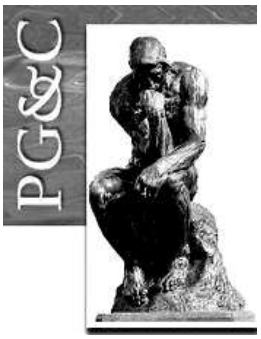

PRÁTICAS ORGANIZACIONAIS EM GESTÃO DO CONHECIMENTO QUE CONTRIBUEM COM A SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO NA UNIVERSIDADE FEDERAL DA PARAÍBA

Sueny Gomes Léda Araújo
Doutoranda em Ciência da Informação pela Universidade Federal da Paraíba, Brasil.
E-mail: suenyleda@gmail.com

Rafaela Romaniuc Bastista
Doutoranda em Ciência da Informação pela Universidade Federal da Paraíba, Brasil.
E-mail: rafaela.romaniuc@gmail.com

Wagner Junqueira de Araújo
Doutor em Ciência da Informação pela Universidade de Brasília, Brasil.
Professor da Universidade Federal da Paraíba, Brasil.
E-mail: wagnerjunqueira.araújo@gmail.com

Resumo
A relação da gestão do conhecimento com a segurança da informação apresenta-se como elemento norteador para uma eficiente gestão. Diante desse argumento, buscou-se com esta pesquisa analisar quais são as práticas organizacionais de gestão do conhecimento que promovem a segurança da informação, utilizadas pelos gestores da Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba, e como estas influenciam na percepção da segurança da informação. Esta pesquisa caracteriza-se como pesquisa descritiva, de abordagem qualitativa e, quanto ao método de investigação, estudo de caso. Como instrumento de coleta de dados foram utilizados questionário e observação participante. Os resultados possibilitaram perceber que as práticas de gestão do conhecimento como: mapeamento de processos, sistema de gestão de documentos, mentoria e comunidade de prática contribuem com a confidencialidade, integridade, disponibilidade e autenticidade da informação criada, manuseada, protegida e/ou disponibilizada pela Pró-Reitoria de Gestão de Pessoas. Contudo ficou evidente nas falas dos gestores que os processos não estão alinhados, apesar de existirem as práticas de GC estas são executadas sem os devidos cuidados para influenciarem a segurança da informação.

Palavras-chave: Gestão do conhecimento. Práticas organizacionais. Aprendizagem organizacional. Segurança da informação.

ORGANIZATIONAL PRACTICES IN KNOWLEDGE MANAGEMENT THAT CONTRIBUTE TO INFORMATION SECURITY: CASE STUDY AT THE FEDERAL UNIVERSITY OF PARAÍBA

Abstract
The connection between knowledge management and information security is a guiding force for efficient management. In view of this point of view, this research was conducted to analyze which organizational practices of knowledge management promote information security, used by the managers of the Dean of People Management of the Federal University of Paraíba, and how they have an impact on the perception of information security. This research is characterized as descriptive research, qualitative approach and, as for the research method, case study. As a data collection instrument, a questionnaire

and participative observation were used. The results made it realizes that knowledge management practices such as: process mapping, document management system, mentoring and community of practices contribute to the confidentiality, integrity, availability and authenticity of the information created, handled, protected and/or made available by the Pro-Rectory of People Management. However, it was evident from the managers' speeches that the processes are not in harmony, although there are GC practices, they are executed without the proper care to influence the security of the information.

Keywords: *Knowledge management. Organizational practices. Organizational learning. Information security.*

1 INTRODUÇÃO

A gestão do conhecimento (GC) tornou-se uma área essencial dentro de muitas organizações, seja pela característica dinâmica do conhecimento na colaboração em rede, seja pela aprendizagem organizacional que precisa de incentivos contínuos visando ao compartilhamento do conhecimento nas organizações. Para Choo (2003), conhecimento resulta dos relacionamentos, quase sempre estratégicos, que a organização mantém ao longo do tempo com seus clientes, fornecedores e parceiros, acelerando seu aprendizado e aumentando seu alcance. Portanto, conhecimento, relacionamentos e aprendizagem estão conectados entre si e há também a associação informação-conhecimento que Burke (2016) explicitou, tomando emprestada a metáfora de Claude Lévi-Strauss, ao afirmar que é válido pensar na informação como algo em seu estado natural e o conhecimento como algo já processado.

Com relação ao "compartilhamento", as organizações devem coletar constantemente as informações adequadas de ambientes internos e externos e convertê-las em conhecimento. Conhecimento esse que é considerado um ativo estratégico para a sobrevivência de organizações dinâmicas e inovadoras (ESLAMKHAH; SENO, 2019, tradução nossa). Para a proteção desse importante ativo, a gestão do conhecimento apresenta-se como suporte aos processos para uma eficiente segurança da informação.

Segurança da informação refere-se à defesa de informações contra acesso não autorizado, divulgação, uso, modificação, interrupção, inspeção e leitura (VON SOLMS; VAN NIEKERK, 2013, tradução nossa). Considerar que a proteção da informação seria feita apenas através de uma perspectiva tecnológica, culminaria numa abordagem incompleta de acordo com estudos realizados que demonstram a necessidade de uma visão ampla através de uma abordagem interdisciplinar, onde o fator principal, o humano, desempenha um papel fundamental (YUPANQUI; ORÉ, 2018, tradução nossa). Ainda nesse sentido, as tecnologias da informação e comunicação trouxeram muitas vantagens para as organizações, mas os processos de gestão de segurança da informação ainda são uma preocupação para as organizações que dependem de tais tecnologias.

Além da associação informação-conhecimento, há a associação conhecimento tácito-explícito existente nos contextos organizacionais. Para Nonaka e Takeuchi (2008), o conhecimento explícito pode ser expresso e rapidamente transmitido aos indivíduos, de maneira formal e sistemática. Por outro lado, o conhecimento tácito é altamente pessoal e difícil de formalizar, estando profundamente enraizado nas ações e experiência corporal do indivíduo, assim como nas ideias, valores ou emoções que ele incorpora. Com isso, observa-se que as associações em torno do conhecimento são relevantes, influenciam no processo de criação do conhecimento organizacional e essa criação precisa ser compreendida como um processo de aprendizagem e crescimento pessoal, uma vez que o conhecimento de cada indivíduo se torna parte da rede de conhecimento da organização.

Assim, percebe-se que, parte da aprendizagem organizacional consiste nesse constante movimento do conhecimento, como um vento que sopra por vezes tácito ou explícito, por vezes indivíduo ou organização. Assim, a aprendizagem envolve as interações indivíduo-indivíduo e indivíduo-grupo por meio de processos de internalização, externalização, socialização e combinação.

Para Eslamkhah e Seno (2019, tradução nossa), embora o estabelecimento, a difusão e a gestão do conhecimento tenham sido amplamente estudados, a questão da segurança do conhecimento tem recebido menos atenção na literatura. Assim, tanto a criação, a manutenção como a proteção do conhecimento organizacional precisam ser geridas, e as práticas de gestão do conhecimento podem auxiliar nesse sentido. Para Burke (2016), práticas são procedimentos formais de obtenção, classificação ou teste do conhecimento. Assim, práticas organizacionais existem em diversas formas, diretas e indiretas, tradicionais ou inovadoras. Descobrí-las, organizá-las e/ou melhorá-las faz-se necessário tanto em instituições privadas como públicas.

No contexto das instituições públicas, estão inseridas as universidades que de acordo com Fullwood, Rowley e Delbridge (2013, tradução nossa) existem poucas pesquisas empíricas especificamente sobre gestão do conhecimento em universidades. Entretanto, os achados das pesquisas de Ramjeawon e Rowley (2017, tradução nossa) demonstram evidências da importância da GC no apoio às universidades em relação a sua missão de ensino, pesquisa e transferência de conhecimento institucional. Apesar de ainda ratificarem que as pesquisas em GC nessas instituições se apresentam de forma limitada, sendo sua maioria realizadas em países onde o ensino superior está mais consolidado como Reino Unido, Índia e Malásia.

Diante desse contexto, na tentativa de contribuir com o preenchimento da lacuna de pesquisa identificada, esta pesquisa se propôs a responder o seguinte questionamento: como as práticas de gestão do conhecimento contribuem para segurança da informação na Pró-Reitoria de Gestão de Pessoas (Progep) da Universidade Federal da Paraíba (UFPB)?. A pesquisa teve como objetivo analisar quais as práticas de GC envolvendo segurança da informação são utilizadas pelos gestores Progep/UFPB.

O corpo deste artigo está organizado da seguinte forma: referencial teórico compreendendo a gestão do conhecimento para segurança da informação e práticas de gestão do conhecimento aplicadas ao setor público, descritos na seção dois. Os procedimentos metodológicos são apresentados na seção três, indicando como foi o desenvolvimento, análise dos dados, discussões e resultados. Na seção quatro são apresentadas as considerações sobre o trabalho.

2 A GESTÃO DO CONHECIMENTO COMO PROCESSO PARA SEGURANÇA DA INFORMAÇÃO EFICIENTE

A gestão do conhecimento, como área de estudo presente dentro da Ciência da Informação, é uma área estratégica para as organizações, pois está relacionada à aprendizagem organizacional. Nesse sentido, Araújo (2014), ao realizar o mapeamento do campo da Ciência da Informação, a partir da identificação das correntes teóricas e da sistematização dos diferentes conceitos de informação presentes na área, identificou a área Gestão da Informação e do Conhecimento, que tem como ponto de partida a informação como recurso e, ao considerar a evolução dessa área, indica que destacam-se estudos específicos, entre estes, os relacionados à gestão da segurança da informação.

O autor evidencia a segurança da informação como uma subárea de Gestão da Informação e do Conhecimento e indica que sua importância se deve exatamente por

perceber a informação como um recurso para uma organização, portanto um ativo que possui valor e deve ser protegido.

Com base nas necessidades organizacionais, ou do indivíduo, as pesquisas estruturam a segurança da informação como uma disciplina, que abrange ações que buscam garantir, conforme necessidades específicas, a preservação da informação com base em quatro propriedades: a) confidencialidade - garante que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação; b) integridade - consiste na fidedignidade de informações, indicando a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados; c) disponibilidade - garante que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido; e d) autenticidade - garantia da veracidade da fonte das informações (INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION, 2012, tradução nossa; SÊMOLA, 2014; TRIBUNAL DE CONTAS DA UNIÃO, 2012). Essas propriedades representam elementos essênciais à sobrevivência de qualquer organização, cuja interferência, direta ou indireta, em algum de seus processos, pode acarretar grandes prejuízos. Assim, ressalta-se a necessidade de uma gestão da segurança da informação que contemple, de forma eficiente, os diversos tipos de informações que são criadas, manuseadas, disponibilizadas e/ou protegidas pelas organizações.

Fontes (2012) esclarece que a segurança da informação não se restringe à tecnologia, mas consiste em um processo que deve considerar a informação nos ambientes tecnológico e convencional, ou seja, desde a informação no papel, bem como o conhecimento das pessoas, tácito ou explícito. Desse modo, observa-se que ações de segurança da informação devem contemplar três dimensões: Pessoas, Processos e Tecnologias.

Nas últimas décadas, diversas organizações têm se concentrado nas soluções baseadas em tecnologia para abordar a segurança da informação, como por exemplo: *anti-vírus, anti-malware, anti-spam, anti-phishing, anti-spywar*e, *firewall*, autenticação e sistemas de detecção de intrusão. Contudo esta abordagem é incompleta, como destaca Safa et al (2015, tradução nossa) os autores argumentam que essa abordagem não garante a seguridade do negócio no contexto da gestão da segurança da informação, indicando que a abordagem tecnológica, como equipamento de hardware e componentes lógicos computacionais, não é capaz de estabelecer a devida proteção da informação contra ameaças. Os autores evidenciam que falhas humanas devem ser consideradas e tratadas.

Doherty e Tajuddin (2018, tradução nossa) destacam que incidentes relacionados à segurança da informação como violações de confidencialidade, fraudes por computador e utilização indevida dos sistemas de informação são comumente relacionados com o comportamento dos funcionários, em vez de problemas puramente técnicos. Para Eslamkhah e Seno (2019, tradução nossa) a falta de conhecimento do corpo funcional é a principal causa de problemas na segurança da informação de uma organização. Hackers mal-intencionados que tentam obter informações, em muitos casos se apresentam como membros autorizados pela organização, utilizando-se do método da engenharia social para burlar os sistemas de segurança.

Safa, Von Solms e Furnell (2016, tradução nossa) e Amayah (2013, tradução nossa) esclarecem que para a garantia de um ambiente seguro para a informação, os aspectos humanos devem ser considerados além dos aspectos tecnológicos, para que possa haver uma efetiva gestão da segurança, cuja raiz das falhas dos usuários da informação estão, essencialmente, vinculados à falta de conscientização dos aspectos da segurança, como: ignorância, negligência, barreiras no compartilhamento do conhecimento em procedimentos de segurança, apatia, dano e resistência.

Percebe-se que a principal ameaça à segurança organizacional está enraizada nos funcionários que não possuem conhecimento adequado sobre as necessidades de segurança organizacional. O conhecimento dos usuários é um dos fatores mais importantes neste tipo de processo, pois quase 70% dos incidentes de segurança ocorrem devido à falta de conhecimento dos usuários.

Novas ameaças à segurança são criadas como resultado de rápidas mudanças nas tecnologias e em seu uso. Portanto, o gerenciamento da segurança da informação consiste em processos e procedimentos em que os funcionários pratiquem para manter a confidencialidade, disponibilidade, integridade e autenticidade. O gerenciamento deste tipo de conhecimento ajuda as organizações e fornece vantagem competitiva quando identifica seus ativos informacionais, seus especialistas e promove gerenciamento destes recursos.

Um exemplo clássico deste tipo de procedimento é quando um funcionário que exerce atividades cruciais sai de uma organização. Neste caso, deve-se explicitar seus conhecimentos e formas de executar suas atividades ao longo dos anos, como registro de sua experiência profissional.

Não basta gerir os recursos informacionais, faz-se necessário também gerir conhecimento no que tange à constante transformação da informação em conhecimento e vice-versa nas organizações. A importância se dá ao considerar que as organizações, como ambiente complexo, demandam um *continuum* informacional para apoiar suas estratégias, ações e construção do conhecimento; sendo uma tarefa difícil a separação informação-conhecimento, uma vez que um alimenta o outro, mas, a partir da gestão dos processos de informação e de conhecimento é possível adaptar-se às mudanças, promover aprendizagem constante, mobilizar o conhecimento e a experiência dos membros para gerar inovação e criatividade e focalizar o conhecimento em ações racionais e decisivas (VALENTIM, 2008).

Dessa forma, é possível observar que gerir conhecimento é uma tarefa complexa e essencialmente estratégica, e pode impactar direta ou indiretamente no desenvolvimento institucional e, quando se inclui neste cenário as instituições públicas, o impacto pode ser relacionado ao desenvolvimento econômico e social. A complexidade dá-se a partir do momento que gerir conhecimento envolve gerenciar a cultura e, consequentemente, a aprendizagem organizacional.

Tomando como premissa que o sucesso no longo prazo dos negócios não pode ser assegurado pelo domínio de recursos como capital, recursos naturais ou competências tecnológicas, Senge (2011) afirma que a competência fundamental para assegurar a continuidade e prosperidade das organizações no longo prazo é a capacidade de aprender. Entretanto, considera-se que as equipes, e não os indivíduos, são a unidade de aprendizagem fundamental nas organizações atuais. Com esse pressuposto, várias práticas de gestão do conhecimento podem existir como as explicitadas por Menezes *et al. (*2017): direcionamento de competências individuais em conhecimento organizacional, desenvolvimento da cultura de compartilhamento de boas práticas, ampliação redes de relacionamento, bem como dar visibilidade e valorizar ativos intelectuais.

Essas práticas quando aplicadas ao conhecimento organizacional em segurança da informação permitem a aprendizagem e manutenibilidade de práticas de segurança da informação como:

a) uma percepção clara da necessidade de proteção da informação institucional;
b) hábitos e crenças de proteção da informação;
c) criar e manter uma visão compartilhada de segurança da informação, onde prevaleceria o compromisso e o comprometimento dos indivíduos com os valores institucionais relacionados à segurança da informação;
d) aprendizagem em grupo;

e) percepção da realidade da segurança da informação considerando toda uma rede integrada de relacionamento, onde o elo mais fraco mostraria o nível de segurança da informação na instituição.

Com base nessa argumentação, é possível inferir que as práticas de gestão do conhecimento aplicadas aos processos de segurança da informação tornam-se essenciais e podem contribuir para uma efetiva proteção da informação e dos recursos informacionais em uma organização.

3 PRÁTICAS DE GESTÃO DO CONHECIMENTO NO SETOR PÚBLICO

Tal qual nas organizações privadas, a gestão do conhecimento na administração pública possibilita a superação de desafios em variados setores, como implantação de novas práticas de gestão, produtos e serviços em benefício do cidadão-usuário e da sociedade como um todo. Logo, na literatura sobre gestão pública contemporânea se reconhece que para administrar instituições públicas torna-se necessário o investimento tanto em tecnologias como também no capital humano.

Na década de 90, houve no Brasil investimentos expressivos em inovações tecnológicas na administração pública, possibilitando o início do processo de interação do cidadão com os diversos órgãos governamentais, como por exemplo: Planejamento Participativo, Orçamento Participativo, Comunidades virtuais e os Instrumentos de Consulta Constitucional.

Apesar disso, Ferreira (2007) e Azevedo (2002) enfatizam algumas dificuldades na administração pública no Brasil para que haja uma gestão do conhecimento efetiva, como: linhas rígidas de demarcação no fluxograma público que geram conhecimento estanque; dificuldade de compartilhamento voluntário entre os atores públicos; utilização do conhecimento como fonte de poder e para proteção do cargo; falta de reconhecimento daqueles que disseminam o conhecimento e assim dinamizam o fluxo informacional; e ausência de formas pecuniárias de recompensas e de incentivos.

Outro problema está na falta de continuidade dos planos e projetos devido às constantes trocas de atores de governo, onde as pessoas são remanejadas e levam consigo experiências e *expertise*, além da ausência de uma política de meritocracia, isto é, reconhecimento e recompensa originados de uma boa produtividade e resultados. Com isso, os autores indicam que não há estímulo à motivação do funcionário público.

Autores como Cong e Pandya (2003), defendem a ideia de que é necessário criar um modelo específico de gestão do conhecimento para as instituições públicas. As tentativas de implementar modelos do setor privado no setor público falharam e, para esses autores há três importantes empecilhos para o sucesso da GC no setor público, que são: tomar consciência do conceito de GC, do diretor ao pessoal da linha de frente que atende aos cidadãos; falta de consenso conceitual sobre: conhecimento, dados e informação, esta situação traz imprecisão e insucessos na implementação da GC; e a sincronia entre pessoas, processos e tecnologia, isso é fundamental para que haja a possibilidade de sucesso na implantação de GC.

Para Alvarenga Neto (2007), a implantação de uma política de GC atinge diretamente a cultura organizacional no que diz respeito ao sentimento de poder. Devido a isso, há necessidade de gestores que trabalhem dando forma ao conhecimento institucional, já que se trata de algo complexo que promove uma mudança cultural e, no contexto das instituições públicas, essa complexidade é ampliada.

Observa-se uma diversidade de práticas para a implementação da GC definidas como o conjunto de métodos e técnicas para apoiar os processos organizacionais de criação,

armazenamento e transferência do conhecimento. Enquanto as tecnologias de GC são especificamente os sistemas que suportam as práticas (CERCHIONE, ESPOSITO, SPADARO 2015, tradução nossa). Ribeiro e Izquierdo (2017) apresentam algumas delas para o setor público no Quadro 1:

Quadro 1 – Práticas de GC no setor público

PRÁTICAS	DEFINIÇÃO
Redes de pessoas	Identificação e montagem de redes de pessoas, trocas espontâneas de informações e conhecimentos entre os funcionários da organização.
Páginas amarelas	Montagem de páginas amarelas trata-se de um ambiente virtual onde as pessoas encontram outros colegas que possuem conhecimentos ou experiências que lhes interessam.
Comunidades de prática	Criação de uma rede de colaboração entre pessoas com objetivos comuns, como um problema ou uma meta, por um tempo determinado.
Compartilhamento de práticas relevantes	Divulgação de práticas relevantes trata-se de compartilhar as melhores formas de realizar determinadas tarefas, gerando assim mais agilidade na organização.
Lições aprendidas	Divulga os pontos positivos dos projetos da organização, os problemas enfrentados e suas soluções.
Brainstorming	Forma coletiva de gerar novas ideias para o aprimoramento ou criação de novos produtos.
Storytelling	Narrações de histórias para promover a motivação dos colaboradores.
Entrevistas de saída	Entrevistas realizadas com pessoas que estão saindo da organização no intuito de reter parte de seus conhecimentos.
Mapas de Conhecimento	Visão geral sobre as fontes de conhecimento dentro da organização para que haja maior eficiência nos processos.
Coaching	As pessoas mais experientes atuam como instrutores internos dos menos experientes, transmitindo assim o seu conhecimento.
Repositórios de conhecimento	São técnicas de armazenamento, recuperação do conhecimento, como também acessibilidade e qualidade do conhecimento a ser armazenado.

Fonte: Adaptado para Quadro de Ribeiro e Izquierdo (2017)

Por sua vez, Menezes (2017), apresenta técnicas, fruto de sua observação em três empresas, enfatizando o papel da cultura colaborativa absorvida, apresentadas no Quadro 2:

Quadro 2 – Práticas de GC no setor privado

PRÁTICA	DEFINIÇÃO
Oficinas de aprendizagem	Compreende o trabalho em equipe para, através da construção coletiva, solucionar problemas. Está ligada aos processos do conhecimento (organizar, compartilhar e criar).
Design Thinking	Está ligada ao pensamento crítico e criação que estimula o surgimento ou a melhoria de novos produtos, projetos ou serviços.
Mapeamento de processos	Metodologia que determina a melhoria dos processos ou a implantação de uma nova cultura, para aumentar o desempenho dos processos e a satisfação dos clientes.
Sistema de gestão de documentos	Sistema que organiza e controla os documentos, com isso os torna mais acessíveis.
Mapa mental	Diagrama estruturado para a gestão de informações, de conhecimento e de capital intelectual com a finalidade de tornar mais claro os problemas e suas soluções.
Coaching	Metodologia que objetiva o desenvolvimento de competências pessoal ou profissional, por meio de reuniões para o desenvolvimento de um

	funcionário.
Aprender trabalhando	Prática onde as pessoas aprendem com outras pessoas, no dia a dia.

Fonte: Adaptado para Quadro de Menezes (2017)

Com isso, é possível observar que as práticas de GC podem ser aplicadas tanto no setor público quanto privado, podendo coincidir como a técnica de *coaching* ou ser especificamente aplicada de acordo com a cultura da organização, se pública ou privada. Ademais, através dessas técnicas, de acordo com PACHECO *et al.* (2015), a gestão do conhecimento pode ter um papel importante no setor público para a promoção de mudanças necessárias, como eficiência, para melhores prestações de serviços à população, tonando-se necessário criar uma cultura administrativa onde a gestão do conhecimento possa contribuir com as transformações da sociedade. Tais técnicas e práticas promovidas pela GC podem ser utilizadas para promoção e disseminação das ações sobre gestão da segurança da informação.

Inseridas no contexto das instituições públicas, encontram-se as universidades que são ambientes intensivos em conhecimento que desempenham um papel central na criação de conhecimento através do desenvolvimento de pesquisas e na disseminação do conhecimento por meio de suas publicações. Estas, desempenham um importante papel na transferência de conhecimento, trabalhando diretamente com os cidadãos, com empresas e outras organizações para apoiar a inovação e empreendimentos sociais e culturais, além de apoiar o aprendizado através de seus programas de ensino, pesquisa e extensão.

Dessa forma, é razoável esperar que as universidades adotem uma abordagem proativa para o desenvolvimento de estratégias de gestão do conhecimento e que tenham um entendimento bem aperfeiçoado de como gerenciar e otimizar o valor de seus ativos de conhecimento (FULLWOOD; ROWLEY; DELBRIDGE, 2013, tradução nossa). Entretanto, de acordo com os achados das pesquisas desenvolvidas por Ramjeawon e Rowley (2017, tradução nossa), nenhuma das universidades pesquisadas naquela ocasião possuía uma estratégia de gestão do conhecimento. Além disso, foram identificadas mais barreiras do que facilitadores para a gestão do conhecimento. Pois as estruturas universitárias diferem invariavelmente da maioria das instituições públicas ou privadas.

A estrutura organizacional funcional das instituições de ensino superior pode ser uma barreira significativa ao compartilhamento de conhecimento. O que nos impele ao tema desta pesquisa, que parte do pressuposto de que a GC pode influenciar nas ações dos atores internos da área de gestão de pessoas da Universidade Federal da Paraíba em relação a sua percepção sobre os elementos de segurança da informação.

4 PROCEDIMENTOS METODOLÓGICOS

Esta pesquisa realizou um estudo sobre práticas de gestão do conhecimento que contribuem com a segurança da informação, a partir da percepção dos gestores da Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba- PROGEP/UFPB.

Quanto à sua tipologia, podemos considerá-la como estudo de caso. Em relação a sua natureza, caracteriza-se como pesquisa descritiva, uma vez que objetiva descrever a relação das práticas de gestão do conhecimento que contribuem com a segurança da informação na Progep. Para coleta de dados, foram utilizados questionário e observação participante.

O questionário foi composto por perguntas fechadas e abertas, abordando as práticas organizacionais de gestão do conhecimento que estão relacionadas aos princípios da segurança da informação. Nas questões não foi explicitado o nome das práticas de GC, mas a definição conforme Menezes *et al.* (2017). Assim, foi possível minimizar possíveis equívocos.

Quanto à sua estrutura, o questionário foi composto por onze questões, sendo seis objetivas e cinco subjetivas.

Por sua vez, a observação participante possibilitou vincular os fatos às suas representações e a desvendar as contradições entre as normas e regras e as práticas vividas cotidianamente pelo grupo observado. O fato de um dos pesquisadores pertencer ao quadro pessoal de servidores da PROGEP/UFPB contribuiu na escolha do referido instrumento de coleta de dados.

A coleta aconteceu no período entre 26 e 29 de dezembro de 2017. O universo foi composto por seis diretores, sendo três da Coordenação de Desenvolvimento de Pessoas – CDP/PROGEP e três da Coordenação de Processos de Gestão de Pessoas – CPGP/PROGEP. O estudo teve uma amostragem por conveniência e acessibilidade.

5 DESENVOLVIMENTO, ANÁLISE e RESULTADOS OBSERVADOS

Com base nos dados coletados por meio da observação participante e questionários aplicados aos diretores da Progep da UFPB, esta seção apresenta a análise realizada para alcançar o objetivo proposto e responder à questão da pesquisa.

Para preservar a identidade dos respondentes, as respostas foram representadas pela letra "G", seguindo a ordem de resposta de cada pergunta. As respostas subjetivas foram transcritas e organizadas em quadros.

As perguntas iniciais do questionário foram relacionadas à existência de mapeamento de processos na PROGEP. Os gestores ficaram divididos entre existir o mapeamento ou estar em fase de implantação. Quando questionados sobre como esse mapeamento pode contribuir para manter em segurança os processos criados ou que transitam na PROGEP, obtiveram-se as seguintes respostas, conforme demonstrado no Quadro 3:

Quadro 3 - Contribuição do mapeamento de processos para SI

GESTORES	RESPOSTAS
G1	O mapeamento pode contribuir para identificar gargalos nos fluxos processuais, extinguir rotas desnecessárias proporcionando maior fluidez, além de gerar maior transparência aos interessados.
G2	Esse mapeamento pode contribuir para a sensibilização e conscientização dos servidores acerca da segurança da informação alterando a cultura organizacional, dando importância à conservação de documentos e à manutenção do histórico funcional e institucional.
G3	O mapeamento contribui para que o cliente identifique os locais por onde irá transitar seu processo, da mesma forma que serve de ferramenta para que a instituição encaminhe o mesmo para o setor subsequente, evitando possíveis desvios e extravios.
G4	A utilização do mapeamento a longo tempo manterá a informação restrita aos setores responsáveis, evitando o vazamento de dados confidenciais ou sigilosos.

Fonte: Dados da Pesquisa (2017)

Com base no exposto, percebe-se que, para os gestores o mapeamento de processos, pode contribuir com a SI a partir da fala de G2 e G4. Corroborando essa ideia, observa-se que Menezes *et al.* (2017) e Sêmola (2014) evidenciam a relação GC com SI da seguinte forma: o primeiro relata que o mapeamento de processos está relacionado aos processos do

conhecimento de organizar, **proteger** e criar, enquanto o segundo coloca a segurança da informação como área do conhecimento dedicada à **proteção** de ativos de informação.

Quando questionados sobre a existência de um sistema de gestão de documentos na PROGEP, a maioria declarou que sim e apenas um relatou que está em fase de implantação. Com isso, podemos inferir, por meio da observação participante, que apesar do sistema ter sido implantado em toda PROGEP, o tempo necessário para cada setor se adequar e utilizar não foi uniforme, evidenciando as peculiaridades de cada ambiente. Observa-se que ao existir um sistema de informação com pouco uso, aumenta a probabilidade de quebra da propriedade de segurança denominada disponibilidade, pois uma vez que se não há uso continuo por todos os envolvidos, o sistema não é alimentado com os dados necessários para disponibilizar a informação aos usuários. Com relação ao modo como esse sistema pode contribuir com o acesso seguro às informações, obteve-se as seguintes declarações, conforme descrito no Quadro 4:

Quadro 4 - Contribuição do sistema de gestão de documentos para o acesso seguro à informação

GESTORES	RESPOSTAS
G1	O SIPAC possui diversas ferramentas de gestão de documentos, contudo, não estou familiarizado com todas, mas tão somente uma parte, como: cadastro e movimentação de processos, cadastro e movimentação de memorandos eletrônicos.
G2	O sistema que existe é o SIPAC. Entretanto, muitas de suas funcionalidades são subutilizadas, de modo que muitos processos e documentos circulam em papel. Quando o processo ou documento está no sistema, facilita o acesso remoto do usuário. Ele pode verificar a movimentação do processo, os documentos, decisões e despachos nele contidos. É possível verificar o status do processo sem precisar ir à PROGEP ou ligar, embora muitas pessoas prefiram o contato pessoal. Creio que o sistema possui um nível de segurança adequado. A insegurança pode surgir no momento em que o usuário compartilha sua senha ou faz uso de senhas fáceis. Outra questão gira em torno da classificação dos documentos e processos no sistema, pois nós servidores não possuímos um parâmetro claro e específico sobre como classificar os documentos por nós manuseados virtualmente.
G3	O sistema informatizado permite aos usuários visualizar a tramitação e os despachos de seus processos a distância, até mesmo de sua residência. Basta o interessado entrar no site da instituição e informar o número de seu processo que foi gerado no ato do cadastramento. Esse número é único, dando-lhes acesso apenas às informações referentes a sua solicitação. Entretanto, o sistema não vem sendo utilizado ou implantado adequadamente, causando dúvidas aos usuários e até mesmo aos servidores que o utilizam para a realização de suas atividades laborais.
G4	Por meio do Sistema Integrado de Gestão – SIG é possível acessar informação acerca dos servidores que são extraídas do banco de dados do Sistema Integrado de Administração de Recursos Humanos – SIAPE (folha de pagamento).

Fonte: Dados da Pesquisa (2017)

Com relação à contribuição do sistema de gestão de documentos para o acesso seguro à informação, percebe-se, a partir do Quadro 06, que os gestores remetem-se aos benefícios que o sistema pode trazer para instituição e ao usuário de forma individual, mas deixam

evidente a dificuldade no manuseio, o que pode ser decorrente de um processo de capacitação deficitário. Embora a própria área, por meio da Divisão de Educação e Capacitação Profissional – DECP, tenha oferecido vários cursos nesse sentido, verificou-se pouca aderência de gestores, o que pode ser decorrente de diferentes motivos, como excesso de atividades, falta de interesse, ou até mesmo falta de normativas que induzam os gestores a efetivamente fazerem os cursos.

Na fala do G2 destaca-se a relação da segurança da informação com o sistema de gestão documental [...] "A insegurança pode surgir no momento que o usuário compartilha sua senha ou faz uso de senhas fáceis" [...]. A ABNT/NBR ISO/IEC 27002 (2013), que aborda o código de prática para controles de segurança da informação, orienta que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade. Para tanto, faz-se necessário algumas orientações, tais como:

- Obrigar o uso individual de ID de usuário e senha para manter responsabilidades;
- Permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;
- Obrigar a escolha de senhas de qualidade;
- Obrigar os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;
- Forçar as mudanças de senha em intervalos regulares, conforme necessário;
- Manter um registro das senhas anteriores utilizadas e bloquear a reutilização;
- Não mostrar as senhas na tela quando forem digitadas;
- Armazenar os arquivos de senha separadamente dos dados do sistema da aplicação; e
- Armazenar e transmitir as senhas de forma protegida.

A declaração, demostra que os gestores não estão confiantes nas ações básicas de segurança que seus subordinados fazem ao acessarem um sistema. Nesse sentido, Mitnick e Simon (2003) aconselham que nenhuma instituição deve permitir qualquer compartilhamento de senhas, e estabeleça regras que proíbam os funcionários de compartilhar ou trocar as senhas confidenciais.

Outro ponto a ser destacado na fala do G2 relata [...] "outra questão gira em torno da classificação dos documentos e processos no sistema, pois nós servidores não possuímos um parâmetro claro e específico sobre como classificar os documentos" [...]. Nesse sentido, Araujo (2016) já alertava para a necessidade da UFPB em elaborar uma política de classificação da informação, uma vez que sua inexistência impossibilita a gestão da segurança da informação. A autora acrescentou, ainda, a indispensabilidade dos resultados dessa classificação serem inseridos no Sistema Integrado de Patrimônio, Administração e Contratos - SIPAC, de forma que sejam discriminados os tipos de processos, permitindo que a tramitação ocorra obedecendo à classificação do processo (sigiloso, pessoal ou ostensivo).

Ainda nesse contexto, de acordo com Menezes *et al.* (2017), o sistema de gestão de documentos é um sistema que organiza e controla os documentos, possibilitando o acesso de forma segura. Está relacionado aos processos do conhecimento – organizar e proteger. Quando os autores se referem ao acesso de forma segura, estão implícitas duas propriedades de segurança da informação: integridade - proteção contra modificação indevida e autenticidade - propriedade de que uma entidade é o que a mesma diz ser. (ISO/IEC 27000, 2014, p. 4, tradução nossa, *INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION,* ISACA, 2012, tradução nossa).

Outro ponto abordado compreendeu o questionamento sobre a existência da prática de GC, registro de lições aprendidas. Nesse sentido, percebeu-se que a totalidade dos respondentes apontou para a não existência dessa prática.

Entretanto, Batista (2012), afirma ser necessário que as instituições compartilhem as melhores práticas e lições aprendidas para que não haja uma constante necessidade de "reinventar a roda" e o retrabalho. Concernente a isso, Menezes *et al.* (2017) esclarecem que a prática de registro de lições aprendidas está relacionada à proteção e compartilhamento do conhecimento institucional. O que demostra que a GC e a SI são engrenagens que devem trabalhar em conjunto em uma instituição.

Quando foram abordados sobre a prática de aprender trabalhando na Progep, inicialmente, questionou-se ao gestor se havia vivenciado algum caso que envolvesse um incidente de segurança da informação e como ocorreu, conforme detalhado no Quadro 5:

Quadros 5 – Relato de incidentes de segurança da informação

GESTORES	RESPOSTAS
G1	Sim. Lembro de um caso no qual um banco de dados em excel foi invadido e alterado, mas não conseguiram identificar quem fez e qual sua motivação. Eram dados sensíveis para a gestão de pessoas da Instituição. Em outro caso, o servidor alterou informações funcionais que geraram ganhos financeiros indevidos, fato que resultou em processo administrativo disciplinar.
G2	Não vivenciei nenhum incidente. Contudo, nosso sistema de consulta (consultasrh) é um banco de dados de acesso vulnerável, no qual qualquer servidor com senha pode consultar dados funcionais de qualquer computador, sem precisar se identificar com senha SIAPE ou CPF.
G3	Sim. No período em que exerço minhas atividades ouvi falar de diversos casos de uso indevido do sistema, onde servidores com acesso ao SIAPE implantaram benefícios para si de forma arbitrária. No entanto, neste período, tomei conhecimento de apenas um caso em que um servidor (com acesso ao SIAPE) cadastrou para si, deliberadamente, um benefício ao qual não fazia jus. A descoberta foi feita por acaso, e com base na experiência de servidores mais antigos, a situação foi reportada aos gestores e a situação acarretou em um processo disciplinar administrativo.
G4	Algumas vezes a informação é antecipada ao usuário por intermédio de pessoas de outros setores não competentes. Sabendo dessa informação previamente, o usuário recorre a superiores hierárquicos que, por sua vez, interferem nos procedimentos e, muitas vezes, atrapalham o planejamento feito pelo setor responsável.

Fonte: Dados da Pesquisa (2017)

Com base no Quadro 07, percebeu-se que os incidentes foram ocasionados por ausência de senhas para acessar arquivos sensíveis, sistema desprotegido, má fé e vazamento de informação, o que afeta diretamente as propriedades de confidencialidade e integridade da informação.

Nesse contexto, questionou-se aos respondentes se a Superintendência de Tecnologia da Informação foi notificada dos incidentes que envolveram invasão ou fragilidade no sistema e a totalidades dos gestores relataram que não. Para Araujo (2014), a ausência de controles como: autenticação individual; ausência de cópias de segurança (realizadas e testadas regularmente); e de um processo disciplinar formal para a violação da segurança da informação, impossibilitam a recuperação da informação excluída ou modificada indevidamente e a identificação e punição do responsável.

Ainda nesse sentido, a ABNT NBR ISO/IEC 27002 (2013) orienta que, quando um incidente de segurança da informação for detectado, torna-se necessário que seja informado imediatamente ao ponto de contato de segurança da informação, uma vez que, pode não ser óbvio se o evento resultará em um inquérito administrativo, uma ação judicial ou simplesmente registrado pelo setor de segurança.

Retomando a prática de aprender trabalhando, ao serem questionados se houve compartilhamento de conhecimento de ações de segurança da informação que pudessem evitar ou mitigar novos incidentes de segurança, os gestores relataram em sua totalidade que não possuíam essa prática, embora reconhecessem sua importância. Menezes *et al.* (2017) destaca a importância de pessoas aprenderem com outras pessoas, no dia a dia, enquanto desempenham suas atividades.

Com relação à prática de mentoria, indagamos se na PROGEP existe o hábito de um servidor com mais experiência ajudar, apoiar e transmitir o seu conhecimento para outros servidores menos experientes, por meio de conversas ou vivências no ambiente de trabalho. Nesse contexto, a maioria dos gestores declarou que sim, mesmo sem existir um processo definido com regras ou uma formação para a execução de tal atividade. Por meio da observação participante, percebeu-se que essa prática com frequência era utilizada não apenas com o objetivo de proteger e compartilhar o conhecimento ou contribuir para o desenvolvimento de competências, mas acabava em uma intricada tentativa de mostrar relação de poder entre o detentor do conhecimento (servidor antigo) e o aprendiz (novo servidor) e por vezes, resulta na transferências dos vícios de trabalho dos antigos para os novatos.

Referente à comunidade de práticas, os gestores indicaram que não existe formalmente. No entanto, o G3 declara que "há conversas em pares ou em grupos, sempre informais, nas quais experiências e sugestões de segurança são compartilhadas de forma aleatória e ocorrem geralmente quando são casos mais graves e que chamam mais atenção". Corroborando a fala do G3, por meio da observação, percebe-se que na hora do cafezinho e no horário do almoço são discutidos problemas e dificuldades relacionados às atividades institucionais, proporcionando um espaço para colaboração e trocas de conhecimento.

6 CONSIDERAÇÕES FINAIS

Esta pesquisa se propôs a analisar quais as práticas organizacionais de GC envolvendo segurança da informação são utilizadas pelos gestores da PROGEP/UFPB, e se estas permitem compreender como as práticas estão relacionadas.

Os resultados descritos possibilitaram perceber que as práticas de GC de mapeamento de processos, sistema de gestão de documentos, mentoria e comunidade de prática contribuem com as propriedades de segurança da informação, visto que tanto a gestão do conhecimento como a segurança da informação possuem objetivos semelhantes na tentativa de proteger e disponibilizar a informação. Mas ficou evidenciado nas falas dos gestores, bem como na observação participante, que os processos ainda são realizados de forma incipiente, pois não existe uma unicidade no entendimento dos processos de gestão e sua relação com a segurança da informação. Mesmo quando se deparam com incidentes de segurança, o registro e o tratamento não acontecem conforme as recomendações.

Alerta-se como um limitador da pesquisa o tamanho da amostra, o que impossibilita a generalização dos resultados para todos os setores da universidade, mas por se tratar da área que cuida dos demais servidores, esperava-se respostas mais assertivas em relação aos temas consultados. Os resultados indicam que a utilização das comunidades de práticas pode auxiliar no processo para conscientização da importância de proteção da informação, além do

reconhecimento das práticas de GC para uma efetiva segurança da informação e sua contribuição com a criação de uma cultura de segurança.

Esta pesquisa não encerra esta discussão. É apenas um ponto de partida para a discussão da relação entre gestão do conhecimento e segurança da informação, uma vez que se trata de duas temáticas complexas e significativas no contexto organizacional, necessitando de uma compreensão, tanto no ambiente institucional quanto nas academias. Para futuras pesquisas, pode-se considerar: ampliar a pesquisa não apenas para toda a UFPB, mas expandir para outras universidades, gerando assim, considerações mais robustas e possíveis de generalização.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013.

ABNT. **NBR ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

ALVARENGA NETO, R. C. D. Gestão do conhecimento ou gestão de organizações da era do conhecimento? Um ensaio teórico-prático a partir de intervenções na realidade brasileira. **Perspectivas em Ciência da Informação,** v.12, n. 1, p. 5-24, jan./abr. 2007.

ARAÚJO, S. G. L. **A dimensão humana no processo de gestão da segurança da informação:** um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba. 2016. 153 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal da Paraíba, João Pessoa, 2016.

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.

AZEVEDO, L. C. S. **Gestão do conhecimento em organizações públicas**. 2002. Disponível em: www2.rio.rj.gov.br/cgm/textos_selecionados/gestão_conhecimento. Acesso em: 05 de dezembro de 2017.

BATISTA, F. F. **Modelo de gestão do conhecimento para a administração pública brasileira**: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão/Fábio Ferreira Batista. Brasília: Ipea, 2012.

BATISTA, F. F. **Governo que aprende**: gestão do conhecimento em organizações do Executivo Federal. Textos para Discussão. Brasília: IPEA, 2004. Disponível em http://www.inei.org.br/inovateca/estudos-e-pesquisas-eminovacao/GC%20em%20Organizacoes%20do%20Executivo%20Federal%20-%20Fabio%20Batista.pdf/view. Acesso em 01 de dezembro de 2017.

BURKE, P. **O que é a história do conhecimento**? 1 ed. São Paulo: Unesp, 2016.

CERCHIONE, R.; ESPOSITO, E.; SPADARO, M.R. The Spread of Knowledge Management in SMEs: A Scenario in Evolution. **Sustainabilit***y,* 2015.

CHOO, C. W. Como ficamos sabendo: um modelo de uso da informação. *In:* CHOO, C. W. **A organização do conhecimento**. São Paulo: Ed. SENAC, 2003.

CONG, X.; PANDYA, K. V. Issues of knowledge management in the public sector. **Electronic Journal of Knowledge Management**, v. 1, n. 2, p. 25-33, 2003.

DOHERTY, N. F.; TAJUDDIN, S. T. Towards a user-centric theory of value-driven information security compliance. **Information Technology and People**, v. 31, n. 2, p. 348–367, 2018. DOI: Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044586438&doi=10.1108%2fITP-08-2016-0194&partnerID=40&md5=b77e25254bf6f4478d8d356788c4b3b9. Acesso em: 19 jul. 2018.

ESLAMKHAH, M.; SENO, S. A. H. Identifying and Ranking Knowledge Management Tools and Techniques Affecting Organizational Information Security Improvement. **Knowledge Management Research & Practice**, 2019. Disponível em: https://www.tandfonline.com/doi/full/10.1080/14778238.2019.1599495. Acesso em: 02 mar. 2020.

FERREIRA, M. K. de B. **As novas configurações da Gestão Pública**: comunicação, conhecimento e pessoas. *In*: CARDOSO, C. M. (org.). **Diversidade e igualdade na comunicação**. Bauru, 2007. Disponível em: http://www.faac.unesp.br/publicacoes/anaiscomunicacao/textos/34.pdf. Acesso em: 07 dez. 2017.

FONTES, E. L. G. **Políticas e normas para a segurança da informação**: como desenvolver, implementar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FULLWOOD, R.; ROWLEY, J.; DELBRIDGE, R. Knowledge sharing amongst academics in UK universities. **Journal of Knowledge Management**, n.17, p. 123-136. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/13673271311300831/full/html. Disponível em: 02 mar. 2020.

ISACA. **ISO/IEC 27000**: information technology: security techniques: information security management systems: overview and vocabulary. 2014. Disponível em: http://k504.org/attachments/article/819/ISO_27000_2014.pdf. Acesso em: 22 abr. 2015

MENEZES, K. C.; JOHANN, J.; VALENTIM, P. P; SCOTT, P. Gestão do conhecimento nas organizações: uma aprendizagem em rede colaborativa. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 7, número especial, p. 145-159, mar. 2017.

MITNICK, K. D.; SIMON, W. L. Mitnick: **A arte de enganar.** São Paulo: Pearson Makron Books, 2003.

NONAKA, I.; TAKEUSCHI, H. Teoria da criação do conhecimento organizacional. *In:* TAKEUCHI, H.; NONAKA, I. **Gestão do conhecimento**. Porto Alegre: Bookman, 2008.

PACHECO, R. M. *et al.* Gestão do conhecimento na administração pública brasileira: seu papel na promoção da sustentabilidade. *In*: CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO & II INOVARSE, 11., **Anais** [...]. Rio de Janeiro, 2015.

RAMJEAWON, P. V.; ROWLEY, J. Knowledge management in higher education institutions: enablers and barriers in Mauritius. **Learning Organization**, v. 24, p. 366-377. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/TLO-03-2017-0030/full/html. Acesso em: 02 mar. 2020.

RIBEIRO, E. M. IZQUIERDO, O. C. **Gestão do conhecimento e governança no setor público**. Salvador: UFBA, 2017.

SAFA, N. S. et al. Information security conscious care behaviour formation in organizations. **Computers & Security**, v. 53, p. 65–78, 2015. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84961148106&doi=10.1016%2fj.cose.2016.01.004&partnerID=40&md5=36e5401e0343f8b1d0e668fdaff1e0c1. Acesso em: 20 jul. 2018.

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=7644d1b633827cf08a854f954cc6157c. Acesso em: 19 jul. 2018.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Campus, 2014.

SENGE, P. M. **A quinta disciplina**: a arte, teoria e a prática da organização que aprende. 27ed. São Paulo: Best Seller, 2011. Parte III

TRIBUNAL DE CONTAS DA UNIAO (TCU). **Boas práticas em segurança da informação**. 4. ed. Brasília: TCU, 2012.

VALENTIM, M. L. P. Informação e conhecimento em organizações complexas. *In:* **Gestão da Informação e do conhecimento no âmbito da Ciência da Informação**. São Paulo: Polis\Cultura Acadêmica, 2008. cap.1, p.11-25.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97-102, 2013. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404813000801?via%3Dihub. Acesso em: 02 mar. 2020.

YUPANQUI, J. R. A.; ORÉ, S. B. Políticas de Seguridad de la Información: Revisión Revisión Sistemática de las Teorías que Explican su Cumplimiento. **RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação Políticas de Seguridad de la Información**, n. 2003, p. 1–15, 2018.

Artigo recebido em 20/11/2019 e aceito para publicação em 15/03/2020