Ontologia para o Gerenciamento de Segurança da Informação em Sistemas-de-Sistemas

Roberto Monteiro Dias[1], **Rodrigo Oliveira Zacarias (Colaborador)**[1], **Rodrigo Pereira dos Santos (Orientador)**[1]

[1]Programa de Pós-Graduação em Informática (PPGI)
Universidade Federal do Estado do Rio de Janeiro (UNIRIO) - Rio de Janeiro - RJ

{roberto.dias,rodrigo.zacarias}@edu.unirio.br,
rps@uniriotec.br

Abstract. *The intense transformations that took place in society in this decade made information systems (IS) more complex. Such complexity relates to a category of systems defined as system-of-systems or simply SoS. Although SoS offer benefits to organizations, the inability of IT managers to deal with information security in these systems can leave them vulnerable to threats and impacts caused by cyber attacks. The goal of this research is to develop a domain ontology to support IT managers in decision-making on information security issues in the context of SoS. To do so, a methodological approach is proposed, consisting of literature review, systematic mapping study, ontology construction, survey research, and evaluation with experts, including a participative case study. This research aims at contributing to the creation of an ontology to aid IT managers holding SoS as well as researchers investigating the field. Moreover, it is expected a technical and practical understanding so that IT managers can prevent risks, vulnerabilities, and threats in a SoS.*

Resumo. *As intensas transformações ocorridas na sociedade nesta década tornaram os sistemas de informação (SI) mais complexos. Tal complexidade se relaciona a uma categoria de sistemas definida como sistema-de-sistemas ou simplesmente SoS (do inglês, systems-of-systems). Embora SoS ofereçam benefícios às organizações, a dificuldade dos gestores de TI em lidar com a segurança da informação nesses sistemas pode deixá-los vulneráveis a ameaças e impactos causados por ataques cibernéticos. Nesse contexto, o objetivo desta pesquisa é desenvolver uma ontologia de domínio para apoiar gestores de TI na tomada de decisão em questões de segurança da informação em SoS. Para isso, é proposta uma abordagem metodológica composta de revisão da literatura, mapeamento sistemático da literatura, construção da ontologia, pesquisa de opinião e avaliação com especialistas, incluindo um estudo de caso participativo. Esta pesquisa almeja como contribuição a criação de uma ontologia para utilização dos gestores de TI das organizações detentoras de um SoS ou por pesquisadores da área. Também é esperado o entendimento técnico e prático para que esses gestores possam evitar que os riscos, as vulnerabilidades e as ameaças sejam explorados no SoS.*

1. Introdução

As intensas transformações ocorridas na sociedade nesta década tornaram os sistemas de informação (SI) mais complexos. Tal complexidade relaciona a uma categoria de sistemas

denominada sistema-de-sistemas ou simplesmente SoS (do inglês, *systems-of-systems*). Um SoS consiste em um sistema complexo que compreende outros sistemas (os sistemas constituintes), que possuem independência operacional e gerencial, distribuição geográfica, comportamento emergente e desenvolvimento evolucionário [Maier 1998]. Além dessas características principais, eles também são intensivos em dados e possuem heterogeneidade [Sommerville 2016]. As cidades inteligentes são um exemplo notável de SoS porque apresentam todas essas características onde diferentes dispositivos e SI atuam para oferecer serviços à população por meio da colaboração de diversas organizações públicas e/ou privadas proprietárias desses sistemas [Fernandes et al. 2019].

De acordo com Boscarioli et al. (2017) nos Grandes Desafios da Pesquisa em SI no Brasil 2016-2026 (GranDSI-BR), transparência e interoperabilidade em SoS ainda são desafios na área de SI, devido à alta dinamicidade de sua arquitetura. Assim, a ocorrência de falhas de segurança da informação, como perda ou acesso não autorizado a dados confidenciais durante a comunicação entre os sistemas constituintes, pode colapsar um SoS e acarretar diversos problemas para o negócio de uma organização.

Em cenários como estes, ainda falta responder à questão de como abordar a segurança da informação de modo a permitir que os gestores de TI possam compreendê-la sem dificuldades. Compreende-se segurança da informação como a proteção da informação e seus elementos críticos, incluindo os sistemas e hardware que usam, armazenam e transmitem a informação [Whitman e Mattord 2009]. Essa definição está relacionada como a preservação da **C**onfidencialidade, **I**ntegridade e **D**isponibilidade de informações (tríade CID) [Malagutti 2016].

Assim, os gestores de TI precisam ser orientados sobre a implementação da segurança da informação no SoS. Por exemplo, eles podem encontrar dificuldades para minimizar os riscos gerados por falhas humanas. Como consequência, por não estarem atentos às questões de segurança, eles podem cometer uma série de erros que aumentariam as oportunidades de ataques cibernéticos serem bem-sucedidos.

Pesquisadores consideram que as ontologias podem ser utilizadas como solução para esse problema porque elas definem estruturas de conhecimento e promovem um entendimento compartilhado de um domínio, tarefa ou aplicação [Chandrasekaran e Benjamins 1998]. Guarino (1998) define uma taxonomia em que considera que ontologias de domínio descrevem o vocabulário de um domínio específico do conhecimento, definindo-o e o caracterizando. A contribuição para o seu uso é a padronização de conceitos, termos e definições, bem como facilidade do compartilhamento de informações para fazer suposições mais explícitas e auxiliar na análise do conhecimento e das relações do domínio.

Nesse sentido, o objetivo desta pesquisa é desenvolver uma ontologia de domínio para apoiar gestores de TI na tomada de decisão em questões de segurança da informação no contexto de SoS. Para isso, é proposta uma abordagem metodológica composta por revisão da literatura, mapeamento sistemático da literatura, construção da ontologia, pesquisa de opinião e avaliação com especialistas, incluindo um estudo de caso participativo. Além da introdução, o artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; na Seção 3, é apresentada a metodologia; a Seção 4 traz o estado atual da pesquisa; e a Seção 5 aponta as contribuições esperadas.

2. Trabalhos relacionados

Em um estudo exploratório de um caso real, Dias et al. (2020) modelaram as tensões na gestão de sistemas de informação federados (SIF) do Programa Bolsa Família (PBF) por meio do uso da Ontologia de Processo Intensivo em Conhecimento (do inglês, Knowledge *Knowledge Intensive Process Ontology*, ou KIPO). Os SIF são uma categoria de SoS que pertence a uma plataforma central que, em conjunto com outros SI, alcançam funcionalidades mais complexas que sozinhos não conseguiriam prover [Sommerville 2016]. Os autores demonstraram a ocorrência de intensas interações entre os sistemas que fazem parte do SIF no contexto do PBF apresentados no Diagrama de Regras de Negócios da KIPO. Isto demonstra a necessidade de garantir a CID nas trocas de informações entre esses sistemas no SIF.

No trabalho de Meriah et al. (2021), pode-se identificar que um dos problemas básicos relacionados à segurança da informação é a falta de uma visualização clara e simples nos SI organizacionais. A terminologia de segurança da informação não é precisamente definida e leva a discordâncias entre os *stakeholders* e os clientes desses sistemas. Eles apresentam como solução uma ontologia de domínio de segurança da informação para o campo de sistemas de informação.

Desse modo, os trabalhos corroboram com a importância da segurança da informação em SI. Além disso, também destacam a construção de uma ontologia de domínio que apoie a representação, recuperação e disseminação desse conhecimento.

3. Metodologia

A partir de uma revisão informal da literatura sobre os temas (SoS e segurança da informação), as demais atividades propostas neste projeto, conforme a Figura 1, são:

I. Estudo Exploratório com o uso de KIPO para mapear tensões na gestão de SIF em um estudo de caso no Programa Bolsa Família [Dias et al. 2020];
II. Mapeamento Sistemático da Literatura (MSL) a partir dos conhecimentos obtidos na atividade I sobre o panorama de segurança da informação em SoS;
III. Pesquisa de opinião para avaliar os resultados obtidos do MSL junto a pesquisadores e profissionais em segurança da informação e SoS;
IV. Construção da ontologia para explicitar os fatores específicos, as principais metodologias de avaliação e tecnologias abordadas em segurança da informação em SoS que foram identificados no MSL;
V. Avaliação da ontologia por meio da aplicação de um grupo focal com especialistas para análise de sua sintaxe e semântica;
VI. Refinamento da ontologia com ajustes e correções sugeridos nas avaliações; e
VII. Realização de Estudo de Caso Participativo para verificar o uso da ontologia em um SoS real.

4. Estado atual da pesquisa

4.1. Mapeamento Sistemático da Literatura

Este trabalho teve como objetivo investigar como tecnologias de segurança da informação têm sido utilizadas no contexto de SoS e retornaram 18 estudos que apresentam uma profusão de métodos, técnicas, modelos e ferramentas com esse intuito. Os trabalhos

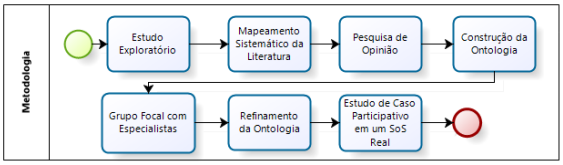

Figura 1. Metodologia aplicada nesta pesquisa.

apresentam diversas perspectivas de análise da temática e sua aplicação em diversos cenários que perpassam pelas dimensões técnicas, de negócio e social da área de SI.

Fatores de segurança da informação que afetam a escolha dos mecanismos de segurança implementados no SoS também foram identificados, como análise de pontos de vulnerabilidade, risco de ataques e integração de políticas de segurança de sistemas constituintes.

4.2. Ontologia SegInfoSoS

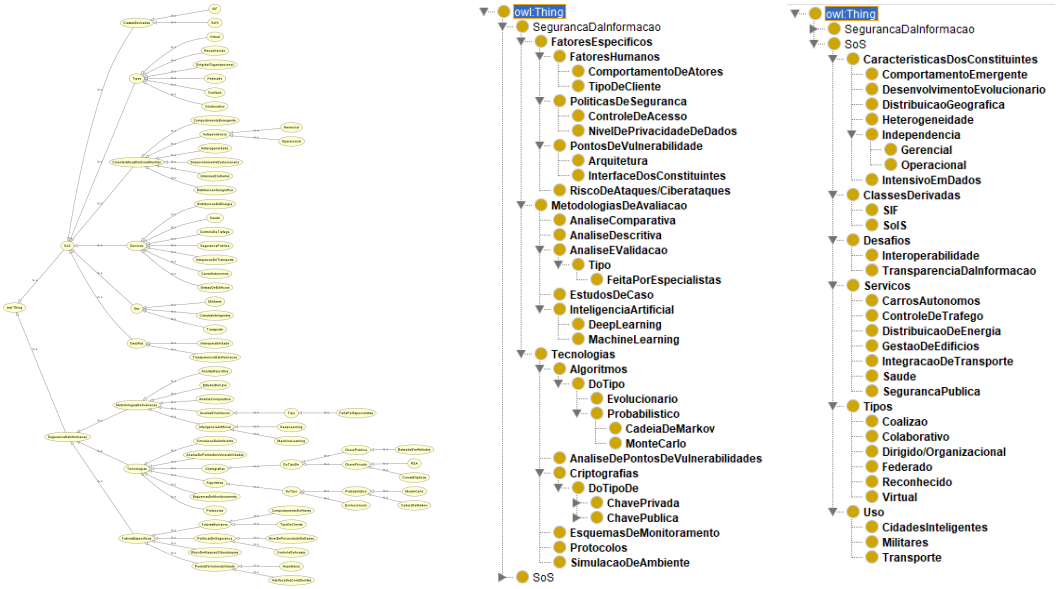

Figura 2. Ontologia SegInfoSoS (esquerda) e Hierarquia de Classes (direita) usando OWLViz no Protégé.

Um dos resultados obtidos neste trabalho foi a versão inicial da ontologia de segurança da informação em SoS (SegInfoSoS) em OWL *(Web Ontology Language)* desenvolvida com base nos resultados do MSL, utilizando o Método 101 proposto por [Noy e Mcguinness 2001] e o editor de ontologias *Protegé* [1]. A ontologia construída conta com 402 axiomas declarados, distribuídos em 75 classes, 8 propriedades de objetos e 3 propriedades de dados. Ela é apresentada na Figura 2, onde é possível ver os campos das classes e subclasses considerando três perspectivas: i) Fatores específicos da segurança da informação no SoS; ii) Principais metodologias de avaliação; e iii) Tecnologias aplicadas. Ela apresenta a resposta para a questão principal da pesquisa do MSL de como as tecnologias de segurança da informação têm sido utilizadas no contexto de um SoS.

[1]https://protege.stanford.edu/

Também foi desenvolvido um programa em Java com o uso de OWL API [2], apresentado na Figura 3, para execução da ontologia com o propósito de demonstrar a sua aplicabilidade, em questões relacionadas à segurança da informação, do ponto de vista de profissionais e pesquisadores, no contexto de SoS. Na Figura 3, são exibidas algumas questões de competência (1 a 7) definidas preliminarmente para execução de testes com a ontologia. Ela responde todas as questões de competência apresentadas. Na Figura 4, tem-se a demonstração do resultado da questão de competência 3 - Quais são os fatores específicos da segurança da informação no SegInfoSoS?

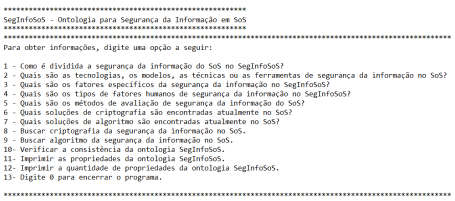

Figura 3. Programa em Java com o uso de OWL API para execução de testes com a ontologia SegInfoSoS.

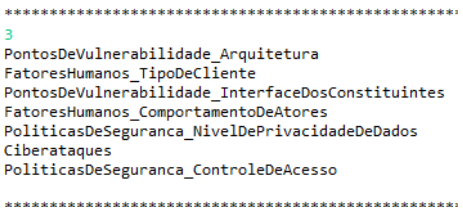

Figura 4. Programa apresenta o resultado para a questão de competência 3 da ontologia SegInfoSoS.

4.3. Próximas etapas

Como próxima etapa, pretende-se avaliar os resultados da pesquisa de opinião para verificar quais aspectos de segurança da informação discutidos no MSL são mais aplicados ao contexto de SoS. A avaliação será realizada sob a perspectiva de pesquisadores e profissionais da academia e indústria para compor a versão de avaliação da ontologia SegInfoSoS com os respectivos pontos de vista.

Será realizada a avaliação desta ontologia por meio da aplicação de grupo focal com especialistas em ontologia e SI bem como gestores de SoS. Os especialistas em ontologia e SI farão a análise do aspecto sintático da ontologia, i.e., se os elementos da ontologia proposta estão modelados corretamente. Os gestores de SoS farão a verificação do aspecto semântico, i.e., o significado adequado do vocabulário utilizado na ontologia. Após a fase da avaliação, será feito o refinamento da ontologia com os ajustes e correções sugeridos.

Além disso, será conduzido um estudo de caso participativo com ontologia em um SoS real para analisar o seu uso na indústria. Espera-se que seja possível avaliar a viabilidade da aplicação da ontologia SegInfoSoS com especialistas e se ela permite a compreensão dos conceitos abordados no gerenciamento de segurança da informação em SoS na prática.

[2]http://owlapi.sourceforge.net//

5. Contribuições esperadas

Esta pesquisa busca oferecer as seguintes contribuições tanto para a academia como para a indústria:

- Entendimento da importância da segurança da informação para os SI e SoS;
- Mapeamento sistemático sobre segurança da informação em SoS;
- Ontologia de domínio em segurança da informação em SoS para gestores de TI das organizações detentoras desses sistemas ou por pesquisadores da área;
- Programa de execução da ontologia para demonstrar a sua aplicabilidade.

Agradecimentos

Os autores agradecem a UNIRIO e FAPERJ (Proc. 211.583/2019) pelo apoio parcial.

Referências

Boscarioli, C., Araujo, R. M., e Maciel, R. S. P. (2017). Introduction. In Boscarioli, C., Araujo, R. M., e Maciel, R. S. P., editors, *I GrandDSI-BR - Grand Research Challenges in Information Systems in Brazil 2016 - 2026*, chapter 1, pp. 7–11. SBC-Sociedade Brasileira de Computação, Porto Alegre.

Chandrasekaran, B., J. J. e Benjamins, R. (1998). The Ontology of Tasks and Methods. In *Knowledge Acquisition Modeling and Mngt*. Workshop, Banff.

Dias, R. M., Antonio, N. P., Horita, F. E. A., e Santos, R. P. (2020). Oportunidades de KIPO para Gestão em Sistemas de Informação Federados no Caso do Programa Bolsa Família. In *Proceedings of the XIII Seminar on Ontology Research in Brazil and IV Doctoral and Masters Consortium on Ontologies (ONTOBRAS 2020), Vitória, Brazil, November 23-26, 2020*, volume 2728 of *CEUR Workshop Proceedings*, pp. 227–234. CEUR-WS.org.

Fernandes, J., Ferreira, F., Cordeiro, F., Graciano Neto, V. V., e Santos, R. (2019). A conceptual model for systems-of-information systems. In *2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI)*, pp. 364–371.

Guarino, N. (1998). *Formal Ontology in Information Systems: Proceedings of the 1st International Conference June 6-8, 1998, Trento, Italy*. IOS Press, NLD, 1st edition.

Maier, M. W. (1998). Architecting principles for systems-of-systems. *Systems Engineering*, 1(4):267–284.

Malagutti, M. A. O. (2016). O papel da dissuasão no tocante a ofensas cibernéticas. *Doutrina Militar Terrestre em Revista*, 4(9):18–27.

Meriah, I., Rabai, L. B. A., e Khedri, R. (2021). Towards an automatic approach to the design of a generic ontology for information security. In *2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS)*, pp. 1–8.

Noy, N. e Mcguinness, D. (2001). Ontology development 101: A guide to creating your first ontology. *Knowledge Systems Laboratory*, 32.

Sommerville, I. (2016). *Software Engineering, 10th Edition*. Pearson.

Whitman, M. E. e Mattord, H. J. (2009). *Principles of information security*. Thompson Course Technology, 3 edition.