Revista ACB: Biblioteconomia em Santa Catarina,
Florianópolis, v. 25, n. 3, p. 477-492, abr./jul., 2020.

COMPETÊNCIA EM INFORMAÇÃO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO: MODELO TEÓRICO-CONCEITUAL PARA O USO SEGURO DA INFORMAÇÃO

Selma Leticia Capinzaiki Ottonicar[1]
Jean Fernandes Brito [2]
Rafaela Carolina da Silva[3]
Edgar Bisset Alvarez[4]

Resumo: O aumento do uso da Internet pela população inferiu na necessidade de garantir a confidencialidade das informações disponíveis em organizações. **Objetivo**: Apresentar um modelo de Competência em Informação no contexto da segurança da informação, partindo da análise das contribuições feitas pelos estudos sobre competência em informação e de segurança da informação, assim como, na inter-relação que se estabelece entre os elementos básicos de ambos. **Metodologia:** A pesquisa teve um olhar multidisciplinar, usando métodos como análise bibliográfica e documental, análise de conteúdo e sínteses. **Conclusões:** Os resultados obtidos permitiram o desenvolvimento de um arcabouço teórico cujos elementos de segurança da informação estão conectados com os padrões e indicadores que regem o desenvolvimento de competências informacionais. Apresentou-se, assim, a criação de um modelo que possibilita a confirmação de que pessoas com determinadas habilidades informacionais podem atuar de forma inteligente em relação à segurança de suas informações, tanto profissionalmente, quanto em nível pessoal e social. É necessário enfatizar que o modelo proposto é um "mapeamento" entre padrões de competência em informação e elementos de segurança da informação, que é o primeiro passo para construir uma sociedade que pense criticamente.

Palavras-chave: Competência em informação. Segurança da informação. Ciber Ataques.

1 INTRODUÇÃO

As ameaças cibernéticas têm colocado em risco as informações disponíveis na web. O ataque de hackers tem ameaçado as leis de privacidade, o que possibilita as guerras digitais. A Rússia, por exemplo, tem *hackeado* informações provenientes de setores nucleares, água e aviação. O Iran roubou quantidade significativa de dados e propriedade intelectual de professores universitários de vários países. Descobriu-se que um hacker pegou informações do Comitê democrático nacional e as enviou para o *Wikileaks.*

[1] Doutorado e Mestrado em Ciência da Informação no Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Graduação em Gestão Empresarial na Faculdade de Tecnologia de Garça (FATEC). E-mail: selma.leticia@hotmail.com.
[2] Mestrado Ciência da Informação no Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Santa Catarina .Graduação em Biblioteconomia na UNESP. E-mail: j.brito@unesp.br.
[3] Mestrado Ciência da Informação no Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Especialização em Psicopedagogia Institucional na Fundação para o Desenvolvimento do Ensino, Pesquisa e Extensão (FUNDEPE). Graduação em Biblioteconomia na UNESP. E-mail: rafaela.c.silva@unesp.br.
[4] Professor do Departamento e Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Santa Cartarina. Doutorado em Ciência da Informação no Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Mestrado em Biblioteconomia e Ciência da Informação na Universidade de Havana. Graduação em Informação Cientifico-Técnica e Biblioteconomia na Universidade de Havana. E-mail: edgar.bisset@ufsc.br.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Alguns meses depois, os investigadores perceberam que, na verdade, o *hacker* trabalhava para a agência de inteligência Russa, a sim de influenciar nas eleições políticas dos Estados Unidos (EUA) [5] (SLAYTON, 2018).

Recentemente, *hackers* roubaram informações sobre as conversas privadas do Facebook a fim de vende-las às empresas. Os invasores conseguiram dados de aproximadamente 120 milhões de contas. Geralmente o indivíduo recebe uma oferta de jogo online ou uma segunda janela abre automaticamente e começa a utilizar esse serviço (BBC, 2018)[6].

Essas e outras situações demonstram a necessidade de compreender a vulnerabilidade do sistema tecnopolítico. A sociedade é facilmente *hackeada* e isso ocorre porque há uma interação entre a tecnologia, leis, interesses empresariais, preconceito social e desigualdades estruturais (SLAYTON, 2018). Devido a esses desafios, os EUA têm aplicado ações e leis a fim de que os estudantes desenvolvam competência crítica em informação e mídia para que sejam capazes de enfrentar as *fake news*[7]. O engajamento com a iniciativa se fortaleceu a partir das eleições para presidente do país (FOLEY, 2017).

A competência em informação (CoInfo), vem sendo estudada desde 1974, principalmente pela área da Ciência da Informação. Diversos autores a consideram como a aprendizagem ao longo da vida, possibilitando ao indivíduo a construção do conhecimento em diversos contextos (LLOYD, 2017; BRUCE, 1999; BELLUZZO, 2007; OTTONICAR; VALENTIM; FERES, 2015; ACRL, 2014).

Nesse sentido, várias pesquisas têm sido realizadas a fim de introduzir e demonstrar a participação desta competência. Ottonicar, Valentim e Feres (2016, p. 133) apontam que a CoInfo é fundamental no contexto tecnológico, educacional, político e organizacional. No que tange às tecnologias, as autoras (2016) ainda defendem que "... a infraestrutura de acesso e distribuição é fundamental, mas os indivíduos necessitam saber acessar, buscar, selecionar e usar as informações contidas na rede, em bancos e bases de dados, de modo a amenizar ou solucionar problemas ou, ainda, tomar decisões...".

Ser competente em informação é primordial para usar as informações disponíveis na web e saber os locais adequados para armazená-la de maneira segura. Tais dados e informações são previamente analisados, bem como suas fontes e os servidores computacionais. A CoInfo também contribui no

[5] Para mais informações acesse os links:
https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it
https://www.cnn.com/2018/03/23/politics/iranian-hackers-indicted-universities-government/index.html.
https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer
https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-

[6] Informações disponíveis em: https://www.bbc.com/portuguese/geral-46070069

[7] Informações disponíveis em: https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

processo de solução de problemas e tomada de decisão dos aspectos da vida do indivíduo (YAFUSHI, 2015).

Além disso, contribui para que as pessoas construam conhecimento e se tornem aprendizes nos diferentes aspectos de sua existência. A tecnologia de informação e comunicação (TIC) participa da rotina das pessoas ao redor do mundo, principalmente nos países que tiveram recursos para financiar tais tecnologias. Essas tecnologias possibilitaram o compartilhamento de informação, assim surgiu e a necessidade de se preservar tais informações, bem como os sistemas de armazenamento. Apesar das TIC terem contribuído com a sociedade, ainda existe a possibilidade de se perder os dados de várias maneiras diferentes, podendo acontecer por erros no sistema, incêndios nos locais onde estão armazenados os dados, vírus, conhecidos como ataques cibernéticos. Tais ataques são motivados devido ao valor do conteúdo da informação.

A segurança da informação é uma área do conhecimento que se preocupa em armazenar e disseminar os dados de maneira segura. Segundo Solms e Niekerk (2013, p. 97) o termo segurança da informação está diretamente "relacionado as pessoas, pois se refere ao papel delas no processo de segurança". Complementando, Whitman e Mattord (2009) explicam que a segurança da informação se refere a proteção dos dados e informações e seus equipamentos.

Os ataques são realizados por pessoas especializadas em burlar os sistemas e, na maioria das vezes, acontecem por meio de formas ilegais. Mediante tais reflexões a presente pesquisa possui os seguintes problemas para responder: Os padrões e indicadores da CoInfo podem ser norteadores do processo de segurança da informação? Qual é a ação desenvolvida pelo indivíduo que os possibilitam ter segurança na sua atuação na web?

O objetivo buscou propor um modelo de CoInfo no contexto da segurança da informação, a partir de um levantamento das principais ações desenvolvidas pelo indivíduo que possibilitam ter segurança na sua atuação na web. Para alcançar tal objetivo, terá que se refletir sobre as principais contribuições da CoInfo e da segurança da informação na *web*, estabelecendo uma interconexão entre os padrões e indicadores desta competência e dos elementos básicos que a segurança em informação traz.

Essa pesquisa tem como metodologia uma revisão bibliográfica nas bases de dados *Web of Science* e *Scopus* sobre os principais conceitos de segurança da informação e competência em informação, bem como a interlocução de um quadro teórico, a fim de demonstrar tais conexões no âmbito da Ciência da Informação. Não obstante, o trabalho é considerado multidisciplinar, levando em conta que a multidisciplinaridade se baseia no compartilhamento de um mesmo objeto, mas as disciplinas não

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

interagem entre si, isto é, ainda compartimentalizada, as disciplinas contribuem cada uma com suas teorias e aplicações, sem fazer correlação com outros vieses teóricos.

Segundo Morin (2003, p. 115), a multidisciplinaridade é como "[...] uma associação de disciplinas, por conta de um projeto ou de um objeto que lhes sejam comuns". Dessa maneira, este trabalho se pauta na Ciência da Computação, que fornece os conceitos, teorias e elementos formadores da segurança da informação e da Ciência da Informação que, entre outros conceitos, estuda os fenômenos relacionados com a CoInfo e seu diálogo com outras áreas do conhecimento prático-científico.

2 COMPETÊNCIA EM INFORMAÇÃO E TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Com a transformação das TIC, em especial na *Web*, o acesso e a disseminação da informação em diferentes ambientes informacionais digitais tornaram-se mais dinâmicos. Por meio dessas tecnologias, a socialização da informação, a comunicação entre os usuários e o compartilhamento do conhecimento foram favorecidos, principalmente pela facilidade de uso (usabilidade).

Nesse contexto, Cusin e Vidotti (2009, p. 46) destacam que "[...] a importância da Competência Informacional na era da Sociedade da Informação para proporcionar a Inclusão Informacional e Digital e melhorar o acesso às [SO1] ao conteúdo informacional digital. Mostram-se mais uma vez a relevância e a necessidade de uma *web* acessível" (CUSIN; VIDOTTI, 2009, p. 44). Para Belluzzo, Kobayashi e Feres (2004, p. 87), a CoInfo "Inegavelmente, está ligada ao aprendizado e à capacidade de criar significado a partir da informação, sendo uma condição indispensável que as pessoas saibam "aprender a aprender" e realizem o "aprendizado ao longo da vida".

Essa necessidade de se ter uma *web* acessível parte das alterações do comportamento informacional que a sociedade tem sofrido com o desenvolvimento das TIC, pois os indivíduos estão cada vez mais dependentes para realizar suas atividades. Portanto, as TIC dissolveram as fronteiras nacionais e propiciaram nova configuração social, política e econômica. Esta mudança ocorreu principalmente na transformação do modo como o conhecimento é adquirido, armazenado, processado, transmitido e disseminado. Dessa forma, o conhecimento ganha centralidade no cotidiano da sociedade, o que gera a necessidade de novas políticas de segurança da informação para que o indivíduo se inclua na Sociedade da Informação, visando o ideal de convivência e desenvolvimento de estado e sociedade (CUBILLOS; SILVA, 2009, p. 36).

De acordo com Vitorino e Piantola (2009), existem quatro dimensões da CoInfo aplicáveis ao cenário das TIC e ao uso seguro da Internet: 1) Dimensão Técnica: o uso das TICs para o acesso às informações - o indivíduo se atualiza constantemente para manuseá-las; 2) Dimensão Estética:

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

capacidade sensível do indivíduo e intransferível: fruto da experiência pessoal; 3) Dimensão Ética: uso consciente e responsável da informação, respeitando os direitos autorais, a propriedade intelectual e a construção da memória do mundo; 4) Dimensão Política: pessoas como cidadãos atuantes em sociedade.

Para medir a dimensão, contexto e ambiência da CoInfo, Belluzzo (2007) estabeleceu padrões e indicadores adequados ao Brasil. A saber: Padrão 1 – A pessoa competente em informação determina a natureza e a extensão da necessidade de informação; Padrão 2 – A pessoa competente em informação acessa a informação necessária com efetividade; Padrão 3 – A pessoa competente em informação avalia criticamente a informação e as suas fontes; Padrão 4 – A pessoa competente em informação, individualmente ou como membro de um grupo, usa a informação com efetividade para alcançar um objetivo/obter um resultado; Padrão 5 – A pessoa competente em informação compreende as questões econômicas, legais e sociais da ambiência do uso da informação e acessa e usa a informação ética e legalmente.

Alguns autores dos EUA têm utilizado o termo *critical media literacy* que segundo Alvermann et. al (2018) possibilita que as pessoas compreendam o papel dos textos impressos e não impressos. Tais textos são parte da vida diária dos indivíduos e atuam na construção do conhecimento. Esse termo advém da sociologia e da área interdisciplinar de estudos da cultura.

Outro termo também utilizado é a *media literacy* e segundo Lee e So (2014, TRADUÇÃO NOSSA) “Embora a competência midiática e a competência em informação pareçam áreas separadas, ambos os conceitos compartilham o mesmo objetivo de cultivar a habilidade das pessoas em acessar, entender, usar e criar mensagens ou informação na mídia. Na família desta competência, ambas tem sido estudada de maneira conectada”.

Essas diferentes nomenclaturas são relevantes para a área das *literacy*, pois estimulam interpretações de diferentes campos do conhecimento. Estas interpretações estimulam a construção do conhecimento interdisciplinar entre a Ciência da Informação, Educação, Sociologia, Antropologia, etc. No caso desse artigo, optou-se pela CoInfo, porém não ignora a relevância das demais nomenclaturas e variações conceituais. De maneira geral a CoInfo está relacionada com a aprendizagem contínua (KUMAR; SURENDRAN, 2015), que pode estar associada à diferentes formas de conhecimento como, por exemplo, o aprendizado especializado, pessoal, profissional, social, entre outros. Tais aprendizados são também relevantes para o contexto da segurança da informação.

A tarefa e a missão de promover o acesso à informação podem estar ancoradas em padrões e indicadores desta competência (LAU, 2007; BELLUZZO, 2007; BUNDY, 2004; ACRL, 2000). Estes padrões e indicadores de CoInfo são estudados principalmente no continente americano e são aplicados

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

no ambiente de trabalho, escolar e nas demais organizações. De maneira geral apresentam cinco padrões relacionados com o acesso, a avaliação, o uso e a aplicação prática da competência em sociedade.

Infere-se, dessa maneira, que a CoInfo é um importante instrumento para a segurança na disseminação, uso e criação da informação, principalmente porque atua como uma norteadora em objetivos de educação de usuários, fomento à utilização das tecnologias, estímulo ao desenvolvimento do pensamento crítico, aprendizagem contínua e consciência cidadã.

3 SEGURANÇA DA INFORMAÇÃO

As TIC conforme discute Le Coadic (1996), surgiram como reflexo da necessidade de aperfeiçoamento memorização e comunicação da informação cada vez mais abundante. O desenvolvimento das TIC ocorreu por meio do progresso técnico e social da linguagem e do raciocínio e transição da oralidade para a escrita.

Na visão de Ilharco (2003), as TIC provocaram a revolução da informação, consubstanciando novas formas de ser e de estar, ou seja, formando novas estruturas políticas, econômicas e sociais tanto ao nível dos Estados, como da própria humanidade, geralmente designadas pelo termo globalização. Nessa premissa vale revisar o conceito de Segurança da Informação (SI) de modo a repensar suas possíveis aplicações em outras áreas do conhecimento.

Assim, Sêmola (2003) define SI como uma área do conhecimento dedicada a proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Destarte ao uso das TIC até aqui discutido, ajuizamos em concordar com a definição de Marciano e Lima-Marques (2006, p. 87) que diz que,

> "Segurança da informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso."

De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos, além da confiabilidade, integridade e disponibilidade da informação em alguns aspectos adicionais de segurança emergem quando precisa ser transmitida num processo de comunicação (BEAL, 2005).

Nessa perspectiva Beal (2005) destaca cinco pontos que a SI trafega com o objetivo de preservar:

a. **Integridade do Conteúdo:** garantia de que a mensagem enviada pelo emissor é recebida de forma completa e exata pelo receptor;
b. **Irretrabilidade da Comunicação:** garantia de que o emissor ou receptor não tenha como alegar que uma comunicação bem-sucedida não ocorreu.
c. **Autenticidade do emissor e do receptor:** garantia de quem se apresenta como remetente ou destinatário da informação é realmente como quem diz ser

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

d. **Confidencialidade do conteúdo:** garantia de que o conteúdo da mensagem somente é acessível a seus destinatários.
e. **Capacidade de recuperação do conteúdo pelo receptor:** garantia de que o conteúdo transmitido pode ser recuperado em sua forma original pelo destinatário.

Visto todo este contexto, propõem-se então novos conceitos, capazes de representar adequadamente os atores e o ambiente envolvidos na sistemática da segurança da informação, bem como a sua relevância nesse processo de produção e uso da informação (MARCIANO; LIMA-MARQUES, 2006).

Conforme apontado por Marciano e Lima-Marques (2006, p. 89) “as políticas de segurança da informação devem contemplar o adequado equilíbrio dos aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos de políticas atuais”

Enfim, deve-se observar que as TIC se relacionam de forma holística em sociedade permeando diversos espaços e ambientes, é nessa discussão que a Segurança da Informação deve ser revista em diveros aspectos considerando aspectos de acesso, uso, representação da informação.

4 PROCEDIMENTOS METODOLÓGICOS

Esta pesquisa se caracteriza como teórica e busca discutir e aprimorar fundamentos teóricos e conceituais. Sua natureza é considerada como pesquisa qualitativa. A pesquisa qualitativa é aquela que “[...] não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização etc.” (GERHARDT; SILVEIRA, 2009, p. 31).

Seu procedimento, como uma pesquisa bibliográfica, valeu-se da abordagem de Gil (1991, p. 48), de que tal pesquisa “[...] é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos.” Assim como afirma Gerhardt e Silveira, (2009), Santos, Molina e Dias (2007), Prodanov e Freitas (2003), uma pesquisa bibliográfica é realizada através de materiais já existentes sobre a temática, como livros, artigos científicos, teses, monografias, vídeos, internet, documentários, dentre outros.

Deste modo a revisão foi realizada nas bases de dados: SCOPUS e WEB OF SCIENCE nas línguas inglesa, espanhola e portuguesa. Portanto, os termos utilizados como palavras-chaves foram: "*information literacy*" e "*information security*"; "segurança da informação" e "ciência da informação"; e "*seguridad de la información*" e "*alfabetización informacional*". Após esse procedimento, foi realizada a leitura, fichamento e análise dos textos, a fim de entender a proposta e objetivos dos trabalhos e posteriormente, realizar a extração e sistematização das informações principais.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

5 RESULTADOS

Na base de dados SCOPUS foram encontrados seis artigos que relacionavam a CoInfo com a segurança da informação. Destes, apenas dois se relacionavam diretamente com a área da Ciência da Informação, sendo que um deles não se apresentava em forma de resumo completo e, portanto, não foi considerado aplicável a esta pesquisa. Para tanto, em relação à base de dados SCOPUS, foi escolhido apenas um artigo para esta análise.

O artigo intitulado "*Research on information literacy training and information security education*", de Jun e Chun Yu (2012), trabalhou a temática da CoInfo como uma medida educacional para o uso seguro da Internet por jovens e adolescentes. O objeto da pesquisa foi a formação de estudantes universitários competentes no uso da informação via Internet na China.

Houve, para tanto, uma comparação entre como as universidades estadunidenses trabalham o desenvolvimento da competência em segurança da informação, para com o cenário chinês. Observou-se que os Estados Unidos estão mais desenvolvidos nessa perspectiva do que a China.

O estudo concluiu que fatores como vírus espalhados pela internet e notícias maliciosas são os itens que mais influenciam de forma negativa no uso seguro da Internet. Destacou-se, também, que a maioria dos estudantes acreditam estar navegando de forma segura, mas que, na verdade, não estão (JUN; CHUN YU, 2012).

Nessa perspectiva, uma pessoa competente em informação, de acordo com o estudo, deve ter a capacidade de atingir os níveis de conscientização dos perigos que a Internet traz, além de seus benefícios, gerar um conhecimento a partir disso e, então, navegar de forma ética. Destacou-se a necessidade de os profissionais de Tecnologia da Informação, assim como as universidades chinesas, levarem mais a sério a formação de seres autônomos e competentes no uso da Internet (JUN; CHUN YU, 2012).

Na base de dados WOS foram recuperados 7 artigos, das quais 6 não atenderam os critérios de inclusão e foram excluídos. O artigo intitulado *Media and information literacy is lifelong education component*, de Svetlana Gudilina (2016) discute a importância da educação ao longo da vida descreve as características da abordagem europeia à alfabetização midiática e informacional.

A necessidade da introdução da educação midiática integrada na educação formal para o desenvolvimento de habilidades meta-sujeitos necessárias para maior aprendizado e formação profissional ao longo da vida (GUDILINA, 2016). A revisão bibliográfica demonstrou, portanto, a necessidade de se estudar a CoInfo para o contexto da segurança de informação, tendo em vista que a informação de qualidade possibilita ao indivíduo interpretar o conteúdo da mensagem de maneira crítica.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Essa inter-relação foi demonstrada pelo Quadro 2. Os princípios de segurança de informação, os padrões de CoInfo e os resultados para os usuários. Posteriormente, a partir da discussão do quadro, sugeriu-se um modelo de conhecimento sobre o tema, representado pela Figura 1.

A segurança da informação possui, segundo Gollmann (2010), quatro princípios básicos, a autenticidade, a confidencialidade, a integridade e a disponibilidade. A autenticidade orienta que o indivíduo recebeu a mensagem pelo remetente esperado e a garantia de que foi o remetente quem modificou a informação da mensagem.

A confidencialidade explica que apenas as pessoas ou objetos autorizados podem ter acesso ao conteúdo da mensagem (GOLLMANN, 2010). A integridade possibilita que o conteúdo da mensagem não tenha nenhuma mudança, que pode ser acidental ou legítima. Por fim, mas não menos importante, a disponibilidade assegura os usuários de que o recurso ou serviço está disponível quando necessário pelos indivíduos (Gollmann, 2010). Estes princípios foram relacionados com os padrões de CoInfo, conforme mostra o Quadro 2.

Quadro 2 - Os princípios de segurança de informação, os padrões de CoInfo e os resultados para os usuários

Princípios da segurança de informação	**Padrões e indicadores de CoInfo**	**Resultados para o usuário no contexto da *Web***
Autenticidade	Padrão 1 - A pessoa competente em informação determina a natureza e a extensão da necessidade de informação.	O usuário competente em informação que atua na segurança da informação percebe sua necessidade de informação e identifica os tipos de fontes que compartilharam a informação. Também define as palavras-chave para realizar a busca.
Autenticidade e Confidencialidade	Padrão 2 - A pessoa competente em informação acessa a informação necessária com efetividade.	O usuário competente em informação que atua na segurança da informação reconhece que a informação foi modificada por uma fonte durante o seu acesso, acessa a informação em diferentes bases de dados e tecnologias e sabe como acessar as informações confidenciais de sua área.
Confidencialidade	Padrão 3 - A pessoa competente em informação avalia criticamente a informação e as suas fontes.	O usuário competente em informação que atua na segurança da informação identifica a intenção dessas fontes e a ideologia que as regem. Além disso, conhecem a cultura de confidencialidade da fonte de informação e avalia seu

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Princípios da segurança de informação	Padrões e indicadores de CoInfo	Resultados para o usuário no contexto da *Web*
		conteúdo de maneira crítica.
Integridade	Padrão 4 - A pessoa competente em informação, individualmente ou como membro de um grupo, usa a informação com efetividade para alcançar um objetivo/obter um resultado.	O usuário competente em informação que atua na segurança da informação sabe como usar a informação com base em sua segurança na web por meio da integridade, ou seja, da interpretação e verificação da legitimidade do conteúdo. Posteriormente, toma decisão e resolve um problema com eficácia, já que se baseia em fontes de informação e conteúdo de qualidade.
Integridade, Disponibilidade	Padrão 5 - A pessoa competente em informação compreende as questões econômicas, legais e sociais da ambiência do uso da informação e acessa e usa a informação ética e legalmente.	O usuário competente em informação que atua na segurança da informação atua nos princípios de autenticidade, confidencialidade, integridade e disponibilidade da informação. Sua atuação acontece por meio do acesso a informação de qualidade e fidedigna para realizar suas atividades. Está atento a ética e as leis de sua área e foca no conteúdo da informação para construir conhecimento crítico, contribuindo com a sociedade.

Fonte: Elaboração própria (2020)

O princípio da autenticidade da segurança da informação trabalha com o conceito de mensagem (GOLLMANN, 2010). Sendo assim, visa garantir que o indivíduo receba esta mensagem, portanto, o indivíduo precisa saber como determinar a natureza e a extensão da necessidade de informação (Belluzzo, 2007; Lau, 2007, ACRL, 2000).

Logo, precisa perceber quais informações o usuário necessita e se certificar de que a informação compartilhada está de acordo com as expectativas. Além disso, o usuário precisa conhecer a fonte de informação como confiável, a fim de demonstrar a qualidade da fonte. Depois de perceber a necessidade de informação, a pessoa precisa acessá-la na web de maneira efetiva (BELLUZZO, 2007; LAU, 2007; ACRL, 2000). O acesso à informação está relacionado com a autenticidade e à confidencialidade, à medida que encontra informações potenciais e as transforma em sigilosas para o usuário (GOLLMANN, 2010).

Além disso, deve buscar em outras fontes (BELLUZZO, 2007) como as bases de dados internas a organização e as demais tecnologias de informação e comunicação. O objetivo é garantir que o usuário receba a mensagem de modo confidencial (GOLLMANN, 2010) e que supra suas necessidades de informação.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Independentemente do local onde a informação se localiza, a pessoa precisa construir e disponibilizar informação de maneira confidencial (GOLLMANN, 2010). Para isso, necessita avaliar o conteúdo da mensagem e as intenções por trás da fonte de informação (BELLUZZO, 2007; LAU, 2007; ACRL, 2000).

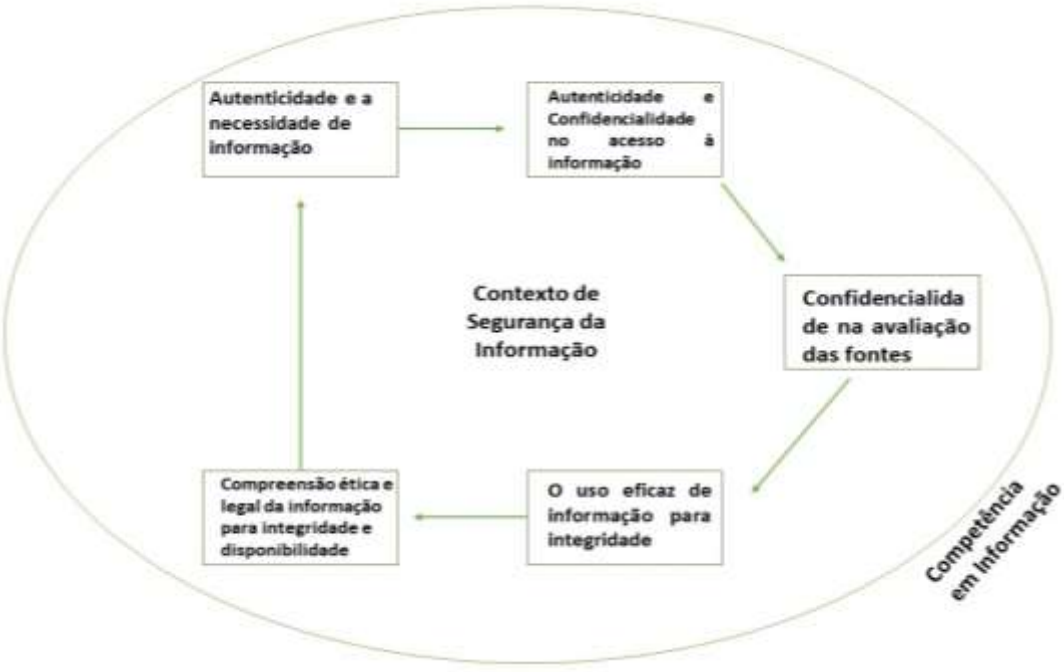
Não obstante, tem como missão assegurar de que o compartilhamento seja feito de maneira segura por meio da *web*. O indivíduo competente em informação que atua com base na segurança, usa a informação com efetividade para alcançar um objetivo/obter um resultado (BELLUZZO, 2007; LAU, 2007; ACRL, 2000).

A integridade é um dos principais objetivos de suas atividades (GOLLMANN, 2010), tendo em vista que o conteúdo da mensagem não pode ser modificado durante seu compartilhamento. A *web* é um local de fácil manipulação de dados e informação, porque os indivíduos consomem, mas também produzem informação (TOFFLER, 1980).

A integridade e a disponibilidade (GOLLMANN, 2010) estão ambas relacionadas com o quinto padrão, pois norteiam os profissionais a garantir a veracidade e a disseminação da informação. Ao estar atento a essas duas questões primordiais, o indivíduo desenvolve o senso crítico e compreende as questões éticas e legais de seu trabalho (BELLUZZO, 2007; LAU, 2007; ACRL, 2000).

A segurança da informação está profundamente atrelada à disponibilização da informação sigilosa de maneira ética, atendendo às necessidades do usuário. A partir da interpretação dos princípios de segurança da informação e dos padrões de CoInfo (quadro 2), desenvolveu-se um modelo de conhecimento generalizado, que explica o contexto dessas relações. Ressalta-se que o modelo é flexível e pode ser utilizado e adaptado em outros estudos científicos.

Figura 1 – Modelo de CoInfo no contexto da segurança da informação



Fonte: Elaboração própria (2020)

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

No modelo, a CoInfo é vista como elemento principal do contexto de segurança da informação. Tal contexto pode ser as organizações formais e informais que necessitam desta segurança. As organizações precisam garantir a confidencialidade das informações como empresas, hospitais, autarquias, escolas, igrejas, organizações não governamentais, grupos religiosos, um time de futebol, entre outras.

Cada padrão de CoInfo foi inter-relacionado com um princípio da segurança da informação. Por exemplo, no quadro "autenticidade e a necessidade da informação" há a inter-relação com o primeiro padrão. O indivíduo ao perceber que precisa de informação deve verificar o porquê e a autenticidade da fonte de informação (emissor). A necessidade de dados e informações surgem na vida cotidiana a medida que o indivíduo aprende.

A autenticidade e confidencialidade foram relacionadas com o padrão 2 (Belluzzo, 2007), pois a busca de informação precisa estabelecer estratégias para selecionar as fontes potenciais com base em sua autenticidade e respeitar a confidencialidade dos dados. O indivíduo deve coletar tais dados de maneira ética, sem violar a legislação.

O princípio da confidencialidade (Beal, 2005) está presente no processo de avaliação das fontes de informação (padrão 3). O indivíduo competente precisa investigar sobre a qualidade e a procedência da fonte. Os interesses do autor que podem ser ideológicos, econômicos, pessoais ou apenas para agradar o público leitor. É fundamental filtrar o conteúdo da informação segundo a sua utilidade para resolver o problema ou tomar a decisão.

O uso eficaz da informação sugerido pelo padrão 4 foi relacionado com o princípio da integridade (BEAL, 2005). O indivíduo precisa garantir que a disseminação da informação seja desenvolvida com qualidade, pois o receptor deve recebê-la de maneira completa e exata. A compreensão ética e legal das questões que envolvem o uso da informação (padrão 5) foram conectados com os princípios da integridade e disponibilidade (BEAL, 2005) a fim de que a pessoa valorize a qualidade da informação emitida e recebida. Há a necessidade em se respeitar as leis de propriedade intelectual e usar a informação de maneira ética.

Os elementos dessas inter-relações acontecem de maneira concomitantes e, por isso, foram inter-relacionados com os princípios da segurança da informação de modo cíclico. Na prática, os processos não ocorrem em etapas, como explicado pelo Quadro 2 de maneira didática, mas perpassam as atividades dos profissionais de segurança da informação e dos indivíduos que necessitam da CoInfo para usar a informação na *web*.

O modelo de CoInfo no contexto da segurança da informação (Figura 1) pode ser norteador de cursos de capacitação e formação tanto para profissionais da segurança da informação quanto para o público em geral.

6 CONCLUSÃO

Há oportunidades de pesquisas que relacionem a temática da CoInfo com a segurança da informação na Ciência da Informação. As interações disciplinares contribuem para que novos conhecimentos sejam desenvolvidos. Desse modo, é possível diagnosticar como a Ciência da Informação influencia em outras áreas.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

O artigo apresentou um quadro relacionando os princípios básicos que constituem a área da segurança da informação e sua inter-relação com os padrões e indicadores da CoInfo. Os padrões demonstraram ser úteis no processo e servem para nortear as práticas dos profissionais e da sociedade em geral. Além disso, podem ser utilizados futuramente no desenvolvimento de cursos de capacitação.

O foco é que os profissionais possam acessar, avaliar e usar a informação para que mantenha sua autenticidade, confiabilidade e integridade, disponibilizando-a de maneira inteligente. O modelo proposto como produto científico de conhecimento se torna o primeiro passo para relacionar essas duas temáticas tratadas no artigo. Ressalta-se que o modelo não é fixo, mas flexível, portanto, poderá ser adaptado com base em diferentes aspectos e interpretações que permeiam tanto a CoInfo quanto a segurança da informação.

Como sugestões a pesquisas futuras têm-se a aplicação de uma pesquisa de campo, assim como estudos práticos em diversos contextos e abordagens. Tais contextos podem ser tanto profissional quanto educacional. Além disso, sugere-se realizar uma investigação fenomenográfica, a fim de analisar como esses profissionais experienciem a CoInfo em suas práticas.

REFERÊNCIAS

ASSOCIATION FOR COLLEGE AND RESEARCH LIBRARIES (ACRL). *First part of the draft framework for information literacy for higher education*, 2014. Disponível em: http://acrl.ala.org/ilstandards/wp-content/uploads/2014/02/Framework-for-IL-for-HE-Draft-1-Part-1.pdf. Acesso em: 13 ago. 2018.

ALVERMANN, D. E.; MOON, J. S.; HAGOOD, M. C. *Popular culture in the classroom*: Teaching and researching media literacy. Athens: Routledge, 2018.

BEAL, A. *Segurança da informação*: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BELLUZZO, R.C.B. *Construção de mapas*: Desenvolvendo competências em informação e comunicação. Bauru: Autores Brasileiros, 2007.

BELLUZZO, R.C.B.; KOBAYASHI, M. C. M.; FERES, G.G. Information Literacy: um indicador de competência para a formação permanente de professores na sociedade do conhecimento. *Educação Temática Digital*, Campinas, SP, v. 6, n. 1, p. 81-99, 2004.

BRUCE, C. S. Workplace experiences of information literacy. *International Journal of Information Management*, v. 19, p. 33-47, 1999. Disponível em: http://www.personal.kent.edu/~wjrobert/images/WorkplaceInfoLit.pdf. Acesso em 07 fev. 2020. Acesso em: 10 nov. 2018.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

BUNDY, A. *Australian and New Zealand Information Literacy Framework*: principles, standards and practice, 2004. Disponível em: http://archive.caul.edu.au/info-literacy/InfoLiteracyFramework.pdf. Acesso em 15 jan. 2020.

CUBILLOS, D.; SILVA, A. S. C. da. Inclusão digital: sistema de engrenagens. *Liinc em Revista*, Rio de Janeiro, v. 5, n. 1, p. 32-44, 2009.

CUSIN, C. A.; VIDOTTI, S. A. B. G. Inclusão digital via acessibilidade web. *Liinc em Revista*, Rio de Janeiro, v. 5, n. 1, p. 45-65, 2009.

FOLEY, R. J. Spread of fake news prompts literacy efforts in schools. *PBSO News Hours Weekend*, 2017. Disponível em: https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools. Acesso em 02 fev. 2020.

GERHARDT, T. E.; SILVEIRA, D. T. (Orgs.). *Métodos de pesquisa*. Porto Alegre: Editora da UFRGS, 2009.

Gil, A. C. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2008.

Gil, A. C. *Como elaborar projetos de pesquisa*. 3. ed. 6. tir. São Paulo: Atlas, 1991.

GOLLMANN, D. Computer security. *Advanced Review*, v. 2, p. 544-556, 2010. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1002/wics.106. Acesso em 02 jan. 2020.

GUDILINA, S. Media and information literacy is lifelong education component. In: INTERNATIONAL CONFERENCE "EDUCATION ENVIRONMENT FOR THE INFORMATION AGE" (EEIA), 2016. *Anais*... SHS Web Conferences, 2016. Disponível em: https://www.shs-conferences.org/articles/shsconf/abs/2016/07/shsconf_eeia2016_01025/shsconf_eeia2016_01025.html?mb=0. Acesso em: 05 jan. 2020.

ILHARCO, F. *Filosofia da Informação*: uma introdução como fundação da ação, da comunicação e da decisão. Lisboa: Universidade Católica, 2003.

JUN, Z. A.; CHUN YU, W. Research on Information Literacy Training and Information Security Education. *Computer Science & Education*, Estados Unidos, Canadá: IEE Explorer, 2012.

KUMAR, S. K.; SURENDRAN, B. Information Literacy for Lifelong Learning. *International Journal of Library and Information Studies*, v. 5, n. 2, abr./jun. 2015.

LAU, J. *Diretrizes sobre desenvolvimento de habilidades de informação para a aprendizagem permanente*. The Haague: IFLA, 2007. Disponível em: http://www.ifla.org/files/assets/information-literacy/publications/ifla-guidelines-pt.pdf. Acesso em 25 jan. 2020.

LE COADIC, Y. F. *A Ciência da Informação*. Brasília: Briquet de Lemos, 1996.

LEE, A.Y.L.; SO, C.Y.K. (2014). Media Literacy and Information Literacy: Similarities and Differences. *Media Education Research Journal*, v. 21, n. 42, p. 137-145, 2014.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

LLOYD, A. Recasting information literacy as sociocultural practice: Implications for library and information science researchers. *Information Research*, v. 12, n. 4, paper colis 34, 2007.

MARCIANO, J. L.; LIMA–MARQUES, M. O enfoque social da segurança da informação. *Ciência da Informação* [online], 2006.

MORIN, E. *A cabeça bem feita*: repensar a reforma, reformar o pensamento. 8. ed. Rio de Janeiro: Bertrand Brasil, 2003.

OTTONICAR, S.L.C.; VALENTIM, M.L.P.; FERES, G.G. Competência em informação e os contextos educacional, tecnológico, político e organizacional**.** *Revista Ibero-americana de Ciência da Informação*, Brasília, v. 9, n. 1, p. 124-142, 2015.

PRODANOV, C. C.; FREITAS, E. C. *Metodologia do trabalho científico*: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2003.

SANTOS, P. L. V. A. DA C.; SANT'ANA, R. C. G. Transferência da Informação: análise para valoração de unidades de conhecimento. *DataGramaZero: Revista de Ciência da Informação*, v. 3, n. 2, 2002.

SANTOS, G. do R. C. M.; MOLINA, N. L.; DIAS, V. F. *Orientações e dicas práticas para trabalhos acadêmicos*. Curitiba: Ibpex, 2007.

SÊMOLA, M. *Gestão da segurança da informação*: Visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003.

SLAYTON, R. *Beyond Cyber-Threats*: the technopolitics of vulnerability. Ithaca: H-Diplo, 2018.

SOLMS, R. V.; NIEKERK, J. V. From Information Security to Cyber Security. *Computers & Security*, v. 38, p. 97-102, 2013.

VITORINO, E. V.; PIANTOLA, D. Competência Informacional: bases históricas e conceituais: construindo significados. *Ciência da Informação*, v. 38, n. 3, p. 130-141, 2009.

WATANABLE, K.; ANDO, M.; SONEHARA, N. Website credibility: a proposal on an evaluation method for ecommerce. In: INTERNATIONAL CONFERENCE ON E-BUSINESS, 1., 2018, Portugal. *Anais*… Portugal: ICE, 2008.

WHITMAN, M. E.; MATTORD, H. J. *Principles of information security***.** 3. ed. Boston: Thompson Course Technology, 2009.

YAFUSHI, C. A. P. *A Competência em informação para a construção de conhecimento no processo decisório*: estudo de caso na Duratex de Agudos (SP). 2015. Dissertação (Mestrado em Ciência da Informação) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2015.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Revista ACB: Biblioteconomia em Santa Catarina,
Florianópolis, v. 25, n. 3, p. 477-492, abr./jul., 2020.

INFORMATION LITERACY IN THE CONTEXT OF INFORMATION SECURITY: CONCEPTUAL MODEL FOR THE SAFE USE OF INFORMATION

Abstract: The increased use of the Internet by the population influenced on the necessity for the confidentiality of the information available in organizations. The purpose was to present a model of information literacy in the context of information security, based on the analysis of the studies about information literacy and information security, as well as on the interrelation between their basic principles. The research had a multidisciplinary approach, using methods such as bibliographical and documentary analysis, content analysis and synthesis. The results obtained allowed the development of a theoretical framework whose elements of information security are connected with the standards and indicators of information literacy. The results also allowed the creation of a theoretical model which explains that people with certain informational skills can act intelligently in relation to the security of their information professionally and in their personal and social contexts. The proposed model is a "mapping" between standards of information literacy and elements of information security. The model is the first step to construct a society that thinks critically.

Keywords: Information literacy. Information security. Cyber Attacks.