ISSN: 2237-826X
ARTIGO | PAPER

Gestão do conhecimento e segurança da informação

Knowledge management and information security

Mateus Buogo [1], Ana Cristina Fachinelli [2] e Cíntia Paese Giacomello [3]

[1] *Universidade de Caxias do Sul, Caxias do Sul, RS, Brasil. ORCID: https://orcid.org/0000-0003-1603-1509*

[2] *Universidade de Caxias do Sul, Caxias do Sul, RS, Brasil. ORCID: https://orcid.org/0000-0003-4136-6933*

[3] *Universidade de Caxias do Sul, Caxias do Sul, RS, Brasil. ORCID: https://orcid.org/0000-0003-3471-6931*

Autor para correspondência/*Mail to:* Ana Cristina Fachinelli, acfachin@ucs.br

Resumo

Introdução: A Gestão do Conhecimento é um desafio para as empresas na Sociedade da Informação. Metodologias como a de Nonaka e Takeuchi vêm ao encontro desse desafio para sistematizar e organizar a criação de conhecimento em todos os níveis das empresas. O conhecimento é considerado um ativo intangível e que pode ser protegido para garantir a manutenção da cadeia de valor das Organizações. Neste contexto, a Segurança da Informação visa proteger informações acessíveis no âmbito organizacional. Uma estrutura de Gerenciamento de Conhecimento Seguro é necessária para obter controles relevantes de segurança na Gestão de Conhecimento.
Metodologia: apresenta caráter qualitativo, com o uso da metodologia Delphi para a construção de uma estrutura de Gerenciamento do Conhecimento Seguro.
Resultados: os pontos de congruência entre Gerenciamento de Conhecimento e Segurança da Informação ficaram evidentes na pesquisa. Na fase de socialização, evidenciam-se dois controles com mais de 80% de congruência. Na fase de externalização, os dois pontos ficaram acima de 70%. Não há uma fase de combinação combinada, resultado de 60% de congruência em quatro controles e fase de internalização, registro de unanimidade na escola de controle, tendo um ponto com 100% de congruência.
Conclusão: os profissionais que adotaram a técnica Delphi conseguiram encontrar pontos de congruência entre os assuntos de pesquisa temática, subsidiando uma retórica da compatibilidade entre gerenciamento de conhecimento e Segurança da Informação. Dessa forma, destaca-se a necessidade de cocriação de conhecimento sob uma ótica de um *framework* que considere Segurança de Informação.

Palavras-chave: Gestão do Conhecimento; Segurança da Informação; Conhecimento.

Abstract

Introduction: *Knowledge management is a challenge for companies in the information society. Methodologies such as Nonaka and Takeuchi's meet this challenge to systematize and organize knowledge creation at all levels of companies. Knowledge is considered an intangible asset and can be protected to ensure the maintenance of the value chain of organizations. In that context, information security aims to protect information that is accessible at the organizational level. A secure knowledge management framework is required to achieve relevant knowledge management security control.*
Method: *it is a qualitative research, using the Delphi methodology to construct a structure of Secure Knowledge Management.*
Results: *the points of congruence between Knowledge Management and Information Security were evident in the research. In the socialization phase, two controls with more than 80% congruence were evidenced. In the outsourcing phase, the two points were above 70%. There is no combined phase, a result of 60% congruence in four controls and internalization phase, unanimity record in the control school, having a point with 100% congruence.*
Conclusions: *the professionals who adopted the Delphi technique were able to find points of congruence between thematic research subjects, supporting rhetoric of the compatibility between knowledge management and information security. Thus, we highlight the need for knowledge co-creation from the perspective of a framework that has information security.*

Keywords: *Knowledge Management; Information security; Knowledge.*

INTRODUÇÃO

O ativo mais importante das Organizações atualmente é o conhecimento. Menezes (2006) afirma que o conhecimento é o principal fator de produção do século XXI, evidenciando sua preponderância para as Organizações. Ativos como o conhecimento são considerados intangíveis e as Organizações criam valor sustentável por meio da alavancagem dos mesmos (Kaplan & Norton, 2004). O conhecimento, neste contexto, torna-se fator estratégico para o desenvolvimento das empresas. Kaplan e Norton (2004) advogam que os ativos intangíveis representam 75% do valor das Organizações.

A sociedade do século XXI é conhecida como sociedade pós-capitalista ou Sociedade do Conhecimento, pois o conhecimento é o recurso econômico mais valioso da sociedade (Drucker, 2000). Sendo assim, o conhecimento transforma-se em um produto 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.

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 é primordial para manutenção dos

negócios das Organizações, pois o conhecimento é fator chave nas tomadas de decisão e deve ser gerenciado. O conhecimento empregado nas decisões que definem as ações da empresa são objeto de gestão especializada: a Gestão da Informação e do Conhecimento (Machado, 2011).

A informação é um ativo da mesma forma importante para as empresas. A sua importância vem aumentando de forma exponencial. Freitas e Kladis (1995) advogam que a importância da informação dentro das Organizações aumenta com o crescimento da sociedade e das Organizações. 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, 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 Segurança da Informação tem como objetivo a salvaguarda das informações 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.

O objetivo desta pesquisa foi encontrar a correlação e os pontos de congruência entre Gestão do Conhecimento e Segurança da Informação, de forma que fosse possível criar um *framework* para aplicar a Gestão do Conhecimento de forma segura, levando em consideração as boas práticas de implementação de segurança descritas em normas conhecidas mundialmente, adaptando-as às metodologias de Gestão do Conhecimento.

Foi conduzida uma pesquisa de metodologia Delphi com 10 profissionais especialistas em Gestão do Conhecimento e Segurança da Informação, a fim de definir um modelo de *framework* aceito por mais de 80% dos entrevistados, com o objetivo de criar um processo seguro de Gestão do Conhecimento.

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 a perspectiva normativa da Segurança da Informação foram adotadas para delinear a base teórica, a qual orientou a pesquisa e a construção do *framework* sobre a temática.

Gestão do conhecimento

Na era da Nova Economia, o conhecimento é a matéria-prima para sustentação empresarial. A vantagem competitiva não é potencializada por fatores tradicionais como localização geográfica e mão de obra barata, sendo eles derrubados pela importância estratégica atribuída ao conhecimento (Terra, 2000). Diante desse ambiente desenvolvido nas empresas, o autor Drucker (1999) advoga que, no século XXI, os ativos resultantes do conhecimento são os que possuem maior valor agregado.

Nonaka e Takeuchi (2008) enfatizam que o indivíduo é o "criador" do conhecimento e a organização é o "amplificador", portanto, a sincronia entre empresa e funcionário é preponderante para a criação de conhecimento no ambiente corporativo. A empresa deve investir em metodologias para criar e reter conhecimento, junto a uma cultura organizacional apropriada para tal objetivo.

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. Drucker (1999) explana que o maior desafio dos gerentes dos países desenvolvidos é aumentar a produtividade dos trabalhadores do conhecimento e da área de serviços.

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) advoga 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 e a mensuração de resultados, as alianças estratégicas e o redesenho de processos.

O conhecimento é formado por dois componentes. Podemos 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).

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.

A complexidade do ambiente corporativo faz com que a Gestão do Conhecimento adentre nesse sistema e se torne paradoxalmente complexa. Os autores enfatizam que o conhecimento é inerentemente paradoxal, pois é formado por opostos, tácito e explícito. Os sucessos nos ambientes complexos das empresas necessitam abordar não apenas um conjunto de opostos, mas também uma completa multidão de opostos ao mesmo tempo.

A empresa consegue criar conhecimento quando há sintonia no processo de conversão dos componentes, tácito e explícito. Machado (2011) defende que a criação de conhecimento ocorre principalmente pela interação dos dois tipos de conhecimento, o tácito e o explícito, nos processos de externalização e internalização quando o conhecimento de um indivíduo consegue ser expresso e é internalizado por outro.

A Gestão do Conhecimento tem como uma de suas características a complexidade em sua implementação. Para que tenha efetividade, vários processos precisam ser implementados e paradigmas repensados. Dalkir (2005) afirma que a Gestão do Conhecimento deve possuir uma estrutura conceitual para que consiga alcançar os benefícios esperados com sua implementação.

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) pondera que ela 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, deve-se ponderar a compatibilidade com o ambiente que irão permear de acordo com as necessidades das empresas, para melhor escolha de modelo.

Posteriormente, Evans, Dalkir, e Bidian (2014) fornecem 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.

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, Karim, Dahlan, & Mohamad Ali, 2017). Fatores subjacentes às condições capacitadoras apontadas por (Nonaka & Takeuchi, 2008), tais como 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 (2019). O modelo SECI (Nonaka & Takeuchi, 2008) é a estrutura conceitual mais conhecida para a compreensão dos processos de geração de conhecimento nas Organizações (Farnese, Barbieri, Chirumbolo, & Patriotta, 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 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).

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.

De acordo com os autores, 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.

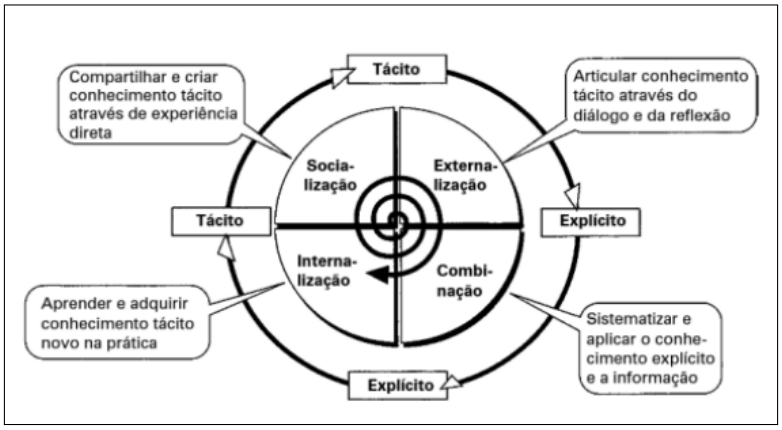

Figura 1. Ciclo de criação do conhecimento
Fonte: Nonaka e Takeuchi (2008, p. 34).

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 (2008):

> 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 sobre para os níveis ontológicos Nonaka e Takeuchi (2008, p. 98).

A diferenciação entre conhecimento tácito e explícito segue quatro padrões de criação. Nonaka e Takeuchi (2008) as definem como: Tácito para Tácito, Explícito para Explícito, Tácito para Explícito e Explícito para Tácito. Os autores afirmam que, em uma empresa criadora de conheci-mento, 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 ambi-ente. 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 as-sim, 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).

Segurança da Informação

A importância da informação vem aumentando de forma exponencial a cada instante dentro das Organizações. Freitas e Kladis (1995) advogam que sua importância aumenta com o crescimento da sociedade e das Organizações. A informação é um recurso fundamental em todos os níveis organizacionais. Quando usada como recurso estratégico, ela torna-se fundamental para a toma-da de decisões. Brito, Antonialli, e Santos (1997) explanam que a informação é um recurso estratégico das Organizações, gerando com elas as condições necessárias para alcançar os objetivos e cumprir a missão corporativa, subsidiando elementos básicos para melhoria da competitividade.

A informação é importante não somente no meio corporativo, mas também para a sociedade. Empresas com uma quantidade expressiva de informações tornam-se um diferencial, pois a in-formação quando bem interpretada agrega valor. Conforme Silva e Tomaél (2007):

> É evidente, na atualidade, que nada poderia funcionar sem uma quantidade significativa de informação como elemento que impulsiona os fenômenos sociais e que é por eles impulsionada. Pessoas e organizações – públicas ou privadas – dependem da informação em seus processos decisórios (Silva & Tomaél, 2007, p. 375).

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 (2001), risco é a probabilidade de uma ameaça explorar vulnerabilidades para causar perdas ou danos a um ativo ou grupo de ativos da Organização.

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. A definição de Segurança da informação de acordo com Dias (2004) perpassa por definições como sendo a proteção de informações, 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 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, 2013).

Sales e Almeida (2007) defendem que o conhecimento não existe se não houver uma fonte, uma origem de informação que forneça subsídios para sua construção. Durante todo o processo histórico do desenvolvimento do conhecimento, o homem dependeu das fontes de informação que se transformaram e continuam se transformando até hoje. De forma indireta, observa-se que a segurança da informação também possui relação com a Gestão do Conhecimento, garantindo a proteção dos insumos necessários para sua construção.

Assim como a Gestão do Conhecimento possui metodologias para sua implementação, a Segurança da Informação possuiu como normativa mais desenvolvida a ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013). Ela auxilia na construção de um SGSI (Sistema de Gestão de Segurança da Informação), levando em consideração temáticas como gestão de riscos e mais 114 controles específicos em sua versão de 2013, que garantem a implementação desse sistema.

Melo (2008) explana que o risco é considerado um evento incerto ou de data incerta que independe da vontade dos envolvidos, sendo um elemento de incerteza que pode afetar a atividade. Oliveira (2001) afirma que risco é a probabilidade de uma ameaça explorar vulnerabilidades do ativo para causar perdas ou danos. A ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 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.

MÉTODO DE 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, adotou-se o método Delphi, devido à sua poderosa técnica de investigação (Facione, 1990), permitindo 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[...]".

Para a realização desta pesquisa, foram envolvidos 10 especialistas nos assuntos de temática deste artigo, sendo cinco especialistas de Segurança da Informação e cinco especialistas em Gestão do Conhecimento. Todos os envolvidos das áreas específicas tinham capacidade analítica para compreender os controles e as fases da espiral do conhecimento. Uma breve descrição de cada etapa também foi realizada nas fases para melhor entendimento. 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 (**?**).

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 congruência entre as respostas.

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. Foram realizadas ao todo 3 rodadas com respostas aos questionários para chegar ao resultado da pesquisa proposta. Os respondentes

foram convidados a associar 19 controles da ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013) aos quatro modos de conversão do conhecimento de acordo com o modelo SECI de Nonaka e Takeuchi (2008). Para a seleção dos 19 controles foi realizada uma análise semântica de seus enunciados em relação aos conceitos expressos na espiral do conhecimento.

A ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013) dispões de 114 controles de segurança, os quais abrangem vários pontos. As cláusulas de controle estão divididas em áreas distintas, desde abordagens técnicas, até abordagens gerenciais. Para o estudo de caso e a criação do questionário da metodologia Delphi, foram selecionados controles que implicam na manipulação de informação e cultura organizacional, bem como o controle de usuários em sistemas e acessos. Os 19 controles são:

Controle	Descrição
Controle 5.1.1. Políticas para Segurança da Informação	A Política de Segurança da Informação estabelece as diretrizes corporativas e regras de segurança que devem ser adotadas por todos nos processos diários da organização
Controle 6.1.1. Responsabilidades e papéis pela segurança interna	Este controle estabelece as responsabilidades que os indivíduos possuem perante a segurança corporativa.
Controle 7.2.2. Conscientização, educação e treinamento em segurança da informação	A recorrência de capacitação das pessoas é necessária para manter a cultura de segurança corporativa. Este controle foca em documentar rotinas e processos que garantam a educação corporativa no tema.
Controle 8.2.1. Classificação da Informação:	Classificação informação permite que seja possível identificar quando a mesma é confidencial ou pública e dessa forma aplicar controles de segurança específicos.
Controle 8.2.2. Rótulos e tratamento da informação	Controle complementar ao 8.2.1, onde são criados os rótulos de classificação.
Controle 9.2.4. Gerenciamento da informação de autenticação secreta de usuários:	O controle se senhas garante que somente pessoas autorizadas tenham acesso à informações não-públicas ou confidenciais.
Controle 9.2.5. Análise crítica dos direitos de acesso de usuário	Garante que cada pessoa possui somente o acesso que lhe é autorizado. Cada acesso é questionado para verificar se realmente ele é necessário.
Controle 9.2.6. Retirada ou ajuste dos direitos de acesso	Complementar ao controle 9.2.5, documenta o processo de retirar de acessos dos indivíduos.
Controle 9.4.1. Restrição de acesso à informação:	Documenta o processo que permite a restrição de acesso às informações de acordo com o direito de acesso de cada um. Pode-se utilizar perfis de acesso para padronização e análise das restrições.
Controle 11.1.3. Segurança em escritórios, salas e instalações	Documenta as boas práticas pessoais no que tange segurança nos ambientes corporativos.
Controle 11.1.5. Trabalhando em áreas seguras	Complementar ao controle 11.1.3, descreve como deve ser realizado o trabalho em áreas seguras, onde circulam informações sensíveis.
Controle 11.2.9. Política de mesa limpa e tela limpa	Boas práticas de organização pessoal no ambiente de trabalho, em específico no local de trabalho de cada indivíduo.
Controle 12.1.1. Documentos dos procedimentos de operação	Documentação dos processos das rotinas diárias da empresa. Tem como objetivo garantir que os processos diários estão em compliance com as políticas de segurança.
Controle 12.3.1. Cópias de segurança das informações	Controle que determina realizar backup das informações para que não sejam perdidas ou corrompidas.
Controle 13.2.1. Políticas e procedimentos para transferência de informação	Documenta o processo de como as informações devem ser transitadas entre sistemas, mídias e portais.
Controle 13.2.4. Acordos de confidencialidade e não divulgação	Tem como objetivo oficializar através de um documento assinado pelas partes de que haverá confidencialidade das informações acessadas, podendo ter sanções administrativas.
Controle 15.1.1. Política de segurança da informação no relacionamento com fornecedores	O foco deste controle é estabelecer as políticas de troca de informações com terceiros, a fim de garantir a confidencialidade, integridade e disponibilidade das mesmas.
Controle 18.1.2.Direitos de propriedade intelectual	Controle que foca no direito do uso da informação. Proteção do capital intelectual da empresa
Controle de Análise de Riscos	Processo em que os riscos são avaliados de forma que possam ser mitigados, minimizando a exposição dos ativos às ameaças, protegendo dessa forma a informação e os processos. Focado na continuidade de negócio da empresa.

Quadro 1. Descrição dos controles ISO
Fonte: Elaborado pelos autores a partir da Norma ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013).

ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS

A primeira rodada de perguntas foi realizada elencando 19 controles da ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013), nas quatro fases da espiral de conhecimento proposta por Nonaka e Takeuchi (2008).

Foi orientado para que os participantes assinalassem um ou mais controles que identificassem como pertinentes em cada etapa da espiral. Dessa forma, pôde-se obter o primeiro resultado, encontrando os primeiros pontos de congruência.

Na etapa de Socialização da espiral do conhecimento, na primeira rodada, foi identificado que controles como Política de Segurança, Conscientização e Direito de Propriedade tiveram maiores pontos de congruência entre as respostas dos entrevistados. Na etapa de Externalização, o controle de Política de Segurança manteve-se como um dos principais pontos, porém houve maior diluição de respostas nos outros 19 controles.

O cenário manteve-se sem alterações quando foram abordadas as etapas de Combinação e Externalização, nas quais o controle de Política de Segurança obteve maior número de congruência das respostas, sendo as outras respostas bem diluídas nos outros controles.

Para o desenvolvimento do segundo questionário, foram desconsideradas respostas que tinham apenas um ou dois pontos congruentes, criando assim um novo modelo para ser submetido aos entrevistados. O número de controle por etapa ficou em: Socialização, 10 controles; Externalização, 11 controles; Combinação, 11 controles; Internalização, 11 controles.

Na segunda fase de respostas, obteve-se predominância dos controles de Política de Segurança, Conscientização, Classificação de Informação e Trabalho em Locais Seguros. Na etapa de Socialização, a predominância que era da Política de Segurança foi alterada para Conscientização, na qual houve maiores pontos congruentes nas respostas. Na fase de Externalização, manteve-se a predominância da Política de Segurança. Na etapa de Combinação, controles de Conscientização obtiveram maior congruência. Já na fase de Internalização, o controle de Trabalho em Local Seguro foi o mais apontado como importante para garantir a segurança do conhecimento.

O terceiro questionário foi elaborado de forma mais estruturada e assertiva. Foram desconsiderados todos os controles que tiveram apenas 1, 2, 3, 4 ou 5 pontos de congruência. O número de controles por etapa ficou em: Socialização, 2 controles; Externalização, 3 controles; Combinação, 4 controles; Internalização, 2 controles. A análise do terceiro questionário foi decisiva para interromper o Delphi e concluir as coletas de informações para elaboração do *framework*.

Foram considerados, para elaboração do *framework*, todos os controles que obtiveram 60%, 70%, 80%, 90% ou 100%. Inicialmente a proposta foi considerar apenas pontos com 80% de congruência, porém as rodadas de respostas em cada fase revelaram que alguns controles chegaram em uma aceitação de 60% e 70% por parte dos entrevistados e uma nova rodada de respostas não alteraria o resultado desta pesquisa. O Quadro 2 demonstra o resultado de cada controle relacionando com cada etapa da espiral do conhecimento.

Controle	Socialização	Externalização	Combinação	Internacionalização
7.2.2. Conscientização, educação e treinamento em segurança da informação	80%		60%	
13.2.1. Políticas e procedimentos para transferência de informação	90%			
5.1.1. Políticas para Segurança da Informação			70%	
6.1.1. Responsabilidades e papéis pela segurança interna	%	80%	%	
8.2.1. Classificação da Informação			60%	
8.2.2. Rótulos e tratamento da informação			60%	
12.3.1. Cópias de segurança das informações			60%	
9.2.5. Análise crítica dos direitos de acesso de usuário				100%

Quadro 2. Resultado do controle da espirado do conhecimento.
Fonte: Elaborado pelos autores (2019).

A espiral do conhecimento demonstra que muitos pontos devem ser levados em consideração em relação à segurança, à criação e ao compartilhamento do conhecimento. A análise dos dados coletados por meio da pesquisa Delphi sustenta a importância e a relevância da temática de Gestão do Conhecimento Seguro.

Salienta-se que, nas etapas de Socialização e Combinação, o controle 7.2.2 foi referenciado, evidenciando que a capacitação das pessoas sobre Segurança da Informação é fator preponderante para obter-se segurança nesses processos de criação e compartilhamento de conhecimento.

A manipulação das informações também se torna importante quando é evidenciado o controle 13.2.1. Em consonância com o controle 5.1.1, pode-se afirmar que as políticas e procedimento são importantes para garantir a segurança. Por meio das políticas, são definidas diretrizes de como cada indivíduo deve se comportar e qual postura deve manter dentro do processo de criação do conhecimento.

A fase de Combinação mostrou-se bem equilibrada entre os controles mapeados durante as fases anteriores do Delphi. Esse equilíbrio mostrou que os quatro controles são importantes para essa etapa, mesmo sem chegar aos 80% de congruência proposto no início das atividades. Optou-se, dessa forma, em manter os quatro controles na construção do *framework*.

Para a fase de Internalização, obteve-se 100% de congruência no controle 9.2.5. Nesta etapa em que o indivíduo internaliza o conhecimento, a análise de direitos de acesso faz com que o conhecimento esteja protegido de acordo com as políticas empregadas e, nesta fase, torna-se importante que o conhecimento seja internalizado no indivíduo de acordo com o acesso às informações que ele pode obter.

Figura 2. Gestão do conhecimento e segurança da informação
Fonte: Elaborado pelos autores (2019).

A metodologia Delphi contribuiu para que o trabalho cumprisse os objetivos propostos. O *framework* de Gestão do Conhecimento Seguro, conforme a Figura 2, foi desenhado de acordo com os resultados obtidos em todas as etapas da pesquisa, evidenciando controles reconhecidos mundialmente, realizando a correlação entre *frameworks* que existem, tanto para metodologia de Gestão do Conhecimento como para Segurança da Informação, criando assim uma proposta de um novo *framework* para Gestão do Conhecimento Seguro.

CONSIDERAÇÕES FINAIS

A Gestão do Conhecimento nos ambientes corporativos é de suma importância para sustentação da cadeia de valor das empresas. Ela emprega metodologias para que haja a criação e o compartilhamento de conhecimento entre os indivíduos em um ecossistema propício para essa construção. Em contrapartida, há o conceito de Segurança da Informação, que visa proteger a informação, orientando os processos para que haja a menor exposição possível. A construção desse artigo evidencia a importância que a Segurança da Informação possui diante da criação do conhecimento nas Organizações, destacando a necessidade de uma Gestão do Conhecimento Segura.

Em relação à pesquisa Delphi, obteve-se êxito para auxiliar a construção de um *framework* de Gestão do Conhecimento Seguro. A participação de profissionais especialistas nas áreas desta pesquisa permitiu identificar as congruências existentes entre as metodologias de Gestão do Conhecimento e Segurança da Informação.

Identificou-se nesta pesquisa que os controles com maior pontuação foram os que envolvem políticas e processos, salientando a importância da capacitação dos indivíduos para que haja compartilhamento e criação de conhecimento seguro. Treinamentos e conscientização sobre a temática são necessários a todos os que participam desse processo, a fim de orientar cada um sobre os conceitos de Segurança da Informação nos seus processos diários.

Portanto, conclui-se que, no cenário corrente, há a necessidade da utilização de boas práticas de Segurança da Informação durante todo processo de criação e compartilhamento do conhecimento nas etapas da espiral do conhecimento. Pondera-se que o *framework* resultante dessa pesquisa foi realizado bom base nos controles da

ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2013) e na metodologia de espiral do conhecimento proposta por Nonaka e Takeuchi (2008), não podendo ser aplicado em outras metodologias de Gestão do Conhecimento sem que haja alterações ou adaptações na metodologia.

Novos estudos sobre a temática precisam ser desenvolvidos para aprimorar o assunto e obter resultados mais precisos. Um estudo de caso utilizando essa metodologia é necessário para comprovar sua eficácia e evoluir para uma metodologia consolidada de Gestão de Conhecimento Seguro.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. (2013). *Nbr iso/iec 27001: gestão de segurança da informação.* Rio de Janeiro: ABNT.

Brito, M. J., Antonialli, L. M., & Santos, A. C. (1997). Tecnologia da informação e processo produtivo de gestão em uma organização. cooperativa: um enfoque estratégico. *Revista de Administração Contemporânea*, *1*(3), 77–95.

Corrêa, F. (2019). Gestão do conhecimento holística: delineamento teórico conceitual. *Perspectivas em Ciência da Informação*, *24*(1), 122–146.

Dalkir, K. (2005). *Knowledge management in theory and practice.* Burlington, MA, EUA: Elsevier.

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

Dias, C. (2004). *Segurança e auditoria na tecnologia da informação.* Rio de Janeiro: Axcel.

Drucker, P. F. (1999). *Desafios gerenciais para o século xxi.* São Paulo: Pioneira.

Drucker, P. F. (2000). O advento da nova organização. In *Gestão do conhecimento.* Rio de Janeiro: Campus.

Evans, M., Dalkir, K., & Bidian, C. (2014). A holistic view of the knowledge life cycle: the knowledge management cycle (kmc) model. *Electronic Journal of Knowledge Management*, *12*(2), 85–97.

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

Farnese, M. L., Barbieri, B., Chirumbolo, A., & Patriotta, G. (2019). Managing knowledge in organizations: a nonaka's seci model operationalization. *Frontiers in Psychology*, *10*, 01–15. doi: doi.org/10.3389/fpsyg.2019.02730.

Freitas, H., & Kladis, C. M. (1995). Da informação è política informacional das organizações: um quadro conceitual. *Revista de Administração Pública*, *29*(3), 73–86.

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

Kaplan, R. S., & Norton, D. P. (2004). *Mapas estratégicos.* Rio de Janeiro: Campus.

Machado, C. P. (2011). *Gestão da informação e do conhecimento.* São Leopoldo, RS: Unisinos.

Marques, J. B. V., & Freitas, D. (2018). Método delphi: caracterização e potencialidades na pesquisa em educação. *Pro-Posições*, *29*(2), 389–415.

Melo, L. P. d. (2008). *Proposta de metodologia de gestão de risco em ambientes corporativos na área de ti* (Dissertação de mestrado). Universidade de Brasília (UnB), Brasília, Brasil.

Menezes, C. (2006). *Gestão da tecnologia da informação.* São Paulo: H. Mizuno.

Nonaka, I., & Takeuchi, H. (2008). *Gestão do conhecimento.* Porto Alegre: Bookman.

Oliveira, W. J. (2001). *Segurança da informação: técnicas e soluções.* Florianópolis, SC: Visual Books.

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

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

Razi, M. J. M., Karim, N. S. A., Dahlan, A. R. A., & Mohamad Ali, N. A. (2017). A holistic approach to measure organizational readiness for knowledge management. *Advanced Science Letters*, *23*(4), 2829–2832. doi: doi.org/10.1166/asl.2017.7693.

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

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

Terra, J. C. C. (2000). *Gestão do conhecimento: o grande desafio empresarial.* São Paulo: Negócio Editora.

Como citar este artigo (APA):
Buogo, M., Fachinelli, A. C. & Giacomello, C. P. (2019). Gestão do conhecimento e segurança da informação. *AtoZ: novas práticas em informação e conhecimento, 8*(2), 49 – 59. Recuperado de: http://dx.doi.org/10.5380/atoz.v8i2.69687