



XX ENANCIB

21 a 25 Outubro/2019 – Florianópolis

A Ciência da Informação e a era da Ciência de Dados

GT-4 – GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

CONTRIBUIÇÕES DA CIÊNCIA DA INFORMAÇÃO PARA A SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM TEÓRICA

INFORMATION SCIENCE CONTRIBUTIONS FOR INFORMATION SECURITY: A THEORETICAL APPROACH

Rafael dos Santos Nonato (Universidade Federal de Minas Gerais - UFMG)

Elisângela Cristina Aganette (Universidade Federal de Minas Gerais - UFMG)

Modalidade: Trabalho Completo

Resumo: A partir da segunda metade do século XX, as tecnologias da informação provocaram uma revolução nas formas e nos métodos de geração, armazenamento, processamento e transmissão da informação, tornando-a um ativo de grande importância para a humanidade. Tanto a Segurança da Informação como a Ciência da Informação têm como propósito o estudo da informação e suas implicações. Assim, buscar-se-á, por meio da aplicação de uma metodologia exploratória, o estudo dos temas Segurança da Informação e Ciência da Informação. Concomitantemente, um levantamento bibliográfico será realizado, com intuito de se identificar as contribuições da Ciência da Informação para a mitigação de riscos, ameaças e vulnerabilidades em Segurança da Informação. Os resultados do presente estudo evidenciam a aplicabilidade da Ciência da Informação, considerando as subáreas definidas por Saracevic (1996), para a criação das barreiras de Segurança da Informação propostas por Sêmola (2014). Destacam-se, ainda, as contribuições das áreas de Biblioteconomia, Comunicação, Ciência da Computação e Ciências Cognitivas. Nas considerações finais, recomenda-se a aplicação de técnicas e teorias oriundas da Ciência da Informação para a criação e implementação de uma política de segurança da informação eficaz em organizações públicas ou privadas. Pretende-se que esse estudo acresça à literatura da área e evidencie a contribuição e relação da Ciência da Informação e Segurança da Informação.

Palavras-Chave: Ciência da Informação, Segurança da Informação, Acesso à Informação, Gestão do Conhecimento, Informação para Negócios.

Abstract: Since the second half of the twentieth century, information technologies have caused a revolution in the forms and methods of information generation, storage, processing and transmission. Making information an asset of great importance to humanity. Both, Information Security and Information Science have as their purpose the study of information and its implications. Thus, it will be sought, through the application of an exploratory methodology, the study of the themes Information Security and Information Science. On the same hand, a bibliographic survey will be conducted to identify the contributions of Information Science to the mitigation of risks, threats and vulnerabilities in Information Security. The results of the present study show the applicability of Information Science, considering the subareas defined by Saracevic (1996), for the creation of the Information Security barriers proposed by Semola (2014). Also noteworthy are the contributions from the areas of Library Science, Communication, Computer Science and Cognitive Science. As final considerations, it is recommended to apply techniques and theories from Information Science to create and implement an effective information security policy in public or private organizations. It is intended that this study can contribute to the literature of the area and thus highlight the contribution and relationship of Information Science and Information Security.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

Keywords: Information Science, Information Security, Information Access, Knowledge Management, Business Information.

1 INTRODUÇÃO

A partir da segunda metade do século XX, as tecnologias da informação provocaram uma revolução nas formas e nos métodos de geração, armazenamento, processamento e transmissão da informação. A mudança do texto do suporte impresso para o suporte eletrônico criou transformações significativas no modo como organizamos e acessamos a informação. Nesse contexto, a Ciência da Informação (CI) vem se consolidando enquanto um vasto campo de pesquisas e estudos. Segundo Carvalho e Crippa (2013) e Saracevic (1996, 1999), essa ciência pertence ao ramo das ciências pós-modernas e possui característica interdisciplinar. Le Coadic (2004, p. 25) a considerou uma ciência social rigorosa que se apoia em uma tecnologia também rigorosa. Seu objeto de estudo são as propriedades gerais da informação (natureza, gênese, efeitos) e a análise de seus processos de construção, comunicação e uso. No contexto de seu objeto de estudo, especificamente o processo de uso da informação, há de se falar em gestão do conhecimento e inteligência organizacional. Segundo Choo (1996), a gestão do conhecimento e a inteligência organizacional atuam como agentes estratégicos na determinação da capacidade de criação de conhecimento e adaptação de uma organização. Para implementação eficaz da gestão do conhecimento e da inteligência numa organização, faz-se necessária a existência de um processo de gestão da informação, pois requer aquisição, extração, organização e disseminação de informações necessárias à rotina organizacional (AHMAD; MING; RAFI, 2018).

Tendo por base a gestão da informação para a gestão do conhecimento e a inteligência organizacional, o tema Segurança da Informação assume importância, pois visa à proteção dos ativos organizacionais da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2014). Ademais, a Segurança da Informação também é tida como uma ciência interdisciplinar apresentada como um ramo internacional de pesquisa em ciências e tecnologia para a segurança humana. Segundo Aven (2014), a segurança da informação se estende desde a segurança das pessoas em seu local de trabalho até os aspectos relacionados ao transporte, recreação e outros campos considerados de risco nas atividades humanas.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

Considerando o aspecto interdisciplinar, comum entre a Segurança da Informação e a Ciência da Informação, este trabalho tem por objetivo principal identificar quais são as principais contribuições da Ciência da Informação para a Segurança da Informação. Outrossim, será respondida a seguinte questão problema: quais são as contribuições da Ciência da Informação para a Segurança da Informação? Busca-se justificar essa questão sob o argumento de que Unidades de Informação, tais como as bibliotecas e os arquivos em organizações públicas e privadas comumente tornam-se custodiantes de ativos informacionais considerados de acesso restrito e, portanto, sensíveis: essas informações requerem ações diferenciadas desde o seu nascimento, passando pelo manuseio, transporte, utilização, acondicionamento até o eventual descarte ou reúso. A não observância de procedimentos de gestão em segurança da informação trará riscos, ameaças e vulnerabilidades aos negócios de uma organização e, por consequência, perdas financeiras, estratégicas e de imagem (DAWEL, 2005). Metodologicamente, foi utilizada uma abordagem exploratória para apresentação dos temas centrais deste estudo e um levantamento bibliográfico aos moldes do proposto por Gil (2010) foi realizado. Os resultados encontrados serão apresentados qualitativamente, considerando as barreiras de segurança da informação de Sêmola (2014) (variáveis) e as intersecções encontradas na Ciência da Informação que foram explicitadas no artigo de Saracevic (1996). Ao final, ficou evidenciada a potencial contribuição da Ciência da Informação para dirimir riscos, ameaças e vulnerabilidades nos processos de gestão de segurança da informação em organizações.

O presente artigo é resultado das primeiras inferências da pesquisa de doutorado dos autores em Gestão e Organização do Conhecimento, em andamento, na Escola de Ciência da Informação da UFMG. Nas seções subsequentes, será apresentado o referencial teórico dos temas Ciência da Informação e Segurança da Informação. Posteriormente, os aspectos metodológicos do estudo realizado e os resultados encontrados também serão expostos. Por fim, as considerações finais com sugestões para trabalhos futuros.

2 DESENVOLVIMENTO

2.1 A interdisciplinaridade da Ciência da Informação

No âmbito internacional, um importante escrito que contribuiu para a análise e discussão sobre o que é o objeto de estudo da Ciência da Informação foi um artigo do

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

pesquisador americano Vannevar Bush (1945 *apud* SARACEVIC, 1996), que, preocupado com o número crescente das publicações ou materiais úteis para a pesquisa e desenvolvimento, pensou em um recurso que facilitasse aos cientistas e à sociedade em geral acesso a essas informações. Com objetivo de organizar e recuperar as informações de forma ágil, propôs a criação de uma máquina, Memory Extension (MEMEX). A proposta de Bush era que esse dispositivo idealizasse uma memória humana estendida que, através de associações, pudesse recuperar informações rapidamente, facilitando assim a sua utilização. Lembrando que o mecanismo de recuperação da época era baseado em sistemas manuais de indexação através de palavras-chaves (SARACEVIC, 1996).

O pós-Segunda Guerra trouxe novos paradigmas para o mundo moderno. A quantidade da informação produzida e registrada vem crescendo exponencialmente, e tratar esse volume exponencial de forma a recuperar a precisão e a relevância tornou-se, desde o surgimento da Ciência da Informação, um ramo de pesquisa bastante desafiador. Calvin Mooers (1951)¹ *apud* Saracevic (1996, p. 44) cunhou o termo recuperação da informação, destacando que ele engloba os aspectos intelectuais da descrição de informações e suas especificidades para a busca, além de quaisquer técnicas, máquinas ou sistemas empregados para o desempenho da operação.

Considerando os problemas da informação, a recuperação da informação tornou-se uma solução bem-sucedida encontrada pela Ciência da Informação. Para Saracevic (1996), toda solução suscita seus próprios e específicos problemas, assim também a recuperação da informação e esses problemas estão contidos na concepção proposta por Mooers (1951)¹ *apud* Saracevic (1996, p. 44): “Como descrever intelectualmente a informação? Como especificar intelectualmente a busca? Que sistemas, técnicas ou máquinas devem ser empregados?”.

Sob o prisma dos problemas da informação, tal qual a recuperação da informação, a Ciência da Informação surge como uma ciência interdisciplinar composta pelas áreas da Biblioteconomia, Ciência da Computação, Ciência Cognitiva e Comunicação. Saracevic (1996) apresenta um marco teórico fundamental para a compreensão daquilo que é a Ciência da Informação. Esse marco teórico apresenta a evolução da definição dessa ciência. Analisar os

¹MOOERS, C.N. Zatocoding applied to mechanical organization of knowledge. *American Documentation*, [s.l.], v. 2, p. 20-32, 1951.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

enunciados destas definições nos permitirá entender a interdisciplinaridade dessa ciência e, posteriormente, identificar suas contribuições para a Segurança da Informação:

Quadro 1 – Evolução das definições da Ciência da Informação

AUTOR	DEFINIÇÃO	CONCEITOS IMPORTANTES
BORKO (1968) ²	CI é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam seu fluxo e os meios de processá-la para otimizar sua acessibilidade e uso. A CI está ligada ao corpo de conhecimentos relativos a: origem, coleta, organização, estocagem, recuperação, interpretação, transmissão, transformação e uso de informação. Ela tem tanto um componente de ciência pura, através da pesquisa dos fundamentos, sem atentar para sua aplicação, quanto um componente de ciência aplicada, ao desenvolver produtos e serviços.	Organização da informação. Uso da informação. Etimologia da Ciência da Informação. Ciências sociais aplicadas.
GOFFMAN (1970) ³	O objetivo da disciplina CI deve ser o de estabelecer um enfoque científico homogêneo para estudo dos vários fenômenos que cercam a noção de informação, sejam eles encontrados nos processos biológicos, na existência humana ou nas máquinas. Consequentemente, o assunto deve estar ligado ao estabelecimento de um conjunto de princípios fundamentais que direcionam o comportamento em todo processo de comunicação e seus sistemas de informação associados. A tarefa da CI é o “estudo das propriedades dos processos de comunicação que devem ser traduzidos no desenho de um sistema de informação apropriado para uma dada situação física”.	Fenômenos e processos da informação. Comunicação humana. Uso da informação. Contexto social, individual e institucional.

²BORKO, H. Information science: what is it? *American Documentation*, v. 19, n.1, p. 3-5, 1968.

³GOFFMAN, W. Information science: discipline or disappearance. *ASLIB Proceedings*, v. 22, n.12, p. 589-596, 1970.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

KOCHEN (1974) ⁴	Podemos conceitualizar o sistema de conhecimento, no qual se inscreve a recuperação de informação, como composto por três partes: (a) as pessoas em seu papel de processadores de informações; (b) os documentos em seu papel de suportes de informações; (c) os tópicos como representações. Estamos interessados no ciclo de vida de cada um desses três objetos e na dinâmica de interação entre eles. Portanto, devemos considerar a variável comum aos três tempos.	Organização da Informação (OI). Sistemas de Recuperação da Informação (SRI). Registros do conhecimento. Necessidades de informação.
BELKIN & ROBERTSON (1976) ⁵	O propósito da CI é facilitar a comunicação de informações entre seres humanos.	Comunicação humana.
BECKER (1976) ⁶	CI como o estudo do modo pelo qual as pessoas criam, usam e comunicam informações.	Usos da informação. Tecnologia da informação. Comunicação humana.
SARACEVIC (1996)	A CI é um campo dedicado às questões científicas e à prática profissional voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. No tratamento dessas questões, são consideradas de particular interesse as vantagens das modernas tecnologias informacionais.	Efetividade. Comunicação humana. Conhecimento. Registros do conhecimento. Necessidades de informação. Usos da informação. Contexto social, institucional e individual. Tecnologia da informação.

Fonte: Adaptado de SARACEVIC, 1996, p. 45-47.

Para Saracevic (1996), a interdisciplinaridade foi introduzida na Ciência da Informação pela própria variedade da formação de todas as pessoas que se ocuparam com os problemas dos processos da informação. Esse autor elucida as relações interdisciplinares entre a Ciência da Informação e quatro campos: Biblioteconomia, Ciência da Computação, Ciência Cognitiva e Comunicação. Para ele, outros campos também mantêm relações interdisciplinares, mas nenhum desenvolveu-as de forma tão pronunciada e significativa como esses quatro. A seguir, apresentaremos as intersecções entre a Ciência da Informação e cada um dos quatro campos:

- Biblioteconomia: o aspecto em comum consiste no compartilhamento de seu papel social e sua preocupação comum com os problemas da efetiva utilização dos registros gráficos. As atividades realizadas sob o olhar biblioteconômico não devem ser vistas apenas como uma organização particular ou um tipo de sistema de informação (acervos organizados de uma biblioteca, por exemplo), mas, principalmente, como uma instituição social, cultural e educacional indispensável, de valor comprovado muitas vezes ao longo da história humana e através das fronteiras das diferentes culturas, civilizações, nações e épocas (SARACEVIC, 1996).

⁴KOCHEN, M. *Principles of information retrieval*. Los Angeles: Melville, 1974.

⁵BELKIN, N.; ROBERTSON, S. Information science and the phenomenon of information. *Journal of American Society for Information Science*. v. 34, n. 4, p. 197-204, jul. / ago. 1976.

⁶BECKER, J. *The first book of information science*. Washington – DF, Energy Research and Develop, 1976.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

- Ciência da Computação: a relação reside na aplicação dos computadores e da computação na recuperação da informação, assim como nos produtos, serviços e redes associados. A Ciência da Computação trata de algoritmos que transformam informações enquanto a Ciência da Informação trata da natureza da informação e sua comunicação para uso pelos humanos. Ambos os objetos são inter-relacionados e não competidores, mas complementares.
- Ciência Cognitiva: seu objetivo é explicar como funciona a mente humana. Embora existam diversos enfoques de pesquisa, os campos que compõem a Ciência Cognitiva compartilham um interesse básico acerca da compreensão dos processos cognitivos, sua realização no cérebro, a estrutura da mente e várias manifestações da mente como inteligência. Na Ciência Cognitiva, o computador desempenha um importante papel, tanto como ferramenta quanto como fonte de modelagem e teste. Exatamente nessa relação forte com os sistemas computacionais surge a relação da Ciência Cognitiva e a Ciência da Informação, tendo como principal elo a Inteligência Artificial (IA). De forma geral, a Inteligência Artificial é a fonte do modelo teórico da cognição, no qual a informação, enquanto fenômeno, desempenha o mais importante papel. Portanto, esse modelo pode também contribuir para a pesquisa básica em Ciência da Informação.
- Comunicação: desenvolvimento da relação entre a Ciência da Informação e a Comunicação apresenta várias dimensões: um interesse compartilhado na comunicação humana, juntamente com a crescente compreensão de que a informação como fenômeno e a comunicação como processo devem ser estudadas em conjunto; uma confluência de certas correntes de pesquisa; algumas permutas entre professores; e o potencial de cooperação na área da prática profissional e dos interesses comerciais/empíricos. Para Saracevic (1996), de forma geral, a busca pelo significado da palavra comunicação e da palavra informação acaba por esbarrar numa discussão por si mesma. Os debates e pesquisas acadêmicos acabam por considerar a relação da informação enquanto fenômeno e a comunicação como um processo.

A seguir apresentamos o tema gestão da Segurança da Informação e seus desafios no mundo contemporâneo.

2.2 A gestão da Segurança da Informação para as organizações

No mesmo caminho da Ciência da Informação, a Segurança da Informação consolidou-se enquanto ciência a partir da segunda metade do século XX. Assim, a busca por uma gestão da informação eficiente e eficaz cumpre um papel vital na gestão dos negócios em organizações (CHOO, 1996). Para Sêmola (2014), todas as organizações, independentemente de seu *core business* e porte, em todas as fases de sua existência, sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, ganhos de *market share*, aumento de agilidade, competitividade e apoio mais eficiente aos processos de tomada de decisão.

Sêmola (2014, p. 41) define Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Para esse autor, devemos entender “informação” como um conjunto de dados utilizados para a transferência de uma mensagem entre os indivíduos e/ou máquinas em processos comunicativos ou transacionais. Já ativos, como sendo todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada, os equipamentos em que é manuseada, transportada e descartada.

Goodrich e Tamassia (2013) consideram a Segurança da Informação definida a partir dos termos do acrônimo CID (Confidencialidade, Integridade e Disponibilidade). Nesse sentido, Confidencialidade tem por objetivo não revelar a informação a pessoas não autorizadas. Já integridade é a propriedade de que a informação não foi alterada de forma não autorizada. Por fim, disponibilidade é propriedade da informação que está acessível no momento oportuno para aqueles que estejam autorizados a fazer isto. Além dos conceitos clássicos de Segurança da Informação (CID), existem diversos conceitos adicionais importantes nas aplicações modernas de Segurança da Informação. Esses conceitos podem ser caracterizados por outro acrônimo: Garantia, Autenticidade e Anonimato (GAA). Garantia se refere a como a confiança é fornecida e gerenciada em sistemas de computação. Autenticidade é a habilidade de determinar que afirmações, políticas e permissões oriundas de pessoas ou sistemas são genuínas. Por último, o Anonimato é a propriedade de que certos registros ou transações não sejam atribuíveis a qualquer indivíduo. Diferentemente dos conceitos do CID, os conceitos GAA são independentes entre si. Além disso, os conceitos do GAA vão além do CID, eles querem proteger e gerenciar a maneira como a informação é utilizada.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

Para Silva e Stein (2007), a maioria das definições de Segurança da Informação pode ser sumarizada como a proteção contra o uso ou acesso não autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. Para essas autoras, a Segurança da Informação não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio dela. É importante lembrar que a segurança da informação também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias e outros. Embora, na prática, não se possa erradicar completamente o risco de uso impróprio ou mal-intencionado de qualquer informação, muitos esforços já foram feitos no sentido de aprimorar os sistemas de segurança da informação.

Dentre esses esforços, um que merece destaque é a publicação da Norma ISO/IEC 27001 (2013), que tem por objetivo estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para a necessidade da organização.

Para Sêmola (2014), ameaças, riscos, vulnerabilidades, impactos e incidentes são conceitos essenciais que devem ser considerados quando da criação de um sistema de gestão da segurança da informação dentro do contexto de uma organização. Entendê-los permitirá implementar ações de segurança da informação. A seguir, apresentaremos uma breve explicação desses conceitos:

- ameaças: são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando a perda de confidencialidade, integridade e disponibilidade, e, conseqüentemente, causando impactos aos negócios da organização. Podem ser classificadas como naturais (terremotos, incêndios naturais, poluição etc.), involuntárias (acidentes, erros, falta de energia etc.); voluntárias (agentes humanos como hackers, invasores, espiões, disseminadores de vírus de computadores etc.);
- impactos: abrangência dos danos causados por um incidente de segurança sobre um processo da organização;

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

- incidente: evento decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: CID;
- riscos: probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, conseqüentemente, trazendo impactos ao negócio da organização;
- vulnerabilidades: são fragilidades presentes ou associadas a ativos que manipulam ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação: CID. Como exemplos de vulnerabilidades, consideram-se: instalações prediais que não atendem às normas e regulamentações vigentes; equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais; equipamentos *hardwares* suscetíveis a poeira, umidade, sujeira; acessos indevidos a recursos inadequadamente protegidos; comunicação telefônica ou amplificador suscetível a interceptação para escuta e roubo de informações; falta de treinamento ou conscientização das pessoas; falta de avaliação psicológica adequada ou de verificação de antecedentes que identifiquem objetivos escusos ou mesmo má-fé de uma parte interessada em potencial.

As ações (as práticas) em segurança da informação podem ser as mais diversas e sempre terão por objetivo evitar a perda dos princípios da segurança da informação. Ainda segundo Sêmola (2014), as ações de segurança da informação devem considerar barreiras de segurança. Cada barreira deve reduzir os riscos e, portanto, deve ser dimensionada para proporcionar a mais perfeita interação e integração para oferecer níveis de resistência e proteção complementares e tendenciosamente crescentes. Para esse autor, devem ser consideradas seis barreiras fundamentais:

- barreira 1 – desencorajar: a simples presença de uma câmera de vídeo, mesmo que falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança da informação ou treinamento dos funcionários informando sobre as práticas de auditoria e monitoramento de acesso aos sistemas são efetivos nessa etapa;
- barreira 2 – dificultar: dispositivos de controle de acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, biométricos, de senhas, de *smart cards* e de certificados digitais e firewall;

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

- barreira 3 – discriminar: processos de avaliação e gestão do volume de uso dos recursos, como e-mail, impressora ou mesmo o fluxo de acesso físico aos ambientes são bons exemplos das atividades dessa barreira;
- barreira 4 – detectar: entram os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intrusos, que reduziram o tempo de resposta de incidentes;
- barreira 5 – deter: aqui, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos;
- barreira 6 – diagnosticar: deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da organização.

Todas as ações de segurança, com o objetivo de proteger a informação nas organizações e permitir a continuidade dos processos de negócio, devem ser planejadas. Para isso, o estabelecimento de uma política de gestão da segurança da informação é necessário. Essa deve ser capaz de estabelecer padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a organização (SÊMOLA, 2014, p. 105). A norma ABNT NBR ISO/ IEC 27001 (2013, p. 3) orienta que a alta administração de uma organização é a responsável por estabelecer uma Política de Segurança da Informação, e que esta deve: “estar disponível como informação documentada, ser comunicada dentro da organização, estar disponível para as partes interessadas, conforme apropriado”.

Segundo estudo realizado pelo *Pricewaterhouse Coopers* (CIO, 2013), considerando os depoimentos de todos os respondentes, cada vez que um sistema de uma organização é invadido, esta gasta cerca de US\$531 dólares. Segundo o website CIO (2013), esse valor pode parecer pouco, mas há organizações que recebem, por dia, mais de mil ataques. O estudo revelou que cerca de 24% dos respondentes relataram ter perdido dados em consequência de incidentes de segurança. Os registros de funcionários (35%) e de clientes (31%) comprometidos lideraram a lista de categorias de dados afetados. Entre as indústrias que informaram perdas de 10 milhões de dólares ou mais está a farmacêutica (20%), serviços financeiros (9%) e tecnologia (9%). A maioria dos respondentes atribuiu os incidentes de

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

segurança a inimigos internos conhecidos, como funcionários ativos (31%) ou ex-funcionários (27%). Alguns inimigos conhecidos cumpriram o seu potencial de risco externo: 32% dos inquiridos atribuíram incidentes de segurança a *hackers*. A segurança ainda foi considerada falha em algumas áreas – 52% não implantaram ferramentas de monitorização e definição de perfis de comportamento, e 46% não implantaram tecnologias de gestão de eventos e informações de segurança.

Para o Centro de Estudos, Resposta e Tratamento de Incidentes do Brasil (CERT-BR, 2019), responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira, o acréscimo do número de incidentes e ataques contra a segurança da informação vem aumentando exponencialmente. De forma contundente, a atuação humana foi que conduziu à quebra de um dos pilares de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Para uma organização, seja ela pública seja privada, ter em sua rotina boas práticas em gestão de segurança da informação vai de encontro à realidade das estatísticas desanimadoras sobre incidentes de segurança da informação.

A discussão teórica sobre o que é Ciência da Informação e Segurança da Informação e quais os seus campos de atuação nos permitirá identificar pontos comuns entre essas ciências e, conseqüentemente, atingir o objetivo principal do trabalho: identificar as contribuições da Ciência da Informação para a Segurança da Informação. Os resultados dessa análise teórica são apresentados a seguir.

3 METODOLOGIA

Pode-se classificar essa investigação como uma pesquisa exploratória – na medida em que buscou maior familiaridade com os temas centrais da questão problema para torná-los mais explícitos – e, concomitantemente, como uma pesquisa bibliográfica – realização de levantamento bibliográfico com o propósito de fornecer fundamentação teórica ao estudo e a identificação do atual estágio das pesquisas sobre os temas (GIL, 2010).

Utilizaram-se aqui as etapas metodológicas descritas por Gil (2010, p. 45) para delinear a pesquisa bibliográfica:

- escolha do tema: foram pesquisados os dois temas centrais da questão problema: Ciência da Informação e Segurança da Informação;

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

- levantamento bibliográfico preliminar: foi utilizada nesta etapa a seleção de livros, teses e monografias com o propósito de dar uma visão geral dos temas e de seus respectivos objetos de estudo;
- elaboração do plano provisório da pesquisa: nesta etapa, foram definidos os subtemas abordados tanto para a Ciência da Informação como para a Segurança da Informação. Os subtemas definidos foram: definições, objeto de estudo (objeto empírico tanto da Ciência da Informação como da Segurança da Informação), características gerais (campo de atuação, pesquisas atuais, etc);
- uso de fontes de informação para pesquisa: foram consultadas diversas bases de dados (*Scopus, Scielo, Proquest, Jstor e Google Acadêmico*). Como estratégia de busca, utilizaram-se as palavras-chaves “ciência da informação” e “segurança da informação”, conjuntamente. Damos preferência aos resultados posteriores a 2005. Aqui, salientamos a dificuldade em recuperar informações que contenham, genuinamente, os dois temas acima descritos e publicados dentro de um contexto de Ciências Sociais Aplicadas;
- levantamento de material com a questão problema semelhante ao estudo deste artigo: durante a análise dos resultados das buscas em fontes de informação, buscamos por trabalhos com objetivo semelhante ao deste. Foi recuperado o trabalho de Ramos (2007), que traz uma proposta de contribuição da Ciência da Informação para a construção de um Plano de Segurança da Informação, porém direcionada à qualidade da informação. A proposta aqui foi mais ampla:
- leitura do material recuperado nas fontes de informação consultadas;
- análise de termos, conceitos e definições sobre Ciência da Informação e Segurança da Informação: a fim de obter os relacionamentos entre as duas áreas e, então, identificar as contribuições da primeira sobre a segunda;
- organização das ideias e redação dos resultados encontrados, que serão apresentados na próxima seção.

4 DISCUSSÃO E RESULTADOS

Para a apresentação e discussão dos resultados, tomou-se por base o conceito de Ciência da Informação enquanto campo interdisciplinar. Para tanto, as intersecções entre a Ciência da Informação e as diversas áreas do conhecimento foram fundamentais (SARACEVIC,

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

1996). Por outro lado, as barreiras de segurança da informação, propostas por Sêmola (2014), serão nossas variáveis: onde a Ciência da Informação apresentou suas contribuições.

A primeira área – Biblioteconomia – apresentada por Saracevic (1996) como parte da Ciência da Informação traz contribuições fundamentais para o desenvolvimento e aplicação de uma política de segurança da informação em organizações. Em especial, relativas à gestão das informações (AHMAD; MING; RAFI, 2018). Tal como argumentado nas seções anteriores, um dos fundamentos para a gestão do conhecimento organizacional é a gestão da informação. Por derradeiro, essa deve ser considerada a “pedra angular” do pilar disponibilidade em segurança da informação (GOODRICH; TAMASSIA, 2013; SEMOLA, 2014).

A Ciência da Computação trará contribuições relativas à tecnologia da informação, atuando em todos os pilares da Segurança da Informação. A norma ABNT ISO/IEC 27001 (2013) ratifica esse entendimento na medida em que apresenta os critérios essenciais para a implementação da segurança da informação em diversas áreas: segurança física, lógica, das pessoas, dos computadores, das redes, dos aplicativos etc. Em todas essas áreas, a Ciência da Computação tem uma atuação de destaque.

Concomitantemente à Ciência da Computação, a Ciência Cognitiva traz importantes avanços relativos ao desenvolvimento de controles de segurança inteligentes. Nesse sentido, a Inteligência Artificial tem atuação fundamental visando ao desenvolvimento de sistemas tecnológicos inteligentes que permitam a manutenção dos princípios de segurança frente às novas ameaças e vulnerabilidades em SI. No atual cenário de virtualização dos processos nas organizações (como, por exemplo, ações de transformação digital), novas tecnologias vêm surgindo. Não obstante, várias organizações já utilizam recursos de *cloud computing* (computação em nuvem), mobilidade e BYOD (*Bring Your Own Device*) e buscam inovação frente a um cenário de *Big Data* e mídias sociais. A tecnologia da informação fundamentada em princípios da Ciência Cognitiva (tal como a Inteligência Artificial) pode estimular o desenvolvimento de uma nova gestão em segurança da informação para organizações, que deverão: ser capazes de tratar grandes volumes informacionais; prever um equilíbrio entre confidencialidade e disponibilidade da informação; ser inovadoras e resilientes nos controles de segurança; e também serem democráticas, tal como as redes sociais.

Por fim, a última área – Comunicação – perpassa todo o processo de implementação e manutenção de uma política de segurança da informação em organizações. A norma ABNT ISO/IEC 27001 (2013) prevê ações a serem implementadas frente a um incidente de segurança

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

da informação. Argumenta-se, por exemplo, a previsibilidade da gestão de continuidade de negócios numa política de segurança da informação para organizações. Ademais, para Sêmola (2014), o grande desafio da gestão em segurança da informação é a conscientização do corpo organizacional: a sinergia entre definições e ações necessárias para a SI nos níveis operacional, tático e estratégico da organização.

Em suma, garantia dos pilares de segurança da informação nas organizações é um processo complexo que envolve ativos tangíveis e intangíveis e todos dos grupos de interesse de uma organização. Em função disso, deve-se planejar e implementar a Gestão da Segurança da Informação de forma interdisciplinar, tal como as áreas que compõem a Ciência da Informação e que foram defendidas há mais de 20 anos por SARACEVIC (1996). Somando-se a esse argumento, destaca-se que o objeto de estudo entre a CI e a SI é o mesmo: a informação.

O Quadro 2, a seguir, sintetiza a análise exploratória realizada, bem como as indicações potenciais de contribuição da Ciência da Informação para a Segurança da Informação.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

Quadro 2: Síntese das contribuições da Ciência da Informação para a Segurança da Informação

BARREIRA DE SEGURANÇA DA INFORMAÇÃO (SÊMOLA, 2014)	CONTRIBUIÇÃO DA CIÊNCIA DA INFORMAÇÃO. (SARACEVIC, 1996)	JUSTIFICATIVA
Barreira 1 – desencorajar: a simples presença de uma câmera de vídeo, mesmo que falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança da informação ou treinamento dos funcionários informando sobre as práticas de auditoria e monitoramento de acesso aos sistemas são efetivos nessa etapa.	Realização de estudos de usuários (Biblioteconomia e Ciência Cognitiva). Aplicação da Disseminação seletiva da Informação (Biblioteconomia). Construção de um Plano de Comunicação sobre conscientização (Comunicação).	Tanto a Comunicação como a Biblioteconomia, por meio de suas experiências com o objeto de estudo específico, poderão subsidiar o estudo da comunidade utilitária da informação para criar ações de desencorajamento mais eficazes e eficientes.
Barreira 2 – dificultar: dispositivos de controle de acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, biométricos, de senhas, de <i>smart cards</i> e de certificados digitais e <i>firewall</i> .	Estudos de leiaute (Organização e Métodos – Biblioteconomia). Aplicação de princípios de Inteligência Artificial (Ciência Cognitiva). Tecnologia de proteção para a informação digital (Ciência da Computação).	Sob a ótica da informação, a utilização da Biblioteconomia, Ciência Cognitiva e Ciência da Computação permitirá a criação de dispositivos de controle mais inteligentes, considerando as lições aprendidas, características de hardware e software, espaço físico e comportamento dos usuários da informação.
Barreira 3 – discriminar: os processos de avaliação e gestão do volume de uso dos recursos, como e-mail, impressora ou mesmo o fluxo de acesso físico aos ambientes são bons exemplos das atividades dessa barreira.	Tecnologia da Informação para estatísticas (Ciência da Computação). Comportamento humano (Ciência Cognitiva).	Aqui é necessário obter recursos que permitam a gestão de acessos, definição de perfis e concessão de permissões aos usuários da informação. É vital a criação de sistemas de gestão inteligentes que reproduzam a mente humana e que sejam de ponta tecnologicamente.
Barreira 4 – detectar: entram os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intrusos, que reduziram o tempo de resposta de incidentes.	Desenvolvimento de softwares (Ciência da Computação). Inteligência Artificial (Ciência Cognitiva).	Como na Barreira 3, por meio do estudo de como pensamos, a Ciência Cognitiva deve auxiliar a Ciência da Computação a desenvolver sistemas capazes de detectar ameaças à segurança da informação: detectar intrusos, vírus, DoS etc.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

Barreira 5 – deter: aqui, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.	Desenvolvimento de um Plano de Comunicação (Comunicação). Desenvolvimento de uma Política de Segurança da Informação através da normalização documentária (Biblioteconomia).	Na organização devem estar estruturadas (claras) as regras de uso da informação. A Biblioteconomia auxiliará a estruturar um documento formal sobre o assunto. Depois, as ações punitivas para deter eventuais delinquentes devem ser conhecidas por todos. Nesse sentido, a Comunicação das informações nos será eficaz.
Barreira 6 – diagnosticar: deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da organização.	Análise de risco utilizando a técnica de representação temática da informação (Biblioteconomia). Gestão da Informação através da Gestão do Conhecimento (Biblioteconomia e Comunicação).	Essa barreira pode permitir a continuidade do processo de segurança da informação. A análise de riscos pode ser aprimorada por meio de técnicas como a representação temática da informação oriunda da Biblioteconomia: buscar-se-á representar os assuntos de um documento. Outra aplicabilidade é o processo de gestão da informação por meio da “gestão do conhecimento”: as lições aprendidas; o negócio intangível da organização em se tratando de gestão de segurança da informação deve tornar-se tangível, registrado.

Fonte: Desenvolvido pelos autores, 2019.

5 CONSIDERAÇÕES FINAIS

A partir da apresentação dos temas centrais deste artigo – Ciência da Informação e Segurança da Informação e, considerando as definições de cada ciência, as características mais importantes e o fato de possuírem a informação como objeto de estudo, constatarem-se diversas contribuições da Ciência da Informação para a implementação de barreiras de proteção em Segurança da Informação.

Notamos que as vulnerabilidades, ameaças, riscos, impactos e incidentes em Segurança da Informação, comumente, possuem os computadores como vetores de ataque. Todavia, por meio da análise dos principais incidentes em segurança citados pelo CERT-BR em 2019, ficou evidente que a atuação humana foi que conduziu à quebra dos pilares de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Essa constatação permitiu identificar não apenas aspectos tecnológicos, mas também aplicações relativas ao comportamento humano e relativas à administração de unidades de informação. Assim sendo,

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

as contribuições da Ciência da Informação apresentaram-se sob o campo tecnológico (Ciência da Computação) e também sob técnicas oriundas da Biblioteconomia, Ciências Cognitivas e Comunicação.

Esperamos que os apontamentos aqui feitos sirvam de insumos para o desenvolvimento de novos trabalhos, bem como sejam um agente direcionador para a pesquisa de doutorado já iniciada pelos autores no primeiro semestre de 2019.

Como trabalhos futuros e temas para aprofundamento, destacam-se:

1. desenvolvimento de uma metodologia de análise de riscos em Segurança da Informação tendo por base a aplicabilidade da técnica de representação temática da informação oriunda da Ciência da Informação, mais especificamente da Biblioteconomia;
2. redação de uma Política de Segurança da Informação, tendo como aporte teórico a realização de um estudo de usuários da informação, tais quais os realizados em unidades de informação ou mesmo em pesquisas de Comunicação;
3. contribuições da Ciência da Informação, mais especificamente da Comunicação, para a criação de um plano de comunicação/divulgação da política de segurança da informação dentro de uma organização;
4. desenvolvimento de sistemas inteligentes para a detecção de intrusos, considerando aspectos da Ciência Cognitiva, mais especificamente da Inteligência Artificial. Que sejam capazes de retroalimentar células de desenvolvimento de softwares que minimizem os riscos de ataques a informações de acesso restrito numa organização.

Por fim, pôde-se concluir que o objetivo principal deste artigo foi alcançado. Foram identificadas várias potenciais contribuições da Ciência da Informação para a Segurança da Informação.

REFERÊNCIAS

AHMAD, Khurshid; MING, Jian; RAFI, Muhammad. Assessing the literature of knowledge management (KM) in the field of library and information science. *Information Discovery and Delivery*, v. 47, n. 1, p. 14–23, 2018.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013. 30 p.

AVEN, Terje. What is safety science. *Safety Science*. Stavanger, Norway, v. 67, p. 15-20, 2014. Disponível em: < <https://www-sciencedirect.ez27.periodicos.capes.gov.br/science/article/pii/S0925753513001768> > Acesso em: 12 set. 2019.

CARVALHO, Larissa Akabochi de; CRIPPA, Giulia. Ciência da informação: histórico, delimitação do campo e a sua perspectiva sobre a área da comunicação. *Perspectivas em Ciência da Informação*, Belo Horizonte, v. 18, n. 4, p. 241-251, out./dez. 2013.

CERT-BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. 2019. Disponível em: < <http://www.cert.br/> >. Acesso em: 12 jul. 2019.

CIO. Incidentes de segurança da informação crescem 25% em 2013. Publicado em: 27 dez. 2013. Disponível em: < <https://cio.com.br/incidentes-de-seguranca-da-informacao-crescem-25-em-2013-afirma-pwc/> >. Acesso em: 12 set. 2019.

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

DAWEL, George. *A segurança da informação nas empresas*: ampliando horizontes além da tecnologia. Rio de Janeiro: Ciência Moderna, 2005. 116 p.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5. ed. São Paulo: Atlas, 2010.

GOODRICH, Michael T.; TAMASSIA, Roberto. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013.

KOBASHI, Nair; TALAMO, Maria de Fátima Gonçalves Moreira. Informação: fenômeno e objeto de estudo da sociedade contemporânea. *Transinformação*, Campinas, p. 7-21, set./dez. 2003. Edição especial.

LE COADIC, Yves-François. *A ciência da informação*. 2. ed. Brasília: Brinquet de Lemos, 2004.

RAMOS, Isaías de Queiros. *Contribuições da ciência da informação para a criação de um plano de segurança da informação*. 2007. 117 f. Trabalho de conclusão de curso. (Especialização em Ciência da Informação) – Pontifícia Universidade Católica de Campinas, Campinas, 2007.

SARACEVIC, Tefko. Ciência da informação: origens, evolução e relações. *Perspectivas em Ciência da Informação*, Belo Horizonte, v. 1, n. 1, p. 41-62, jan./ jun. 1996.

XX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2019
21 a 25 de outubro de 2019 – Florianópolis – SC

SARACEVIC, Tefko. Information Science. *Journal of the American Society for Information Science*, v. 50, n. 12, p. 1051-1063, 1999.

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

SILVA, Denise Ranghetti Pilar da; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, Porto Alegre, v. 10, 2007; p. 46-53. Disponível em: < <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf> >. Acesso em: 12 set. 2019.