um papel preponderante ao proporcionar uma vantagem competitiva diferenciada. Au, Li e Shen (2019) corroboram que os ativos intangíveis estão se tornando cada vez mais importantes para as empresas.

Os ativos intangíveis são importantes para a segurança econômica das empresas modernas que os aplicam juntamente com a propriedade intelectual em suas atividades para obter um desenvolvimento sustentável (RODIONOV; PEREPECHKO; NADEZHINA, 2020) sendo também um ativo estratégico para a sustentação das empresas em um ambiente inovador e dinâmico (ESLAMKHAH; SENO, 2019). Para proteção dos ativos intangíveis, algumas empresas utilizam cláusulas de “não concorrência” para impedir que a propriedade intelectual seja perdida (AN, 2019).

As empresas precisam perceber a informação como um ativo a ser protegido

(CAMPOS, 2007; ARAÚJO, 2014). A sua importância vem aumentando de forma exponencial. A importância da informação dentro das Organizações aumenta com o crescimento da sociedade e das organizações em um mundo contemporâneo (NUNES; RIBEIRO; OLIVEIRA, 2019). Em todos os níveis organizacionais, a informação é um recurso fundamental.

Todos os ativos estão sujeitos a ameaças e riscos que podem comprometer sua integridade. De acordo com Dias (2004), as informações são consideradas patrimônio de uma organização e estão também sob constante risco. Com isso, surge a Segurança da Informação para proteção desse ativo com técnicas e metodologias específicas. A norma ISO/IEC 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013) define que o objetivo da Segurança da Informação é proteger as infraestruturas críticas, viabilizar os negócios e evitar ou reduzir os riscos relevantes. A família da ISO/IEC 27000 é utilizada por muitas empresas, por ser um padrão consolidado no que tange à Segurança da Informação (FILHO; IDE; NAKAMURA, 2019).

A Segurança da Informação também está ligada à adaptação das empresas às legislações referentes à proteção de dados. Para isso é necessário adaptar os *frameworks* ou padrões de segurança existentes e consolidados de mercado aos processos diários das organizações (IDE; FILHO; NAKAMURA, 2019).

A Segurança da Informação, pode ser conceituada como a proteção da informação, em todas suas formas, tendo como objetivo salvaguardar contra ameaças que podem expor os processos a riscos (ALESSI *et al*., 2017). Os principais objetivos são a salvaguarda das informações preponderantes para que não sejam manipuladas de forma indevida e a mitigação dos riscos que podem deixar a informação indisponível ou com perda de suas propriedades. Para Diefenthäler (2020, p. 15)

> a segurança da informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Na percepção de Alhogail (2020), a preocupação com a segurança da informação, nas organizações, está em constante crescimento, devido ao aumento da quantidade e impacto dos ataques à segurança em sistemas de informações pessoais, governamentais e empresariais.

No que tange à segurança da informação, um conhecimento robusto sobre o

assunto também é necessário para escolhas adequadas de controles, políticas e procedimentos de segurança da informação, a fim de obter uma melhor implementação dos mesmos na proteção dos ativos (SAFA; VON SOLMS, 2016; ESLAMKHAH; SENO, 2019).

Um ponto chave para o sucesso da implantação da segurança da informação é considerar o fator humano e não somente o tecnológico, pois a informação e conhecimento são difundidos entre as pessoas. A construção de um ambiente seguro perpassa esses aspectos, sustentando uma efetiva gestão da segurança (SAFA; VON SOLMS; FURNEL, 2016).

Outra abordagem para proteção da informação leva em consideração o que as empresas sabem sobre os seus ativos de informação. Wisniewska e Wisniewski (2019) afirmam que um nível satisfatório de segurança exige uma visão clara da empresa quanto aos recursos que se pretende proteger e às ameaças que podem incidir sobre eles.

Para implementação de controles de segurança, existem melhores práticas que podem ser adotadas. Algumas delas, como a ISO/IEC 27001, são de reconhecimento mundial. Essas práticas orientam os profissionais de segurança da informação sobre a melhor maneira de adaptar os controles de segurança sugeridos nas atividades diárias, evidenciando o que deve ser protegido, sugestionando como proteger (KAILA; NYMAN, 2018).

A gestão da Segurança da Informação nas empresas se torna cada vez mais importante uma vez que a sociedade do século XXI é conhecida como Sociedade do Conhecimento. Atualmente, o conhecimento é o recurso econômico mais valioso da sociedade (DRUCKER, 2000; BARANES; HAKE, 2018). Oliveira (2019) defende que o conhecimento é fator determinante para o desenvolvimento econômico das nações. Sendo assim ele se transforma em um ativo concreto quando aplicado de forma direta nos processos da cadeia de valor das empresas.

Dentro das organizações, o conhecimento gerado deriva dos processos diários e do conhecimento individual de cada colaborador. O conhecimento organizacional está ligado às pessoas. Nonaka e Takeuchi (2008) afirmam que o conhecimento é criado apenas pelos indivíduos. Santos e Valentin (2014, p. 25) corroboram neste sentido quando afirmam: “o conhecimento gerado por cada sujeito organizacional necessita ser compartilhado aos demais membros, fator que depende de ações sistemáticas voltadas a isso.”

A Gestão do Conhecimento surge neste contexto com o objetivo de proteger o conhecimento, garantindo a proteção desse ativo e a manutenção da cadeia de valor das empresas. Ela abrange iniciativas que contribuem para a manipulação do conhecimento sob o ponto de vista da empresa e de sistemas computacionais (COLOMÉ; NUNES; SILVA, 2019).

Alvares, Itaborahy e Machado (2021, p. 10) abordam que a gestão da informação está correlacionada diretamente com a Gestão do Conhecimento, quando afirmam que "[...] muito do que se entende de Gestão do Conhecimento, é de fato, gestão da informação[...]", dessa forma a informação é o subsídio para a Gestão do Conhecimento.

Araújo, Araújo e Batista (2020) explanam que gerir o conhecimento é um processo complexo e essencialmente estratégico. Os processos de Gestão do Conhecimento, de forma estratégica, têm como objetivo melhorar a qualidade dos produtos e serviços ofertados por uma empresa sustentados pela criação, disseminação e retenção de conhecimentos organizacionais aumentando a competitividade (KRÜGER; PINTO, 2020).

O conhecimento pode impactar diretamente ou indiretamente no crescimento das empresas e da sociedade. O compartilhamento de conhecimento fortalece a união das organizações, incentiva que as pessoas trabalhem de forma colaborativa e aumenta a capacidade de atingir metas individuais e organizacionais (EPURE, 2016).

Para as empresas é primordial que conheçam os seus ativos de conhecimento, sejam eles processos ou o próprio conhecimento em si. Krüger e Pinto (2020) advogam que quando há mensuração dos processos de Gestão do Conhecimento, a empresa tem a habilidade necessária para identificar se está utilizando de forma adequada seu capital intelectual.

No processo de Gestão do Conhecimento estão contemplados sua criação, informações, tecnologias e inovação como campo de estudo (CANTO *et al*., 2018). Empresas que conseguem criar e mobilizar conhecimento, transformando-o em inovação e competitividade, possuem a capacidade de explorar o ambiente de maneira adaptativa com flexibilidade e promovem sua perpetuidade (BANISKI; CIESLAK, 2018). Dandolini, Kautnick e Valdati (2018) corroboram ainda que o conhecimento e a Gestão do Conhecimento estão relacionados à capacidade de inovação de uma organização. Para a manutenção dos negócios das organizações, a Gestão do Conhecimento torna-se essencial por causa do seu dinamismo no

compartilhamento do conhecimento (ARAÚJO; ARAÚJO; BATISTA, 2020), pois ele é fator chave nas tomadas de decisão e deve ser gerenciado.

Nonaka e Takeuchi (2008), propõem como modelo de Gestão do Conhecimento, um processo de quatro etapas denominado SECI (Socialização, Externalização, Combinação, Internalização), onde é desenvolvida a transformação do conhecimento e a criação de novos conhecimentos através de um objeto denominado pelos autores como espiral do conhecimento. O modelo SECI é uma das principais metodologias de Gestão do Conhecimento. Farnese *et al.* (2019, p. 3) salienta a relevância do SECI afirmando que:

> Dentro desta infinidade de teorias baseadas no conhecimento, conceitos e ferramentas, o modelo SECI é amplamente reconhecido como um marco teórico e adotado como estrutura para a maioria das conceituações de gestão do conhecimento ou propósitos descritivos em estudos de caso.

Runte (2016) afirma que durante o processo de implantação de um sistema de Gestão de Conhecimento surgem muitos desafios que podem envolver rompimento de hábitos, crenças e valores, que estão incorporados indiretamente na cultura organizacional. Neste sentido, pode-se também elencar a segurança e proteção desse conhecimento como um desafio das etapas do processo de Gestão do Conhecimento. Eslamkhah e Seno (2019) destacam que existem muitos estudos e trabalhos na área de Gestão do Conhecimento, porém a segurança do conhecimento é um assunto que não tem recebido a devida atenção na literatura.

A Gestão do Conhecimento auxilia as organizações a sustentarem uma vantagem competitiva, porém o vazamento de conhecimento pode resultar na perda de competitividade da organização (AHMAD *et al.*, 2015). Dessa forma pondera-se que identificar os pontos de consenso entre Gestão do Conhecimento e segurança da informação é necessário para estabelecer a Gestão do Conhecimento Segura.

Desta forma pondera-se que a Gestão do Conhecimento também necessita atentar para a segurança do conhecimento gerado e compartilhado nas organizações. Ide, Nakamura e Reynaldo (2019) explanam que a proteção de dados pode ser realizada através da adaptação dos frameworks e padrões de segurança existentes, portanto, mesmo que não haja uma metodologia específica para Gestão do Conhecimento Seguro, pode-se utilizar processos de segurança consolidados mundialmente para adaptá-los à Gestão do Conhecimento.

1.1 TEMA E PROBLEMA

Diante dos argumentos expostos, pondera-se que a informação e o conhecimento, mais do que ativos, são atores essenciais para o desenvolvimento sustentável das organizações. O gerenciamento da informação e do conhecimento é algo desafiador no cotidiano das empresas, devido à característica de intangibilidade que possuem. Outra característica desafiadora, é a segurança aplicada sobre esses ativos. Todos os ativos estão expostos a riscos e por isso é importante que eles sejam mitigados ao máximo, a fim de proteger a cadeia de valor das empresas.

Existem abordagens, metodologias, modelos e *frameworks* distintos para o gerenciamento do conhecimento. O modelo SECI, neste contexto, tem como objetivo delinear processos e ações focadas na criação e compartilhamento do conhecimento entre os indivíduos de uma organização. A retenção e a redundância do conhecimento também são partes deste processo.

No campo da segurança, existem normas e orientações para a proteção dos ativos de informação. O foco da segurança da informação é a proteção dos ativos contra perda, danos ou manipulação indevida, estando em consonância com as legislações que auditam a proteção de dados e informações dentro de um sistema de gestão de segurança (ABNT, 2013b).

Neste contexto, surge um paradoxo entre os objetivos de cada temática. O modelo SECI busca a criação e compartilhamento de conhecimentos entre os indivíduos de forma irrestrita e a Segurança da Informação, por outro lado, tem como foco a restrição de acesso a informações e conhecimento, logo, conhecimento. Pondera-se que as duas abordagens são coerentes e necessárias nos ambientes empresariais pelos mesmos motivos de sustentação de negócio.

Existem conhecimentos que não devem ser expostos de maneira irrestrita, pois podem comprometer a estratégia das organizações ou expor dados sensíveis. O modelo SECI não preconiza em sua estrutura o controle de acesso ou compartilhamento desses conhecimentos. Já os controles de Segurança da Informação propostos pela ISO/IEC 27001, se implementados em sua plenitude, tornam os processos muito restritos no que tange acesso e compartilhamento de informações.

Diante deste paradoxo surge o problema de compartilhamento de conhecimento de forma irrestrita, sem considerar aspectos de Segurança da

Informação. O problema de pesquisa é observar os processos do modelo SECI e propor controles de segurança específicos para adequá-los às boas práticas de Segurança da Informação, sem que as restrições impeçam o compartilhamento do conhecimento e ao mesmo tempo melhore a proteção e evite divulgações e compartilhamentos indevidos.

1.2 OBJETIVOS

Dada a importância da Gestão do Conhecimento e da Informação de forma segura alguns objetivos para esse trabalho foram elencados.

1.2.1 Objetivo geral

O objetivo geral desta pesquisa foi propor a inserção de controles de Segurança da Informação no modelo de Gestão do Conhecimento SECI, considerando as boas práticas de implementação de segurança em cada uma das fases da espiral do conhecimento.

1.2.2 Objetivos específicos

Para alcançar o objetivo principal desta pesquisa, alguns objetivos específicos foram elencados:

a) analisar os processos do modelo SECI de Gestão do Conhecimento;
b) analisar os controles de Segurança da Informação presentes na ISO/IEC 27001;
c) identificar os pontos de consenso entre gestão de conhecimento e segurança da informação;
d) validar junto aos especialistas as práticas de gestão de conhecimento e segurança da informação.

1.3 JUSTIFICATIVA DO ESTUDO

A fundamentação teórica relevante à Gestão do Conhecimento e segurança da informação demonstra fundamental importância nos estudos das temáticas, a fim

de melhorar processos dentro das empresas. As metodologias de Gestão do Conhecimento e as melhores práticas de segurança da informação já são de reconhecimento global e entendendo de forma coesa cada uma delas pode-se aplicar melhorias significativas nos processos, em uma junção delas em seus pontos de consenso.

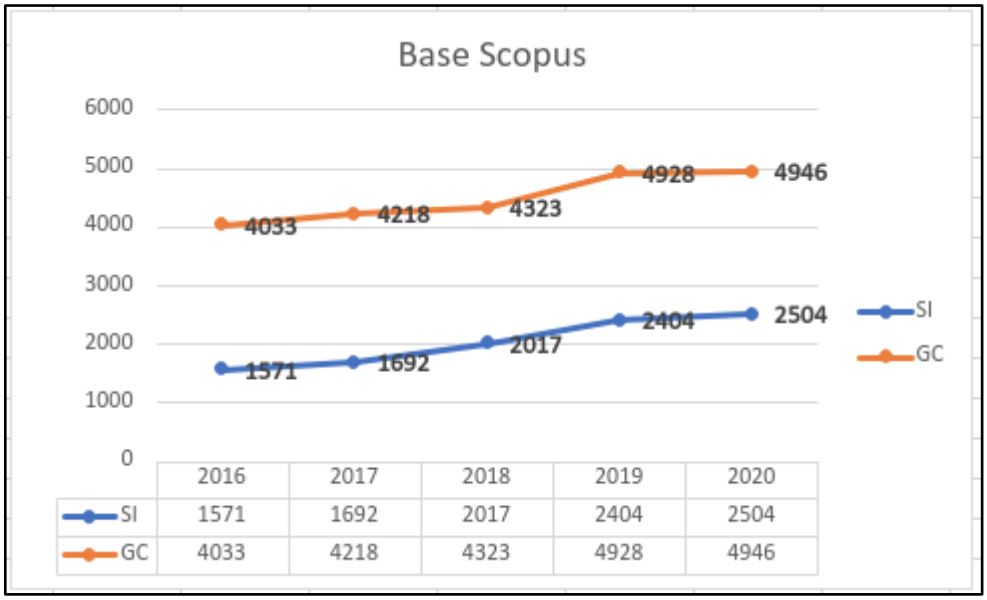
O conhecimento é preponderante para a manutenção e operacionalização dos processos empresariais, por isso faz-se necessário gerenciar este ativo. Brito e Sartori (2019) salientam que a importância da Gestão do Conhecimento nas empresas, a fim de reter e gerenciar o capital humano, recurso preponderante para a sustentação empresarial.

Nunes, Oliveira e Ribeiro (2019) explanam que a informação desempenha um papel de grande importância afetando o desempenho das organizações, tendo em vista que a informação é primordialmente necessária para a tomada de decisões no mundo organizacional. Sendo assim a informação juntamente com o conhecimento que ela gera devem ser tratadas de forma diferenciada na gestão empresarial. Neste contexto a Segurança da Informação pode agregar controles de proteção do conhecimento em um framework padronizando processos.

A pesquisa realizada por artigos publicados em duas bases, Scopus e Science Direct, no período de 2016 a 2020, referente às temáticas de Gestão do Conhecimento e Segurança da Informação, demonstra que a produção acadêmica de trabalhos está em constante crescimento, salientando a relevância dos assuntos abordados neste trabalho.

A Figura 1, referente à base Science Scopus, demonstra que as publicações de trabalhos apresentam tendência de crescimento. Destaca-se o ano de 2020 para Segurança da Informação com 2.504 publicações, sendo 100 publicações a mais que o ano anterior, 2019, que atingiu a marca de 2.404 publicações. Para Gestão do Conhecimento pode-se destacar o ano de 2020 com 4.946 publicações, sendo 18 publicações a mais que no ano anterior, 2019, com 4.928 publicações.

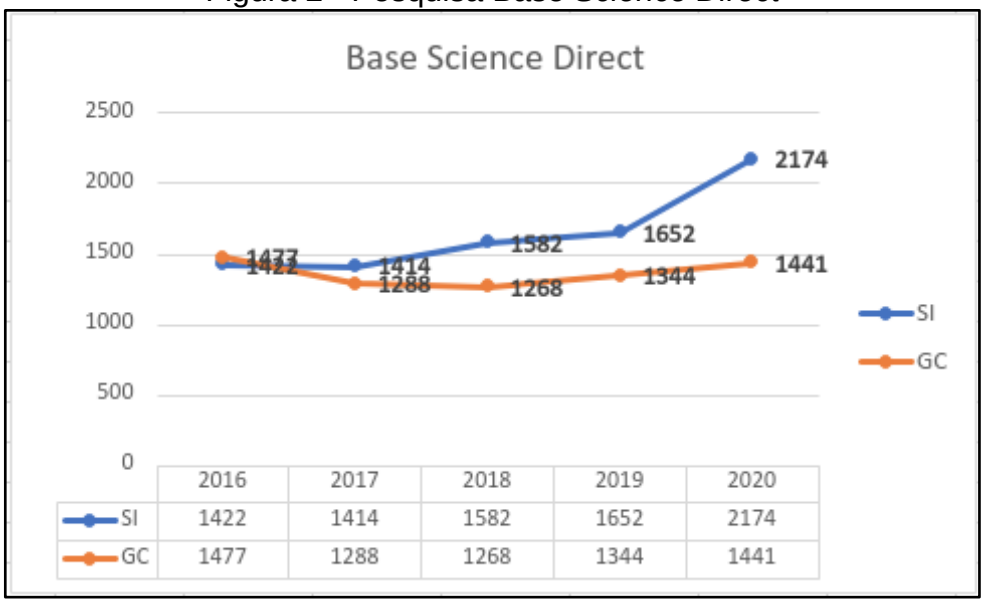
Figura 1 - Pesquisa Base *Scopus*



Fonte: Elaborado pelo autor (2022).

A Figura 2, referente à base Science Direct, também demonstra a tendência de crescimento. Destaca-se o ano de 2020 para Segurança da Informação com 2.174 publicações, sendo 522 publicações a mais que o ano anterior, 2019, que atingiu a marca de 1.652 publicações. Para Gestão do Conhecimento pode-se destacar o ano de 2020 com 1.441 publicações, sendo 97 publicações a mais que no ano anterior, 2019, com 1.344 publicações.

Figura 2 - Pesquisa Base *Science Direct*



Fonte: Elaborado pelo autor (2022).

Este estudo corrobora com a produção científica sobre os temas, seguindo a

tendência de crescimento das publicações sobre os assuntos. É evidente a importância que a academia associa a essas abordagens, pois a cada ano novos trabalhos são desenvolvidos.

Ao realizar o cruzamento das duas temáticas, identificando os pontos de consensos, possibilita-se a abertura de novos caminhos de pesquisa, buscando a interdisciplinaridade e a evolução delas, com uma abordagem mais holística do panorama em que as empresas e a sociedade estão inseridas, identificando assim novas oportunidades de estudos.

Como visto, existe a preocupação acadêmica em estudar esses temas. Também pode-se evidenciar a preocupação das organizações com a segurança da informação. A quantidade de empresas que obtiveram a certificação na ISO/IEC 27001 ao longo do tempo é crescente. Dados da organização ISO apontam que no ano de 2015 havia 9.094 empresas certificadas (INTERNACIONAL ORGANIZATION FOR STANDARDIZATION, 2019). Nos anos seguintes o crescimento foi exponencial: em 2018, chegou-se na marca de 31.910 empresas que conquistaram a certificação. O último *survey,* realizado no ano de 2019, apontou crescimento de 4.452 empresas certificadas, fechando a pesquisa em 36.362 certificações em organizações do mundo inteiro.

Pensando na evolução do tema, a criação de normativas como a Lei de Proteção de Dados Pessoais (LGPD) e a lei de Privacidade de Dados (GDPR), ambas de 2018, deverá fortalecer o tema. O conhecimento está inserido neste contexto quando pessoas manipulam informações para geração de novos conhecimentos e que muitas vezes necessitam de acessos privilegiados a informações sensíveis. O tratamento de dados está passando por uma reformulação de processo, fortalecendo a segurança na manipulação de dados, informação e conhecimento dento das empresas.

Inevitavelmente o processo de Gestão do Conhecimento pode estar acessando ou compartilhando informações deste cunho, ou seja, um processo de segurança da informação precisa ser implementado, a fim de proteger o compartilhamento do conhecimento dentro das organizações. Neres (2020) salienta que a LGPD não determina os controles de segurança necessários para estar em *compliance* com a norma, porém, ela menciona muitas regras que devem ser seguidas. O autor ainda defende que o método mais eficaz para garantir que o resultado de um processo está em conformidade é padronizá-lo. A padronização de processo de segurança está

descrita na norma ISO/IEC 27001.

Dentre os controles propostos pela LGPD (2018), pode-se destacar o acesso às informações sensíveis, pré-estabelecidos pela própria lei. São eles: dado pessoal sobre origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso filosófico ou político; dado referente à saúde ou à vida sexual; dado genético ou biométrico; quando vinculado a uma pessoa natural.

Atualmente os modelos de Gestão do Conhecimento, têm como premissa o acesso e compartilhamento do conhecimento e informação entre os indivíduos, sem barreiras diretas. Este comportamento vai de encontro a normas de segurança propostas pela LGPD (2018). O Caput 6º da lei, inciso VII, salienta a importância da implementação de processos de segurança quando explana que a segurança deve: *"garantir medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;"*

A Segurança da Informação neste estudo é direcionada pelos preceitos, filosofia e controles da ISO/IEC 27001, sendo dessa forma totalmente aderente às milhares de empresas que estão certificando-se com esta norma, ou que seguem as boas práticas na condução dos processos internos em seus sistemas de gestão de segurança da informação (SGSI), além de estar aderente às leis de proteção de dados vigentes no Brasil e no mundo.

Tratar a Gestão do Conhecimento de forma segura, potencializaria a sustentação das empresas, uma vez que ambas as abordagens, de Gestão do Conhecimento e Segurança da Informação, são focadas na sustentabilidade das organizações.

A criação de um framework de Gestão do Conhecimento seguro vai ao encontro das necessidades que as empresas detêm no que tange gerir conhecimento de forma segura em *compliance* com metodologias já consolidadas de Gestão do Conhecimento e Segurança da Informação, além de contribuir ativamente para que pesquisadores possam desenvolver novos estudos ou replicar esse framework em vários ambientes, possibilitando pesquisas profundas na temática e melhoria contínua do objeto.

1.4 ADERÊNCIA DO PROJETO À LINHA DE PESQUISA

A linha de pesquisa de Inovação e Competitividade tem como objetivo estudar as dimensões relacionadas à inovação e à competitividade como fontes de crescimento, desenvolvimento e sustentabilidade das organizações. Esta linha de pesquisa estuda os componentes e recursos relacionados com os processos organizacionais capazes de potencializar a capacidade inovadora das organizações, incluindo a geração e o fluxo de informações, os processos de aprendizagem e a Gestão do Conhecimento.

Neste contexto, este projeto corrobora para a melhoria dos processos de Gestão do Conhecimento nas empresas, protegendo não somente o conhecimento, mas também o processo de criação e compartilhamento do mesmo. Em consonância com as normativas, como LGPD (Lei Geral de Proteção de Dados Pessoais) e GDPR (Regulamento Geral sobre a Proteção de Dados), o projeto demonstra aderência às questões socioeconômicas de forma inovadora no que tange o gerenciamento de informação e conhecimento.

2 REFERENCIAL TEÓRICO

Nesta seção são apresentados conceitos relativos à Gestão do Conhecimento e Segurança da Informação. A abordagem holística identificada nos trabalhos de Nonaka e Takeuchi e a perspectiva normativa da Segurança da Informação foram adotadas para delinear a base teórica, a qual irá orientar a pesquisa e a construção do framework sobre a temática.

2.1 CONHECIMENTO

Na era da Nova Economia, o conhecimento é a matéria-prima para sustentação empresarial. A vantagem competitiva não é mais potencializada por fatores tradicionais como localização geográfica e mão de obra barata, sendo eles derrubados pela importância estratégica atribuída ao capital intelectual, como o conhecimento (ATAWNAH *et al.*, 2021). A valorização dos trabalhadores, neste cenário, também está atrelada ao conhecimento. Park e Scoresby (2021) corroboram neste sentido afirmando que colaboradores que possuem conhecimentos relevantes, dentro de um ambiente organizacional, serão atraentes para as empresas. O conhecimento, na nova economia, deixa de ser um coadjuvante e torna-se o fator principal de sustentabilidade.

Anas *et al.* (2021) advogam que, na atual sociedade, os ativos intangíveis, tornam-se fundamentais para o desenvolvimento e manutenção das organizações, sendo eles uma ferramenta crucial para vantagem competitiva. Empresas que não entendem esse novo cenário correm risco de não conseguir manter suas operações, dessa forma é preponderante que ativos intangíveis como conhecimento e informação sejam tratados como valiosos para manutenção da cadeia de valor. O conhecimento auxilia na criação, obtenção e melhor gestão dos recursos necessários para as empresas (MACHADO; SPRAKEL, 2021).

Drucker (1999) já explanava há mais de 20 anos que o maior desafio dos gerentes dos países desenvolvidos era aumentar a produtividade dos trabalhadores do conhecimento e da área de serviços. Carvalho e Favoretto (2021) e Barbosa (2020) atualmente concordam reforçam Drucker (1999), afirmando que o conhecimento é tratado como uma força motriz crítica para alcançar metas de desempenho das empresas.

A criação de conhecimento é o conjunto de atividades referentes ao processo de entrada de novos conhecimentos, desenvolvimento, descoberta e captura do mesmo (MARCÃO; PESTANA; SOUZA, 2021). Para que haja criação de conhecimento nas organizações, é necessário que haja sincronia entre empresa e funcionário pois o indivíduo é o “criador” do conhecimento e a organização é o “amplificador” (NONAKA; TAKEUCHI, 2008). Dessa forma, a empresa deve investir em metodologias para criar e reter conhecimento, junto a uma cultura organizacional apropriada para tal objetivo.

O conhecimento é formado por dois componentes. Pode-se classificar esses componentes em conhecimento tácito e conhecimento explícito. A principal caraterística do conhecimento tácito é o fato dele ser intrínseco, ou seja, é o conhecimento que se adquire ao longo da vida por meio de experiências e situações; já o conhecimento explícito é de conhecimento público e compartilhado entre todos, não é exclusivo de um indivíduo (NONAKA; TAKEUCHI, 2008).

O conhecimento tácito, de forma geral, pode estar relacionado, direta ou indiretamente, aos paradigmas humanistas e organizacionais. Já o conhecimento explícito pode estar relacionado, direta ou indiretamente, aos paradigmas tecnológicos e sociotécnicos (ÁLVARES *et al.*, 2020).

O conhecimento de um indivíduo pode ser utilizado para realizar ações, tarefas e processos previamente descritos e exemplificados. Pode também ser utilizado para resolver problemas ou canalizado para melhoria contínua de tarefas e processos em um ambiente (CARVALHO; FAVORETTO, 2021).

Nonaka e Takeuchi (2008) explicitam que um indivíduo possui tanto o conhecimento tácito, como o explícito e que isso é o fator chave para criação de conhecimentos e a harmonia entre os componentes organizacionais. O conhecimento é um ativo intangível, porém mesmo possuindo essa caraterística ele não é gerado no vácuo. Nonaka e Takeuchi (2008, p. 99) afirmam que: “o conhecimento não pode ser criado no vácuo e necessita de um lugar onde a informação receba significado através da interpretação para tornar-se conhecimento.”

A esse ambiente dá-se o nome de BA (NONAKA; TAKEUCHI, 2008). As organizações devem fomentar a criação do conhecimento através da criação desses ambientes. Entende-se por BAs tudo o que for necessário para cocriação de valores entre os indivíduos através de meios tecnológicos ou não. O mais importante é o ambiente ser “energizado” para dar energia e qualidade ao processo de criação do

conhecimento (NONAKA; TAKEUCHI, 2008). Barbosa (2020), corrobora com Nonaka e Takeuchi (2008) destacando o conceito de “Ba”. Para o autor ele se refere a contextos compartilhados, focados na criação de conhecimento. Pode-se criar ambientes virtuais, apoiados pela tecnologia, ou ambientes físicos, como salas de reuniões, ambos permitindo a interação entre os indivíduos.

Ativos de conhecimento originados do processo de criação de conhecimento, podem ser considerados recursos de alta qualidade que podem trazer valor às organizações (GUO; XUE, 2020). Santos e Zattar (2019) preponderam que a Gestão do Conhecimento não é responsável apenas pelos ativos de conhecimento, pois ela torna-se responsável também em manter todos os processos que atuam de forma direta ou indireta sobre esses ativos, sejam eles processos de desenvolvimento, utilização, preservação ou compartilhamento do conhecimento.

2.2 GESTÃO DO CONHECIMENTO

A importância do conhecimento para as empresas é notória e expressiva, portanto, ele deve ser gerenciado de forma adequada. Para atender essa necessidade, surge a Gestão do Conhecimento, que dedica esforços na geração e retenção do conhecimento em linhas gerais. Ela pode ser caracterizada como uma série de técnicas e processos que tem o objetivo de criar, representar e distribuir conhecimento, com foco na melhoria do desempenho organizacional, estimulando a inovação e compartilhando lições aprendidas (MARCÃO; PESTANA; SOUSA, 2021).

O comprometimento da alta administração das organizações é de suma importância para a Gestão do Conhecimento, uma vez que barreiras culturais deverão ser rompidas e investimentos meramente financeiros não garantem o sucesso da Gestão do Conhecimento. Davenport (1998) já advogava que a Gestão do Conhecimento vai muito além de investimento em tecnologias ou gerenciamento da informação. Alguns aspectos são relevantes, como o papel da alta administração, a cultura e as estruturas organizacionais, as práticas de gestão de recursos humanos, os impactos dos sistemas de informação, a mensuração de resultados, as alianças estratégicas e o redesenho de processos. Valentim (2021), em consonância com o autor, salienta que a cultura organizacional e a cultura informacional representam elementos significativos para a Gestão do Conhecimento.

As características do ambiente corporativo fazem com que a Gestão do

Conhecimento nesse sistema se torne paradoxalmente complexa. Uma vez que o conhecimento é formado por opostos, o tácito e explicito, o sucesso no ambiente das empresas necessita abordar não apenas um conjunto de opostos, mas também uma completa multidão de opostos ao mesmo tempo (NONAKA; TAKEUCHI, 2008). Ainda, outros fatores como a heterogeneidade de interesses, perspectivas e questões de pesquisa (ÁLVARES *et al.*, 2020) e os processos organizacionais (SILVA, 2020) contribuem para essa complexidade. Em uma visão utilitarista, Santos e Zattar (2019), advogam que a Gestão do Conhecimento tem como um dos seus objetivos identificar os recursos gerados pelo conhecimento, visando o aproveitamento dos mesmos dentro da organização. Pode-se citar o aproveitamento das principais competências comerciais, a aceleração da inovação e a melhoria dos tempos de tomada de decisões (DAVENPORT, 1998).

2.3 PROCESSO PARA GESTÃO DO CONHECIMENTO

O modelo de gestão é um aspecto importante na Gestão do Conhecimento. É necessário que ele contemple, mesmo que de forma genérica, a concepção de como a empresa deve compreender e adotar práticas de Gestão do Conhecimento. Dalkir (2005) e Hjørland (2021) ponderam que o modelo precisa ter uma estrutura conceitual, para que possa alcançar os benefícios esperados com sua implementação. Existem diversas metodologias que guiam a implementação de Gestão do Conhecimento. Cada modelo possui uma abordagem diferenciada de gestão, portanto, salienta-se que a compatibilidade com o ambiente que irão permear é importante, a fim de ir ao encontro das necessidades das empresas, para melhor escolha de modelo.

Valentim (2021) salienta que um processo de Gestão do Conhecimento metodologicamente pode seguir alguns passos para obter sucesso. A autora destaca os seguintes pontos: descobrir conhecimentos; assegurar que o conhecimento esteja disponível; facilitar o desenvolvimento efetivo de novos conhecimentos; assegurar que os novos conhecimentos sejam disseminados a todos os segmentos da organização; assegurar que o público interno da organização saiba onde estão os conhecimentos e como acessá-los.

Para Anupan (2020), a Gestão do Conhecimento pode também estar focada na integração do conhecimento e a gestão com foco nos processos de gestão da informação através do armazenamento sistemático do conhecimento em um ambiente

organizacional e social.

Bidian (2014) fornece uma visão histórica e cronológica de alguns dos modelos mais influentes do ciclo de vida da Gestão do Conhecimento, com base na sua adoção acadêmica e frequência de utilização pelos praticantes. Cada um deles representa um avanço no pensamento sobre o ciclo de vida de Gestão do Conhecimento e introduz novos elementos a serem considerados na compreensão de como o conhecimento organizacional é processado ao longo de sua vida útil. O trabalho dos autores fornece uma visão holística do ciclo de vida do conhecimento, incluindo diferentes formas de conhecimento, integrando a noção de aprendizagem de segunda ordem ou de ciclo duplo e associando iniciativas e tecnologias facilitadoras dos processos.

2.4 MODELOS DE GESTÃO DO CONHECIMENTO

Alguns modelos de Gestão do Conhecimento surgiram ao longo do tempo. Pode-se salientar os modelos de Krogh e Ross (1995), Choo (1996) e Nonaka e Takeuchi (2008). Cada um desses modelos possui especificações singulares. Um aspecto importante na utilização da Gestão do Conhecimento em uma organização é a adoção de um modelo que contemple, mesmo que de forma genérica, a concepção de como a empresa deve compreender e adotar práticas de Gestão do Conhecimento.

O foco da Gestão do Conhecimento para Krogh e Roos (1995) tem como base as suas epistemologias, ou seja, está focado na origem do conhecimento. Com base no tipo de conhecimento, já existente ou um conhecimento novo, que está sendo acessado, usam-se dois conjuntos de atividades de Gestão do Conhecimento, *exploitation* e *exploration*. A *exploitation* está relacionada ao aproveitamento dos domínios de conhecimento existentes. Este é o conhecimento que está embutido nas diferentes áreas funcionais de uma unidade de negócios. A ideia-chave na *exploration* é a alavancagem do conhecimento de diferentes unidades funcionais para responder às mudanças ambientais. A *exploration* está relacionada à proteção e ao desenvolvimento do conhecimento de novos domínios (NAZIR; PINSONNEAULT, 2021).

Diferente do anterior, no modelo proposto por Choo (1996) o foco está em como as informações manipuladas no dia a dia podem resultar na criação de novos conhecimentos e dar posteridade a ele. A absorção de informações do ambiente

externo em cada ciclo de aprendizagem é o propulsor desse modelo. Pinheiro (2020) explana que o objetivo deste modelo é focado no longo prazo. Ele busca garantir que as organizações vão conseguir se adaptar ao longo do tempo a um ambiente dinâmico e complexo, utilizando-se de atividades de prospecção e interpretação de informação que são consideradas relevantes. Essa abordagem permite que as empresas compreendam as mudanças, tendências e cenários sobre clientes, fornecedores, concorrentes e outros agentes externos.

Por outro lado, o modelo proposto por Nonaka e Takeuchi (2008) é holístico para criação de conhecimento e está direcionado para criação de inovação com o conhecimento produzido. A abordagem desse modelo está focada na integração do conhecimento tácito e explícito. Upadhaya *et al.* (2021) enfatizam que o modelo proposto de Nonaka e Takeuchi pode ser interpretado como o processo de conversão de conhecimento explícito, adquirido externamente, para o conhecimento tácito pelos indivíduos. Tal conversão, inserida neste modelo, é denominada de modelo SECI (Socialização, Externalização, Combinação e Internalização) e tem como resultado esperado melhorar a competitividade da organização e também seu desempenho de inovação.

O presente estudo assume a abordagem holística da Gestão do Conhecimento como uma tendência no campo da administração, conforme tem sido demonstrado em publicações recentes (CORRÊA, 2019; EVANS *et al.*, 2014; RAZI, *et al*., 2017). Fatores subjacentes às condições capacitadoras apontadas por Nonaka e Takeuchi (2008), tais como cultura organizacional, estrutura organizacional e infraestrutura de tecnologia da informação, formam a dimensão holística da Gestão do Conhecimento (RAZI *et al.*, 2017) e definem a característica holística do modelo de Nonaka e Takeuchi.

O modelo SECI (NONAKA; TAKEUCHI, 2008) é a estrutura conceitual mais conhecida para a compreensão dos processos de geração de conhecimento nas organizações (FARNESE *et al.*, 2019). Ao buscar suporte empírico para o modelo SECI, Farnese *et al.* (2019) forneceram uma base atual de evidências sobre os modos de conversão de conhecimento teorizados por Nonaka e Takeuchi e reforçaram a relevância de se desenvolver pesquisas adotando o modelo SECI em diferentes contextos e desafios organizacionais, devido à sua consistência epistemológica no campo da Gestão do Conhecimento (FARNESE *et al.*, 2019).

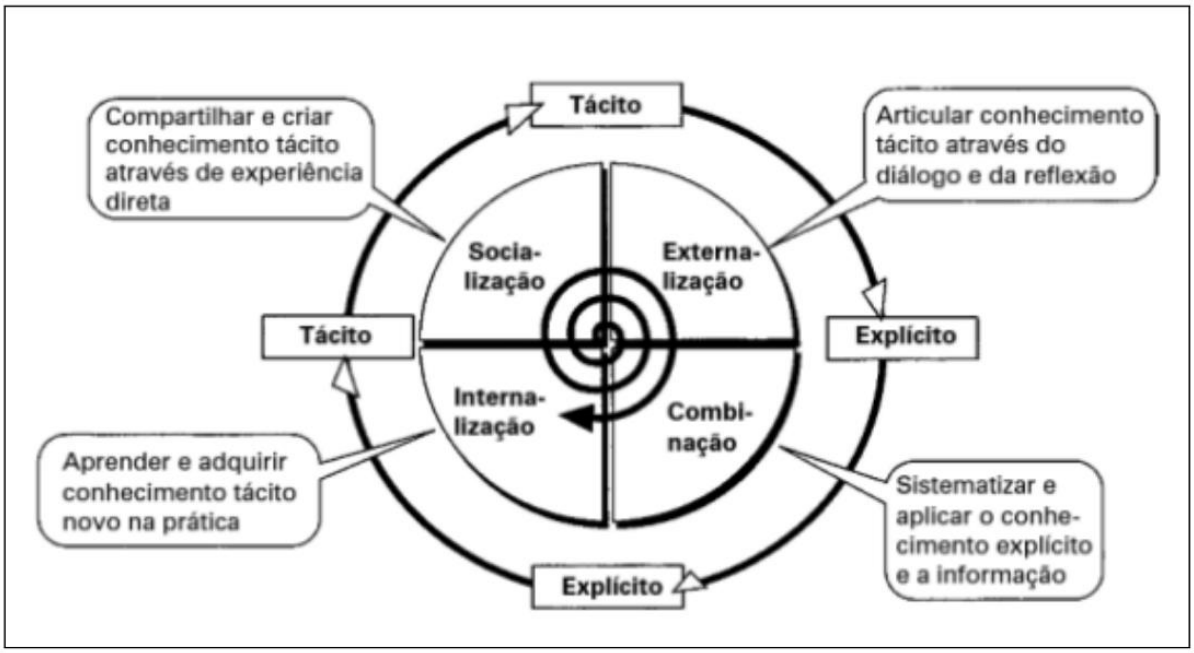
2.5 GESTÃO DO CONHECIMENTO SOB A ÓTICA DE NONAKA E TAKEUCHI

A criação do conhecimento depende da conversão e interação entre o conhecimento tácito e o explícito. Nonaka e Takeuchi (2008) defendem a conversão de quatro formas: (1) Socialização: de tácito para tácito; (2) Externalização: de tácito para explícito; (3) Combinação: de explícito para explícito; e (4) Internalização: de explícito para tácito. A esse ciclo os autores deram o nome de espiral do conhecimento, ou modelo SECI.

Os autores Dai, Liu e Shan (2021) definem o SECI como uma representação abstrata do processo de criação de conhecimento. Essa abstração fornece uma referência para o modelo de formação de aprendizagem moderna. Em consonância com os autores, Silva (2020) defende que o SECI é muito importante, pois ele ressalta a necessidade de se mobilizar e articular, no âmbito organizacional, o conhecimento tácito gerado individualmente pelos indivíduos na organização, para que dessa forma haja a criação de novos conhecimentos.

De acordo com Nonaka e Takeuchi (2008), o primeiro processo é a socialização, na qual o indivíduo compartilha o seu conhecimento com outro, por meio de experiências diretas. Logo após esse compartilhamento, o indivíduo articula esse conhecimento para um grupo de pessoas, sendo esse o processo de Externalização. Havendo a sistematização desse conhecimento, ocorre a Combinação, que flui do grupo para toda organização e, ao final, cada indivíduo recebe esse conhecimento e efetua a sua Internalização, aprendendo o novo conhecimento, transformando-o em tácito novamente, completando o ciclo de criação de conhecimento.

Figura 3 - Ciclo de criação do conhecimento



Fonte: Nonaka e Takeuchi (2008, p. 34).

O processo de criação do conhecimento, de acordo com os autores, orienta-se pela interação entre os processos de conversão do conhecimento tácito, comportando-se de forma espiral, gerando o que os autores chamam de espiral do conhecimento, conforme advogam Nonaka e Takeuchi:

> É importante observar que o movimento através dos quatro modos de conversão do conhecimento forma uma espiral, e não um círculo. Na espiral da criação do conhecimento, a interação entre o conhecimento tácito e o conhecimento explícito é amplificada por meio de quatro modos de conversão do conhecimento. A espiral torna-se maior em escala a medida que sobe para os níveis ontológicos (NONAKA; TAKEUCHI, 2008, p. 98).

Os autores afirmam que, em uma empresa criadora de conhecimento, os quatro padrões listados possuem uma interação dinâmica entre eles, gerando a espiral do conhecimento. A conversão do conhecimento deve chegar aos níveis mais altos da organização e, ao mesmo tempo, no operacional da empresa, ou seja, deve ser criado em qualquer ambiente. Sem esse cenário, não há como surgir a espiral do conhecimento, conforme Nonaka e Takeuchi (2008, p. 55) “A espiral emerge quando a interação entre conhecimento tácito e o explícito é elevada dinamicamente de um nível ontológico mais baixo para níveis mais elevados.”

Nonaka e Takeuchi (2008) advogam que o fator primordial para criação do conhecimento está nos esforços dedicados à conversão do conhecimento tácito, sendo ele a base de criação do conhecimento organizacional dentro da espiral do

conhecimento. Nem todo conhecimento tácito consegue tornar-se explícito para toda a organização. A Gestão do Conhecimento evoluiu nos últimos anos, porém ainda enfrenta algumas barreiras para sua aplicação nas Organizações.

Os autores afirmam que, embora muito se tenha falado sobre a importância do conhecimento na administração, pouco se despendeu recursos para gerir como o conhecimento é criado e administrado (NONAKA; TAKEUCHI, 2008). A partir dos trabalhos originais de Nonaka, estudos recentes têm atualizado os desafios encontrados para a Gestão do Conhecimento, mas, ainda assim, reconhecem que a problemática da não suficiência dos recursos empregados para a criação e administração do conhecimento permanece (FARNESE *et al.*, 2019; PHILIPSON; KJELLSTRÖM, 2020).

2.6 SEGURANÇA DA INFORMAÇÃO

A importância da informação vem aumentando de forma exponencial a cada instante dentro das Organizações, tornando-se um fator chave de produção (KOLO; MIERZEJEWSKA, 2019) em todos os níveis organizacionais. Quando a informação é adquirida, organizada e disseminada, torna-se um recurso estratégico fundamental para a tomada de decisões (BARBOSA, 2020). Neste sentido Silveira e Varvakis (2020) defendem que as empresas que utilizam informações e conhecimento para melhorar seu desempenho, conseguem obter maior vantagem competitiva.

A informação é um ativo e, por isso, precisa ser gerenciada e protegida. Todo ativo está sujeito a ameaças e riscos que podem comprometer sua utilização. Os ativos estão sob constantes riscos, pois existem inúmeras ameaças que podem explorar as suas vulnerabilidades. Conforme Oliveira (2021), Aiqon (2020) e Amorim (2020), o risco, em segurança da informação, é a probabilidade de uma ameaça explorar vulnerabilidades para causar perdas ou danos a um ativo ou grupo de ativos da Organização. O risco é considerado um evento incerto com uma data incerta.

É possível destacar dois pontos importantes sobre a segurança da informação. Por um lado, as tecnologias e o uso da internet ampliaram a geração, armazenamento e distribuição de informações. Por outro, tem sido registrado um crescente número de ataques cibernéticos (LIU *et al.*, 2021). Bennet *et al.* (2021) afirmam que a segurança cibernética é um problema constante para as organizações, porém os estudos organizacionais ainda não entraram nesta arena da pesquisa, deixando esta temática

descoberta nas organizações.

A Segurança da Informação e todos os seus conceitos e práticas surgem nesse ambiente com o intuito de proteger e gerenciar a informação, com foco na continuidade do negócio. Dutra *et al.* (2019) afirmam que a segurança da informação não está limitada somente aos controles computacionais, isso permite que diferentes abordagens sejam utilizadas para a sua definição conceitual.

A definição de Segurança da informação de acordo com Zeferino (2020) e Bennet *et al.* (2021), perpassa por definições como sendo a proteção de informações, dados, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a mitigar o impacto de incidentes de segurança que possam comprometer a informação. A segurança da informação, para ter sucesso de implementação, necessita de um conjunto adequado de controles, políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013)

Para que a segurança da informação seja alcançada em um ambiente, é necessária a implementação de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Os controles necessitam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, e dessa forma assegurar que a segurança da informação ganhe forma nas organizações (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(b), 2013).

A Segurança da Informação também é definida por meio de três pilares: a integridade, que se relaciona com a fidedignidade e totalidade da informação bem como sua validade; a disponibilidade, que se relaciona com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro; e a confidencialidade, que está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013; ESWARAN; VINAYAGAMOORTHI, 2019; BARTH *et al.*, 2021).

Corroborando com a definição dos três pilares documentada na ISO 27001, Bennet *et al.* (2021) afirmam que essa tríade tem como objetivo permitir o acesso de indivíduos autorizados a registros completos e inalterados ao mesmo tempo em que desabilita o acesso de indivíduos não autorizados.

Aramuni e Maia (2020) sustentam a retórica dos pilares de segurança. Os autores explanam que:

> A integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental; A disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário; A confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo; (2020, p. 33).

Assim como a Gestão do Conhecimento possui metodologias para sua implementação, a Segurança da Informação possui como normativa mais desenvolvida a NBR ISO/IEC 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013). Ela auxilia na construção de um Sistema de Gestão de Segurança da Informação (SGSI), levando em consideração temáticas como gestão de riscos e mais 114 controles específicos em sua versão de 2013, que garantem a implementação desse sistema. Os autores Ide, Nakamura e Reynaldo (2019) salientam que a família da ISO 27001 é um dos *frameworks* mais utilizados no mundo para criar esse sistema de gestão.

A NBR ISO/IEC 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013) define gestão de risco como toda a atividade que coordena o rumo dos processos da organização em relação aos riscos. A norma esmiúça as ramificações da gestão de risco, tendo no escopo do Sistema de Gestão da Segurança da Informação (SGSI) controles e conformidades específicas do tratamento de riscos. O processo de implantação de Segurança da Informação inicia-se com uma avaliação e análise de riscos, listando-os e desenvolvendo planos de ação para mitigá-los ao máximo.

Vale destacar que o processo de segurança da informação está relacionado diretamente às pessoas, assim como a criação de conhecimento. Por isso, pode-se afirmar que a maior ameaça para a segurança da informação é o fator humano (MITNICK, 2003). Para reduzir os riscos relacionados a erros humanos ou atos criminosos por parte das pessoas, recomenda-se que as empresas estabeleçam políticas de informação, controles e procedimentos, a fim de mitigá-los, reduzindo a probabilidade de incidentes (ARAMUNI; MAIA, 2020).

2.7 NBR ISO/IEC 27001 E ISO/IEC 27002

A Norma NBR ISO/IEC 27001 foi desenvolvida com o objetivo de prover, estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão

de Segurança da Informação (SGSI). Adotar um SGSI é uma decisão estratégica para as empresas (NBRISO/IEC 27001, 2013).

Em consonâncias com os pilares de segurança da informação, já citados e defendidos por vários autores, o SGSI tem como premissa a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de processos de gestão de riscos, e dessa forma fornecer a confiança para as partes interessadas (NBRISO/IEC 27001, 2013).

Os controles e seus objetivos de controles estão listados no Anexo A da norma entre as seções 5 e 18, totalizando 114 controles de segurança da informação. O Anexo A é representado pela NBR ISO/IEC 27002:2013. Uma empresa para obter a certificação na ISO 27001, precisa cumprir ou justificar a não aplicabilidade de cada um dos controles. Em anexo à essa proposta está o Anexo A da norma ISO/IEC 27001.

Os 114 controles estão divididos em 14 sessões de acordo com o objetivo de cada um deles. A norma enumera as sessões em: Políticas de segurança da informação, Organização da segurança da informação, Segurança em recursos humanos, Gestão de ativos, Controle de acesso, Criptografia, Segurança física e do ambiente, Segurança nas operações, Segurança nas comunicações, Aquisição, desenvolvimento e manutenção de sistemas, Relacionamento na cadeia de suprimento, Gestão de incidentes de segurança da informação, 17 Aspectos da segurança da informação na gestão da continuidade do negócio e Conformidade.

A norma ISO/IEC 27002 foi criada para servir como referência na seleção de controles dentro do processo de implementação do SGSI, podendo ser utilizada como um documento de orientação para as organizações implementarem controles de segurança da informação. Nelas estão descritos os 114 controles de acordo com cada seção de forma detalhada e com orientações de como cada controle pode ser implementado (NBR ISO/IEC 27002, 2013). Cada seção possui um foco específico de tratativa sendo:

a) Políticas de segurança da informação: os controles contidos nesta seção estão focados na construção de políticas de segurança para a empresa. Essa política abrange processos e pessoas com orientações de como todos devem seguir um comportamento seguro e respeitar as regras de segurança impostas;
b) Organização da segurança da informação: nesta seção os controles estão

direcionados para a organização dos papéis dentro do SGSI, como a definição de responsabilidades e cargos;

c) Segurança em recursos humanos: a área de recursos humanos é primordial para o sucesso do SGSI. Nesta seção são estabelecidos controles focados em todas as fases de contratação e desligamento de funcionários, bem como a coleta de assinaturas nos termos de responsabilidade;
d) Gestão de ativos: a identificação dos ativos é um fator preponderante para o sucesso de um SGSI. A ISO 27002, enfatiza que os ativos devem ser classificados e responsáveis atrelados a eles. Destaca-se aqui os controles de classificação de informação e rótulos;
e) Controle de acesso: controlar o acesso é crucial para a segurança da informação. Nesta seção a norma evidencia controles de acesso às informações, impedindo que sejam expostas informações sigilosas para pessoas que não podem ter acesso;
f) Criptografia: os controles contidos nesta seção são para padronização os controles de chaves criptográficas utilizadas no ambiente;
g) Segurança física e do ambiente: Os controles de segurança também estão atrelados ao ambiente físicos das empresas. A seção de segurança física e do ambiente possui controles focados na proteção dos equipamentos e no acesso físico;
h) Segurança nas operações: os processos diários de operação de tecnologia devem ser padronizados e auditáveis para a manutenção do ambiente. Nesta seção a norma pondera controles focados na operacionalização das tarefas diárias de segurança como backup, gestão de mudança e registro de logs;
i) Segurança nas comunicações: os meios de comunicação necessitam ser administrados da forma correta, por isso nesta seção a norma exibe controles direcionados para a tecnologia de comunicação como controles e segmentação de redes de computadores;
j) Aquisição, desenvolvimento e manutenção de sistemas: a utilização de sistemas cresce de forma exponencial e a norma neste ponto possui controles de segurança específicos voltados para a escolha correta de tecnologias que atendam às necessidades de segurança da empresa, tanto

no desenvolvimento de sistemas como na escolha de parceiros de tecnologia;

k) Relacionamento na cadeia de suprimento: o fornecimento de serviços e suprimentos é vital para o bom funcionando do SGSI, por isso a norma abrange controles focados em fornecedores que serão contratados e também acordos de confidencialidades nesta cadeia;
l) Gestão de incidentes de segurança da informação: todos os incidentes de segurança precisam ser documentados e a norma neta seção explana os controles necessários para documentar e organizar os incidentes, juntamente com os seus planos de resposta;
m) Aspectos da segurança da informação na gestão da continuidade do negócio: um dos principais objetivos da segurança da informação é a continuidade de negócio e proteção da cadeia de valor. A norma possui controles específicos no que tange o negócio e a manutenção dos processos diários. Eles estão contidos nesta seção e abrangem a análise crítica recorrente dos processos do SGSI;
n) Conformidade: na última seção, a norma abrange controles focados às legislações vigentes para que o SGSI esteja adaptado de acordo com a necessidade da legislação de cada local, como por exemplo, a LGPD Brasileira.

Em um processo de certificação na ISO/IEC 27001, todos os 114 controles contidos nas 14 seções devem ser implementados ou justificados em um Plano de Aplicabilidade, semelhante a um *checklist* que irá orientar a conformidade do ambiente. Os recursos dispendidos para a implementação dos controles precisam ser balanceados, levando em consideração a probabilidade de danos ao negócio, resultado dos problemas de segurança pela ausência desses controles (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013).

2.8 PONTOS DE CONSENSO ENTRE GESTÃO DO CONHECIMENTO E SEGURANÇA DA INFORMAÇÃO

Schwartz (2006b) defende que a Gestão do Conhecimento é multidisciplinar. Como característica a Gestão do Conhecimento recebe contribuições das ciências cognitivas, educação, inteligência artificial, psicologia, tecnologia e sistemas de

informação e teoria organizacional.

Schwartz (2006a) divide a GC em camadas que se interligam entre si, estruturando a multidisciplinariedade. A primeira camada apresenta-se como o abrigo de questões filosóficas e pressupostos fundamentais que fomentam a escolha de processos de Gestão do Conhecimento. A segunda camada é representada por processos de aquisição, organização e distribuição da informação, que devem ser implementados e adaptados para atender a terceira camada. A terceira camada é a Gerencial, Social e Organizacional, onde destacam-se os processos aprendizagem organizacional, capital intelectual, comunidades de prática, cultura organizacional, estratégia, motivação e vantagem competitiva.

A quarta, e última camada, é onde residem as tecnologias de informação e comunicação essenciais para a Gestão do Conhecimento. Nesta camada trata-se da representação da informação, recuperação da informação, disseminação da informação e segurança, entre outros aspectos. Vale destacar a Segurança Cibernética que tem como objetivo a proteção do ativo, informação e conhecimento.

Um aspecto importante do processo de Gestão do Conhecimento defendido por Santos e Zattar (2019) é que ele deve garantir a disponibilização do conhecimento quando ele for necessário para ser utilizado. Esse aspecto vai ao encontro de um dos pilares de segurança da informação, o de disponibilidade, que visa manter a informação disponível quando requisitada pelo negócio. Neste sentido, pode-se identificar que existe um ponto de consenso entre as premissas da segurança da informação e a Gestão do Conhecimento.

Além de disponibilidade, a segurança da informação tem como pilar a integridade e a confidencialidade. Pode-se correlacionar o conceito de integridade com o processo de armazenamento do conhecimento, quando externalizados, seja em meio físico ou digital. Na conversão do conhecimento de tácito para explicito é necessário que ele seja documentado e esse processo deve garantir que a informação armazenada não seja corrompida para que possa ser utilizada posteriormente.

No que tange à confidencialidade, pode-se determinar que nem todo conhecimento pode ser acessado por qualquer pessoa. Conhecimentos estratégicos ou de produto necessitam de controle em seu compartilhamento, pois são sensíveis ao negócio das empresas. A adaptação dos controles de segurança da informação, pode melhorar o processo de Gestão do Conhecimento, fazendo com que o conhecimento esteja disponível quando for requisitado, íntegro e acessado somente

por pessoas autorizadas, pois o vazamento de um conhecimento sensível pode comprometer a cadeia de valor da empresa.

Para definição de alguns pontos de consenso entre o processo de Gestão do Conhecimento criado por Nonaka e Takeuchi (2008), denominado SECI, e os controles de Segurança da Informação proposto pela ISO/IEC 27001, utilizou-se uma matriz de priorização a fim de elucidar como cada um dos 114 controles podem estar relacionados em cada fase do SECI, para contribuir positivamente no processo de segurança.

Para essa matriz, definiu-se parâmetros numéricos para a intensidade de aderência dos controles a cada um dos processos do SECI. Os valores de aderência, que também podem ser entendidos como associação ou até impacto, foram arbitrados pelo autor deste trabalho a partir da literatura, com valores entre 0 e 9, onde 0 corresponde à inexistência de associação e 9 associação forte, conforme Tabela 1.

Tabela 1 - Intensidade

Intensidade	Valor
Inexistente	0
Fraca	1
Moderada	3
Forte	9

Fonte: Elaborado pelo autor (2022).

Cada um dos 114 controles recebeu a numeração de intensidade na relação de segurança com os processos de socialização, externalização, combinação e internalização. Para a seleção dos controles foi realizada uma análise semântica de seus enunciados em relação aos conceitos expressos na espiral do conhecimento.

A somatória resultante evidencia quais controles possuem maior consenso, onde entende-se que a soma de 36 pontos representa uma correlação muito alta em todos os processos e somatórias menores que 12 pontos representam uma correlação baixa em todos os processos. A descrição completa do nome de cada controle está ao final do trabalho, no Anexo A. A Tabela 2 apresenta os resultados obtidos nos cruzamentos das relações de segurança com os processos do SECI.

Tabela 2 - Relação de Consenso

Cláusula	Código de Controle	Socialização	Externalização	Combinação	Internalização	Soma
5 Políticas de segurança da informação	5.1.1	9	9	9	9	36
	5.1.2	1	1	1	1	4
6 Organização da segurança da informação	6.1.1	9	9	9	9	36
	6.1.2	1	3	3	9	16
	6.1.3	0	0	0	0	0
	6.1.4	0	0	0	0	0
	6.1.5	0	0	0	0	0
	6.2.1	0	0	0	0	0
	6.2.2	0	0	0	0	0
7 Segurança em recursos humanos	7.1.1	0	0	0	0	0
	7.1.2	3	3	3	3	12
	7.2.1	9	9	9	9	36
	7.2.2	9	9	9	9	36
	7.2.3	3	3	3	0	9
	7.3.1	0	9	9	0	18
8 Gestão de ativos	8.1.1	0	0	0	0	0
	8.1.2	0	0	0	0	0
	8.1.3	0	0	0	0	0
	8.1.4	0	0	0	0	0
	8.2.1	9	9	9	3	30
	8.2.2	9	9	9	3	30
	8.2.3	0	0	0	0	0
	8.3.1	0	0	0	0	0
	8.3.2	0	0	0	0	0
	8.3.3	0	0	0	0	0
9 Controle de acesso	9.1.1	3	9	9	0	21
	9.1.2	0	0	0	0	0
	9.2.1	0	0	0	0	0
	9.2.2	0	0	0	0	0
	9.2.3	3	9	9	0	21
	9.2.4	3	9	9	0	21
	9.2.5	3	9	9	0	21
	9.2.6	9	9	9	0	27
	9.3.1	0	0	0	0	0
	9.4.1	3	9	9	0	21
	9.4.2	0	0	0	0	0
	9.4.3	0	0	0	0	0
	9.4.4	0	0	0	0	0

	9.4.5	0	0	0	0	0
10 Criptografia	10.1.1	0	0	0	0	0
	10.1.2	0	0	0	0	0
11 Segurança física e do ambiente	11.1.1	0	0	0	0	0
	11.1.2	0	0	0	0	0
	11.1.3	0	0	0	0	0
	11.1.4	0	0	0	0	0
	11.1.5	0	0	0	0	0
	11.1.6	0	0	0	0	0
	11.2.1	0	0	0	0	0
	11.2.2	0	0	0	0	0
	11.2.3	0	0	0	0	0
	11.2.4	0	0	0	0	0
	11.2.5	0	0	0	0	0
	11.2.6	0	0	0	0	0
	11.2.7	0	0	0	0	0
	11.2.8	0	0	0	0	0
	11.2.9	0	0	0	0	0
12 Segurança nas operações	12.1.1	0	0	0	0	0
	12.1.2	0	0	0	0	0
	12.1.3	0	0	0	0	0
	12.1.4	0	0	0	0	0
	12.2.1	0	0	0	0	0
	12.3.1	0	0	0	0	0
	12.4.1	0	0	0	0	0
	12.4.2	0	0	0	0	0
	12.4.3	0	0	0	0	0
	12.4.4	0	0	0	0	0
	12.5.1	0	0	0	0	0
	12.6.1	0	0	0	0	0
	12.6.2	0	0	0	0	0
	12.7.1	0	0	0	0	0
13 Segurança nas comunicações	13.1.1	0	0	0	0	0
	13.1.2	0	0	0	0	0
	13.1.3	0	0	0	0	0
	13.2.1	0	0	0	0	0
	13.2.2	0	0	0	0	0
	13.2.3	0	0	0	0	0
	13.2.4	0	0	0	0	0
14 Aquisição, desenvolvimento e manutenção de sistemas	14.1.1	0	0	0	0	0
	14.1.2	0	0	0	0	0
	14.1.3	0	0	0	0	0
	14.2.1	0	0	0	0	0

	14.2.2	0	0	0	0	0
	14.2.3	0	0	0	0	0
	14.2.4	0	0	0	0	0
	14.2.5	0	0	0	0	0
	14.2.6	0	0	0	0	0
	14.2.7	0	0	0	0	0
	14.2.8	0	0	0	0	0
	14.2.9	0	0	0	0	0
	14.3.1	0	0	0	0	0
15 Relacionamento na cadeia de suprimento	15.1.1	9	9	9	0	27
	15.1.2	9	9	9	0	27
	15.1.3	0	0	0	0	0
	15.2.1	0	0	0	0	0
	15.2.2	0	0	0	0	0
16 Gestão de incidentes de segurança da informação	16.1.1	0	0	0	0	0
	16.1.2	3	3	3	0	9
	16.1.3	3	3	3	0	9
	16.1.4	0	0	0	0	0
	16.1.5	0	0	0	0	0
	16.1.6	0	0	0	0	0
	16.1.7	0	0	0	0	0
17 Aspectos da segurança da informação na gestão da continuidade do negócio	17.1.1	0	0	0	0	0
	17.1.2	0	0	0	0	0
	17.1.3	0	0	0	0	0
	17.2.1	0	0	0	0	0
18 Conformidade	18.1.1	9	9	9	3	30
	18.1.2	9	9	9	3	30
	18.1.3	0	0	0	0	0
	18.1.4	9	9	9	3	30
	18.1.5	0	0	0	0	0
	18.2.1	0	0	0	0	0
	18.2.2	0	0	0	0	0
	18.2.3	0	0	0	0	0

Fonte: Elaborado pelo autor (2022).

A aplicação da matriz evidenciou 20 controles com correlações importantes em uma ou mais das fases do SECI. Destaca-se que alguns controles da ISO/IEC 27001 possuem alto nível de consenso com a somatória de 36 pontos. Na Tabela 3, está exposto o nome de cada controle e a sua pontuação.

Tabela 3 - Controles Selecionados

Controle	S	E	C	I	Soma
Políticas para segurança da informação	9	9	9	9	36
Responsabilidades e papéis pela segurança da informação	9	9	9	9	36
Segregação de funções	1	3	3	9	16
Termos e condições de contratação	3	3	3	3	12
Responsabilidades da direção	9	9	9	9	36
Conscientização, educação e treinamento em segurança da informação	9	9	9	9	36
Responsabilidades pelo encerramento ou mudança da contratação	0	9	9	0	18
Classificação da informação	9	9	9	3	30
Rótulos e tratamento da informação	9	9	9	3	30
Política de controle de acesso	3	9	9	0	21
Gerenciamento de direitos de acesso privilegiados	3	9	9	0	21
Gerenciamento da informação de autenticação secreta de usuários	3	9	9	0	21
Análise crítica dos direitos de acesso de usuário	3	9	9	0	21
Retirada ou ajuste de direitos de acesso	9	9	9	0	27
Restrição de acesso à informação	3	9	9	0	21
Política de segurança da informação no relacionamento com os fornecedores	9	9	9	0	27
Identificando segurança da informação nos acordos com fornecedores	9	9	9	0	27
Identificação da legislação aplicável e de requisitos contratuais	9	9	9	3	30
Direitos de propriedade intelectual	9	9	9	3	30
Proteção e privacidade de informações de identificação pessoal	9	9	9	3	30

Fonte: Elaborado pelo autor (2022).

Todos os controles resultantes possuem pontuação maior ou igual a 12 pontos, indicando grau de consenso, mesmo que baixo, em algum dos processos. Com esse resultado é possível evidenciar que existe correlação entre Gestão do Conhecimento e Segurança da Informação e que ambas as metodologias podem interagir para uma melhoria de processo.

No próximo capítulo apresentam-se os procedimentos metodológicos que serão desenvolvidos para que esta proposta seja validada junto aos especialistas.

3 PROCEDIMENTOS METODOLÓGICOS

Este capítulo explana como a pesquisa foi desenvolvida detalhando o delineamento da pesquisa, sua unidade de análise, as técnicas de coleta e de análise utilizadas, além das limitações do método.

3.1 DELINEAMENTO DA PESQUISA

A abordagem escolhida para este estudo foi a qualitativa, sendo ela apropriada para a análise de casos concretos em suas peculiaridades locais e temporais, partindo das expressões e atividades das pessoas em seus contextos locais.

Como estratégia de pesquisa, foi adotado o método Delphi. (HSU; SANDFORD, 2007) explanam que o método Delphi é uma pesquisa de consenso de especialistas, onde é coletada uma variedade de opiniões, em várias rodadas, até que haja consenso entre elas. Devido à sua poderosa técnica de investigação (FACIONE, 1990), ela permite reunir um conjunto de especialistas, alcançando resultados densos sobre a temática proposta. Marques e Freitas (2018, p. 98) enfatizam que: "Tal potencialidade possibilita fazer leituras profundas da realidade e serve de base para uma melhor compreensão dos fenômenos [. . .]".

O método Delphi foi desenvolvido por órgãos de defesas norte-americanos no início da década de 1950, no auge da Guerra Fria (LINSTONE; TUROFF, 2002). Originalmente o objetivo deste método era obter um consenso confiável de um grupo de militares especialistas em defesa sobre possíveis ataques com bombas atômicas (BOBERG; MORRIS-KHOO, 1992). Mukherjee *et al.* (2015) consideraram que o método Delphi é uma abordagem eficiente, inclusiva, sistemática e estruturada que pode ser aplicada para abordar questões complexas em uma variedade de disciplinas distintas.

Durante o processo do Delphi, pode-se observar a dissonância entre as opiniões dos especialistas, permitindo a sistematização, a compilação delas e, posteriormente, o reenvio ao grupo, buscando o consenso. Desta forma após conhecer as opiniões dos outros especialistas e as respostas do grupo, os participantes podem refinar, alterar ou defender as suas respostas e enviar novamente aos pesquisadores, onde um novo questionário é elaborado a partir dessas novas informações (FREITAS; MARQUES, 2018). Em suma, o método Delphi está

alicerçado em rodadas de questionários estruturados, seguidos por *feedback* anônimo para os participantes (WALTERS *et al.*, 2021).

Existem, na literatura, três tipos de técnicas Delphi: Convencional, Normativo e *Policy Delphi*. O Delphi convencional tem o objetivo de buscar a construção de opinião sobre um determinado assunto. O Delphi normativo está direcionado para a identificação e estabelecimento de objetivos e prioridades, em vez de especulações e previsões. No *Policy Delphi*, a busca é por pontos de vista opostos sobre um determinado assunto e tende a envolver assuntos como políticas e sua implementação - nesse caso, o foco não é o consenso, mas a identificação das opiniões divergentes (YOUSUF, 2007). A técnica utilizada nesta pesquisa foi a Delphi Convencional, pois o objetivo principal deste trabalho é encontrar a opinião dos especialistas sobre um assunto determinado.

Nas três abordagens, algumas semelhanças de características predominam de acordo Linstone e Turoff (2002), Silva e Tanaka (1999) e Yousuf (2007):

a) anonimato;

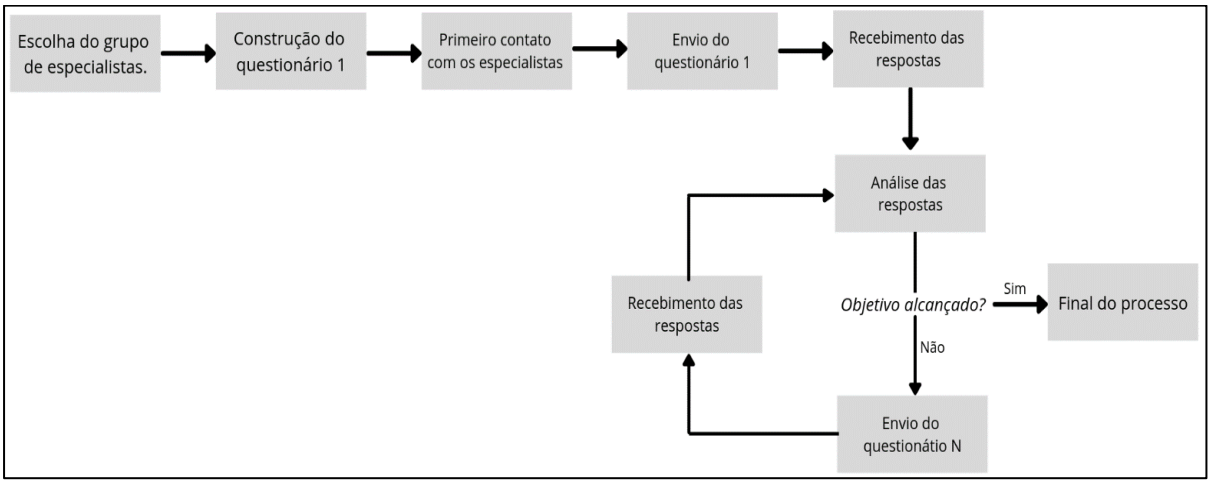
b) *feedback* das contribuições individuais;

c) construção e apresentação da resposta do grupo como um todo;

d) possibilidade de revisão e alteração das respostas.

Para a implementação do processo do método Delphi, pode-se seguir uma sequência de atividades, a fim de organizar cada uma das etapas, segundo os mesmos autores.

Figura 4 - Fluxo *Delphi*



Fonte: Elaborado pelo autor (2022) a partir de Linstone e Turoff (2002), Silva e Tanaka (1999) e Yousuf (2007).

Um dos pontos mais fortes do método Delphi, em comparação com outras técnicas, é o fato de que as influências sobre as respostas são reduzidas de pressões sociais entre os entrevistados. Como é respondido de forma anônima, os especialistas podem expressar suas opiniões sem receberem influências externas para obtenção do consenso (WALTERS *et al.*, 2021).

A seguir estão detalhados os principais aspectos que foram necessários para execução deste trabalho.

3.2 DEFINIÇÃO DOS PARTICIPANTES DA PESQUISA

A seleção dos especialistas é fundamental no método Delphi. É preponderante que o grupo de especialistas tenha imparcialidade e interesse no assunto (MARQUES; FREITAS, 2018). Para a realização desta pesquisa, foram envolvidos 20 especialistas nos assuntos da temática desta dissertação, sendo dez especialistas de Segurança da Informação e dez especialistas em Gestão do Conhecimento. Todos os envolvidos das áreas específicas possuem capacidade analítica para compreender os controles e as fases da espiral do conhecimento.

O número necessário de especialistas para aplicar esse método é muito variado (POWELL, 2003), porém existe a indicação que um número coerente não deve ser inferior a 10, tendo no máximo algumas dezenas de membros (GRISHAM, 2009). Outro ponto preponderante para essa metodologia é que as pessoas escolhidas estejam comprometidas com todo o processo.

Para comprovar o conhecimento em Segurança da Informação, os especialistas selecionados foram todos profissionais do círculo de contato do pesquisador de empresas privadas e prestadoras de serviços de Segurança da Informação. Eles possuíam pelo menos uma das seguintes certificações na área de Segurança da Informação:

a) DCPT (*Desec Certified Penetration Tester*);

b) CISSP (*Certified Information System Security Professional*);

c) Sophos Certified Architect;

d) Sophos Certified Engineer.

A certificação DCPT (*Desec Certified Penetration Tester*) é expedida pela Desec Security. A empresa é a principal formadora de profissionais da área de Segurança Ofensiva da América Latina. Sua certificação é altamente reconhecida no

mercado da segurança da informação. Para conquistar a certificação os candidatos precisam realizar uma prova prática de 24 horas consecutivas para validar seus conhecimentos.

A CISSP *(Certified Information System Security Professional*) é uma certificação emitida e mantida pela instituição ISO. O objetivo dela é avaliar o conhecimento em Segurança da Informação dos profissionais que trabalham na área. São reconhecidos como padrão de excelência global em segurança da informação.

As certificações *Sophos Certified Architect* e *Sophos Certified Engineer,* são emitidas exclusivamente pela *Sophos*. Ela é líder mundial em tecnologias de Segurança Cibernéticas. Um profissional que deseja possuir essas certificações é submetido a provas avançadas envolvendo conceitos de Segurança da Informação e tecnologia.

Os profissionais selecionados para fazer parte do grupo de especialistas que fizeram parte de todas as rodadas de perguntas foi composto por dois profissionais certificados DCPT, um profissional certificado CISSP, sete profissionais *Sophos Certified Architect* e um profissional *Sophos Certified Engineer*.

Os especialistas em Gestão do Conhecimento são envolvidos ativamente no estudo da temática ou na produção de material acadêmico. Como critério de escolha para fazer parte do grupo de especialistas, foram selecionados docentes ou discentes que realizam pesquisas na área de administração, com foco em Gestão do Conhecimento e pelo menos uma publicação realizada sobre a temática, comprovando seu envolvimento e conhecimento.

Desta forma todos os dez especialistas respondentes foram docentes ou discentes da área de administração, com publicações específicas sobre Gestão do Conhecimento. Destaca-se que, dos dez, seis especialistas são membros da SBGC (Sociedade Brasileira de Gestão do Conhecimento) e já implantaram projetos ou desenvolveram pesquisas empresariais na área de Gestão do Conhecimento de forma nacional ou internacional.

3.3 PROCEDIMENTOS DE COLETA DE DADOS

Para coleta de dados foram criados questionários, vinculando os controles de segurança selecionados para cada fase do SECI e foram direcionados para os especialistas responderem de acordo com suas percepções. Os questionários

gerados para as rodadas com os especialistas foram elaborados de forma direcionada, sendo eles estruturados. A construção foi realizada a partir da literatura da área e técnicas de coleta de dados.

Marques e Freitas (2018) advogam que existem estudos que começam de forma mais direcionada, sem a necessidade de utilizar questionários com perguntas mais abertas. Grisham (2009) defende que 80% de consenso nas respostas entre os especialistas é um bom objetivo, dessa forma definiu-se que os processos de rodada seriam interrompidos quando houvesse 80% de consenso entre as respostas. Uma breve descrição de cada etapa também foi realizada nas fases para melhor entendimento.

Os respondentes foram convidados a associar os controles da ISO/IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(b), 2013) aos quatro modos de conversão do conhecimento de acordo com o modelo SECI de Nonaka e Takeuchi (2008).

Os controles que foram utilizados neste processo são oriundos da Tabela 3 – Controles e Consenso, onde já estava evidenciada a relação entre cada um deles e seu grau de importância em cada processo do SECI. O refinamento dos controles mais preponderantes foi realizado durante as rodadas de respostas, resultando no modelo final do *framework*.

Para a realização das rodadas de questionários, foi utilizada a ferramenta *Google Forms*, que possibilitou maior agilidade, praticidade, interação com os especialistas e otimização da tabulação de resultados.

O processo de envio dos questionários iniciou-se no dia 02 de outubro de 2021 com o primeiro ciclo de coleta de dados. Os especialistas responderam aos questionários da primeira etapa do método Delphi no intervalo de aproximadamente 10 dias. Após realizar a compilação de dados obtidos na primeira etapa a segunda rodada do método Delphi teve início.

No dia 14 de outubro de 2021, iniciou-se a etapa 2 do método Delphi. Os especialistas responderam aos questionários da segunda rodada do método Delphi no período aproximado de 10 dias. Após realizar a compilação de dados obtidos na segunda etapa, iniciou-se a terceira rodada do método Delphi.

A terceira rodada de respostas do método Delphi, teve seu início em 23 de outubro de 2021, sendo ela encerrada no dia 05 de novembro de 2021, quando o último especialista respondeu aos questionários, encerrando os ciclos de coleta de

dados.

4 ANÁLISE DE DADOS E DISCUSSÕES

Neste capítulo será apresentada a análise dos dados extraídos da pesquisa realizada utilizando os métodos e instrumento descritos no Capítulo 3. Para cada fase de respostas será apresentada a análise dos dados coletados, tanto geral, como de acordo com cada grupo de especialistas.

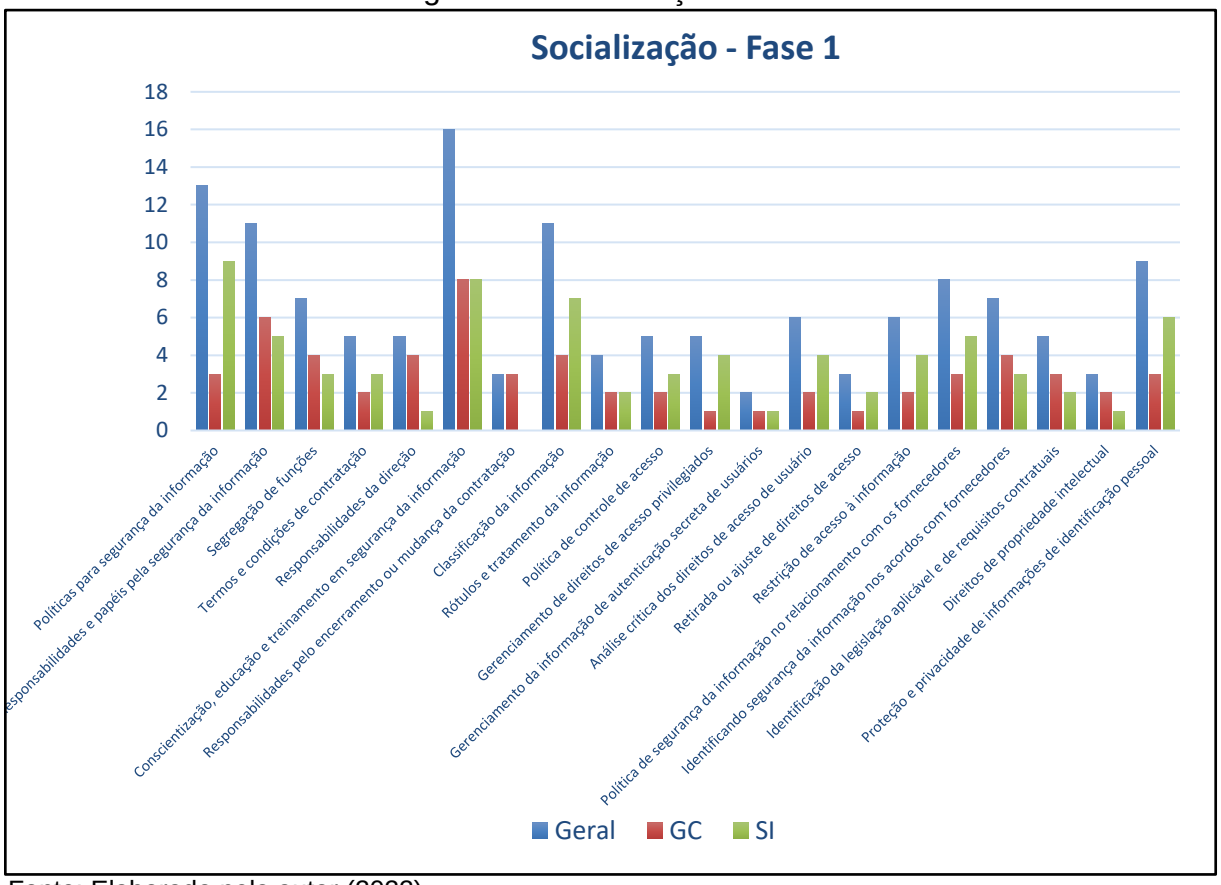
4.1 FASE 1

A primeira fase de rodadas de respostas ocorreu em um período de 10 dias e todos os 20 especialistas responderam os questionários. Nesta fase as respostas foram pulverizadas entre todos os 20 controles que foram selecionados e na maioria dos casos não se obteve uma consolidação de opiniões.

4.1.1 Socialização

Na primeira rodada de respostas, com relação à fase de Socialização que compõe o SECI, as escolhas dos controles foram pulverizados entre os 20 controles. Pondera-se que já nesta fase o controle de “Conscientização, educação e treinamento” obteve 80% de escolhas, sendo o primeiro controle selecionado nesta fase do SECI. Na Figura 5 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 5 - Socialização Fase 1



Fonte: Elaborado pelo autor (2022).

Quando analisadas as respostas na fase de Socialização, segregando apenas especialistas de Gestão do Conhecimento, pode-se perceber o mesmo comportamento de pulverização de respostas, indicando que o consenso entre eles ainda estava disperso. O controle de “Conscientização, educação e treinamento” obteve 80% de escolhas, refletindo que esse controle é preponderante para a Socialização de acordo com os especialistas de Gestão do Conhecimento.

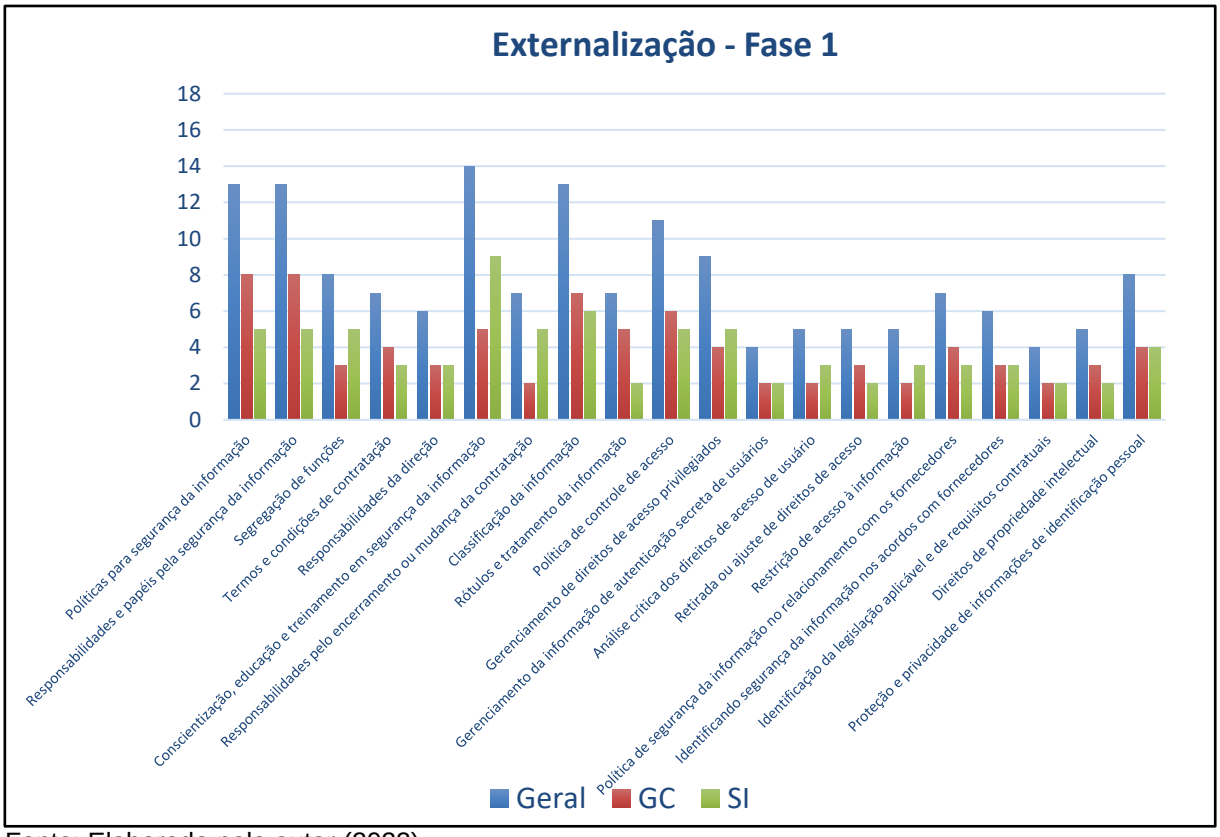
As respostas dos especialistas em Segurança da Informação também foram pulverizadas entre os controles, porém destaca-se 80% de consenso no controle de “Conscientização, educação e treinamento”, evidenciando uma proporção igualitária de importância a esse controle com relação aos especialistas de Gestão do Conhecimento.

4.1.2 Externalização

Na etapa de Externalização, observa-se que há um direcionamento maior nas escolhas dos especialistas, onde aparecem quatro controles que obtiveram mais de

65% de escolhas, porém nenhum deles obteve, pelo menos, 80% de consenso neste processo. Na Figura 6 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 6 - Externalização Fase 1



Fonte: Elaborado pelo autor (2022).

Quando analisado de forma segregada, as escolhas dos especialistas em Gestão do Conhecimento, pode-se observar que 2 controles atingiram 80% de consenso, o que indica um alinhamento na forma de pensar entre eles. Os controles de “Responsabilidade e papéis da Segurança da Informação” e “Políticas de Segurança da Informação” destacaram-se com 80% e o controle de “Classificação da informação” com 70% de consenso entre os especialistas de Gestão do Conhecimento.

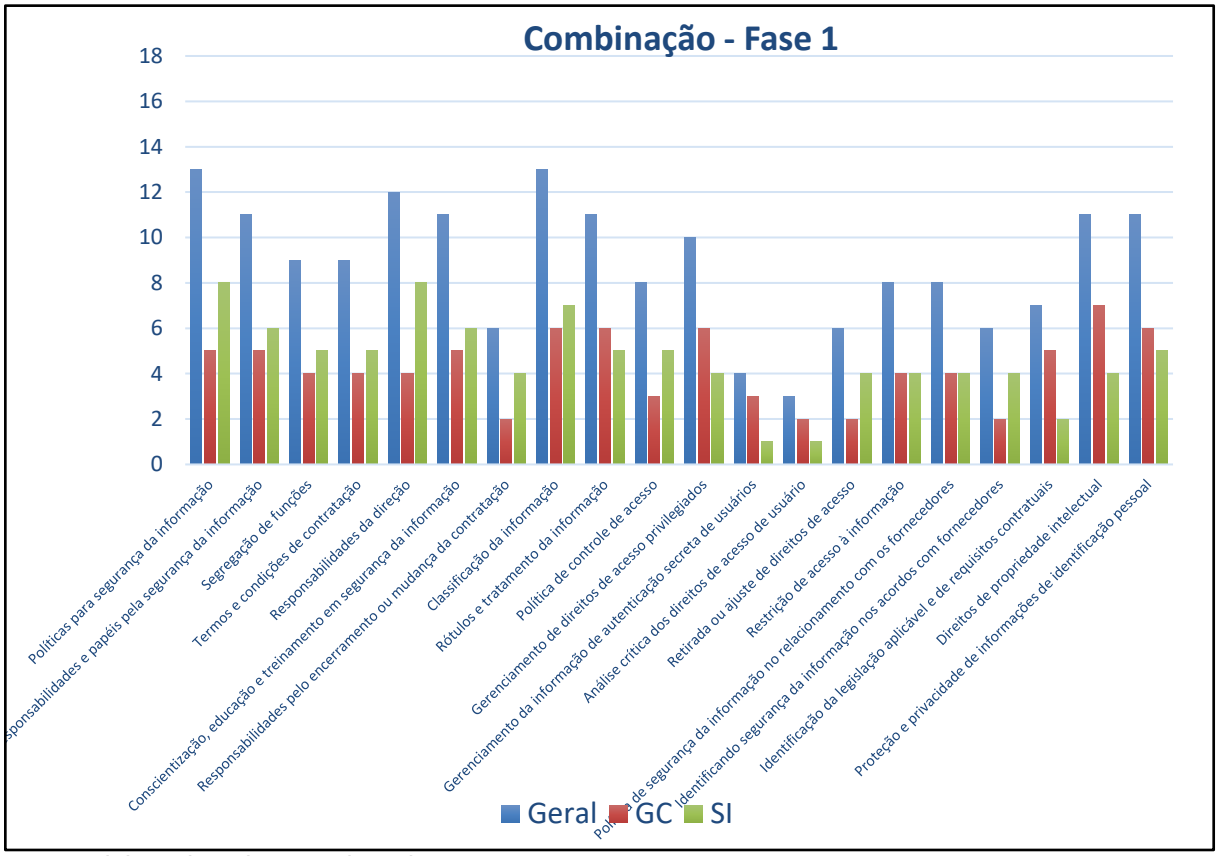
A análise das escolhas, considerando somente os especialistas de Segurança da Informação, mostrou uma maior pulverização em relação as escolhas dos especialistas em Gestão do Conhecimento. Apenas um controle destacou-se com 90% de escolhas. Diferentemente do outro grupo de especialistas, o controle com maior consenso foi “Conscientização, educação e treinamento”. Pondera-se que nesta etapa, os especialistas de Segurança da Informação possuem pensamento

heterogêneo com relação aos controles a serem utilizados.

4.1.3 Combinação

Na fase da Combinação, muitos controles obtiveram entre 45% e 65% das escolhas e mesmo com a dispersão, evidencia-se que as opiniões entre os especialistas estiveram bem divididas nesta etapa. Na Figura 7 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 7 - Combinação Fase 1



Fonte: Elaborado pelo autor (2022).

A análise das respostas dos especialistas em Gestão do Conhecimento demonstra uma dispersão maior entre 40% e 60% das escolhas, demonstrando que não há consenso de pensamento nesta etapa da pesquisa. Nenhum dos controles chegou a 80% de consenso na opinião isolada desses especialistas.

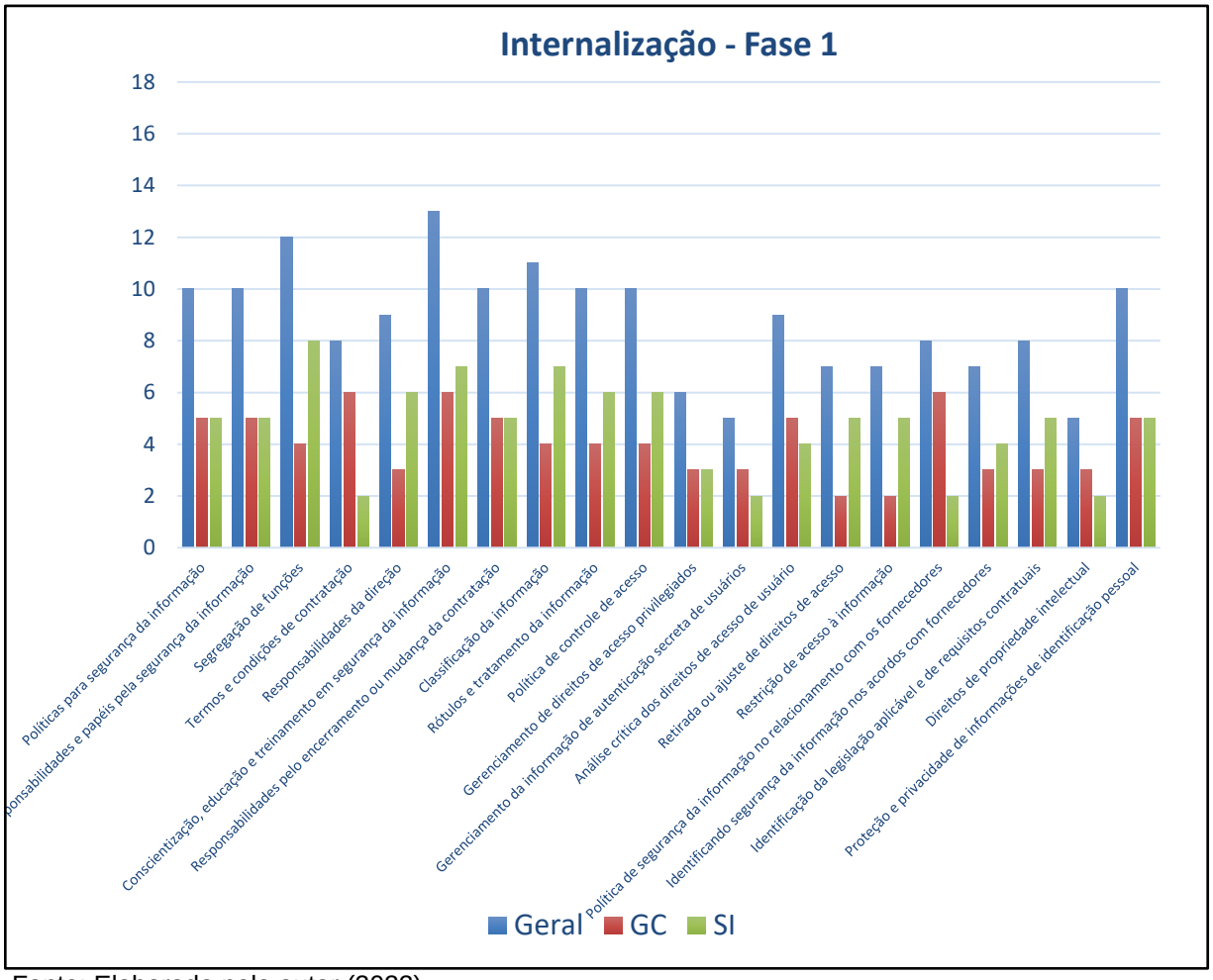
A análise das respostas dos especialistas em Segurança da Informação demonstra uma dispersão menor, onde temos controles concentrados entre 60% e 80% das escolhas. Nesta etapa, analisando de forma isolada, os especialistas de

Segurança da Informação elegeram 2 controles com 80% de consenso, sendo eles “Responsabilidades da Direção” e “Políticas para Segurança da Informação”.

4.1.4 Internalização

Na fase da Internalização, muitos controles obtiveram entre 45% e 65% das escolhas e mesmo com a dispersão, evidencia-se que as opiniões entre os especialistas estiveram bem divididas nesta etapa, de igual modo da etapa anterior. Neste ponto não pode ser evidenciado um consenso. Na Figura 8 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 8 - Internalização Fase 1



Fonte: Elaborado pelo autor (2022).

A análise das respostas dos especialistas em Gestão do Conhecimento demonstra uma dispersão maior entre 40% e 60% das escolhas. Demonstrando que

não há consenso de pensamento nesta etapa da pesquisa. Nenhum dos controles chegou a 80% de consenso na opinião isolada desses especialistas.

Nesta etapa, assim como na anterior, as respostas dos especialistas em Segurança da Informação demonstram uma dispersão menor, onde temos controles concentrados entre 60% e 80% das escolhas. Analisando de forma isolada, os especialistas de Segurança da Informação elegeram o controle “Segregação de Funções” com 80% de consenso.

4.1.5 Fechamento Fase 1

A primeira rodada de respostas, aqui denominada como Fase 1, foi mais dispersa e as escolhas estiveram mais espalhados entre todos os controles e em todas as quatro etapas do SECI. Quando os dados são analisados em sua totalidade, evidencia-se a divergência de opinião entre os vinte especialistas participantes desta pesquisa.

Ao analisar os dados de forma segredadas, pode ser ponderado que a divergência de opiniões entre os especialistas de Gestão do Conhecimento é maior do que a opinião dos especialistas em Segurança da Informação, pois em todas as etapas do SECI, esses especialistas obtiveram pelo menos um controle com 80% de consenso, diferentemente dos especialistas em Gestão do Conhecimento, que alcançaram pelo menos 80% de consenso em apenas duas etapas.

Essa pulverização de consenso entre os controles, fez com que durante a Fase 1 da pesquisa Delphi, apenas na etapa de Socialização do modelo SECI, fosse alcançado pelo menos 80% de consenso em um dos controles.

4.2 FASE 2

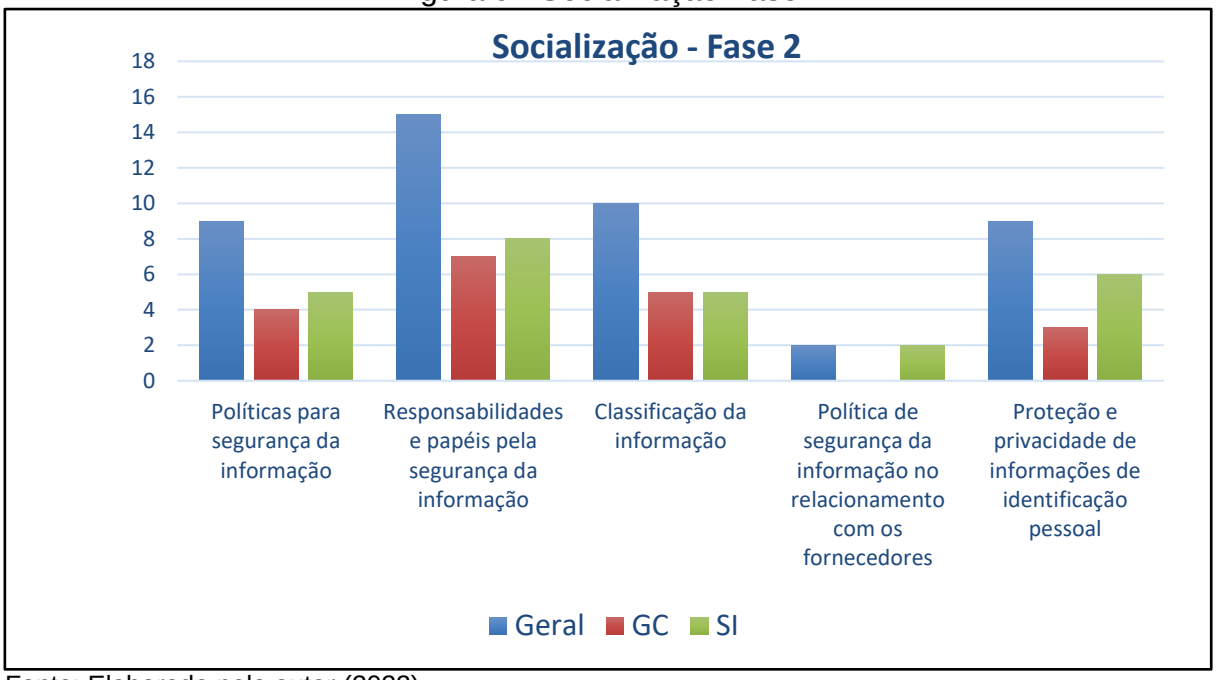
A segunda fase de rodadas de respostas ocorreu em um período de 10 dias e todos os 20 especialistas responderam os questionários. Nesta fase, todos os controles com menos de 50% de escolhas, em relação ao controle mais votado, em cada etapa do SECI, durante a Fase 1, foram descartados e um novo questionário com menos opções de escolhas foi criado e enviado a todos os especialistas que participaram desta pesquisa. Questões que já tiveram os 80% de consenso também foram retiradas de cada etapa em específico.

Devido ao número menor de opções, as escolhas ficaram mais concentrados e os especialistas puderam utilizar a expertise adquirida na Fase 1 para direcionar suas escolhas nos controles com mais clareza e critério.

4.2.1 Socialização

Na primeira etapa do SECI, pode-se destacar que houve equilibro de escolhas entre os controles, somente o controle “Responsabilidade e papéis pela Segurança da Informação” teve destaque com 75% das escolhas, chegando muito próximo aos 80% definido como pontuação de consenso necessária nesta pesquisa. Na Figura 9 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 9 - Socialização Fase 2



Fonte: Elaborado pelo autor (2022).

A análise das respostas dos especialistas em Gestão do Conhecimento, demonstra um pensamento equilibrado entre todos, destacando, da mesma forma que na análise geral, o controle de Responsabilidade e papéis pela Segurança da Informação” que obteve 70% de consenso das escolhas.

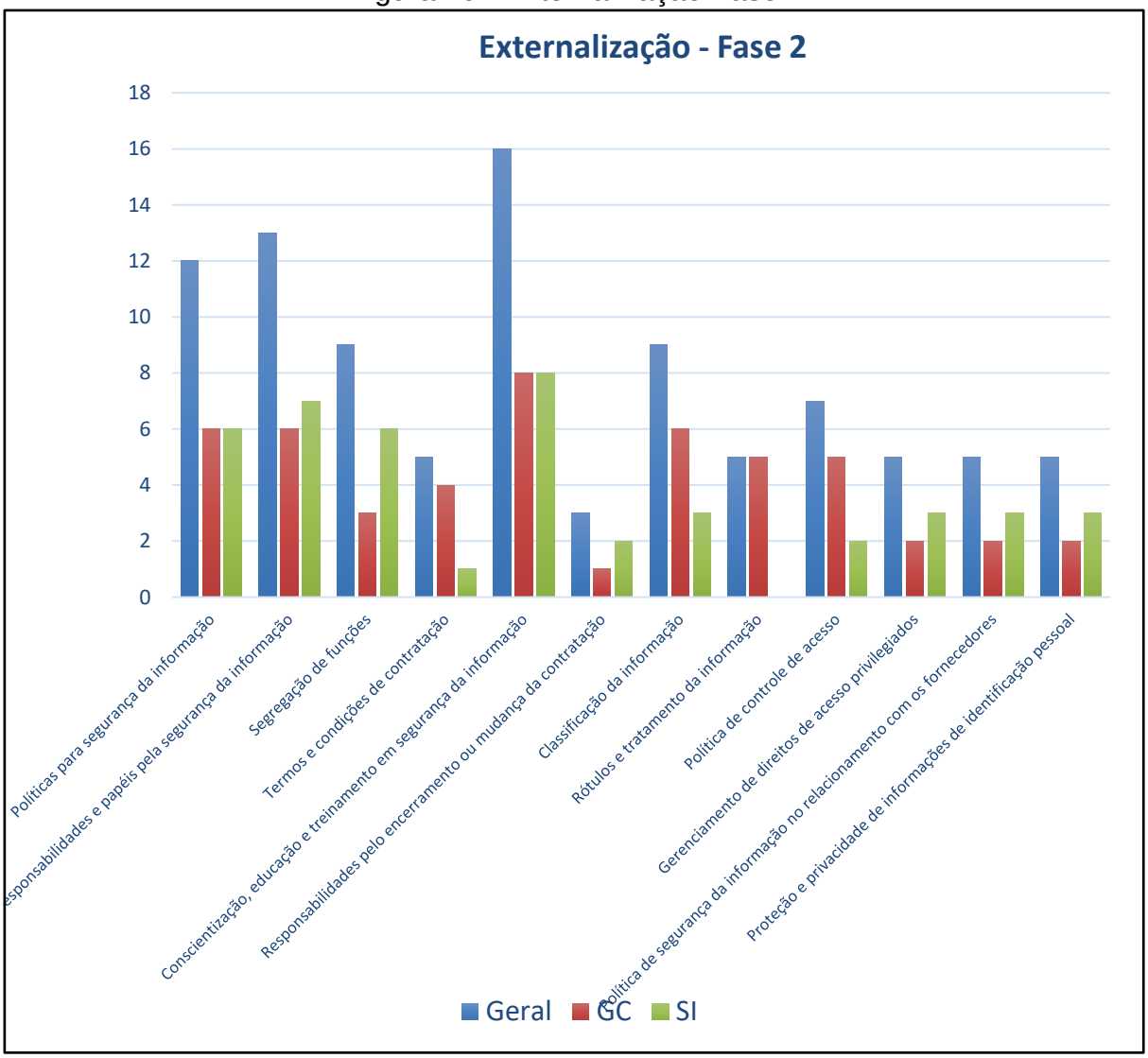
A análise das respostas dos especialistas em Segurança da Informação, demonstra um pensamento equilibrado entre todos, da mesma forma que as respostas do grupo de especialistas em Gestão do Conhecimento, porém destaca-se

que o controle de Responsabilidade e papéis pela Segurança da Informação” obteve 80% de consenso das escolhas, demonstrando um maior alinhamento de pensamento entre esses especialistas.

4.2.2 Externalização

Observa-se que nesta fase do SECI houve maior dispersão, mesmo comportamento da primeira rodada de respostas. Destaca-se que existiam muitas opções que os especialistas poderiam escolher, de forma análoga a fase 1. Nesta etapa o controle de “Conscientização, educação e treinamento”, alcançou os 80% de consenso de repostas entre os especialistas. Na Figura 10 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 10 - Externalização Fase 2



Fonte: Elaborado pelo autor (2022).

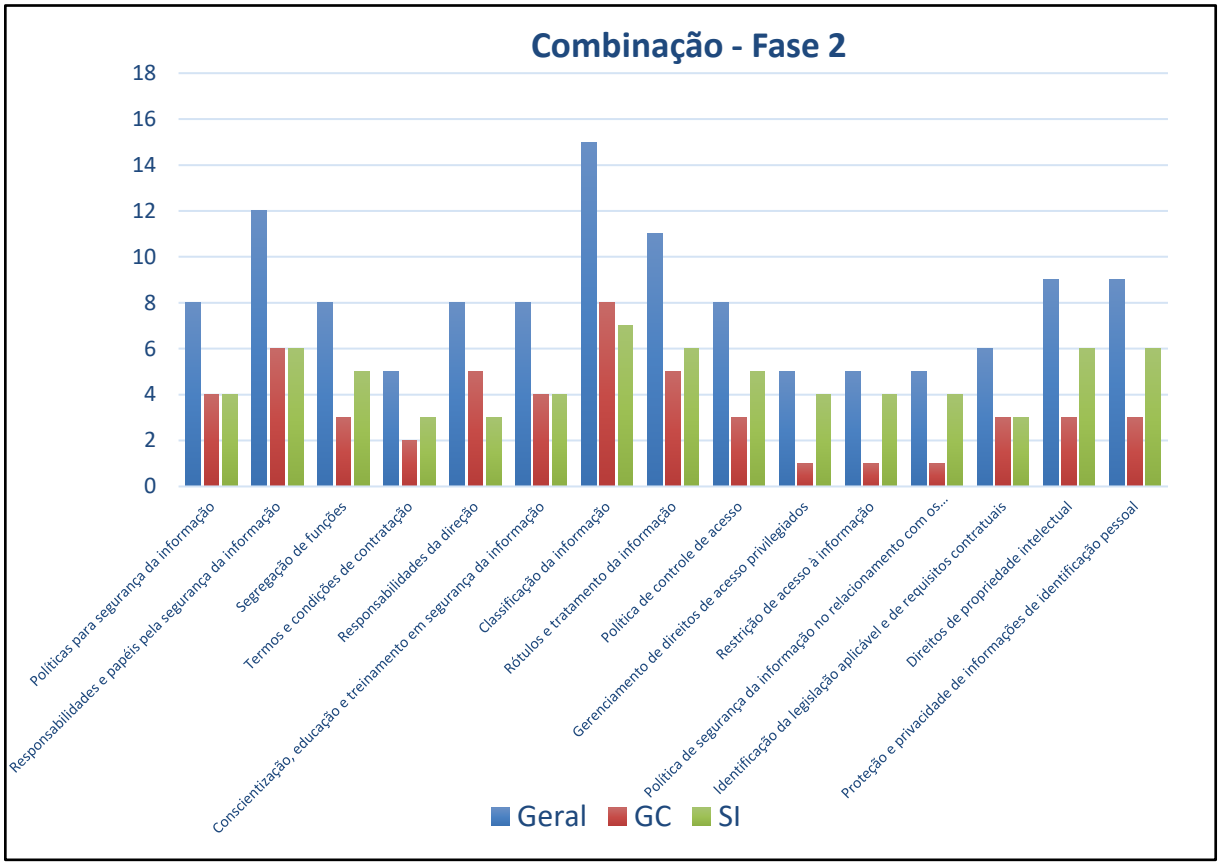
Os especialistas em Gestão do Conhecimento, apesar da dispersão entre os controles, obtiveram certa homogeneidade na escolha de alguns controles, tendo alguns entre 50% e 60% de consenso. Como reflexo da votação geral nos controles, nesta etapa também se chegou em 80% de consenso no controle de “Conscientização, educação e treinamento”, indicando um direcionamento de pensamento entre os especialistas.

Os especialistas em Segurança da Informação, tiveram mais dispersão entre os controles, tendo poucas escolhas que alcançaram entre 60% e 70% de consenso. Como reflexo da votação geral nos controles, nesta etapa também se chegou em 80% de consenso no controle de “Conscientização, educação e treinamento”, indicando um direcionamento de pensamento entre os especialistas neste quesito.

4.2.3 Combinação

A terceira etapa do SECI, apresentou votação dispersa e sem consenso entre os especialistas. Nesta etapa ainda houve muitas opções de controles para serem votados. Poucas escolhas tiveram votação igual ou superior a 50%, evidenciando a assimetria de consenso entre os especialistas sobre quais controles seriam preponderantes para esta etapa de Combinação do conhecimento. Na Figura 11 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 11 - Combinação Fase 2



Fonte: Elaborado pelo autor (2022).

Assim como na análise geral de escolhas, os especialistas de Gestão do Conhecimento, tiveram suas escolhas muito dispersas entre as opções de escolha dos controles. Destaca-se o controle de “Classificação da Informação” que obteve 80% da escolha dos especialistas, demonstrando que para eles, esse é um controle preponderante nesta etapa do SECI.

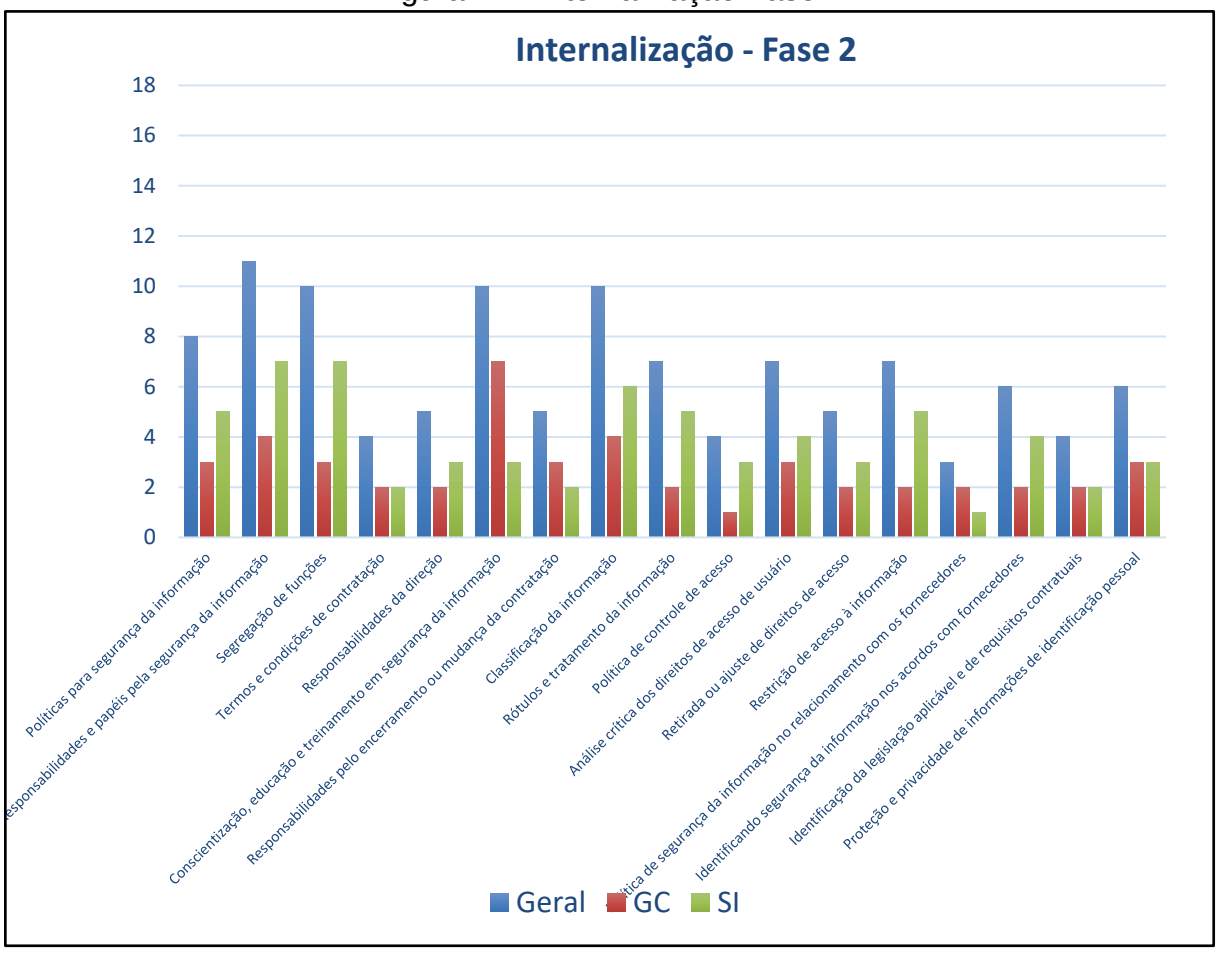
As escolhas dos especialistas em Segurança da Informação foram menos dispersas, tendo controles variando entre 50% e 70% das escolhas, porém sem alcançar a marca de 80% em nenhum dos controles. O controle de “Classificação da informação”, obteve 70% das escolhas, muito próximo ao cenário dos especialistas em Gestão do Conhecimento que obtiveram 80% de consenso em suas escolhas para essa etapa.

4.2.4 Internalização

A quarta etapa do SECI, apresentou votação dispersa e com menor consenso entre os especialistas durante a Fase 2 de respostas. Nesta etapa ainda houve muitas

opções de controles para serem votados. Poucas escolhas tiveram votação igual ou superior a 50%, evidenciando a assimetria de consenso entre os especialistas sobre quais controles seriam preponderantes para esta etapa de Internalização do conhecimento. Na Figura 12 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 12 - Internalização Fase 2



Fonte: Elaborado pelo autor (2022).

Refletindo a análise geral dos dados, quando observada as respostas dos especialistas em Gestão do Conhecimento na etapa da Internalização do modelo SECI, observa-se uma grande dispersão entre os controles propostos. Somente o controle de “Conscientização, educação e treinamento” obteve 70% das escolhas, os demais, obtiveram 40% ou menos de escolhas nesta etapa, evidenciando grande assimetria de pensamento entre os especialistas.

As escolhas dos especialistas em Segurança da Informação também apresentaram grande assimetria, refletindo o resultado geral das escolhas nesta etapa do SECI. Os controles “Responsabilidade e papéis pela Segurança da Informação” e

“Segregações de Funções”, obtiveram 70% de escolhas, os outros controles, em sua grande maioria, obtiveram 40% o menos de escolhas. Houve grande dispersão de consenso nesta etapa.

4.2.5 Fechamento Fase 2

A segunda rodada de respostas, aqui denominada como Fase 2, manteve grande índice de dispersão entre os especialistas nas etapas de Combinação e Internalização do conhecimento. Apenas na etapa de externalização, houve consenso de 80% em um controle.

Ao analisar os dados de forma segredadas, pode ser ponderado que houve muitas divergências de opiniões entre os especialistas de Gestão do Conhecimento e Segurança da Informação, mas também ocorreram divergências entre a opinião interna de cada grupo, refletindo o resultado desta rodada de pesquisa, onde praticamente não se obteve consenso entre os especialistas.

4.3 FASE 3

A terceira fase de rodadas de respostas ocorreu em um período de 10 dias e todos os 20 especialistas responderam os questionários. Nesta fase, todos os controles com menos de 50% de escolhas durante a Fase 2 foram descartados e um novo questionário com menos opções de escolhas foi criado e enviado a todos os especialistas que participaram desta pesquisa. Questões que já tiveram os 80% de consenso também foram retiradas de cada etapa em específico.

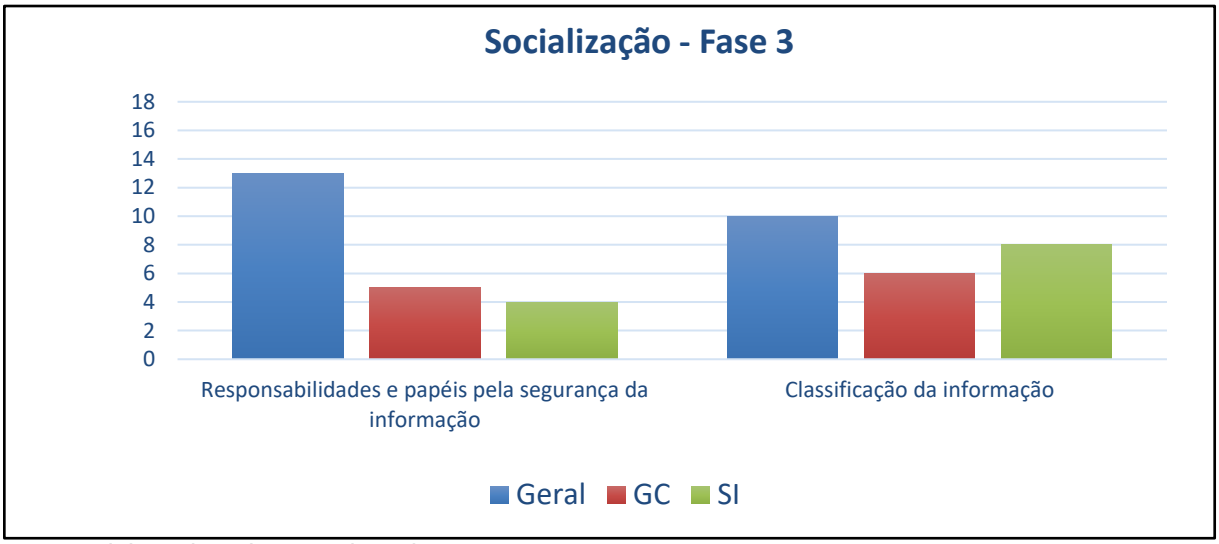
Devido ao número menor de opções, as escolhas ficaram mais concentrados e os especialistas puderam utilizar a expertise adquirida na Fase 1 e na Fase 2 para direcionar suas escolhas nos controles com mais clareza e critério. A Fase 3 foi a última, pois chegou-se em um cenário que realizar novas rodadas não alteraria o resultado, devido ao número reduzido de opções restantes.

4.3.1 Socialização

Na etapa de Socialização nesta última fase de respostas, nenhum dos controles obteve pelo menos 80% de consenso de escolhas entre os especialistas. O

controle mais votado foi “Responsabilidades e papéis pela Segurança da Informação” que obteve 65% de escolhas. Dessa forma nenhum desses controles fará parte do framework, devido aos critérios estabelecidos. Na Figura 13 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 13 - Socialização Fase 3



Fonte: Elaborado pelo autor (2022).

De acordo com as respostas dos especialistas em Gestão do Conhecimento, nesta etapa, nenhum dos controles obteve os 80% de consenso. De forma inversa ao cenário geral, o controle com mais escolhas, 60%, foi “Classificação da informação”. As escolhas foram bem divididos, mostrando que não há um consenso entre os especialistas.

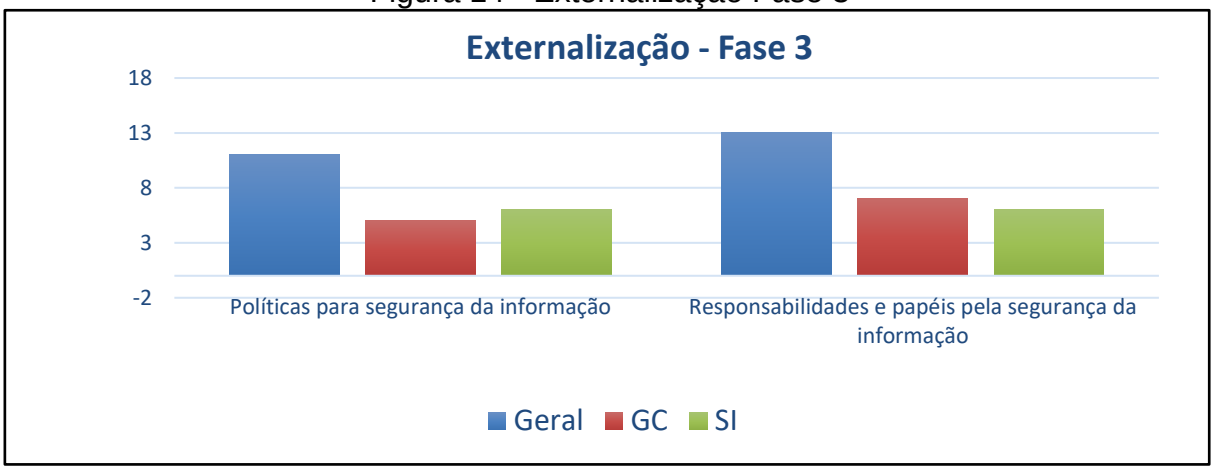
Os especialistas de Segurança da Informação nesta mesma etapa demonstraram sincronia de pensamentos. O controle de “Responsabilidade e papéis pela Segurança da Informação”, apresentou 80% de consenso de escolhas, sendo considerado preponderante por esses profissionais, porém esses escolhas foram diluídos no cenário geral, fazendo com que nesta etapa não obtivéssemos singularidade de opiniões em algum controle.

4.3.2 Externalização

Na etapa de Externalização, nesta última fase de respostas, nenhum dos

controles obteve pelo menos 80% de consenso de escolhas entre os especialistas. O controle mais votado, assim como na etapa anterior, foi “Responsabilidades e papéis pela Segurança da Informação” que obteve 65% de escolhas. Dessa forma nenhum desses controles fará parte do framework, devido aos critérios estabelecidos. Na Figura 14 pode-se observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 14 - Externalização Fase 3



Fonte: Elaborado pelo autor (2022).

De acordo com as respostas dos especialistas em Gestão do Conhecimento, nesta etapa, nenhum dos controles obteve os 80% de consenso. Houve um direcionamento de escolhas para o controle de “Responsabilidade e papéis pela Segurança da Informação”, que chegou a 70% das escolhas.

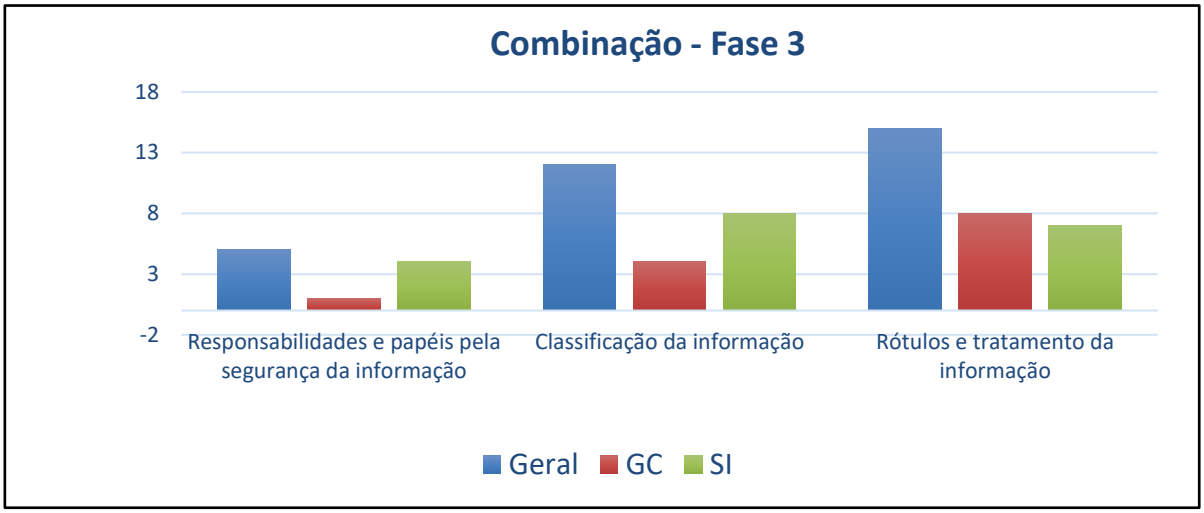
A opinião dos especialistas em Segurança da Informação nesta etapa demonstrou-se dividida. Os 2 controles obtiveram 60% de consenso de escolhas. Isso contribuiu para que no cenário geral houvesse a diluição de escolhas, logo, não chegando em 80% de consenso entre a opinião de todos em algum controle.

4.3.3 Combinação

Na etapa de Combinação também não se obteve 80% de consenso em algum controle proposto. O controle com maior votação foi o “Rótulos e tratamento da informação” que alcançou 75% de consenso entre os especialistas, porém abaixo da métrica considerada nesta pesquisa para seleção de um controle para compor o framework. Na Figura 15 pode-se observar os resultados compilados com o totalizador

de respostas gerais e por perfil de especialista.

Figura 15 - Combinação Fase 3



Fonte: Elaborado pelo autor (2022).

Quando os dados relativos aos especialistas de Gestão do Conhecimento são analisados de forma segredada, pode-se perceber que o controle de “Rótulos e tratamento de informação” obtém 80% de consenso das escolhas e os demais controles ficam com 40% ou menos de escolhas. Evidencia-se a sincronia de pensamento entre esses especialistas na etapa da Combinação.

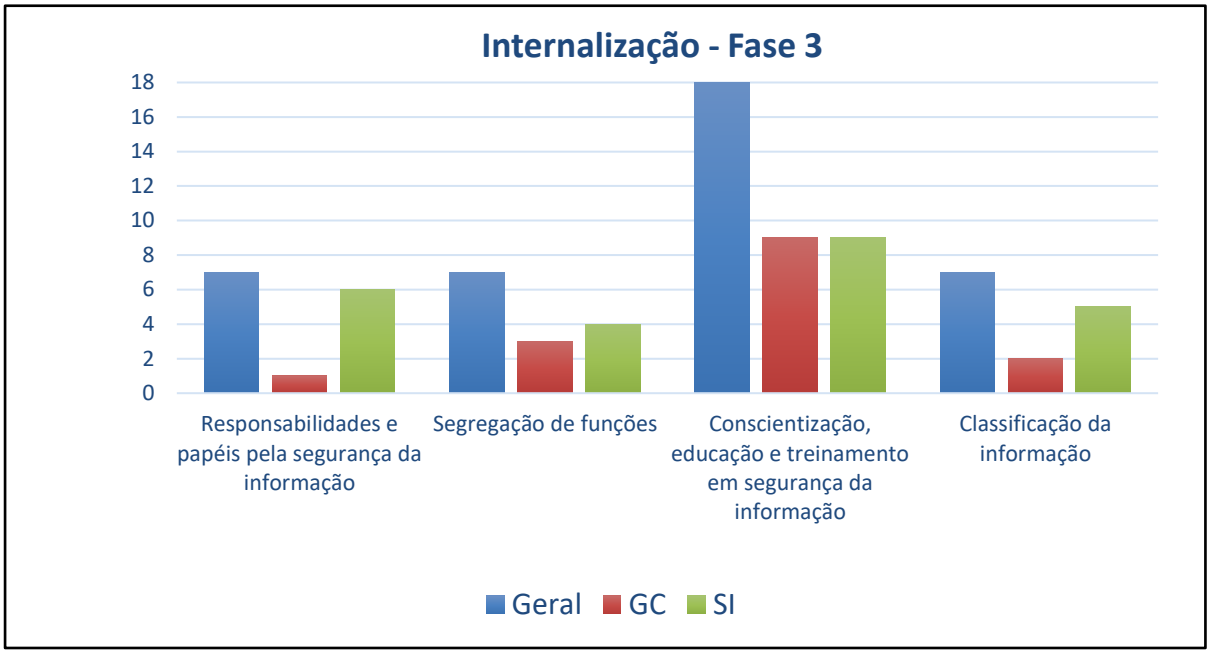
Quando os dados relativos aos especialistas de Segurança da Informação são analisados de forma segredada, pode-se perceber que o controle de “Classificação da informação” obtém 80% de consenso das escolhas evidencia-se também que há sincronia de pensamento entre esses especialistas na etapa da Combinação. Percebe-se que cada um dos grupos de especialistas elegeu um controle como sendo mais preponderante de forma distinta entre eles, dessa forma houve a pulverização de escolhas entre os controles e não se chegou a nenhum controle a 80% de consenso na abordagem geral dos dados.

4.3.4 Internalização

Na etapa de Internalização, pode-se observar escolhas massivos no controle “Conscientização, educação e treinamento em Segurança da Informação”, que obteve 90% de consenso. Os demais controles tiveram votação irrisória com apenas 35% das escolhas. A opinião dos 20 especialistas nesta etapa foi quase que em sua totalidade homogênea, evidenciando a preponderância deste controle. Na Figura 16 pode-se

observar os resultados compilados com o totalizador de respostas gerais e por perfil de especialista.

Figura 16 - Internalização Fase 3



Fonte: Elaborado pelo autor (2022).

A análise em separado das respostas dos especialistas em Gestão do Conhecimento reflete o resultado geral. O mesmo controle de “Conscientização, educação e treinamento em Segurança da Informação”, obteve 90% de consenso entre eles e os demais controles tiveram votação irrisória.

O mesmo cenário se repete com os especialistas em Segurança da Informação, onde o controle de “Conscientização, educação e treinamento em Segurança da Informação” também apresentou 90% de consenso, fortalecendo a importância deste controle. Os demais controles obtiveram votação menos expressiva e isso se reflete no quadro geral dos dados.

4.3.5 Fechamento Fase 3

A terceira rodada de respostas, aqui denominada como Fase 3, manteve grande índice de dispersão entre os especialistas nas etapas de Socialização, Externalização e Combinação do conhecimento. Apenas na etapa de Internalização, houve consenso de 80% ou mais em um controle.

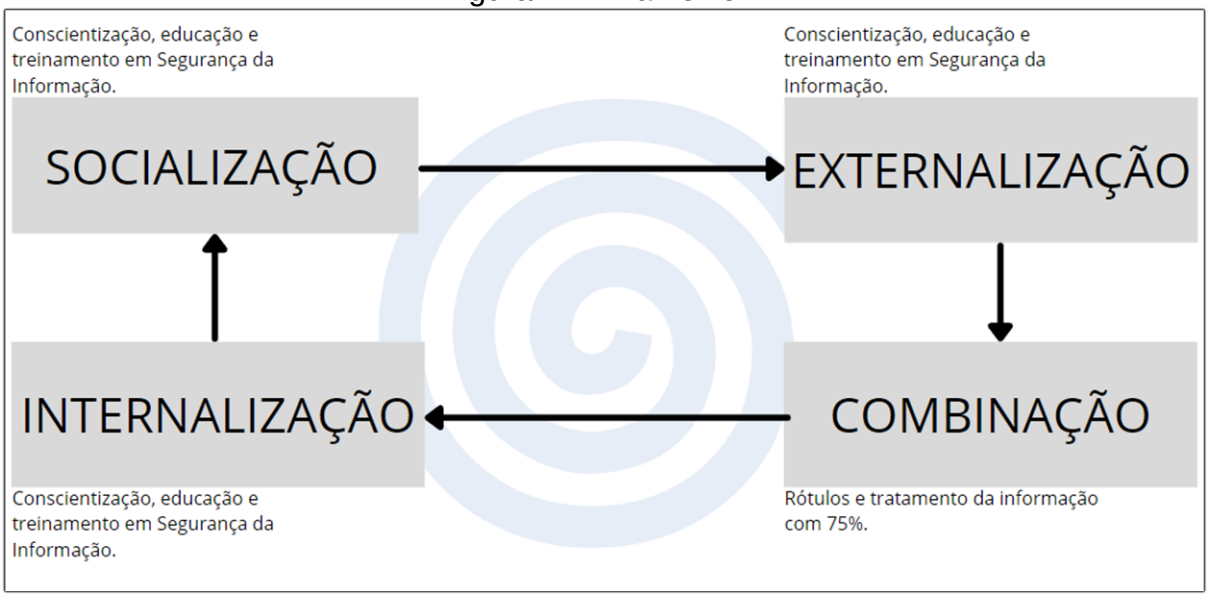
Ao analisar os dados de forma segredadas, pode ser ponderado que houve

muitas divergências de opiniões entre os especialistas de Gestão do Conhecimento e Segurança da Informação, mas também ocorreram divergências entre a opinião interna de cada grupo, refletindo no resultado desta última rodada de pesquisa, onde praticamente não obteve consenso entre os especialistas.

4.4 DISCUSSÃO DOS RESULTADOS

Ao finalizar a pesquisa, observa-se que apenas um controle obteve 80% ou mais de consenso de acordo com a opinião dos especialistas. O controle de “Conscientização, treinamento e educação em Segurança da Informação” apareceu em três etapas do SECI, sendo elas Socialização, Externalização e Internalização. A etapa de Combinação não obteve nenhum controle com 80% de consenso de escolhas, porém o controle de “Rótulos e tratamento da informação” obteve 75% de consenso nesta etapa. Na Figura 17, pode-se observar como o *framework* pode estar constituído.

Figura 17 - *Framework*



Fonte: Elaborado pelo autor (2022).

Pode-se observar que o controle predominante em consenso na opinião, dos especialistas das duas áreas, é o de “Conscientização, educação e treinamento em Segurança da Informação”. Como ponto comum entre a área de Gestão do Conhecimento e Segurança da Informação, pode-se salientar o fato de que ambas definem como sucesso de implementação de suas práticas a capacitação e

treinamento dos indivíduos e a conscientizando sobre o tema.

Rios, Teixeira e Rios (2017) corroboram para a necessidade de capacitação por parte dos colaboradores de uma empresa no que tange Segurança da Informação, quando afirmam que é inviável construir um sistema de gestão de segurança com suas documentações sem que haja a capacitação das pessoas envolvidas no processo. O tema ainda é abordado na pesquisa de Souza, Arima e Belda (2020), que ao conduzir um estudo quantitativo sobre a percepção da temática de Segurança da Informação em uma instituição de ensino público federal destacou a preponderância de treinamentos e conscientização da cultura de segurança, entre outros pontos abordados.

Como resultado do estudo pode-se identificar que não há uma aplicação eficaz de treinamentos e conscientização dos usuários quanto ao tema Segurança da Informação. Essa percepção de falta de treinamentos e capacitação sobre a temática pode ser o reflexo da concordância entre os especialistas de segurança no que tange à capacitação das pessoas como ponto chave do sucesso de um sistema de Segurança da Informação.

Um dos principais objetivos da Gestão do Conhecimento, como já supracitado neste trabalho, é transformar o conhecimento em capacidades de indivíduos. A Gestão do Conhecimento constrói, de forma consciente, um modelo em que o conhecimento certo seja disponibilizado para a pessoa certa no momento certo, ou seja, permitindo que elas coloquem em prática suas novas habilidades, a fim de a melhorar o desempenho da organização (HCI, 2019). Desta forma está claro que para os especialistas de Gestão do Conhecimento, conscientizar e treinar pessoas é o pilar essencial para construção de um novo conhecimento, que neste caso é o conhecimento de Gestão do Conhecimento de forma segura.

A alta consenso no controle “Conscientização, educação e treinamento em Segurança da Informação” é explicada através da importância da capacitação de indivíduos que ambas as áreas de conhecimento, Gestão do Conhecimento e Segurança da Informação, vinculam à essa abordagem específica. De acordo com o resultado da opinião dos especialistas, o ponto inicial é capacitar e treinar os individuo sobre as temáticas e incutir em cada um o conhecimento necessário para que possam melhorar seus processos diários. O sucesso de um possível framework ou metodologia de Gestão do Conhecimento Segura, necessita, primeiramente, da capacitação das pessoas.

No que tange à fase da Combinação no processo do SECI, 75% dos especialistas concordaram que rotular as informações é algo necessário para que seja possível estabelecer o compartilhamento do conhecimento de forma segura. Na fase de Combinação, tem-se a maior amplificação da disseminação do conhecimento na organização. Dessa forma mais pessoas terão acesso às informações e conhecimentos, sendo um ponto crucial para ser observado e tratado no que tange Segurança da Informação.

A ISO/IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013), neste controle específico, explana que se faz necessário criar um conjunto apropriado de procedimentos com objetivo de rotular e tratar a informação organizacional. A classificação da informação está correlacionada à sua rotulação. Rótulos definem em qual classificação uma informação está, como por exemplo confidencial, privada, pública, entre outras.

Viana e Fernandes (2015) afirmam que a ausência de classificação da informação pode potencializar o tratamento inadequado da informação, resultando em divulgação ostensiva de dados confidenciais. Alhogail (2020) propõe um processo de melhoria de segurança em cinco etapas, dentre elas a da classificação, onde é sugestionado identificar e classificar conhecimentos importantes para a organização. No viés de Segurança da Informação a classificação para estabelecimento de controle é uma prática comum, o que pode explicar o alto número de consenso entre os especialistas de segurança na fase de Combinação para proteção do conhecimento.

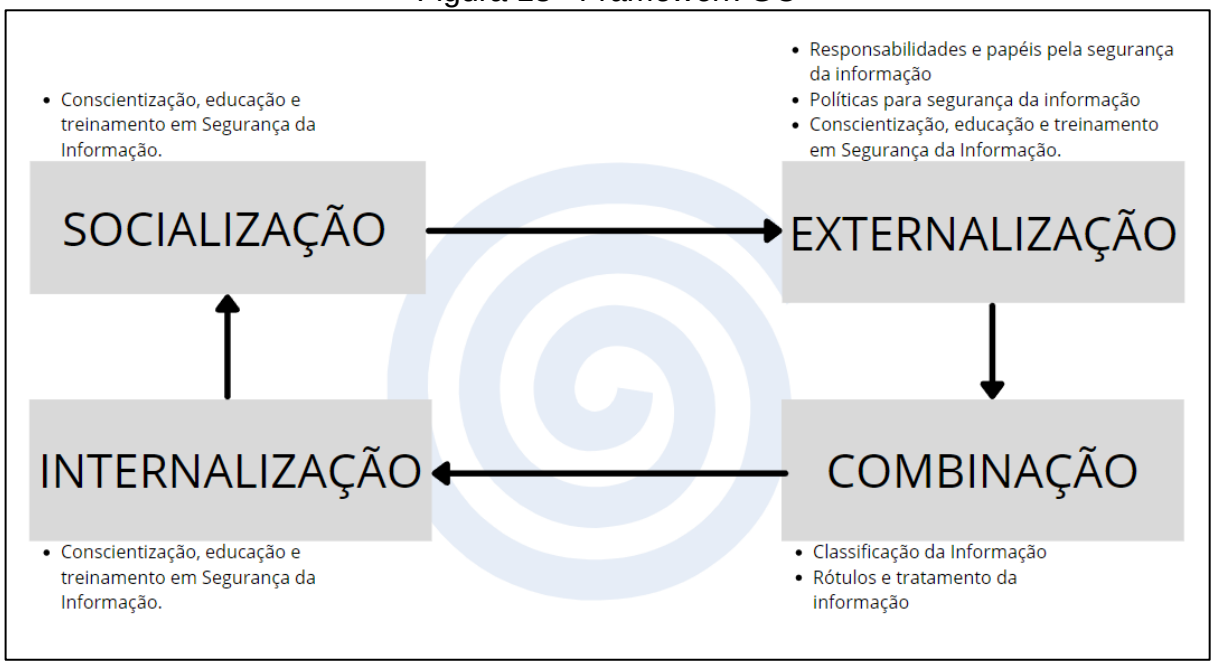
A Gestão do Conhecimento também adota processos de classificação para melhor entendimento e construção de conhecimento. Para Pizzaia et al. (2018) os ativos do conhecimento podem estar dispostos em um espaço tridimensional que é dividido em dimensões, sendo uma delas a codificação que está relacionado diretamente com a categorização e classificação do conhecimento. A categorização é uma forma de rótulo que pode ser inserido no conhecimento de acordo com sua classificação. No contexto de Gestão do Conhecimento Seguro, utilizando-se desta abordagem, ocorre a rotulação do conhecimento.

Em linhas gerais, o processo de Combinação obteve alto grau de consenso entre os especialistas das duas áreas de conhecimento, mesmo não alcançando os 80% necessários para se tornar um controle do framework. Evidencia-se que nesta etapa o controle de “Conscientização, educação e treinamento em Segurança da Informação”, não obteve votação expressiva, ou seja, nesta fase do SECI, para os

especialistas, é o momento de observar com mais atenção quais os conhecimentos que serão compartilhados para toda organização. Nas fases de Socialização e Externalização, a capacitação dos indivíduos é necessária, para que na fase de Combinação eles possam ser capazes de entender quais conhecimentos podem ou não ser compartilhados com toda a organização de forma irrestrita.

Outra abordagem de análise é isolar as respostas de cada grupo de especialistas e desenhar o framework de acordo com a visão de cada área de conhecimento e observar as discrepâncias entre elas para entender melhor o *mindset* de cada grupo. O framework de Gestão do Conhecimento Seguro de acordo com as respostas isoladas dos especialistas de Gestão do Conhecimento está representado na Figura 18.

Figura 18 - *Framework* GC



Fonte: Elaborado pelo autor (2022).

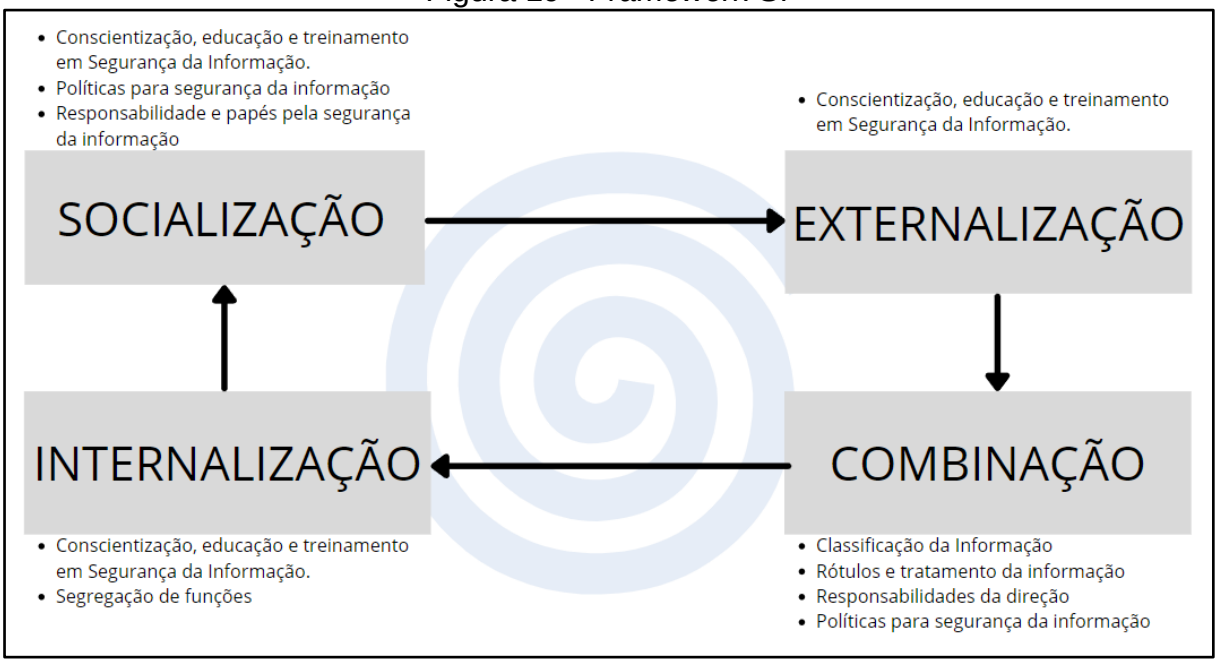
Destacam-se as fases de Externalização e Combinação, que tiveram resultados diferentes. Na fase de Externalização há controles específicos para definição de políticas de Segurança da Informação e a atribuição de responsabilidades individuais no que tange à segurança para cada indivíduo, reforçando desta forma que além de capacitar cada um é necessário estabelecer obrigações e políticas para regrar o compartilhamento de conhecimentos nas organizações.

Na fase de Combinação, o controle de “Classificação da informação” entra em destaque. Esse controle tem como objetivo criar a base de classificação das

informações que será utilizado para rotular cada uma delas. São controles complementares e que juntos propiciam a melhor gestão da informação e conhecimento de acordo com sua criticidade.

Isolando as respostas dos especialistas em Segurança da Informação, chega-se a um outro modelo de framework. O framework de Gestão do Conhecimento Seguro de acordo com as respostas isoladas dos especialistas de Segurança da Informação está representado na Figura 19.

Figura 19 - *Framework* SI



Fonte: Elaborado pelo autor (2022).

Para os profissionais de Segurança da Informação, em três das quatro etapas do SECI necessitam de mais controles. Na fase de Socialização, onde o indivíduo começa compartilhar o seu conhecimento de forma direta com outro indivíduo, na visão dos especialistas de segurança, já se faz necessário estabelecer políticas para direcionar o comportamento de cada um. As políticas vão estabelecer as regras desde a primeira etapa, juntamente com a explanação das responsabilidades de cada um diante da segurança das informações e conhecimento que forem manipular. Somando ao controle de conscientização e treinamento, esses controles vão construir a base para iniciar-se um melhorias de segurança no processo de Gestão do Conhecimento.

Na fase de Combinação pode-se destacar o controle de Responsabilidade da direção e novamente Políticas para Segurança da Informação, que não há no framework resultante da análise isolada das respostas dos especialistas em Gestão

do Conhecimento. Isso demonstra que os especialistas de Segurança da Informação, veem importância da participação da direção para garantir o *enforcement* das políticas de segurança, a partir do momento que o conhecimento é disseminado para toda a empresa.

Na última fase de Internalização, o controle de “Segregação de funções”, demonstra que para os especialistas de segurança, se faz necessário a padronização de cargos e funções, no momento que o conhecimento se transforma em tácito novamente. Cada indivíduo deve saber se aquele conhecimento faz parte de sua função ou cargo, para então internalizá-lo.

As discrepâncias nas respostas entres os especialistas e os frameworks criados de forma isolada, de acordo com cada área de conhecimento, expõe que os especialistas em Segurança da Informação preocupam-se em estabelecer políticas e controles em mais fases do compartilhamento do conhecimento por causa do viés em não permitir acesso a informações, a não ser que seja realmente necessário. Já os especialistas de Gestão do Conhecimento possuem o viés de compartilhar o conhecimento de forma menos restritiva e controlada. Ainda assim destaca-se a concordância macro entre todos que a capacitação dos indivíduos é a melhor estratégia neste contexto.

Considerando o *framework* geral, com destaque primário para o controle de “Conscientização, educação e treinamento em Segurança da Informação”, pode-se melhorar os processos encadeados do modelo SECI, desenvolvendo rotinas de treinamentos internos para os colaboradores da empresa. Esses treinamentos podem abordar a temática da Segurança da Informação, com foco nos riscos inerentes à divulgação não autorizada de conhecimentos estratégicos ou sigilosos. Para auxiliar na compreensão de quais são esses conhecimentos, pode-se utilizar-se do controle “Rótulos e tratamento da informação”, que tem como objetivo rotular as informações e conhecimentos de acordo com a sua criticidade para a manutenção da cadeia de valor da empresa.

Desta forma, seguindo a orientação dos especialistas que julgaram os dois controles como mais preponderantes para o sucesso da proposta de melhoria dos processos do SECI, pode-se definir o processo de melhoria de forma global e não isolada em cada fase. O treinamento que pode ser apoiado pelos rótulos dos conhecimentos, deve ser construído ao longo de todo processo, sendo complementar em cada fase.

5 CONCLUSÃO

Informação e conhecimento sempre obtiveram destaque durante o processo de evolução social e empresarial, tornando-se um diferencial competitivo em um mercado cada vez mais globalizado. Devido à importância desses ativos, torna-se primordial aplicar práticas de gestão e proteção deles.

Criar e compartilhar conhecimento é primordial para o crescimento e desenvolvimento socioeconômico. As metodologias de Gestão do Conhecimento, de forma geral, têm como objetivo a criação e propagação do conhecimento na sociedade e nas empresas. A adoção de uma metodologia pode agregar valor ao ambiente capacitando pessoas que estarão aptas para melhorar os processos e otimizar tarefas.

A proteção das informações sensíveis é o objetivo das boas práticas de Segurança da Informação. A informação é o ativo principal de uma empresa para diferenciação de mercado. As metodologias de Segurança da Informação, juntamente com as boas práticas, buscam a proteção dos ativos de informação contra uso indevido, indisponibilidade ou fragmentação de dados.

Existe uma pequena lacuna de conhecimento que aborde de forma síncrona as duas temáticas, abrindo possibilidades de estudos científico para melhoria de gestão do ativo conhecimento nas empresas e sociedade. Pode-se utilizar as boas práticas de Segurança da Informação para melhorar os processos de Gestão do Conhecimento.

A realização desse trabalho permitiu destacar a importância dos temas abordados para manutenção da cadeia de valor das empresas e da evolução da sociedade. Da mesma forma pode-se criar uma interface entre os dois temas para que haja a Gestão do Conhecimento de forma segura.

Através de revisão bibliográfica e opinião de especialistas o objetivo geral desta pesquisa foi alcançado com sucesso ao propor melhorias no modelo de Gestão do Conhecimento SECI, considerando as boas práticas de implementação de Segurança da Informação em cada uma das fases da espiral do conhecimento. Para alcançar o objetivo geral desse trabalho fez-se necessário primeiramente cumprir alguns objetivos específicos que serviram para estruturar uma possível metodologia de Gestão do Conhecimento Seguro na criação de um *framework*.

O primeiro e segundo objetivo foram alcançados utilizando-se de revisão

bibliográfica sobre os temas abordados. A fonte de pesquisa bibliográfica principal para Gestão do Conhecimento esteve focada na metodologia de Nonaka e Takeuchi (2008) utilizando a abordagem de espiral do conhecimento, onde foi possível analisar cada fase do processo SECI (Socialização, Externalização, Combinação e Internalização) que serviu como base para construção de um possível framework. Como fonte primária de conceitos e boas práticas de Segurança da Informação, foi realizada a análise da documentação da NBR ISO/IEC 27001:2013 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013), com suas cláusulas de controles e controles, sendo possível compreender todo processo de criação de um Sistemas de Gestão de Segurança da Informação. Dessa forma os dois primeiros objetivos foram alcançados de forma satisfatória.

O terceiro objetivo que contribuiu de forma essencial para alcançar o objetivo principal de pesquisa foi desenvolvido a partir da criação da matriz de prioridade realizando o *crossover* entre as temáticas e a partir do conhecimento empírico do pesquisador no tema de Gestão do Conhecimento e Segurança da Informação, selecionando os controles presentes na NBR ISSO/IEC 27001:2013 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013) que poderiam ser utilizados nos processos de Gestão do Conhecimento.

O último objetivo específico foi alcançado com êxito, porém com algumas ressalvas. Para validar junto aos especialistas as práticas de Gestão de Conhecimento e Segurança da Informação utilizou-se a metodologia Delphi de pesquisa, cujo objetivo é comprar respostas de especialistas para chegar a um consenso sobre uma temática.

O framework final, resultando da pesquisa, não é complexo, pois apenas um controle obteve 80% de consenso entre os especialistas. Pondera-se que apenas um controle não compõe um framework de alta complexibilidade, porém esse controle pode melhorar o processo de Gestão do Conhecimento e dessa forma alcança-se o objetivo geral dessa pesquisa, em melhorar o modelo de Gestão de Conhecimento SECI nas fases da espiral do conhecimento.

O framework não obteve uma melhor composição de controles em virtude de alguns pontos de podem ser discutidos e melhorados para pesquisas futuras sobre a temática em questão, a fim de obter resultados mais concretos. Um dos pontos diz respeito à composição do grupo de especialistas em Segurança da Informação. Eles possuíam, em sua maioria, certificações técnicas da área de Segurança da

Informação. Especialistas em Segurança da Informação com certificações de gestão e experiência ampla em sistemas de gestão diversos poderiam responder a pesquisa de forma mais precisa, devido à visão holística que possuem de processos, ambientes e negócio.

Os especialistas em Gestão do Conhecimento não tinham conhecimento prévio profundo sobre o tema de Segurança da Informação. Mesmo havendo um descritivo explicativo dos conceitos de segurança, disponibilizado nos questionários, a especificidade do tema e sua abrangência podem ter dificultado a compreensão e objetivo de cada controle exposto da NBR ISO/IEC 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS(a), 2013).

Além disso, os especialistas em Segurança da Informação não tinham conhecimento prévio profundo sobre o tema de Gestão do Conhecimento ou do processo SECI. Mesmo havendo um descritivo explicativo dos conceitos e fases do SECI, disponibilizado nos questionários, a especificidade do tema e sua abrangência podem ter dificultado a compreensão de cada fase do SECI.

Novos estudos sobre a temática precisam ser desenvolvidos para aprimorar o assunto e obter resultados mais precisos. O grupo de especialistas é essencial para o resultado da metodologia Delphi. Pode-se observar a lacuna de conhecimento sobre os temas opostos à especialidade de cada especialista envolvido na pesquisa. Os temas formam um paradoxo em sua essência de abordagem, como evidenciado neste trabalho.

A escolha de profissionais para futuros estudos sobre o tema deve considerar a escolha por especialistas que tenham conhecimento profundo nas duas temáticas, a fim de poderem realizar melhores conexões entre os assuntos e chegarem a conclusões de forma mais precisa em suas escolhas. Outra possibilidade pode ser escolher um grupo menor de especialistas e capacitar cada um deles de forma inversa à sua especialidade e dessa forma chegar a resultados mais precisos.

Portanto, conclui-se este trabalho deixando como contribuição maior uma visão disruptiva sobre Gestão do Conhecimento e Segurança da Informação e colocando à disposição dos estudiosos sobre as temáticas um rol de observações e recomendações oportunas para serem utilizadas em melhorias de processos e sistemas de gestão.

REFERÊNCIAS

AHMAD, A.; AGUDELO, C. A.; BOSUA, R.; MAYNARD, S. B. Understanding knowledge leakage & BYOD (bring your own device): A mobile worker perspective. **ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems**, 1-13, 2015.

AIQON. **Checklist**: Avaliação de risco segurança da informação. Publicado em 02/03/2020. Disponível em: <https://aiqon.com.br/blog/avaliacao-de-risco/#:~:text=O%20risco%20%C3%A9%20o%20potencial,ativos%2C%20resultando%20em%20perda%20monet%C3%A1ria.>. Acessado em 21/04/2021

ALESSI, C, H.; ALESSI, M. R.; FERRARI, J. D.; PEREIRA, D. R.; RAMOS, K. S.; RUIZ, A.; SAPIA, M.H. Gestão de Segurança da Informação em uma empresa do setor de saúde: um estudo de caso. **Colloquium Exactarum**, v. 9, n. 4, p. 33–40. https://doi.org/10.5747/ce.2017.v09.n4.e213, 2017.

AMORIM, Y. **Análise de risco da segurança da informação**. Publicado em 07/07/2020. Disponível em <https://infoserver.net.br/2020/07/07/analise-de-risco-da-seguranca-da-informacao/>. Acesso em: 21 abr. 2021.

AL-MATARI, O. M. M.; ELHENNAWY, S.; HELAL, I. M. A.; MAZEN, S. A. Adopting security maturity model to the organizations' capability model. **Egyptian Informatics Journal**, xxxx, 1–7. https://doi.org/10.1016/j.eij.2020.08.001, 2020.

ALHOGAIL, A. Enhancing information security best practices sharing in virtual knowledge communities. **VINE Journal of Information and Knowledge Management Systems**. 2020. https://doi.org/10.1108/VJIKMS-01-2020-0009

ALVARES, L.; ITABORAHY, A., L. C.; MACHADO, R. P. M. Modelo de Maturidade em Inteligência Organizacional: uma visão integrada à gestão da informação, Gestão do Conhecimento e inteligência competitiva. **Informação & Sociedade**: Estudos, 30(4), 1–21, 2021. https://doi.org/10.22478/ufpb.1809-4783.2020v30n4.57352

ÁLVARES, L. M. A. R.; SOARES, C. M. L. C.; MACHADO, N. J. P.; VIANNA, E. W.; SILVA, T. F.; ARAGÃO, J.; GREENHALGH, M. Interfaces disciplinares selecionadas da Gestão do Conhecimento: características, contribuições e reflexões. **Em Questão**, Porto Alegre, v.26, n.2, p.132-160, maio/ago. 2020. Disponível em: https://seer.ufrgs.br/EmQuestao/article/view/94524/56604 Acesso em: 13 abr. 2021.

AMRAM, D. Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks. **Computer Law and Security Review**, 37. https://doi.org/10.1016/j.clsr.2020.105413, 2020.

AN, W. **Suggestion on intellectual property protection for entrepreneurial firms**. 2019. Retrieved from http://news.zhichanli.cn/article/8099.html on 1 may 2019.

ANAS, M.; HIDAYAT, M. T.; IRIYANTO, S.; SUHARMONO. Do intangible assets and

innovation orientation influence competitive advantages? A case study of SMEs in Indonesia. **Universal Journal of Accounting and Finance**, 9(1), 105–115. https://doi.org/10.13189/ujaf.2021.090111, 2021.

ANUPAN, A. A Framework of Knowledge Management in Classroom Action Research on Cloud Computing for Pre-Service Teachers. **International Conference on ICT and Knowledge Engineering**, 2020-Novem, 3–6, 2020. https://doi.org/10.1109/ICTKE50349.2020.9289862

ARAÚJO, S. G. L.; ARAÚJO, W. J. de.; BATISTA, R. R. Práticas Organizacionais Em Gestão do Conhecimento Que Contribuem Com a Segurança Da Informação: Estudo De Caso Na Universidade Federal Da Paraíba. **Perspectivas Em Gestão & Conhecimento**, 10(Special), 38–53. https://doi.org/10.21714/2236-417x2020v10nep38, 2020.

ARAÚJO, C. A. Á. Fundamentos da ciência da informação: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 1, p. 57-79, jan./jun. 2014.

ARAMUNI, J. P.; MAIA, L. C. O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. AtoZ: **Novas Práticas em Informação e Conhecimento**, 7(1), 31, 2020. https://doi.org/10.5380/atoz.v7i2.64640

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Gestão de Segurança da Informação. Rio de Janeiro: ABNT, 2013(a).

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Gestão de Segurança da Informação. Rio de Janeiro: ABNT, 2013(b).

ATAWNAH, N.; NADEEM, M.; SULEMAN, T.; ZAMAN, R. CEO ability, career concerns, firms' lifecycle and investments in intellectual capital. **International Review of Economics & Finance**, 75(December 2020), 237–251. https://doi.org/10.1016/j.iref.2021.04.023, 2021.

AU, K.; Li, W.; SHEN, N. Strategic alignment of intangible assets: The role of corporate social responsibility. **Asia Pacific Journal of Management**, 37(4), 1119–1139. https://doi.org/10.1007/s10490-019-09681-1, 2020.

BANISKI, G. M.; CIESLAK, R. A interculturalidade e sua influência na Gestão do Conhecimento: A experiência da Volvo do Brasil. **Perspectivas Em Gestão & Conhecimento**, 8(Número Especial), 70–85, 2018. https://doi.org/10.21714/2236-417x2018v8nep70

BARANES, A. I. Intangible Assets and the Financialized Business Enterprise: A Veblen-Commons Approach. **Journal of Economic Issues**, 54(3), 692–709, 2020. https://doi.org/10.1080/00213624.2020.1778973

BARANES, A.I.; HAKE, E.R. The Institutionalist Theory of Capital in the Modern Business Enterprise: Appropriation and Financialization. **Journal of Economic Issues** 52 (2): 430–437, 2018. doi:10.1080/00213624.2018.1469895 [Taylor &

Francis Online], [Web of Science ®], [Google Scholar]

BARBOSA, R. R. Gestão da informação e Gestão do Conhecimento: evolução e conexões. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 25, n. esp., p.168-186, fev. 2020. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/4303/2354 Acesso em: 13 abr. 2021.

BARTH, J. R.; LEE, J.; RICHEY, R. G.; XU, P. Blockchain as supply chain technology: considering transparency and security. **International Journal of Physical Distribution and Logistics Management**, 51(3), 305–324. https://doi.org/10.1108/IJPDLM-08-2019-0234, 2021.

BENNET, R. J.; BRUMMEL, B. J.; DALAL, R. S.; HOWARD, D. J.; POSEY, C.; ZACCARO, S. J. Organizational science and cybersecurity: abundant opportunities for research at the interface. **Journal of Business and Psychology**, 2021. https://doi.org/10.1007/s10869-021-09732-9

BOBERG, A. L.; MORRIS-KHOO, S. A. The Delphi method: a review of methodology and an application in the evaluation of a higher education program. **The Canadian Journal of Program Evaluation**, 7(1) 27-39, 1992.

BRITO, H. L. de.; SARTORI, J. J. D. S. **Capital intelectual e gestão do conhecimento**: Percepção dos funcionários da Holding de um grupo de empresas goianas. Revista Estudos e Pesquisas em Administração, 3(3), 98. https://doi.org/10.30781/repad.v3i3.9153, 2019.

CARVALHO, M. M.; FAVORETTO, C. An analysis of the relationship between knowledge management and project performance: Literature review and conceptual framework. **Gestão e Produção**, 28(1), 1-21, 2021. https://doi.org/10.1590/0104-530X4888-20

CHOO, C. W. “The knowing organization: how organizations use information to construct meaning, create knowledge and make decisions”, **International Journal of Information Management**, v. 16, n. 5, pp. 329-340, 1996.

COLOMÉ, M.; NUNES, R. C.; SILVA, L.; A. L. Pós-graduação, P. De, & Ppgcc, C. Técnica para Retenção e Recuperação de Conhecimento na Resolução de Incidentes de Segurança. **XIX Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais**, 2019.

CAMPOS, A. **Sistema de segurança da informação**: controlando os riscos. 2. ed., Florianópolis: Visual Books, 2007.

CANTO, C. A.; FREIRE, P.; SOUZA, J. A.; TIBOCHA, C. Y.; VIOLADA, P. A. Estruturação da Gestão do Conhecimento para inovação em modelos de negócio. **14 Congresso Brasileiro de Gestão do Conhecimento**, 17, 2018.

CORRÊA, F. Gestão do Conhecimento holística: de-lineamento teórico conceitual. **Perspectivas em Ciência da Informação**,24 (1), 122–146. Dalkir, K. (2005). Knowledge management in theory and practice. Burlington, MA, EUA: Elsevier,

2019.

DAI, H.; HU, X.; LIU, X.; SHAN, Z. Research on the Guidance Relationship Construction of Modern Apprenticeship in Enterprises Based on SECI Model**. Journal of Physics**: Conference Series, 1744(3), 2021. https://doi.org/10.1088/1742-6596/1744/3/032097

DANDOLINI, G.; KAUTNICK, A.; VALDATI, A. Modelos de maturidade de e-gov baseados na Gestão do Conhecimento. **14º Congresso Brasileiro de Gestão do Conhecimento**, ISSN: 1678-1546. Páginas 1-28, 2018.

DAVENPORT, T. H. **Ecologia da informação**: porque só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DAVENPORT, Thomas H. *et al.* **Working knowledge**: How organizations manage what they know. Harvard Business Press, 1998.

DRUCKER, P. F. **Desafios gerenciais para o século XXI**. São Paulo: Pioneira, 1999.

DRUCKER, P. F. **O advento da nova organização**. In Gestão do Conhecimento. Rio de Janeiro: Campus, 2000.

DUTRA, M. L.; FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. de. Mecanismos tecnológicos de segurança da informação no tratamento da veracidade dos dados em ambientes Big Data. **Perspectivas em Ciência da Informação**, v. 24, n. 2, p. 124–142, 2019. https://doi.org/10.1590/1981-5344/3348

ELLIS, J.; HERTIG, C. A.; METSCHER, R. **Concepts and Evolution of Asset Protection and Security**. Brad Spicer, The Professional Protection Officer Practical Security Strategies and Emerging Trends, Chapter 1. Pages 3-18, 2020. https://doi.org/10.1016/B978-0-12-817748-8.00001-8

EPURE, M. Knowledge management – capturing, distributing and effectively use of knowledge. **Ann Acad Rom Sci New Ser Econ Law Sociol**; 2(2): 5-18, 2016.

ESLAMKHAH, M.; SENO, H. S. Identifying and ranking knowledge management tools and techniques affecting organizational information security improvement. **Knowledge Management Research and Practice**, v. 17, n. 3, pp. 276-305, 2019.

ESWARAN, R.; VINAYAGAMOORTHI, G. Cyber security and information security. **International Journal of Recent Technology and Engineering**, 8(3 Special Issue), 372–374. https://doi.org/10.35940/ijrte.C1079.1083S19, 2019.

EVANS, M.; DALKIR, K.; BIDIAN, C. A holistic view of the knowledge life cycle: the knowledge management cycle (kmc) model. **Electronic Journal of Knowledge Management**, 12 (2), 85–97, 2014.

FACIONE, P. A. **Critical thinking**: a statement of expert consensus for purposes of educational assessment and instruction. research findings and recommendations (report). Newark, EUA: American Philosophical Association, 1990.

FARNESE, M. L.; BARBIERI, B.; CHIRUMBOLO, A.; PATRIOTTA, G. Managing knowledge in organizations: a nonaka's seci model operationalization. **Frontiers in Psychology**, 10, 01–15, 2019. doi: doi.org/10.3389/fpsyg.2019.02730.

FILHO, R., J.; IDE, M. C.; NAKAMURA, E. T. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados pessoais**. Sbseg2019.Ime.Usp.Br. https://sbseg2019.ime.usp.br/anais/197877.pdf, 2019.

GUO, X.; XUE, Y. The professional education ecosystem of industrial design at Georgia Institute of technology based on SECI model. **E3S Web of Conferences**, 179, 1–7, 2020. https://doi.org/10.1051/e3sconf/202017902032

GRISHAM, T. The delphi technique: a method for testing complex and multifaceted topics. **International Journal of Managing Projects in Business**,2 (1), 120-130, 2009. doi: 10.1108/17538370910930545.

HCI Profesional Services. **Knowledge Management 10 Point Checklist**, 2019. Disponível em: https://www.hci.com.au/km-checklist. Acesso em: 10 mar. 2022

HSU, C. C.; SANDFORD, B. A. The Delphi technique: Making sense of consensus. **Practical Assessment, Research and Evaluation**, 12(10), 1–8, 2007.

HJøRLAND, B. Information retrieval and knowledge organization: A perspective from the philosophy of science. **Information (Switzerland),** 12(3). https://doi.org/10.3390/info12030135, 2021.

IDE, M. C.; NAKAMURA, E. T.; REYNALDO, J.; Filho, F. **Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais**. Sbseg2019.Ime.Usp.Br, 2019. https://sbseg2019.ime.usp.br/anais/197877.pdf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO Survey Data**. Disponível em < https://www.iso.org/the-iso-survey.html >, 2019, acesso em 06/07/2021.

KAILA, U.; NYMAN, L. Information security best practices: first steps for startups and SMEs. **Technology Innovation Management Review**, v. 8, n. 11, pp. 32-42, 2018.

KAPLAN, R. S.; NORTON, D. P. **Mapas estratégicos**. Rio de Janeiro: Campus, 2004.

KOLO C.B.; MIERZEJEWSKA B.I. **Economics of information and cultural goods**. Edward Elgar Publishing Limited, UK, 77-102, 2019. DOI:https://doi.org/10.4337/9781788119061

KROGH, V. G., ROSS, J. A perspective on knowledge, competence and strategy. **Personnel Review**, 24(3), 56–76, 1995. https://doi.org/10.1108/00483489510089650

KRÜGER, T. C.; PINTO, M. D. de S. Avaliação da maturidade de gestão da

informação e do conhecimento: um estudo aplicado em três editoras universitárias federais do sul do Brasil. **Perspectivas em Gestão & Conhecimento**, 10(2), 120–142, 2020. https://doi.org/10.21714/2236-417x2020v10n2p120

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS, 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27/04/2021.

LINSTONE, H. A.; TUROFF, M. **The Delphi method**: Techniques and applications. Addison Wesley Newark, NJ: New Jersey Institute of Technology, 2002.

LIU, X.; QIAN, X.; PARDALOS, P. M.; PEI, J.; YANG, W. A game of information security investment considering security insurance and complementary information assets. **International Transactions in Operational Research**, 0, 1–34, 2021. https://doi.org/10.1111/itor.12972

MACHADO, A.; SPRAKEL, E. Open innovation strategies and appropriability in knowledge-intensive business services: Evidences and implications in the brazilian context. **Brazilian Business Review**, 18(1), 62–81. https://doi.org/10.15728/BBR.2021.18.1.4, 2021.

MARCÃO, R. P.; PESTANA, G.; SOUSA, M. J. Knowledge management and gamification in pharma: An approach in pandemic times to develop product quality reviews. **Electronic Journal of Knowledge Management**, 18(3), 255–268. https://doi.org/10.34190/EJKM.18.03.005, 2021.

MARQUES, J. B. V.; FREITAS, D. de. Método DELPHI: caracterização e potencialidades na pesquisa em Educação. **Pro-Posições**, 29(2), 389–415. https://doi.org/10.1590/1980-6248-2015-0140, 2018.

MITNICK, K. **A arte de enganar**. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Pearson Education, 2003.

MUKHERJEE, N.; HUG, J.; SUTHERLAND, W.; MCNEILL, J.; VAN OPSTAL, M.; DAHDOUH-GUEBAS, F.; KOEDAM, N. The Delphi technique in ecology and biological conservation: applications and guidelines. **Methods Ecol. Evol.** 2015 (6), 1097–1109, 2015.

NAZIR, S.; PINSONNEAULT, A. Relating agility and electronic integration: The role of knowledge and process coordination mechanisms. **Journal of Strategic Information Systems**, 30(2), 101654, 2021. https://doi.org/10.1016/j.jsis.2021.101654

NERES, T. **Políticas de Segurança da Informação x LGPD**. Disponível em <https://triplait.com/politicas-de-seguranca-da-informacao-x-lgpd/>. Publicado em 15/07/2020. Acesso em 27/04/2021.

NONAKA, I.; TAKEUCHI, H. **Gestão do Conhecimento**. Porto Alegre: Bookman, 2008.

NUNES, P. C. R.; OLIVEIRA, N., Q., S.; RIBEIRO, D. F. O jogo da imitação: O papel

da informação na tomada de decisão nas organizações. **ECCOM**, v. 10, n. 20,157157–166, 2019.

OLIVEIRA, T. As políticas científicas na era do conhecimento: uma análise de conjuntura sobre o ecossistema científico global. **Perspectivas em Ciência da Informação**, 24(1), 191–215. https://doi.org/10.1590/1981-5344/3520, 2019.

OLIVEIRA, W. **Riscos, Vulnerabilidade e Ameaça em Segurança da Informação**. Publicado em 16/04/2021. Disponível em: <https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca>. Acesso em 21/04/2021

PARK, H.; SCORESBY, R. B. The joint effects of individual and firm level knowledge attributes on inventor mobility to entrepreneurial and established firms. **Journal of Business Research**, 133(April), 218–230. https://doi.org/10.1016/j.jbusres.2021.04.059, 2021.

PINHEIRO, J. Modelos de GC: Choo. **Sociedade Brasileira de Gestão do Conhecimento**, 2020. Disponível em: <http://www.sbgc.org.br/blog/modelos-de-gc-modelo-de-choo>. Acesso em 21/04/2021.

PHILIPSON, S.; KJELLSTRÖM, E. When objects are talking: How tacit knowing becomes explicit knowledge. **Journal of Small Business Strategy**,30 (1), 68–82, 2020.

PIZZAIA, A.; PEGINO, P. M. F.; COLLA, J. E.; TENÓRIO, N. O papel da comunicação na gestão do conhecimento: aspectos relevantes e estímulo a novas pesquisas. **Perspectivas em Gestão & Conhecimento**, v. 8, n. 2, p. 62-81, 2018.

POWELL, C. The delphi technique: myths and rea-lities. **Journal of Advanced Nursing**,41 (4), 376–382, 2003. doi: 10.1046/j.1365-2648.2003.02537.x.

RAZI, M. J. M.; KARIM, N. S. A.; DAHLAN, A. R. A.; MOHAMAD A, N. A. A holistic approach to measure organizational readiness for knowledge manage-ment. **Advanced Science Letters**, 23 (4), 2829–2832, 2017. doi: doi.org/10.1166/asl.2017.7693.

RIOS, O. K. L.; TEIXEIRA F, J. G. de A.; RIOS, V. P. da S. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. **Navus - Revista de Gestão e Tecnologia**, 49–65, 2017. https://doi.org/10.22279/navus.2017.v7n2.p49-65.482

RODIONOV, D.; PEREPECHKO, O.; NADEZHINA, O. Determining economic security of a business based on valuation of intangible assets according to the international valuation standards (IVS). **Risks**, 8(4), 1–14, 2020. https://doi.org/10.3390/risks8040110

RUNTE, G. I. B. C. **Gestão do Conhecimento**: os desafios da implantação de um modelo integrado: o caso ANS. 2011. 146 f. Dissertação (Mestrado em Administração Pública) - Fundação Getúlio Vargas, Rio de Janeiro. 2016.

SILVEIRA, M. M.; VARVAKIS, G. Gestão do Conhecimento e co-criação de valor em

Serviços Informacionais. **Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información**, 35(86), 73, 2020. https://doi.org/10.22201/iibi.24488321xe.2021.86.58255

SCHWARTZ, D. G. Aristotelian view of knowledge management. In: SCHWARTZ, D. G.(ed.) **Encyclopedia of knowledge management**. 2. ed. New York: IGI Global, 2006a.

SCHWARTZ, D. G. **Encyclopedia of knowledge management**. London: Idea Group Reference, 2006b.

SAFA, N. S.; VON SOLMS, R.; FURNELL, S. Information security policy compliance model in organizations. **Computers and Security**, v. 56, p. 1–13, 2016. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84954106648&doi=10.1016%2fj.chb.2015.12.037&partnerID=40&md5=7644d1b633827cf08a8 54f954cc6157c. Acesso em: 16 dez. 2020

SAFA, N.S. VON SOLMS, R. “An information security knowledge sharing model in organizations”, **Computers in Human Behavior**, Vol. 57, pp. 442-451, 2016.

SALES, R.; ALMEIDA, P. P. Avaliação de fontes de informação na internet: avaliando o site nupill/ufsc. **Revista Digital de Biblioteconomia e Ciência da Informação**,4 (2), 67–87, 2007.

SANTOS, C. D.; VALENTIM, M. L. P. As interconexões entre a gestão da informação e a Gestão do Conhecimento para o gerenciamento dos fluxos informacionais. **Perspectivas em Gestão & Conhecimento**, v. 4, n. 2, p. 19-33, 2014. Disponível em: http://hdl.handle.net/20.500.11959/brapci/49728. Acesso em: 17 dez. 2020.

SANTOS, D, M. L. B.; ZATTAR, I. C. A Importância da Gestão do Conhecimento para o Funcionamento dos Ecossistemas de Inovação. **Journal on Innovation and Sustainability**. RISUS ISSN 2179-3565, 10(1), 48–56, 2019. https://doi.org/10.24212/2179-3565.2019v10i1p48-56

SILVA, R. F.; TANAKA, O. Y. Técnica Delphi: identificando as competências gerais do médico e do enfermeiro que atuam em atenção primária de saúde. **Revista da Escola de Enfermagem – USP**, 33(3), 207-216, 1999.

SILVA, T.; TOMAÉL, M. I. A gestão da informação nas organizações. **Revista Informação & Informação**,12 (2), 375–397, 2007.

SOUZA, J. G. S.; ARIMA, C. H.; BELDA, F. R. Análise de tratamento da segurança da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, 15(3), 1309-1321, 2020. https://doi.org/10.21723/riaee.v15i3.13584

UPADHAYA, B.; ZHAO, S.; WANG, Y.; Yi, L. YIN, Y. Knowledge spillover, knowledge management capabilities, and innovation among returnee entrepreneurial firms in emerging markets: Does entrepreneurial ecosystem matter? **Journal of Business Research**, 130, 283–294, 2021. https://doi.org/10.1016/j.jbusres.2021.03.024

VALENTIM, M. L. P. Conceitos sobre Gestão do Conhecimento: uma revisão sistemática da literatura brasileira. **Informação & Sociedade: Estudos**, 30(4), 1–34, 2021. https://doi.org/10.22478/ufpb.1809-4783.2020v30n4.57186

VIANNA, E. W.; FERNANDES, J. H. C. O gestor da Segurança da Informação no espaço cibernético governamental: Grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science**, 9(1), 2015.

ZEFERINO, D. **O que é Segurança da Informação e qual sua importância?** Publicado em 27/07/2020. Disponível em: <https://www.certifiquei.com.br/seguranca-informacao/>. Acesso em 21/04/2021.

WALTERS, D.; KOTZE, D. C.; REBELO, A.; PRETORIUS, L.; JOB, N.; LAGESSE, J. V.; RIDDELL, E.; COWDEN, C. Validation of a rapid wetland ecosystem services assessment technique using the Delphi method. **Ecological Indicators**, 125(February), 107511. https://doi.org/10.1016/j.ecolind.2021.107511, 2021.

WISNIEWSKA, M.; WISNIEWSKI, Z. The relationship between knowledge security and the propagation of innovation. **Advances in Intelligent Systems and Computing**, 783, 176–184. https://doi.org/10.1007/978-3-319-94709-9_18, 2019.

YOUSUF, M. I. Using experts' opinions through Delphi technique. **Practical Assessment, Research & Evaluation**, 12(4), 1-9, 2007.

ANEXO A

Controles NBR ISO/IEC 27002:2013

ISO 27001:2013 Controles de Segurança		
Clausula	**Secção**	**Objetivo de controle / controle**
5 Políticas de segurança da informação	5.1	Orientação da direção para segurança da informação
	5.1.1	Políticas para segurança da informação
	5.1.2	Análise crítica das políticas para segurança da informação
6 Organização da segurança da informação	6,1	Organização interna
	6.1.1	Responsabilidades e papéis pela segurança da informação
	6.1.2	Segregação de funções
	6.1.3	Contato com autoridades
	6.1.4	Contato com grupos especiais
	6.1.5	Segurança da informação no gerenciamento de projetos
	6,2	Dispositivos móveis e trabalho remoto
	6.2.1	Política para o uso de dispositivo móvel
	6.2.2	Trabalho remoto
7 Segurança em recursos humanos	7,1	Antes da contratação
	7.1.1	Seleção
	7.1.2	Termos e condições de contratação
	7,2	Durante a contratação
	7.2.1	Responsabilidades da direção
	7.2.2	Conscientização, educação e treinamento em segurança da informação
	7.2.3	Processo disciplinar
	7,3	Encerramento e mudança da contratação
	7.3.1	Responsabilidades pelo encerramento ou mudança da contratação
8 Gestão de ativos	8,1	Responsabilidade pelos ativos
	8.1.1	Inventário dos ativos
	8.1.2	Proprietário dos ativos
	8.1.3	Uso aceitável dos ativos
	8.1.4	Devolução de ativos
	8,2	Classificação da informação
	8.2.1	Classificação da informação
	8.2.2	Rótulos e tratamento da informação
	8.2.3	Tratamento dos ativos
	8,3	Tratamento de mídias
	8.3.1	Gerenciamento de mídias removíveis
	8.3.2	Descarte de mídias
	8.3.3	Transferência física de mídias

9 Controle de acesso	9,1	Requisitos do negócio para controle de acesso
	9.1.1	Política de controle de acesso
	9.1.2	Acesso às redes e aos serviços de rede
	9,2	Gerenciamento de acesso do usuário
	9.2.1	Registro e cancelamento de usuário
	9.2.2	Provisionamento para acesso de usuário
	9.2.3	Gerenciamento de direitos de acesso privilegiados
	9.2.4	Gerenciamento da informação de autenticação secreta de usuários
	9.2.5	Análise crítica dos direitos de acesso de usuário
	9.2.6	Retirada ou ajuste de direitos de acesso
	9,3	Responsabilidades dos usuários
	9.3.1	Uso da informação de autenticação secreta
	9,4	Controle de acesso ao sistema e à aplicação
	9.4.1	Restrição de acesso à informação
	9.4.2	Procedimentos seguros de entrada no sistema (log-on)
	9.4.3	Sistema de gerenciamento de senha
	9.4.4	Uso de programas utilitários privilegiados
	9.4.5	Controle de acesso ao código-fonte de programas
10 Criptografia	10,1	Controles criptográficos
	10.1.1	Política para o uso de controles criptográficos
	10.1.2	Gerenciamento de chaves
11 Segurança física e do ambiente	11,1	Áreas seguras
	11.1.1	Perímetro de segurança física
	11.1.2	Controles de entrada física
	11.1.3	Segurança em escritórios, salas e instalações
	11.1.4	Proteção contra ameaças externas e do meio-ambiente
	11.1.5	Trabalhando em áreas seguras
	11.1.6	Áreas de entrega e de carregamento
	11,2	Equipamentos
	11.2.1	Escolha do local e proteção do equipamento
	11.2.2	Utilidades
	11.2.3	Segurança do cabeamento
	11.2.4	Manutenção dos equipamentos
	11.2.5	Remoção de ativos
	11.2.6	Segurança de equipamentos e ativos fora das dependências da organização
	11.2.7	Reutilização e alienação segura de equipamentos
	11.2.8	Equipamento de usuário sem monitoração
	11.2.9	Política de mesa limpa e tela limpa
12 Segurança nas operações	12,1	Responsabilidades e procedimentos operacionais
	12.1.1	Documentação dos procedimentos de operação
	12.1.2	Gestão de mudanças
	12.1.3	Gestão de capacidade

	12.1.4	Separação dos ambientes de desenvolvimento, teste e de produção
	12,2	Proteção contra códigos maliciosos
	12.2.1	Controles contra códigos maliciosos
	12,3	Cópias de segurança
	12.3.1	Cópias de segurança das informações
	12,4	Registros e monitoramento
	12.4.1	Registros de eventos
	12.4.2	Proteção das informações dos registros de eventos (logs)
	12.4.3	Registros de eventos (log) de administrador e operador
	12.4.4	Sincronização dos relógios
	12,5	Controle de software operacional
	12.5.1	Instalação de software nos sistemas operacionais
	12,6	Gestão de vulnerabilidades técnicas
	12.6.1	Gestão de vulnerabilidades técnicas
	12.6.2	Restrições quanto à instalação de software
	12,7	Considerações quanto à auditoria de sistemas de informação
	12.7.1	Controles de auditoria de sistemas de informação
13 Segurança nas comunicações	13,1	Gerenciamento da segurança em redes
	13.1.1	Controles de redes
	13.1.2	Segurança dos serviços de rede
	13.1.3	Segregação de redes
	13,2	Transferência de informação
	13.2.1	Políticas e procedimentos para transferência de informações
	13.2.2	Acordos para transferência de informações
	13.2.3	Mensagens eletrônicas
	13.2.4	Acordos de confidencialidade e não divulgação
14 Aquisição, desenvolvimento e manutenção de sistemas	14,1	Requisitos de segurança de sistemas de informação
	14.1.1	Análise e especificação dos requisitos de segurança da informação
	14.1.2	Serviços de aplicação seguros em redes públicas
	14.1.3	Protegendo as transações nos aplicativos de serviços
	14,2	Segurança em processos de desenvolvimento e de suporte
	14.2.1	Política de desenvolvimento seguro
	14.2.2	Procedimentos para controle de mudanças de sistemas
	14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
	14.2.4	Restrições sobre mudanças em pacotes de Software
	14.2.5	Princípios para projetar sistemas seguros
	14.2.6	Ambiente seguro para desenvolvimento
	14.2.7	Desenvolvimento terceirizado
	14.2.8	Teste de segurança do sistema
	14.2.9	Teste de aceitação de sistemas
	14,3	Dados para teste
	14.3.1	Proteção dos dados para teste

15 Relacionamento na cadeia de suprimento	15,1	Segurança da informação na cadeia de suprimento
	15.1.1	Política de segurança da informação no relacionamento com os fornecedores
	15.1.2	Identificando segurança da informação nos acordos com fornecedores
	15.1.3	Cadeia de suprimento na tecnologia da comunicação e informação
	15,2	Gerenciamento da entrega do serviço do fornecedor
	15.2.1	Monitoramento e análise crítica de serviços com fornecedores
	15.2.2	Gerenciamento de mudanças para serviços com fornecedores
16 Gestão de incidentes de segurança da informação	16,1	Gestão de incidentes de segurança da informação e melhorias
	16.1.1	Responsabilidades e procedimentos
	16.1.2	Notificação de eventos de segurança da informação
	16.1.3	Notificando fragilidades de segurança da informação
	16.1.4	Avaliação e decisão dos eventos de segurança da informação
	16.1.5	Resposta aos incidentes de segurança da informação
	16.1.6	Aprendendo com os incidentes de segurança da informação
	16.1.7	Coleta de evidências
17 Aspectos da segurança da informação na gestão da continuidade do negócio	17,1	Continuidade da segurança da informação
	17.1.1	Planejando a continuidade da segurança da informação
	17.1.2	Implementando a continuidade da segurança da informação
	17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação
	17,2	Redundâncias
	17.2.1	Disponibilidade dos recursos de processamento da informação
18 Conformidade	18,1	Conformidade com requisitos legais e contratuais
	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.2	Direitos de propriedade intelectual
	18.1.3	Proteção de registros
	18.1.4	Proteção e privacidade de informações de identificação pessoal
	18.1.5	Regulamentação de controles de criptografia
	18,2	Análise crítica da segurança da informação
	18.2.1	Análise crítica independente da segurança da informação
	18.2.2	Conformidade com as políticas e procedimentos de segurança da informação
	18.2.3	Análise crítica da conformidade técnica

ANEXO B

Questionário primeira rodada:

Segurança da Informação Aplicada no Modelo SECI: Desenvolvimento de um Framework para Gestão do Conhecimento Seguro

Você está sendo convidado(a) a participar voluntariamente da pesquisa Segurança da Informação Aplicada no Modelo SECI: Desenvolvimento de um framework para Gestão do Conhecimento Seguro, a qual objetiva identificar os controles de Segurança da Informação sob a ótica da ISO27001 que possam contribuir no processo de Gestão do Conhecimento. Sua participação consistirá em responder ao questionário que segue durante algumas rodadas de respostas. O tempo médio de conclusão de suas respostas será entre 7 e 10 minutos. O questionário está estruturado com 20 controles pré-selecionados e vinculados às fases do SECI. Sua colaboração na pesquisa resultará na proposta de um framework de Gestão do Conhecimento Seguro. Para entender o processo, por favor assista o vídeo a seguir: https://youtu.be/G4A9xexi3fwPor tratar-se de pesquisa cujo armazenamento das respostas ao formulário se dará em nuvem durante o período de coleta, o pesquisador se compromete a fazer o download dos dados imediatamente após o encerramento da coleta, assim como a retirá-los da nuvem. Por um período de cinco anos, o pesquisador manterá sob sua guarda, em computadores privados, os documentos e dados atinentes à pesquisa. Se você aceitar fazer parte do estudo, selecione “SIM”. O envio de suas respostas será entendido como expressão formal de seu consentimento livre e esclarecido em participar da pesquisa. Se restarem dúvidas, poderá consultar o pesquisador cujos dados para contato encontram-se neste Termo. Mateus Buogo (mestrando)

E-mail: mbuogors@gmail.com

1.Aceita fazer parte deste estudo?

Marcar apenas uma.

- ☐ Sim
- ☐ Não

Descritivos

Nesta sessão, estão descritos de forma breve os processos do SECI e também uma descrição breve de cada um dos 20 controles da ISO27001.

Processo SECI de criação e compartilhamento do conhecimento proposto por Nonaka e Takeuchi (2008).

(S)ocialização do Conhecimento - Onde o indivíduo compartilha o seu conhecimento com outro indivíduo através de experiências diretas. Nesta fase o conhecimento tácito de um indivíduo é compartilhada com o outro, que irá criar um novo conhecimento também tácito. As experiências pessoais que ocorrem em relação mestre e aprendiz, observação das atividades, ou mesmo aquela "conversinha do cafezinho" são exemplos de socialização.

(E)xternalização do Conhecimento - Após compartilhar o conhecimento, o indivíduo articula esse conhecimento cocriado para um grupo de pessoas. O conhecimento tácito criado pelos os indivíduos, agora é transformado em explícito para um grupo maior de pessoas. Um ótimo exemplo é a documentação do conhecimento, onde um individuo externaliza o seu conhecimento podendo disponibilizara-lo a outros indivíduos.

(C)ombinação do Conhecimento - Sistematização do conhecimento, ocorre do grupo para toda organização. O conhecimento que já está explicito é compartilhado e criado também de forma explicita para um grupo maior de pessoas. A combinação pode ser caracterizada também como uma integração de novos conhecimentos explícitos, e ocorre na manipulação de dados por indivíduos como, por exemplo, em reuniões.

(I)nternalização do Conhecimento - Cada indivíduo em particular recebe esse conhecimento e efetua a internalização dele, ele aprende o novo conhecimento transformando-o em tácito novamente. A internalização refere-se à incorporação do conhecimento explícito em conhecimento tácito no sentido da organização para indivíduo.

Controles ISO27001

- Políticas para Segurança da Informação: Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. Nas políticas estão descritas as diretrizes que devem ser seguidas por todos e também documentar os processos de segurança vigentes.

- Responsabilidades e Papéis pela Segurança da Informação: Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas. Controle responsável por definir as responsabilidades de cada individuo e garantir a conformidade com as políticas de segurança da informação.

- Segregação de Funções: Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização. A segregação garante que informações de níveis mais críticos só possam ser acessadas por pessoas em funções autorizadas.

- Termos e Condições de Contratação: Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.

- Responsabilidades da Direção: Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

- Conscientização, educação e treinamento em Segurança da Informação: Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

- Responsabilidades pelo encerramento ou mudança da contratação: Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, sejam definidas, comunicadas aos funcionários ou partes externas e sejam cumpridas.

- Classificação da informação: Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

- Rótulos e tratamento da informação: Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

- Política de controle de acesso: Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

- Gerenciamento de direitos de acesso privilegiados: Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.

- Gerenciamento da informação de autenticação secreta de usuários: Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

- Análise crítica dos direitos de acesso de usuário: Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

- Retirada ou ajuste de direitos de acesso: Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

- Restrição de acesso à informação: Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

- Política de segurança da informação no relacionamento com os fornecedores: Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

- Identificando segurança da informação nos acordos com fornecedores: Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização.

- Identificação da legislação aplicável e de requisitos contratuais: Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

- Direitos de propriedade intelectual: Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de softwares proprietários.

- Proteção e privacidade de informações de identificação pessoal: Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

Especialista

2.Você é um especialista:

Marcar apenas uma.

- Gestão do Conhecimento
- Segurança da Informação

SECI – Socialização do Conhecimento

Socialização é criar e compartilhar conhecimento tácito, a partir de experiência direta de indivíduo para indivíduo. Na prática, ela pode ocorrer através de atividades interativas entre os indivíduos no local de trabalho como brainstorms e reuniões.

3. Assinale as opções que você considera que são as mais importantes para a fase de SOCIALIZAÇÃO. Pode ser mais de uma. Marque todas que se aplicam.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso

- Gerenciamento de direitos de acesso privilegiados
- Gerenciamento da informação de autenticação secreta de usuários
- Análise crítica dos direitos de acesso de usuário
- Retirada ou ajuste de direitos de acesso
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificando segurança da informação nos acordos com fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Direitos de propriedade intelectual
- Proteção e privacidade de informações de identificação pessoal

SECI – Externalização do Conhecimento

Externalização está relacionado com articular o conhecimento através do diálogo e da reflexão de um de indivíduo para um grupo. Nesta fase o conhecimento é compartilhado com um grupo de pessoas utilizando técnicas que permitam esse compartilhamento como reuniões, conferências, entre outras.

4.Assinale as opções que você considera que são as mais importantes para fase de EXTERNALIZAÇÃO. Pode ser mais de uma.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso
- Gerenciamento de direitos de acesso privilegiados
- Gerenciamento da informação de autenticação secreta de usuários
- Análise crítica dos direitos de acesso de usuário
- Retirada ou ajuste de direitos de acesso
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificando segurança da informação nos acordos com fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Direitos de propriedade intelectual
- Proteção e privacidade de informações de identificação pessoal

SECI – Combinação do Conhecimento

Combinação é sistematizar e aplicar o conhecimento e a informação, de grupo para organização. Seguindo o fluxo do compartilhamento, o conhecimento que foi criado na fase

da Externalização, é difundido para um grupo maior ainda, toda a organização utilizando-se de várias técnicas e tecnologias para isso, podendo ser murais espalhadas na empresa, fóruns digitais entre outras.

5.Assinale as opções que você considera que são as mais importantes para fase de COMBINAÇÃO. Pode ser mais de uma.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso
- Gerenciamento de direitos de acesso privilegiados
- Gerenciamento da informação de autenticação secreta de usuários
- Análise crítica dos direitos de acesso de usuário
- Retirada ou ajuste de direitos de acesso
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificando segurança da informação nos acordos com fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Direitos de propriedade intelectual
- Proteção e privacidade de informações de identificação pessoal

SECI – Internalização do Conhecimento

Internalização é aprender e adquirir novo conhecimento, de organização para indivíduo. Aqui as organizações passariam a vivenciar o resultado prático do novo conhecimento; ou seja, desenvolveriam um conhecimento operacional. Nesta fase as pessoas absorvem todo o conhecimento, internalizando-o e colocando em prática em seu dia-a-dia.

6.Assinale as opções que você considera que são as mais importantes para fase de INTERNALIZAÇÃO. Pode ser mais de uma.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação

- Política de controle de acesso
- Gerenciamento de direitos de acesso privilegiados
- Gerenciamento da informação de autenticação secreta de usuários
- Análise crítica dos direitos de acesso de usuário
- Retirada ou ajuste de direitos de acesso
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificando segurança da informação nos acordos com fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Direitos de propriedade intelectual
- Proteção e privacidade de informações de identificação pessoal

Questionário segunda rodada:

DELPHI - ETAPA 2: Segurança da Informação Aplicada no Modelo SECI: Desenvolvimento de um Framework para Gestão do Conhecimento Seguro

Estágio 2 de respostas do método Delphi. Para facilitar sua escolha e contexto nas próximas etapas do Delphi, criamos um documento com o detalhamento de cada objeto da ISO27001 no contexto da pesquisa. Podes consulta-lo neste link se necessário: https://docs.google.com/document/d/1IAzxeWateQbDyIuRDAEruwNHTv-ZaATTf2_4KIRcfj8/edit?usp=sharingDesta fase em diante, solicitamos que sejam marcadas as alternativas mais preponderantes no seu ponto de vista, com maior critério de análise. Neste ponto já excluímos todas as alternativas sem votos ou com menos de 50% de escolha em relação a alternativa mais votada, ou seja, em casos que a alternativa mais votada recebeu 70% de votos, foram eliminadas todas alternativas com menos de 35% de votos para essa segunda rodada. Controles que já tiveram 80% de congruência também foram retirados desta etapa de pesquisa. Reiteramos que desta fase em diante, sejam marcadas as alternativas com mais critério. Ainda pedimos que seja assinalada no mínimo 1 alternativa por etapa.

Ficamos à disposição

Mateus Buogo

E-mail: mbuogors@gmail.com

Descritivos

Nesta sessão, estão descritos de forma breve os processos do SECI e também uma descrição breve de cada um dos 20 controles da ISO27001.

Processo SECI de criação e compartilhamento do conhecimento proposto por Nonaka e Takeuchi (2008).

(S)ocialização do Conhecimento - Onde o indivíduo compartilha o seu conhecimento com outro indivíduo através de experiências diretas. Nesta fase o conhecimento tácito de um indivíduo é compartilhada com o outro, que irá criar um novo conhecimento também tácito. As experiências pessoais que ocorrem em relação mestre e aprendiz, observação das atividades, ou mesmo aquela “conversinha do cafezinho” são exemplos de socialização.

(E)xternalização do Conhecimento - Após compartilhar o conhecimento, o indivíduo articula esse conhecimento cocriado para um grupo de pessoas. O conhecimento tácito criado pelos os indivíduos, agora é transformado em explícito para um grupo maior de pessoas. Um ótimo exemplo é a documentação do conhecimento, onde um individuo externaliza o seu conhecimento podendo disponibilizara-lo a outros indivíduos.

(C)ombinação do Conhecimento - Sistematização do conhecimento, ocorre do grupo para toda organização. O conhecimento que já está explicito é compartilhado e criado também de forma explicita para um grupo maior de pessoas. A combinação pode ser caracterizada também como uma integração de novos conhecimentos explícitos, e ocorre na manipulação de dados por indivíduos como, por exemplo, em reuniões.

(I)nternalização do Conhecimento - Cada indivíduo em particular recebe esse conhecimento e efetua a internalização dele, ele aprende o novo conhecimento transformando-o em tácito novamente. A internalização refere-se à incorporação do conhecimento explícito em conhecimento tácito no sentido da organização para indivíduo.

Especialista

1.Você é um especialista:

Marcar apenas uma.

- Gestão do Conhecimento
- Segurança da Informação

SECI – Socialização do Conhecimento

Socialização é criar e compartilhar conhecimento tácito, a partir de experiência direta de indivíduo para indivíduo. Na prática, ela pode ocorrer através de atividades interativas entre os indivíduos no local de trabalho como brainstorms e reuniões.

2. Assinale as opções que você considera que são as mais importantes para a fase de SOCIALIZAÇÃO. Pode ser mais de uma. Marque todas que se aplicam.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Classificação da informação
- Política de segurança da informação no relacionamento com os fornecedores
- Proteção e privacidade de informações de identificação pessoal

SECI – Externalização do Conhecimento

Externalização está relacionado com articular o conhecimento através do diálogo e da reflexão de um de indivíduo para um grupo. Nesta fase o conhecimento é compartilhado com um grupo de pessoas utilizando técnicas que permitam esse compartilhamento como reuniões, conferências, entre outras.

3.Assinale as opções que você considera que são as mais importantes para fase de EXTERNALIZAÇÃO. Pode ser mais de uma. Marque todas que se aplicam.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso
- Gerenciamento de direitos de acesso privilegiados
- Política de segurança da informação no relacionamento com os fornecedores
- Proteção e privacidade de informações de identificação pessoal

SECI – Combinação do Conhecimento

Combinação é sistematizar e aplicar o conhecimento e a informação, de grupo para organização. Seguindo o fluxo do compartilhamento, o conhecimento que foi criado na fase da Externalização, é difundido para um grupo maior ainda, toda a organização utilizando-se de várias técnicas e tecnologias para isso, podendo ser murais espalhadas na empresa, fóruns digitais entre outras.

4.Assinale as opções que você considera que são as mais importantes para fase de COMBINAÇÃO. Pode ser mais de uma. Marque todas que se aplicam.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação

- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso
- Gerenciamento de direitos de acesso privilegiados
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Direitos de propriedade intelectual
- Proteção e privacidade de informações de identificação pessoal

SECI – Internalização do Conhecimento

Internalização é aprender e adquirir novo conhecimento, de organização para indivíduo. Aqui as organizações passariam a vivenciar o resultado prático do novo conhecimento; ou seja, desenvolveriam um conhecimento operacional. Nesta fase as pessoas absorvem todo o conhecimento, internalizando-o e colocando em prática em seu dia-a-dia.

5.Assinale as opções que você considera que são as mais importantes para fase de INTERNALIZAÇÃO. Pode ser mais de uma.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação
- Segregação de funções
- Termos e condições de contratação
- Responsabilidades da direção
- Conscientização, educação e treinamento em segurança da informação
- Responsabilidades pelo encerramento ou mudança da contratação
- Classificação da informação
- Rótulos e tratamento da informação
- Política de controle de acesso
- Análise crítica dos direitos de acesso de usuário
- Retirada ou ajuste de direitos de acesso
- Restrição de acesso à informação
- Política de segurança da informação no relacionamento com os fornecedores
- Identificando segurança da informação nos acordos com fornecedores
- Identificação da legislação aplicável e de requisitos contratuais
- Proteção e privacidade de informações de identificação pessoal

Questionário terceira rodada:

DELPHI - ETAPA 3: Segurança da Informação Aplicada no Modelo SECI:

Desenvolvimento de um Framework para Gestão do Conhecimento Seguro

Estágio 3 de respostas do método Delphi. Desta fase em diante, solicitamos que sejam marcadas as alternativas mais preponderantes no seu ponto de vista, com maior critério de análise. Cremos que essa será a última rodada da pesquisa com questionário. Eliminamos todos os controles com menos de 50% de votação em relação ao número total de especialistas, ou seja, menos de 10 votos. Controles que já tiveram 80% de congruência também foram retirados desta etapa de pesquisa. Reiteramos que desta fase em diante, sejam marcadas as alternativas com mais critério. Ainda pedimos que seja assinalada no mínimo 1 alternativa por etapa. Para facilitar sua escolha e contexto nas próximas etapas do Delphi, criamos um documento com o detalhamento de cada objeto da ISO27001 no contexto da pesquisa. Podes consulta-lo neste link se necessário: https://docs.google.com/document/d/1IAzxeWateQbDyIuRDAEruwNHTv-ZaATTf2_4KIRcfj8/edit?usp=sharingApós terminarmos a compilação dos resultados vamos enviar mais o framework pronto para obter o OK de todos especialistas.

Ficamos à disposição

Mateus Buogo

E-mail: mbuogors@gmail.com

Descritivos

Nesta sessão, estão descritos de forma breve os processos do SECI e também uma descrição breve de cada um dos 20 controles da ISO27001.

Processo SECI de criação e compartilhamento do conhecimento proposto por Nonaka e Takeuchi (2008).

(S)ocialização do Conhecimento - Onde o indivíduo compartilha o seu conhecimento com outro indivíduo através de experiências diretas. Nesta fase o conhecimento tácito de um indivíduo é compartilhada com o outro, que irá criar um novo conhecimento também tácito. As experiências pessoais que ocorrem em relação mestre e aprendiz, observação das atividades, ou mesmo aquela “conversinha do cafezinho” são exemplos de socialização.

(E)xternalização do Conhecimento - Após compartilhar o conhecimento, o indivíduo articula esse conhecimento cocriado para um grupo de pessoas. O conhecimento tácito criado pelos os indivíduos, agora é transformado em explícito para um grupo maior de pessoas. Um ótimo exemplo é a documentação do conhecimento, onde um individuo externaliza o seu conhecimento podendo disponibilizara-lo a outros indivíduos.

(C)ombinação do Conhecimento - Sistematização do conhecimento, ocorre do grupo para toda organização. O conhecimento que já está explicito é compartilhado e criado também de forma explicita para um grupo maior de pessoas. A combinação pode ser caracterizada também como uma integração de novos conhecimentos explícitos, e ocorre na manipulação de dados por indivíduos como, por exemplo, em reuniões.

(I)nternalização do Conhecimento - Cada indivíduo em particular recebe esse conhecimento e efetua a internalização dele, ele aprende o novo conhecimento transformando-o em tácito novamente. A internalização refere-se à incorporação do conhecimento explícito em conhecimento tácito no sentido da organização para indivíduo.

Especialista

1.Você é um especialista:

Marcar apenas uma.

- Gestão do Conhecimento
- Segurança da Informação

SECI – Socialização do Conhecimento

Socialização é criar e compartilhar conhecimento tácito, a partir de experiência direta de indivíduo para indivíduo. Na prática, ela pode ocorrer através de atividades interativas entre os indivíduos no local de trabalho como brainstorms e reuniões.

2. Assinale as opções que você considera que são as mais importantes para a fase de SOCIALIZAÇÃO. Pode ser mais de uma. Marque todas que se aplicam.

- Responsabilidades e papéis pela segurança da informação
- Classificação da informação

SECI – Externalização do Conhecimento

Externalização está relacionado com articular o conhecimento através do diálogo e da reflexão de um de indivíduo para um grupo. Nesta fase o conhecimento é compartilhado com um grupo de pessoas utilizando técnicas que permitam esse compartilhamento como reuniões, conferências, entre outras.

3.Assinale as opções que você considera que são as mais importantes para fase de EXTERNALIZAÇÃO. Pode ser mais de uma.

- Políticas para segurança da informação
- Responsabilidades e papéis pela segurança da informação

SECI – Combinação do Conhecimento

Combinação é sistematizar e aplicar o conhecimento e a informação, de grupo para organização. Seguindo o fluxo do compartilhamento, o conhecimento que foi criado na fase da Externalização, é difundido para um grupo maior ainda, toda a organização utilizando-

se de várias técnicas e tecnologias para isso, podendo ser murais espalhadas na empresa, fóruns digitais entre outras.

4.Assinale as opções que você considera que são as mais importantes para fase de COMBINAÇÃO. Pode ser mais de uma.

- Responsabilidades e papéis pela segurança da informação
- Classificação da informação
- Rótulos e tratamento da informação

SECI – Internalização do Conhecimento

Internalização é aprender e adquirir novo conhecimento, de organização para indivíduo. Aqui as organizações passariam a vivenciar o resultado prático do novo conhecimento; ou seja, desenvolveriam um conhecimento operacional. Nesta fase as pessoas absorvem todo o conhecimento, internalizando-o e colocando em prática em seu dia-a-dia.

5.Assinale as opções que você considera que são as mais importantes para fase de INTERNALIZAÇÃO. Pode ser mais de uma.

- Segregação de funções
- Conscientização, educação e treinamento em segurança da informação

Classificação da informação