



UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA - CCET
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA - PPGI

ONTOLOGIA PARA O GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO
EM SISTEMAS-DE-SISTEMAS

Roberto Monteiro Dias

Orientador

Rodrigo Pereira dos Santos

RIO DE JANEIRO, RJ - BRASIL
ABRIL DE 2022

ONTOLOGIA PARA O GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO
EM SISTEMAS-DE-SISTEMAS

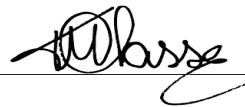
Roberto Monteiro Dias

DISSERTAÇÃO APRESENTADA COMO REQUISITO PARCIAL PARA OBTENÇÃO
DO TÍTULO DE MESTRE PELO PROGRAMA DE PÓS-GRADUAÇÃO EM
INFORMÁTICA DA UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE
JANEIRO (UNIRIO). APROVADA PELA COMISSÃO EXAMINADORA ABAIXO
ASSINADA.

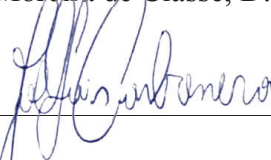
Aprovada por:



Rodrigo Pereira dos Santos, D.Sc. - UNIRIO



Tadeu Moreira de Classe, D.Sc. - UNIRIO



Joel Luís Carbonera, D.Sc. - UFRGS

RIO DE JANEIRO, RJ - BRASIL

ABRIL DE 2022

Catálogo informatizado pelo(a) autor(a)

M541	Monteiro Dias, Roberto Ontologia para o gerenciamento de segurança da informação em Sistemas-de-Sistemas / Roberto Monteiro Dias. -- Rio de Janeiro, 2022. 113 f. Orientador: Rodrigo Pereira dos Santos. Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Informática, 2022. 1. Ontologia. 2. Segurança da Informação. 3. Sistemas-de-Sistemas. I. Pereira dos Santos, Rodrigo, orient. II. Título.
------	---

Dedico este trabalho aos meus pais, irmãos e amigos por suas orações para o cumprimento desta etapa na minha trajetória profissional e pessoal.

Agradecimentos

Agradeço ao professor Rodrigo Pereira dos Santos pela orientação, compartilhamento de conhecimentos e oportunidades de crescimento profissional e pessoal proporcionados ao longo do período da pesquisa de dissertação.

Também quero agradecer ao doutorando Rodrigo Oliveira Zacarias por sua colaboração diligente e conselhos perspicazes que me guiaram por todas as etapas da minha pesquisa.

Deixo também meu agradecimento aos alunos e professores que participaram das reuniões e prévias de apresentação do Laboratório de Engenharia de Sistemas Complexos (LabESC), em especial para Bruno Lopes Xavier, Juliana Costa Fernandes, Jorge Varela, Nadja Piedade de Antonio, Paulo Malcher e Victor Garcia Farias.

Por fim, agradeço ao Seminário de Pesquisa em Ontologias no Brasil (ONTOBRAS), que contribuiu para a realização desta dissertação.

DIAS, Roberto Monteiro. **Ontologia para o Gerenciamento de Segurança da Informação em Sistemas-de-Sistemas**. UNIRIO, 2022. 113 páginas. Dissertação de Mestrado. Programa de Pós-Graduação em Informática, UNIRIO.

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 sistemas-de-sistemas (SoS). Embora o SoS ofereça benefícios às organizações, a dificuldade dos gestores de Tecnologia da Informação (TI) em lidar com a segurança da informação nesses sistemas pode deixá-los vulneráveis a ameaças e impactos causados por ataques cibernéticos. 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. 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, foi conduzido um mapeamento sistemático da literatura (MSL) para identificar quais tecnologias de segurança da informação vêm sendo aplicadas no contexto de SoS. Uma pesquisa de opinião foi realizada para analisar como estes aspectos tem sido percebidos pelos especialistas que atuam profissionalmente na indústria ou possuem projetos de pesquisa aplicados em cenários reais no âmbito desses sistemas. Também foi aplicada a Metodologia 101 para o desenvolvimento de uma ontologia de domínio de segurança da informação em SoS. Por fim, foi executada a avaliação da ontologia por meio de grupo focal com especialistas, o refinamento da ontologia e o estudo de viabilidade. A ontologia desenvolvida tem como objetivo garantir a gestão do conhecimento em segurança em SoS e o seu entendimento compartilhado de modo que os *stakeholders*, gestores de TI e suas equipes possam evitar os riscos, as vulnerabilidades e as ameaças em SoS. A sua contribuição 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.

Palavras-chave: Sistemas-de-Sistemas; Segurança da Informação; Ontologias.

DIAS, Roberto Monteiro. **Ontology for Information Security Management in Systems-of-Systems**. UNIRIO, 2022. 113 pages. Master's Thesis. Graduate Program of Informatics, UNIRIO.

ABSTRACT

The intense transformations that have taken place in society in this decade have made information systems (IS) more complex. Such complexity relates to a category of systems defined as systems-of-systems (SoS). Although SoS offers benefits to organizations, the difficulty of Information Technology (IT) managers in dealing with information security in these systems can leave them vulnerable to threats and impacts caused by cyber attacks. Researchers consider that ontologies can be used as a solution to this problem because they define knowledge structures and promote a shared understanding of a domain, task or application. The objective 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. For this, a systematic mapping study (SMS) was conducted to identify which information security technologies have been applied in the context of SoS. A survey research was carried out to analyze how these aspects have been perceived by specialists who work professionally in the industry or have research projects applied in real scenarios within the scope of these systems. Methodology 101 was also applied for the development of an information security domain ontology in SoS. Finally, the ontology evaluation was performed through a focus group with specialists, the ontology refinement and the feasibility study. The ontology aims to ensure the management of security knowledge in SoS and its shared understanding so that *stakeholders*, IT managers and their teams can avoid risks, vulnerabilities and threats in SoS. Its contribution is the standardization of concepts, terms and definitions, as well as the ease of sharing information to make more explicit assumptions and assist in the analysis of knowledge and domain relationships.

Keywords: Systems-of-Systems; Information Security; Ontologies.

Sumário

1	Introdução	1
1.1	Contexto	1
1.2	Motivação	1
1.3	Problema	3
1.4	Objetivo	4
1.5	Metodologia	4
1.6	Organização	5
2	Fundamentação Teórica	7
2.1	Sistemas-de-Sistemas	7
2.2	Segurança da Informação	10
2.3	Ontologia	11
2.3.1	Características	12
2.3.2	Classificação	13
2.4	Metodologia 101	14
2.4.1	Etapa 1: Determinar o domínio e o escopo da ontologia	15
2.4.2	Etapa 2: Considerar o reúso de outras ontologias	16
2.4.3	Etapa 3: Enumerar os termos importantes da ontologia	16
2.4.4	Etapa 4: Definir classes e a hierarquia de classes	16
2.4.5	Etapa 5: Definir as propriedades das classes	17
2.4.6	Etapa 6: Definir os valores das propriedades	17
2.4.7	Etapa 7: Criar instâncias	18
2.5	Considerações Finais	18
3	Trabalhos Relacionados	19
3.1	Introdução	19
3.2	Contexto	19
3.3	Considerações Finais	21
4	Mapeamento Sistemático da Literatura	22
4.1	Introdução	22

4.2	Protocolo e Execução	22
4.2.1	Planejamento	23
4.2.1.1	Questão de Pesquisa:	23
4.2.2	Estratégia de Busca	23
4.2.2.1	Definição dos Termos de Pesquisa:	24
4.2.2.2	Crerios de Seleção dos Estudos:	24
4.2.3	Execução	25
4.2.3.1	Processo de Seleção dos Estudos	25
4.2.3.2	Procedimento de Extração de Dados:	25
4.2.4	Apresentação dos Resultados	26
4.2.4.1	Dados Demográficos	26
4.2.4.2	Análise dos Resultados:	28
4.3	Limitações	30
4.4	Discussão	31
4.5	Considerações Finais	33
5	Pesquisa de Opinião	35
5.1	Introdução	35
5.2	Planejamento	36
5.2.1	Execução	37
5.3	Resultados	38
5.4	Limitações	41
5.5	Discussão	41
5.6	Considerações Finais	43
6	Ontologia SegInfoSoS	45
6.1	Introdução	45
6.2	Processo de construção da ontologia	45
6.2.1	Etapas 1 - Determinar o domínio e o escopo da ontologia.	46
6.2.2	Etapas 2 - Considerar o reuso de outras ontologias.	47
6.2.3	Etapas 3 e 4 - Enumerar os termos importantes da ontologia e definir as classes e a hierarquia de classes.	47
6.2.4	Etapas 5 - Definir as propriedades das classes	51
6.2.5	Etapas 6: Criar as instâncias	52
6.3	Representação da ontologia SegInfoSoS	54
6.4	Execução de testes	54
6.4.0.1	DL Query para consultas na ontologia SegInfoSoS	55
6.4.1	Programa em Java para consultas na ontologia SegInfoSoS	62

6.5	Considerações Finais	68
7	Avaliação da Ontologia SegInfoSoS	70
7.1	Introdução	70
7.2	Questão de Pesquisa	71
7.3	Grupo Focal	71
7.3.1	Objetivo do Estudo	71
7.3.2	Subquestão de Pesquisa	71
7.3.3	Papéis	72
7.3.4	Participantes	72
7.3.5	Localidade	72
7.3.6	Roteiro	72
7.3.7	Execução	74
7.3.8	Resultado	74
7.4	Refinamento da Ontologia	76
7.5	Estudo de Viabilidade	77
7.5.1	Cenário Hipotético	78
7.5.1.1	Questões de reflexão do Cenário Hipotético	79
7.5.2	Questões de avaliação	80
7.5.3	Execução	80
7.5.4	Resultado	80
7.6	Considerações Finais	81
8	Conclusão	83
8.1	Epílogo	83
8.2	Contribuições	85
8.3	Limitações	87
8.4	Trabalhos Futuros	87
	Apêndice I. Formulário da Pesquisa de Opinião	97

Lista de Figuras

Figura 1	Metodologia aplicada nesta pesquisa.	6
Figura 2	Visão parcial da classificação de uma ontologia no cenário de uma rede inter-organizacional de gestão do conhecimento: (a) representa livreria da universidade A e (b) representa a editora XYZ. Os retângulos redondos representam os conceitos, e os retângulos, e os rótulos nos arcos representam as propriedades (LEUNG et al., 2009).	13
Figura 3	Classificação de Ontologias segundo Guarino (1998).	14
Figura 4	Metodologia 101 para o desenvolvimento de ontologias (Adaptado) (BREITMAN, 2005)	15
Figura 5	Taxonomia de meios de transporte (BREITMAN, 2005).	17
Figura 6	Resultados do processo de seleção de estudos.	26
Figura 7	Estudos publicados no período de 1994 a 2020.	28
Figura 8	Distribuição dos estudos selecionados por país no período de 1994 a 2020.	29
Figura 9	Tempo de experiência sobre as áreas de conhecimento dos respondentes.	37
Figura 10	Percentual de concordância da questão 11 relacionada ao uso de análise de pontos de vulnerabilidades durante a interoperação entre os sistemas constituintes.	38
Figura 11	Percentual de concordância da questão 16 relacionada uso de protocolos de segurança seguro e eficiente na transmissão de dados para proteção da comunicação.	39
Figura 12	Percentual de concordância da questão 35 que está relacionada à falta de padronização dos métodos de segurança da informação.	39
Figura 13	Resultados da pesquisa de opinião com a participação de 32 especialistas.	40
Figura 14	Representação da subclasse SegurancaDaInformacao conforme o modelo conceitual de ontologia definida por Parkin et al. (2021).	55
Figura 15	Representação da subclasse SoS na ontologia SegInfoSoS conforme o modelo conceitual de ontologia definida por Parkin et al. (2021).	55

Figura 16 Programa em Java com o uso de OWL API no <i>prompt</i> de comando do Windows para execução de consultas na ontologia SegInfoSoS. .	62
Figura 17 Representação da subclasse <i>Component__Information__of__Security</i> da ontologia InfoSecSoS. As subclasses em amarelo são de SegInfoSoS e as subclasses em verde são de <i>Security Storytelling Ontology</i> . .	76
Figura 18 Representação da subclasse <i>Component__Systems__of__Systems</i> da ontologia InfoSecSoS. As subclasses em amarelo são de SegInfoSoS e as subclasses em verde são de OntoSoS	77
Figura 19 Classes, propriedade de objetos, propriedade de dados e instâncias da ontologia InfoSecSoS no <i>Protegé</i>	77
Figura 20 Site Web InfoSecSoS Ontology	78

Lista de Tabelas

Tabela 1	Critérios de PIO	23
Tabela 2	Critérios de Seleção	24
Tabela 3	Dados extraídos dos estudos selecionados.	27
Tabela 4	Estudos que possuem métodos, técnicas, modelos e ferramentas utilizados na segurança da informação em SoS com maior nível de concordância de profissionais e pesquisadores.	42
Tabela 5	Template de especificação da ontologia SegInfoSoS.	46
Tabela 6	Rastreabilidade dos estudos selecionados do MSL.	48
Tabela 7	Rastreabilidade dos estudos selecionados da revisão informal da literatura.	49
Tabela 8	<i>Template</i> de especificação das propriedades da ontologia SegInfoSoS.	51
Tabela 9	<i>Template</i> de especificação das instâncias da ontologia SegInfoSoS.	52
Tabela 10	Tabela com a execução de consulta DL Query 1 na ontologia SegInfoSoS.	55
Tabela 11	Tabela com a execução de consulta DL Query 2 na ontologia SegInfoSoS.	56
Tabela 12	Tabela com a execução de consulta DL Query 3 na ontologia SegInfoSoS.	58
Tabela 13	Tabela com a execução de consulta DL Query 4 na ontologia SegInfoSoS.	59
Tabela 14	Tabela com a execução de consulta DL Query 5 na ontologia SegInfoSoS.	60
Tabela 15	Tabela com a execução de consulta DL Query 6 na ontologia SegInfoSoS.	61
Tabela 16	Tabela com a execução de consulta DL Query 7 na ontologia SegInfoSoS.	61
Tabela 17	Tabela com a execução da questão 1 do programa em Java em OWL API.	62
Tabela 18	Tabela com a execução da questão 2 do programa em Java em OWL API.	63

Tabela 19	Tabela com a execução da questão 3 do programa em Java em OWL	
	API.	65
Tabela 20	Tabela com a execução da questão 4 do programa em Java em OWL	
	API.	66
Tabela 21	Tabela com a execução da questão 5 do programa em Java em OWL	
	API.	67
Tabela 22	Tabela com a execução da questão 6 do programa em Java em OWL	
	API.	67
Tabela 23	Tabela com a execução da questão 7 do programa em Java em OWL	
	API.	68
Tabela 24	Perfil dos participantes do grupo focal.	74
Tabela 25	Perfil dos participantes do estudo de viabilidade.	80

Lista de Nomenclaturas

API	<i>Application Programming Interface</i>
CadÚnico	Cadastro Único
CE	Critério de Exclusão
CI	Critério de Inclusão
CID	Confidencialidade, Integridade e Disponibilidade
ERP	<i>Enterprise Resource Planning</i>
KIPO	<i>Knowledge Intensive Process Ontology</i>
LOV	<i>Linked Open Vocabularies</i>
MSL	Mapeamento Sistemático da Literatura
ONTOBRAS	Seminário de Pesquisa em Ontologias no Brasil
OWL	<i>Web Ontology Language</i>
PBF	Programa Bolsa Família
PICOC	<i>Population, Intervention, Comparison, Outcome, Context</i>
QP	Questão de Pesquisa
SBSI	Simpósio Brasileiro de Sistemas de Informação
SCDP	Sistema de Concessão de Diárias e Passagens
SGDB	Sistema de Gerenciamento de Banco de Dados
SIAFI	Sistema Integrado de Administração Financeira
SIAPE	Sistema Integrado de Administração de Recursos Humanos
SIASG	Sistema Integrado de Administração de Serviços Gerais
SIBEC	Sistema de Benefício ao Cidadão
SICES	Sistema Conta Caixa Fácil
SIF	Sistema de Informação Federado
SIISO	Sistema de Informações Sociais
SIPAS	Sistema de Pagamento Social
SoIS	<i>Systems-of-Information Systems</i>
SoS	<i>Systems-of-Systems</i>
TI	Tecnologia da Informação
WTDO	<i>Workshop de Teses e Dissertações em Ontologias</i>

1. Introdução

Esse capítulo tem o objetivo de apresentar o contexto, motivação, caracterização do problema, objetivo, questões de pesquisa e a metodologia científica utilizadas nesta dissertação. Ao final deste capítulo, é apresentada a organização do documento e uma breve descrição de cada capítulo.

1.1 Contexto

As intensas transformações organizacionais, que ocorreram na sociedade nesta década, pressionaram os sistemas de informação (SI) de tal forma que um conjunto ou arranjo de sistemas interoperáveis seja formado e gerenciado independentemente, formando os chamados sistemas-de-sistemas (do inglês, *systems-of-systems*, ou SoS). Isso significa que os diferentes *stakeholders* no SoS estão sujeitos a diversas políticas e regras de gerenciamento e controle de numerosas organizações (SOMMERVILLE, 2016).

No cenário sociotécnico e organizacional, é um desafio manter a transparência das informações e a interoperabilidade entre os sistemas constituintes do SoS. Isso ocorre em virtude da interconectividade e a interação que devem ser preservadas para o cumprimento de uma ou mais objetivos globais (BOSCARIOLI et al., 2017; FERNANDES et al., 2018).

1.2 Motivação

De acordo com Graciano Neto et al. (2017), transparência e interoperabilidade em SoS ainda são um desafio da área devido à alta dinamicidade de sua arquitetura. Nesse sentido, a ocorrência de falhas de segurança da informação, como perda ou acesso não autorizado a dados confidenciais, durante a comunicação entre os constituintes pode colapsar o SoS como um todo e acarretar diversos problemas para o negócio. Por exemplo, nas cidades

inteligentes, as falhas podem comprometer a segurança de pessoas e bens patrimoniais, além de causar impacto na economia e até mesmo a insolvência dos sistemas constituintes.

Em um exemplo prático hipotético, pode-se depreender que três gestores gerenciam partes de um SoS com seus sistemas constituintes espalhados pelos diferentes estados do Brasil. A comunicação do SoS com os sistemas constituintes é realizada por uma API (do inglês, *Application Programming Interface*, ou Interface de Programação de Aplicação). O gestor A é responsável pela política de segurança da informação no SoS e gerenciamento do sistema constituinte A. Os gestores B e C são responsáveis pelo gerenciamento dos respectivos sistemas constituintes B e C de suas organizações. O gestor A precisa comunicar informações específicas de segurança da informação para os gestores dos sistemas constituintes B e C. O sistema constituinte A vai passar por atualização de software em sua plataforma, o sistema constituinte B será descontinuado e o sistema constituinte C passará por integração com o ERP (do inglês, *Enterprise Resource Planning*, ou Planejamento de Recursos Empresariais) para acessar os dados e processos dos departamentos de uma instituição financeira. Houve a descoberta de uma nova categoria de vírus que permite que *hackers* mal-intencionados acessem os sistemas operacionais e enviem comandos remotos às máquinas para obter informações sigilosas dos usuários. Deste modo, como evitar que estes *hackers* acessem o SoS e os seus sistemas constituintes?

Em tal situação, devem ser implementados mecanismos e/ou tecnologias que possam garantir que a comunicação entre os sistemas seja tratada sob o prisma da segurança da informação: confiabilidade, integridade e disponibilidade (ELMAGHRABY; LOSAVIO, 2014). A partir desta solução e respeitando as políticas de segurança previamente estabelecidas, é possível minimizar e até mesmo evitar a ocorrência de ciberataques bem sucedidos. Pesquisadores, que investigam o tema ontologias nos âmbitos da Ciência da Computação e da Ciência da Informação, consideram que as ontologias podem ser utilizadas como solução para essa questão porque elas definem estruturas de conhecimento e promovem um entendimento compartilhado de um domínio, tarefa ou aplicação (CHANDRASEKAN et al., 1998).

Para tal, o uso destas ontologias, no contexto e problema abordado na Seção 1.3, é de especialização da taxonomia de ontologias definida por Guarino (1998) como ontologias de domínio. Elas descrevem o vocabulário de um domínio específico do conhecimento, definindo-o e o caracterizando. A sua contribuição 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.

1.3 Problema

Em uma realidade de intensas transformações no cenário político, econômico e social que pressionaram os SI, os gestores encontraram muitas dificuldades de gerenciamento desses SI nas organizações (JAY, 2013; SMITH; LEWIS, 2011) com foco na segurança da informação (WHITMAN; MATTORD, 2009). Uma categoria de sistema complexo, como o SoS, está sujeita a diversas políticas e regras de gerenciamento e controle de numerosas organizações (SOMMERVILLE, 2016).

Além disso, a arquitetura do SoS é dinâmica, influenciada pelo nível de liberdade dos sistemas constituintes, que podem deixá-lo sem aviso ou alterar suas regras e nível de contribuição, conforme as políticas organizacionais de suas respectivas organizações (FERREIRA; SANTOS, 2019). Assim, os gestores desses sistemas 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 a essas características, eles podem cometer uma série de erros que aumentam as oportunidades de ataques cibernéticos serem bem-sucedidos. Como exemplo, pode-se destacar (FONTES, 2008):

1. **Não alinhar os modelos, métodos, técnicas ou ferramentas de segurança no SoS.**

A tecnologia não é mais apenas o suporte técnico de uma corporação: ela faz parte das tomadas de decisão de negócios e é essencial para as atividades da empresa. Portanto, as escolhas de soluções e medidas de segurança devem estar alinhadas com os objetivos do SoS;

2. **Não padronizar os métodos de segurança da informação.** Muitas vezes, as falhas que levam a vulnerabilidades na segurança da informação estão relacionadas a métodos informais realizados pela equipe de tecnologia da informação. Portanto, para resolver esse problema, o gestor deve considerar a padronização destes métodos;

3. **Não realizar treinamentos.** O investimento em treinamentos especializados e na educação em todos os níveis dos colaboradores, desde funcionários não técnicos até as equipes de tecnologia da informação, é tarefa essencial para garantir a proteção geral do SoS;

4. **Não criar um plano estratégico eficiente.** É responsabilidade do gestor estar atento às características de segurança da informação em SoS e, assim, criar um planejamento eficiente, buscando as tecnologias de segurança da informação que melhor atendam as políticas organizacionais;

5. **Falhas de comunicação** entre colaboradores, técnicos e gestores devido à complexidade do SoS, causando dificuldade de refletir a segurança da informação nesse sistema.

Com base nas características do contexto e problema, foi possível identificar a principal questão de pesquisa (QPP): **Como abordar a segurança da informação de modo a permitir que os *stakeholders*, gestores de TI e equipes que atuam no âmbito de SoS possam compreendê-la sem dificuldades?**

1.4 Objetivo

Com base na *QPP*, o objetivo geral 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.

Os objetivos específicos são:

- Formalizar uma estrutura padronizada para representar o domínio segurança da informação em SoS de modo a apoiar pesquisadores e profissionais da indústria na especificação, tratamento e mitigação de riscos de segurança no gerenciamento desses sistemas;
- Aperfeiçoar a comunicação entre os *stakeholders*, gestores de TI e suas equipes, reduzindo possíveis mal-entendidos sobre questões de segurança em SoS;
- Demonstrar o uso de ontologias para facilitar o reuso, a padronização e o conhecimento de segurança da informação em SoS;
- Propiciar os fundamentos para construção de outras ontologias do domínio de segurança da informação em SoS;
- Demonstrar a aplicação de uma ontologia de domínio em segurança da informação em SoS por meio da sua execução em um site web.

1.5 Metodologia

As atividades propostas neste projeto de pesquisa conforme a Figura 1 são:

1. Revisão Informal da Literatura realizada de forma ad hoc com a seleção de estudos que trazem uma visão do contexto SoS, segurança da informação e ontologia;
2. Estudo Exploratório com o uso da Ontologia de Processo Intensivo em Conhecimento (do inglês *Knowledge Intensive Process Ontology*, ou KIPO) para mapear tensões na gestão de sistemas de informações federados (SIF) em um estudo de caso no Programa Bolsa Família (DIAS et al., 2020);
3. Mapeamento Sistemático da Literatura (MSL) a partir dos conhecimentos obtidos na atividade 1 sobre o panorama de segurança da informação em SoS;
4. Pesquisa de opinião para avaliar os resultados obtidos do MSL junto a pesquisadores e profissionais em segurança da informação e SoS;
5. 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 e ratificados pela pesquisa de opinião;
6. Avaliação da ontologia por meio da condução de grupo focal com especialistas para análise de sua sintaxe e semântica;
7. Refinamento da ontologia com ajustes e correções sugeridos nas avaliações;
8. Realização de Estudo de Viabilidade para verificar o uso da ontologia em um SoS real.

1.6 Organização

Esta dissertação está organizada em sete capítulos. Neste capítulo de introdução, foram abordados o contexto, a motivação e o problema desta pesquisa. O objetivo e a questão de pesquisa foram construídos conforme o contexto, possibilitando a descrição da metodologia e a organização deste trabalho.

O Capítulo 2 apresenta os conceitos fundamentais de SoS, segurança da informação e ontologia.

O Capítulo 3 menciona alguns trabalhos relacionados que abordam estes conceitos, indicando o diferencial desta pesquisa.

O Capítulo 4 aborda o MSL para identificar como as tecnologias de segurança da informação são utilizadas no contexto de SoS.

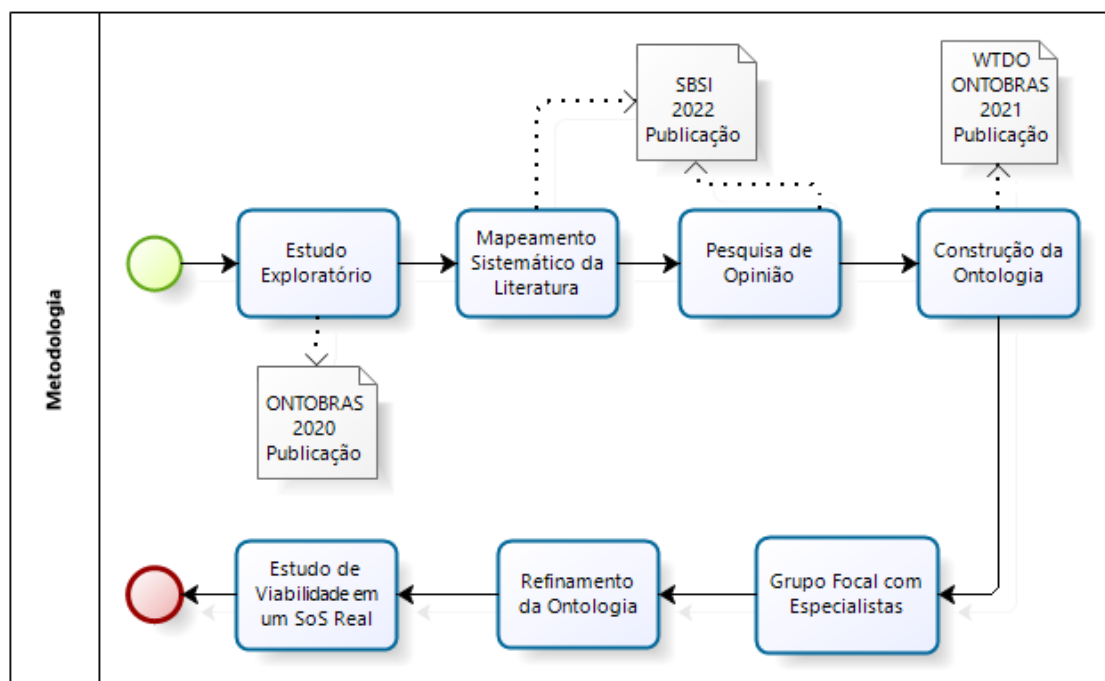


Figura 1: Metodologia aplicada nesta pesquisa.

O Capítulo 5 apresenta o planejamento e resultados da pesquisa de opinião. A pesquisa de opinião foi realizada para analisar aspectos de segurança da informação com o propósito de avaliar a sua aplicabilidade na indústria do ponto de vista de pesquisadores e profissionais no contexto de SoS.

O Capítulo 6 aborda como foi aplicada a metodologia 101 na criação da ontologia SegInfoSoS¹ e apresenta o modelo da ontologia construída.

O Capítulo 7 aborda o planejamento da avaliação da ontologia por meio da condução de um grupo focal com especialistas, o refinamento da ontologia e um estudo de viabilidade em um SoS real.

Por fim, o Capítulo 8 conclui a pesquisa com algumas considerações finais, apresenta a consolidação das contribuições, algumas limitações e trabalhos futuros. Em seguida, são listados as referências bibliográficas e o apêndice com o formulário da pesquisa de opinião.

¹<https://doi.org/10.5281/zenodo.6621882>

2. Fundamentação Teórica

Este capítulo apresenta as definições dos termos e conceitos utilizados durante a pesquisa, destaca alguns trabalhos relacionados e encerra com algumas considerações. O capítulo está organizado da seguinte forma: A Seção 2.1 explora a definição de Sistemas-de-Sistemas. A Seção 2.2 introduz a definição sobre segurança da informação. A Seção 2.3 aborda a definição e conceitos sobre ontologia. A Seção 2.4 apresenta as etapas da Metodologia 101 para construção de ontologias. Por fim, a Seção 2.5 conclui este capítulo e elenca como a pesquisa foi desenvolvida no contexto de Sistemas-de-Sistemas.

2.1 Sistemas-de-Sistemas

De acordo com Maier (1998), sistema-de-sistemas ou simplesmente SoS pode ser definido como um conjunto de sistemas, gerencialmente e operacionalmente independentes (conhecidos como constituintes), que trabalham em conjunto de modo a obter funcionalidades complexas, correspondendo à missão global ou o objetivo do sistema formado pelo arranjo. Cada sistema constituinte realiza sua missão de forma individual e contribui para a realização da missão global. Pode-se destacar como um exemplo clássico desses sistemas as cidades inteligentes, onde diferentes dispositivos e SI atuam para oferecer serviços à população por meio da colaboração de diferentes organizações públicas e/ou privadas proprietárias desses sistemas (FERNANDES et al., 2019).

Nesse ambiente, os sistemas, compostos por recursos humanos e tecnológicos, provêm serviços essenciais tais como distribuição de energia, controle de tráfego, integração de transporte, saúde, segurança pública, carros autônomos, gestão de edifícios etc. (INO-CÊNCIO et al., 2019).

As características dos sistemas constituintes podem ser observadas a partir da sua participação em SoS, tais como (MAIER, 1998):

- *operacionalmente independentes*: os constituintes possuem operações próprias mesmo trabalhando dentro do escopo do SoS;
- *gerencialmente independentes*: os constituintes podem ser gerenciados de forma independente por organizações e diferentes partes interessadas;
- *distribuição geográfica*: os constituintes podem estar distribuídos geograficamente;
- *desenvolvimento evolucionário*: a evolução dos constituintes ocorre em tempo de execução, nas funções e no propósito do SoS, e podem ser agregados novos constituintes para realizar novas tarefas;
- *comportamento emergente*: os SoS podem fornecer novas funcionalidades a partir das interações e do trabalho em conjunto dos seus constituintes. Essas funcionalidades não podem ser fornecidas isoladamente pelos constituintes.

Sommerville (2016) acrescenta duas características a essa lista que são particularmente relevantes para o SoS. São eles:

- *intensivos em dados*: um grande volume de dados interoperam no SoS e seus sistemas constituintes;
- *heterogeneidade*: os SoS e seus sistemas constituintes podem ter sido desenvolvidos por diferentes linguagens de programação e métodos de engenharia de software.

Maier (1998) identificou três tipos de SoS: *dirigido*, *virtual* e *colaborativo*. Posteriormente, um novo tipo, *reconhecido*, foi proposto por Dahmann e Baldwin (2008):

- *Dirigido*: Os SoS são controlados por uma entidade centralizada e/ou uma parte interessada e projetados e operados com fins específicos;
- *Virtual*: Sem controle central e propósitos universais. Esses propósitos não são projetados nem previsíveis em muitos casos, tal que os constituintes operam em um ambiente distribuído e descoordenado onde a forma para manter o SoS não são evidentes;
- *Colaborativo*: Os constituintes colaboram em maior ou menor grau para realizar interesses comuns ou compartilhados;

- *Reconhecido*: As metas, recursos e controle centralizados do SoS são na sua totalidade reconhecidos, mas os constituintes mantêm totalmente sua independência gerencial e seu comportamento não é dependente do propósito gerenciado centralmente;

Para Sommerville (2016), a definição dos tipos de SoS elaborada por Maier (1998) não reflete as diferenças entre esses diversos tipos de sistemas, sendo então elaborada uma nova definição de termos que este autor considera mais descritivos. São eles:

- *Organizacional*: a governança e gestão do sistema residem na mesma organização ou empresa e corresponde ao “SoS dirigido” de Maier (1998). A colaboração entre os proprietários do sistema é gerenciada pela organização. O SoS pode ser distribuído geograficamente, com diferentes partes do sistema sujeitas a diferentes leis e regulamentos nacionais;
- *Federado*: a governança do SoS depende de um órgão participativo voluntário onde todos os proprietários do sistema estão representados. Os proprietários do sistema concordam em colaborar e acreditam que as decisões tomadas pelo órgão de governança são vinculativas. Ou seja, eles implementam essas decisões em suas políticas de gestão individuais, embora as implementações possam ser diferentes devido a leis, regulamentos e cultura nacionais;
- *De Coalizações*: não possuem mecanismos formais de governança mas colaboram informalmente e gerenciam seus próprios sistemas para manter o sistema como um todo. Ou seja, não há governança no nível organizacional, mas a colaboração informal existe no nível gerencial.

Algumas classes de sistemas podem ser derivadas de um SoS conforme o tipo dos sistemas que o constituem. Dentre elas, pode-se destacar o Sistema-de-Sistemas de Informação (SoIS, do inglês *Systems-of-Information Systems*) e os Sistemas de Informações Federados (SIF).

Os SoIS são um tipo derivado de SoS formado por SI, que trabalham, gerencialmente e operacionalmente, de forma independente para obter sucesso nos objetivos do negócio. Além disso, cada sistema forma uma rede em torno de si, por meio de relações técnicas, sociais e de negócio, que conduz como este sistema contribui para o negócio que integra (FERNANDES et al., 2018). Como exemplo de SoIS, pode-se destacar um Sistema Integrado de Gestão Ambiental que possui três sistemas constituintes (i.e., Sistema Integrado de Gestão Ambiental e Água, Sistema Nacional de Controle da Origem de Produtos

Florestais e Sistema de Registro Ambiental Rural) e que interoperam entre si para dar suporte gerencial a liberação de licenças ambientais no Estado do Piauí (FERNANDES et al., 2020).

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).

Como exemplo de SIF, pode-se destacar os sistemas que faziam parte do Programa Bolsa Família (i.e., CadÚnico, Sistema de Informações Sociais - SIISO, Sistema do Ministério do Desenvolvimento Social, Sistema de Benefício ao Cidadão – SIBEC, Sistema Conta Caixa Fácil - SICES e Sistema de Pagamento Social - SIPAS) (DIAS et al., 2020).

2.2 Segurança da Informação

A norma internacional ISO/IEC 27002:2013 (ISO, 2013) enfatiza que segurança da informação é alcançada por meio da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

Whitman e Mattord (2009) definem segurança da informação (InfoSec, do inglês *Information Security*) como a proteção da informação e seus elementos críticos, incluindo os sistemas e hardware que usam, armazenam e transmitem essa informação. Também identificam várias características críticas da informação que lhe conferem valor nas organizações. Essa definição está relacionada como a preservação da Confidencialidade, Integridade e Disponibilidade de informações, entendidas como a tríade CID (MALAGUTTI, 2016).

A tríade CID constitui um ponto de referência para avaliar a segurança do SI e processos de auditoria de segurança da informação. A confidencialidade garante que as informações somente serão compartilhadas com pessoas ou entidades autorizadas. A integridade é a garantia de que a informação é confiável, completa, correta e autêntica. A disponibilidade é a garantia de que os sistemas responsáveis pelo provisionamento serão responsivos, ágeis, acessíveis e atendam aos padrões acordados (DHILLON; KOLKOWSKA, 2011; OUEDRAOGO et al., 2015). Whitman e Mattord (2009) ainda acrescentam precisão, autenticidade, utilidade e posse para a lista de características da informação que precisa ser

protegida.

2.3 Ontologia

Ontologia tem sua origem na filosofia e, segundo Almeida e Bax (2003), é o ramo da Metafísica que estuda os tipos de coisas que existem no mundo. A palavra Ontologia vem do grego “Ontos” que significa ser e “Logos” que significa palavra. No entanto, seu termo de origem surgiu com Aristóteles que a definiu como um conjunto de categorias para estruturar modelos específicos da realidade.

Segundo Studer et al. (1998), a ontologia é descrita como uma especificação formal explícita de uma conceitualização compartilhada. A palavra “conceitualização” pode ser entendida como um modelo abstrato de algum fenômeno do mundo real que identifica os conceitos relevantes desse fenômeno. A palavra “formal” destaca que a ontologia deve ser passível de ser processada por máquinas. Em “compartilhada”, tem-se a compreensão que a ontologia captura o conhecimento consensual que, segundo Fensel (2003), não deve ser restrito a alguns indivíduos, mas aceito por um grupo de pessoas.

Para a compreensão mais concreta sobre o conceito de ontologia, imagine, por exemplo, em um cenário hipotético, o processo de comunicação entre duas pessoas em uma conferência. Para haver comunicação entre elas, além de ser necessário conhecerem a mesma linguagem e as regras formais dessa linguagem, é preciso acontecer uma interpretação simultânea sobre as categorias e símbolos dessa linguagem em termos de uma conceitualização, isto é, um modelo mental sobre a realidade que está sendo compartilhada.

Como os seres humanos conseguem criar modelos mentais e as máquinas não possuem acesso a essa conceitualização, existe a necessidade de construir esses modelos mentais de determinada porção da realidade para elas poderem utilizá-los e, dessa forma, interpretar o conteúdo da linguagem. Porém, como as máquinas operam apenas com modelos formais, isto é, modelos matemáticos, então tais modelos mentais devem ser realizados de forma matemática para elas poderem raciocinar sobre eles.

Nesse sentido, as mensagens trocadas entre máquinas podem também ser realizadas em forma de modelos. Esses modelos podem ser utilizados por empresas que queiram trocar conhecimento e informação e desejam integrar suas aplicações e bases de dados. Um modelo é uma representação simplificada da realidade que se deseja compreender (ALMEIDA, 2013).

Para Guizzardi (2000), uma ontologia pode ser utilizada para descrever os aspectos

do mundo físico e social ao nosso redor para fins de compreensão e comunicação, em modelagem conceitual. Tal compreensão implica no entendimento que uma ontologia pode descrever modelos mentais de porção da realidade.

2.3.1 Características

O mundo é complexo e modelos são produzidos para que a compreensão humana possa apreendê-los em partes, visto que não consegue abrangê-los em sua totalidade. Assim pode-se depreender que ontologias são o meio para modelar formalmente a estrutura desses modelos que podem ser compreendidos como o domínio de conhecimento.

Para Almeida et al. (2020), as ontologias promovem a compreensão do domínio, permitem a classificação de seus termos e possibilitam também a criação de vocabulários controlados e a recuperação da informação. Dessa forma, os engenheiros de ontologia as desenvolvem com o intuito de explicitar quais são os conceitos e as relações existentes entre estes conceitos relevantes para modelagem de um determinado domínio.

Para formalização desses conceitos, Gruber (1995) definiu alguns componentes:

- **Classes:** representam grupos de indivíduos que possuem características em comum. Em um domínio de viagens, por exemplo, as classes podem ser representadas por localização (cidades e povoados), alojamento (hotel, hostel e camping) e meio de transporte (aviões, automóveis, motos e navios);
- **Relações:** representação de um tipo de interação entre os conceitos no domínio, ou seja, entre as classes e os elementos do domínio;
- **Axiomas:** representam as sentenças que são sempre verdadeiras, independentemente da situação e aplicadas na definição de restrições sobre relações e classes. Um axioma é uma afirmação lógica;
- **Instâncias:** instanciam conceitos que são geralmente representados pelas classes. No domínio de viagem, por exemplo, as instâncias podem ser representadas por Rio de Janeiro (instância de localizações), Hotel Palace (instância de alojamentos) e Peugeot 208 (instância de meio de transporte).

A Figura 2 representa uma visão parcial da classificação de uma ontologia adotada por Leung et al. (LEUNG et al., 2009) para descrever cenário de funcionamento de uma rede inter-organizacional de gestão do conhecimento na prática da indústria.

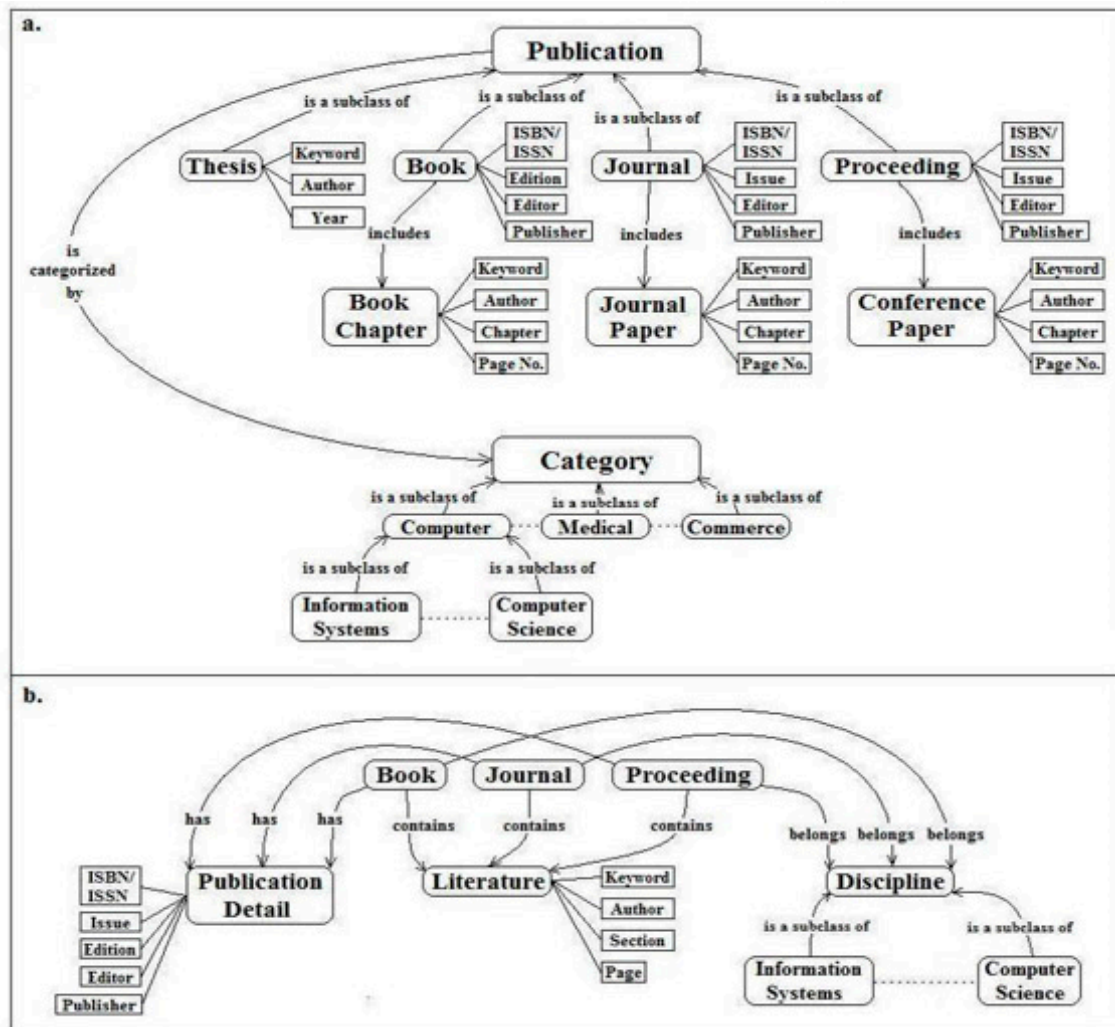


Figura 2: Visão parcial da classificação de uma ontologia no cenário de uma rede inter-organizacional de gestão do conhecimento: (a) representa livraria da universidade A e (b) representa a editora XYZ. Os retângulos redondos representam os conceitos, e os retângulos, e os rótulos nos arcos representam as propriedades (LEUNG et al., 2009).

2.3.2 Classificação

Segundo Guarino (1998), as ontologias podem ser classificadas em:

- **Ontologias de Alto Nível:** definem conceitos bem gerais como espaço, tempo, matéria, objeto, evento, ação etc., sendo independentes de um domínio específico. Pode ser compartilhado por diversas comunidades;
- **Ontologias de Domínio:** são responsáveis pela modelagem de um domínio específico ou parte deste domínio, ou seja, ela representa o conhecimento sobre um determinado tópico, o definindo e caracterizando. São exemplos de ontologia de domínio ontologias de veículos, documentos, entre outros;

- **Ontologias de Tarefa:** descrevem conceitos relacionados a tarefas ou atividades genéricas (como diagnosticar uma doença ou vender um produto), independentes do domínio em que ocorram;
- **Ontologias de Aplicação:** descrevem conceitos que dependem tanto de um domínio específico como de uma tarefa específica, e geralmente é uma especialização desse domínio ou tarefa específica. Estes conceitos frequentemente correspondem a papéis desempenhados por entidades do domínio quando da realização de uma certa tarefa.

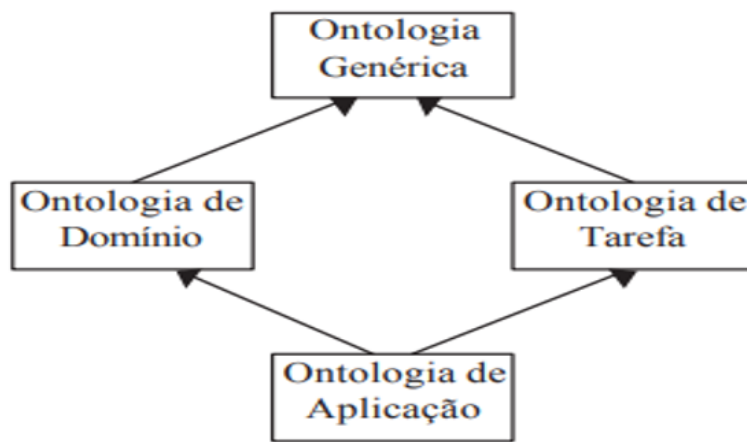


Figura 3: Classificação de Ontologias segundo Guarino (1998).

2.4 Metodologia 101

Para que os engenheiros de ontologias pudessem seguir uma abordagem sistêmica, disciplinada e quantificável na construção de ontologias, várias metodologias foram elaboradas. Tal como acontece nas metodologias de desenvolvimento de software, essas metodologias consistem na aplicação do conceito de dinamização de processos de desenvolvimento.

Dentre as metodologias criadas para o desenvolvimento de ontologias, destaca-se a Metodologia 101 proposta por Noy e McGuinness (2001), que é um roteiro para criação de ontologias. Atualmente, é a metodologia mais utilizada para a construção de ontologias devido à sua simplicidade (ISOTANI; BITTENCOURT, 2015). Ela foi desenvolvida com base na experiência dos autores no processo de desenvolvimento de ontologias por meio

da utilização de editores de ontologias *Protégé*¹, *Ontolingua*² e *Chimaera*³. Há algumas regras a serem seguidas para o desenvolvimento de ontologias por meio desta metodologia, como:

- Não existe um único método correto para modelar um domínio - sempre vão existir preferências;
- O processo de desenvolvimento de ontologias é iterativo, ou seja, durante o processo será necessário revisá-lo;
- Os conceitos na ontologia devem ser bem próximos dos objetos reais e relacionamentos.

Como apresentado na Figura 4, esta metodologia é basicamente composta por sete etapas para auxiliar o processo de construção de ontologias. Estas etapas são explicadas nas subseções a seguir.

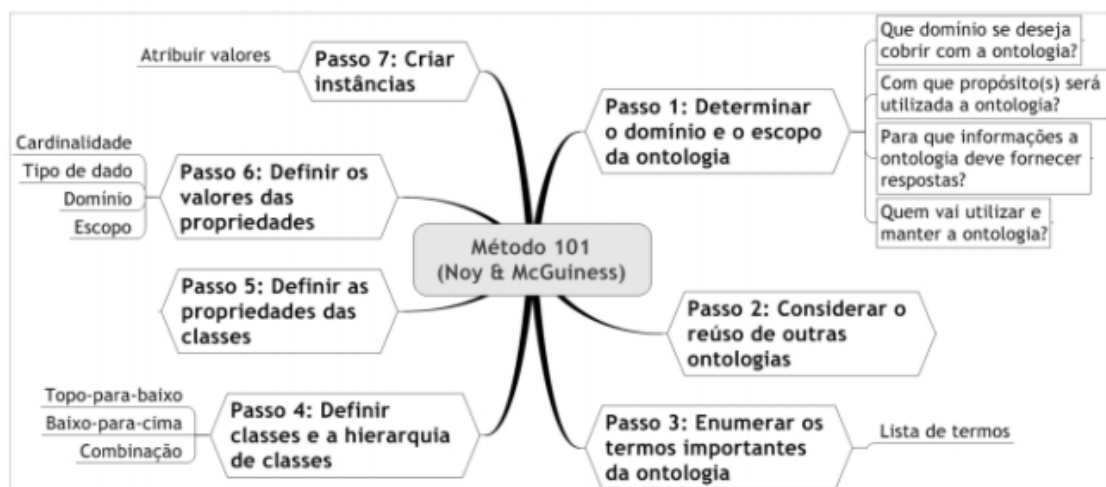


Figura 4: Metodologia 101 para o desenvolvimento de ontologias (Adaptado) (BREITMAN, 2005)

2.4.1 Etapa 1: Determinar o domínio e o escopo da ontologia

Para se determinar o domínio e o escopo, a metodologia sugere que deve iniciar o desenvolvimento da ontologia respondendo às seguintes perguntas:

¹<https://protege.stanford.edu/>

²<http://www.ksl.stanford.edu/software/ontolingua/>

³<http://www.ksl.stanford.edu/software/chimaera/>

- Que domínio que se deseja cobrir com a ontologia?
- Com que propósito(s) será utilizada a ontologia?
- Para que informações a ontologia deve fornecer respostas?
- Quem vai utilizar e manter a ontologia?

A penúltima questão tem o propósito de definir as questões de competência da ontologia (USCHOLD; GRUNINGER, 1996), em que os desenvolvedores farão questões específicas sobre o domínio. Estas questões serão utilizadas não apenas como um limite do escopo da ontologia, mas também como base para sua validação.

2.4.2 Etapa 2: Considerar o reuso de outras ontologias

É importante considerar o que já existe e verificar se pode refinar e estender as fontes para o seu domínio e tarefas específicos. Muitas ontologias estão disponíveis atualmente e podem ser importadas para editores e ambientes de desenvolvimento com relativa facilidade.

2.4.3 Etapa 3: Enumerar os termos importantes da ontologia

É importante definir os termos para a descrição do domínio, com o objetivo principal de conseguir uma lista abrangente dos termos relativos à ontologia, sem se preocupar com os conceitos que eles representam estão sobrepostos ou se esses conceitos são classes, propriedades ou relações (NOY; MCGUINNESS, 2001).

2.4.4 Etapa 4: Definir classes e a hierarquia de classes

Nesta etapa, é preciso definir as classes e hierarquias de classes. A estratégia de desenvolvimento da hierarquia de classes pode ser desenvolvida em (USCHOLD; GRUNINGER, 1996):

- **Top-Down** - O processo tem início com a definição da maioria dos conceitos gerais do domínio e a subsequente especialização dos conceitos;
- **Bottom-Up** - O processo se inicia com a definição das classes mais específicas e o subsequente agrupamento dessas classes em conceitos mais gerais;

- **Combinação das duas** - Tem-se a combinação dos dois processos anteriores. Define-se primeiro os conceitos mais ressaltados e, depois, faz-se a generalização e a especialização de forma adequada.

Pode-se organizar as classes por meio de uma hierarquia taxonômica com o seguinte questionamento: *Se uma classe A é superclasse de uma classe B, então toda instância de B também é instância de A.*

Por exemplo, observe a hierarquia de conceitos representada pela Figura 5. A classe Automóvel é subclasse da classe Meio de Transporte. Portanto, toda instância de Automóvel (por exemplo, carro Fiat Palio preto, placa RIO2A22) também é instância de Meio de Transporte.

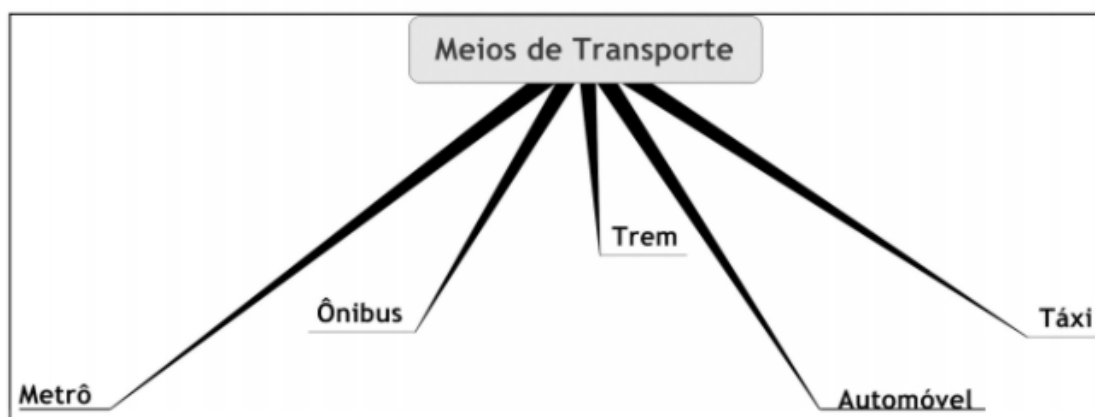


Figura 5: Taxonomia de meios de transporte (BREITMAN, 2005).

2.4.5 Etapa 5: Definir as propriedades das classes

Como as classes já foram definidas, é importante descrever as relações entre as classes quanto os atributos de cada classe, ou seja, as propriedades das classes. Por exemplo, a classe Meio de Transporte está relacionada a Classe Departamento de Trânsito (Detran). Assim, a propriedade que se relaciona com essas duas classes é “possui licença no Detran”. No exemplo da classe Automóvel, as propriedades representam os atributos do carro que é cor, modelo, tipo de motor, tipo de câmbio, quantidade de portas, entre outros.

2.4.6 Etapa 6: Definir os valores das propriedades

As propriedades podem assumir diferentes valores. Por exemplo, a placa de um carro registrada no Detran possui cardinalidade única, porém a lista de registros de motoristas pode incluir vários valores. Em OWL, os tipos mais comuns são:

- Cadeia de caracteres;
- Números (Inteiros ou ponto flutuante);
- Booleanos;
- Listas enumerada de elementos.

2.4.7 Etapa 7: Criar instâncias

Nesta etapa, é criada as instâncias individuais para as classes na hierarquia. Para isso, é necessário escolher uma classe, criar uma instância individual dessa classe e preencher os valores da propriedade.

Uma instância nada mais é que um objeto cujo comportamento e estado são definidos pela classe. Por exemplo, pode-se pensar em “cachorro” como uma subclasse da classe animal e um cão específico chamado “Lupito” como uma instância dessa subclasse.

2.5 Considerações Finais

Este capítulo teve como objetivo trazer definições sobre os conceitos de SoS, os tipos, as características e classes derivadas, bem como conceitos sobre segurança da informação, ontologia e a Metodologia 101.

3. Trabalhos Relacionados

Este capítulo está organizado da seguinte forma: a Seção 3.1 apresenta a motivação para o levantamento dos trabalhos relacionados encontrados na revisão informal da literatura. A Seção 3.2 traz o contexto dos trabalhos relacionados utilizados no desenvolvimento desta pesquisa. Por fim, a Seção 3.3 apresenta algumas considerações finais.

3.1 Introdução

Com base no levantamento dos trabalhos relacionados realizado de forma *ad hoc*, foram encontrados três trabalhos recentes que apresentam como solução proposta o uso de ontologias de domínio em SI. A partir da verificação do desenvolvimento de cada solução proposta dos respectivos trabalhos, foi possível vislumbrar a oportunidade para esta pesquisa.

3.2 Contexto

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. 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 Confidencialidade, Integridade e Disponibilidade (CID) nas trocas de informações entre esses sistemas no SIF.

Nesse sentido, a Organização Internacional de Normalização (do inglês, *International Organization for Standardization*, ou ISO) já preconizava a necessidade de regulamentações adicionais para aumentar a conscientização sobre a segurança da informação na gestão das empresas, visando serviços essenciais, incluindo, por exemplo, infraestruturas nacionais críticas. Os padrões de segurança fornecem controles de segurança obrigatórios a serem observados. Eles são medidas mínimas de segurança a serem implementados, destinados a proteger as informações e todas as atividades vinculadas das empresas. Estas atividades vinculadas são atividades técnicas e gerenciais de realização de ações necessárias para o cumprimento da família ISO 27000 e respectiva certificação. Para isso, a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) para sistemas e ferramentas corporativas é o passo inicial, mas infelizmente tanto os relatórios quanto os documentos que as empresas precisam produzir para atender aos requisitos da ISO são múltiplos e heterogêneos, levando a atividades muito complexas a ser executada durante as fases de projeto, implementação e auditoria de segurança.

Assim, Casola et al. (2019) apontaram problemas durante o processo de certificação da família ISO 27000 relacionados à falta de diretrizes claras na implementação dos controles de segurança de informação e ao alto nível de flexibilidade da estruturação e produção da documentação. Isso leva a uma proliferação de Sistema de Gestão da Segurança da Informação (SGSI) diferentes e heterogêneos, gerando dificuldades para os auditores identificarem as informações necessárias para a avaliação da segurança da informação. Como solução para esses problemas, estes autores focam na construção de uma ontologia de domínio de segurança da informação com base na ISO para facilitar o gerenciamento de documentos relacionados a padrões e conformidade durante todo o ciclo de vida de um SGSI.

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. No que lhe concerne, o trabalho de Meriah et al. (2021) considera que um dos problemas básicos relacionados à segurança da informação é a falta de uma visualização clara e simples nos sistemas de informação organizacionais. A terminologia de segurança informação não é precisamente definida e leva a confusões entre os stakeholders e os clientes desses sistemas.

No trabalho de Parkin et al. (2021), os autores exploraram as oportunidades criadas ao reconhecer a conversa entre líderes de negócios e especialistas em segurança como uma

“zona de negociação”. Eles abordaram que apoiar essas conversas por meio de uma “zona de negociação” pode ser o caminho para melhorias de segurança sustentáveis e viáveis nas organizações. Uma conversa é motivada por detalhes de um incidente no centro de uma história, com potencial para se conectar a informações com as quais o líder de negócios ou consultor de segurança está mais familiarizado em seu próprio domínio de negócio. Assim, esta “zona de negociação” ocorre com a troca de conhecimento nas histórias de fontes de notícias ou como anedotas de colegas confiáveis que chegam a estes líderes empresariais. Estes autores entendem que uma ferramenta de suporte à decisão que pode favorecer a troca de experiências em segurança da informação é a ontologia. Esta ontologia é denominada *Security Storytelling Ontology*¹ e está relacionada ao conhecimento de segurança de informação organizacional. Ela é um ponto de referência que ajuda a relacionar diferentes perspectivas sobre questões de segurança, no que se refere a esta “zona de negociação”.

3.3 Considerações Finais

A percepção para construção de uma ontologia de domínio para representação da segurança da informação em SoS emergiu do trabalho de Dias et al. (2020) que demonstrou a necessidade de se observar questões de segurança em SIF que é um tipo de SoS.

Para tanto, os autores Casola et al. (2019), Meriah et al. (2021) e Parkin et al. (2021) trazem importantes discussões e contribuições para a pesquisa em segurança da informação em SI. Estes autores apresentam como solução uma ontologia de domínio de segurança da informação para o campo de SI em seus respectivos domínios. O diferencial desta pesquisa em relação aos trabalhos dos respectivos autores está na caracterização de um corpo de conhecimento que permita o planejamento e desenvolvimento de soluções de problemas de segurança da informação para os profissionais que atuam no âmbito de SoS. Dessa forma, não foi identificado, até o momento, um trabalho que direcionasse esforços para o desenvolvimento de uma ontologia de domínio para o campo de segurança da informação em SoS. Isso gerou a oportunidade para a realização deste estudo.

¹<https://github.com/simonarnell/security-storytelling-ontology>

4. Mapeamento Sistemático da Literatura

Este capítulo está organizado da seguinte forma: a Seção 4.1 traz a motivação e justificativa para o mapeamento sistemático realizado nesta pesquisa. A Seção 4.2 apresenta a metodologia, detalhando o planejamento e execução do mapeamento. A Seção 4.3 apresenta as limitações do mapeamento sistemático. A Seção 4.4 aborda a discussão dos resultados. Finalmente, a Seção 4.5 fornece uma visão geral da contribuição do mapeamento para a pesquisa.

4.1 Introdução

Nos últimos anos, as organizações têm enfrentado dificuldades no gerenciamento de segurança da informação em sistemas complexos como o SoS em um ambiente globalizado e dinâmico. Um dos desafios é manter a transparência de como os dados são visualizados no SoS e a interoperabilidade de como os seus sistemas constituintes se comunicam.

Neste contexto, o principal objetivo deste estudo é identificar quais tecnologias de segurança da informação são utilizadas no contexto de SoS. Neste trabalho, são considerados como tecnologias os modelos, métodos, técnicas ou ferramentas de segurança da informação que podem ser implementados em SoS. Para obter estas respostas, foi planejado e conduzido um Mapeamento Sistemático da Literatura (MSL).

4.2 Protocolo e Execução

Este estudo teve como base as diretrizes de Kitchenham e Charters (2007) e inspirado em Fernandes et al. (2018). Dessa forma, este protocolo foi elaborado para a execução do mapeamento sistemático, composto pelas seguintes fases: (1) Planejamento, (2) Execução e (3) Apresentação dos Resultados.

4.2.1 Planejamento

4.2.1.1 Questão de Pesquisa:

Visando expressar os objetivos deste estudo, a questão de pesquisa (QP) foi formulada seguindo os critérios especificados no PIO (*Population, Intervention e Outcome*), como pode ser visto na Tabela 1.

Tabela 1: Critérios de PIO

População	Sistemas-de-Sistemas
Intervenção	Tecnologias de Segurança da Informação
Resultado	Técnicas / Modelos / Métodos / Ferramentas

Com isso, foi formalizada a seguinte QP:

QP: *Como as tecnologias de segurança da informação têm sido utilizadas no contexto de um SoS?*

Para ajudar a responder a QP, também foram elaboradas as seguintes subquestões (SQ):

SQ1: *Que métodos, técnicas, modelos e ferramentas têm sido utilizados para a segurança da informação em SoS?*

SQ2: *Como é feita a avaliação desses métodos, técnicas, modelos e ferramentas?*

SQ3: *Quais fatores mais específicos são considerados no contexto de segurança da informação em SoS?*

4.2.2 Estratégia de Busca

A estratégia de pesquisa se baseou em uma combinação de buscas eletrônicas em bases de dados de literatura científica, bibliotecas digitais e pesquisas manuais em anais de eventos específicos da área de SoS. As buscas eletrônicas foram realizadas na base Scopus¹ e nas bibliotecas digitais ACM Digital Library², IEEE Xplore³ e Science Direct⁴. Essas bases de dados foram escolhidas, pois armazenam um grande volume de trabalhos científicos relevantes da área de Ciência da Computação, seguindo as recomendações de Dyba et al. (2007). As pesquisas manuais foram realizadas nos anais do *Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems* (WDES)⁵ que não estavam indexados em bibliotecas digitais, por ser um workshop internacional de

¹<https://www.scopus.com/>

²<https://dl.acm.org/>

³<https://ieeexplore.ieee.org/Xplore/home.jsp>

⁴<https://www.sciencedirect.com/>

⁵<http://sesos-wdes-2020.icmc.usp.br/Previous.php>

referência no assunto.

4.2.2.1 Definição dos Termos de Pesquisa:

Para a pesquisa nas bases de dados definidas, foi criada uma *string* de busca com a junção dos termos, que representam a população e a intervenção que compõem os critérios PIO apresentados na Tabela 1. Também foram adicionados alguns sinônimos e/ou termos variantes para ampliar os resultados das buscas. Os termos foram escritos em língua inglesa, por ser o idioma amplamente adotado na literatura científica e em diversos periódicos e conferências internacionais. Após a realização de alguns testes, chegou-se à seguinte *string* de busca:

(“systems of systems” OR “system of systems” OR “system-of-systems” OR “systems-of-systems”) AND (“information security” OR “InfoSec” OR “IT security”)

4.2.2.2 Critérios de Seleção dos Estudos:

A Tabela 2 descreve os critérios de inclusão (CI) e exclusão (CE) a serem aplicados sobre os estudos retornados pela *string* de busca, conforme Kitchenham e Charters (2007).

Tabela 2: Critérios de Seleção

	Código	Descrição
Critérios de Exclusão	CI1	O estudo aborda tecnologias de segurança da informação em SoS.
	CI2	O estudo aborda fatores de segurança da informação em SoS.
Critérios de Exclusão	CE1	O estudo não está escrito em inglês.
	CE2	O estudo não é um artigo de pesquisa científica ou artigo de conferência.
	CE3	O estudo não está disponível para download abertamente ou através de IP institucional.
	CE4	O estudo não está relacionado à área de Ciência da Computação.
	CE5	O estudo está duplicado e/ou reporta resultados de outro estudo (neste caso, será considerado o estudo mais atual para a análise).
	CE6	O estudo não atende os critérios de inclusão.

4.2.3 Execução

4.2.3.1 Processo de Seleção dos Estudos

O processo de seleção foi constituído de cinco etapas: (1) execução da busca; (2) remoção de duplicados; (3) 1º filtro: leitura de títulos, resumos e palavras-chave; (4) 2º filtro: leitura da introdução e conclusão; e (5) 3º filtro: leitura completa do estudo. Com o intuito de garantir a confiabilidade dos resultados obtidos, cada estudo foi analisado por dois pesquisadores nas etapas 3 a 5 e as divergências foram debatidas até se atingir o consenso.

O processo de seleção dos estudos foi executado nas bases no início do mês de outubro de 2020. Na etapa 1, foi executada a busca eletrônica com a *string* de pesquisa nas bases selecionadas. Com auxílio dos filtros automáticos disponibilizados em algumas bases, foram excluídos também alguns estudos que não estão escritos na língua inglesa, que não estão relacionados à área de Ciência da Computação e que não se enquadram nas categorias artigo de periódico (*research article*) e artigo de conferência (*conference paper*). Os resultados recuperados foram armazenados na ferramenta Parsifal⁶ para execução da etapa 2 (remoção de duplicados), quando foram removidos os estudos duplicados de forma automatizada.

Após essa etapa, a filtragem dos resultados ocorreu em três etapas. Nos dois primeiros filtros (etapas 3 e 4), os estudos foram analisados e selecionados por meio da aplicação dos critérios de inclusão e exclusão apresentados na Tabela 2. Na etapa 5, foi realizada a leitura completa dos estudos que restaram dos filtros anteriores. A análise nesta etapa teve como foco identificar quais estudos poderiam fornecer resultados que auxiliem na resposta da QP. Caso não cumprissem essa condição, os estudos eram excluídos do mapeamento, restando 18 (dezoito) estudos para o procedimento de extração de dados. A Figura 6 ilustra uma visão geral dos resultados quantitativos obtidos em cada etapa do processo.

4.2.3.2 Procedimento de Extração de Dados:

O processo de extração foi realizado sistematicamente, com o auxílio da ferramenta Parsifal para o registro das informações necessárias para responder às questões de pesquisa por meio de um formulário contendo os seguintes campos: (1) identificador do estudo (ID), (2) título, (3) autores, (4) ano, (5) tecnologia utilizada para segurança da informação em SoS, (6) avaliação da tecnologia apresentada no estudo (e.g., experimento, ensaio,

⁶<https://parsif.al/>

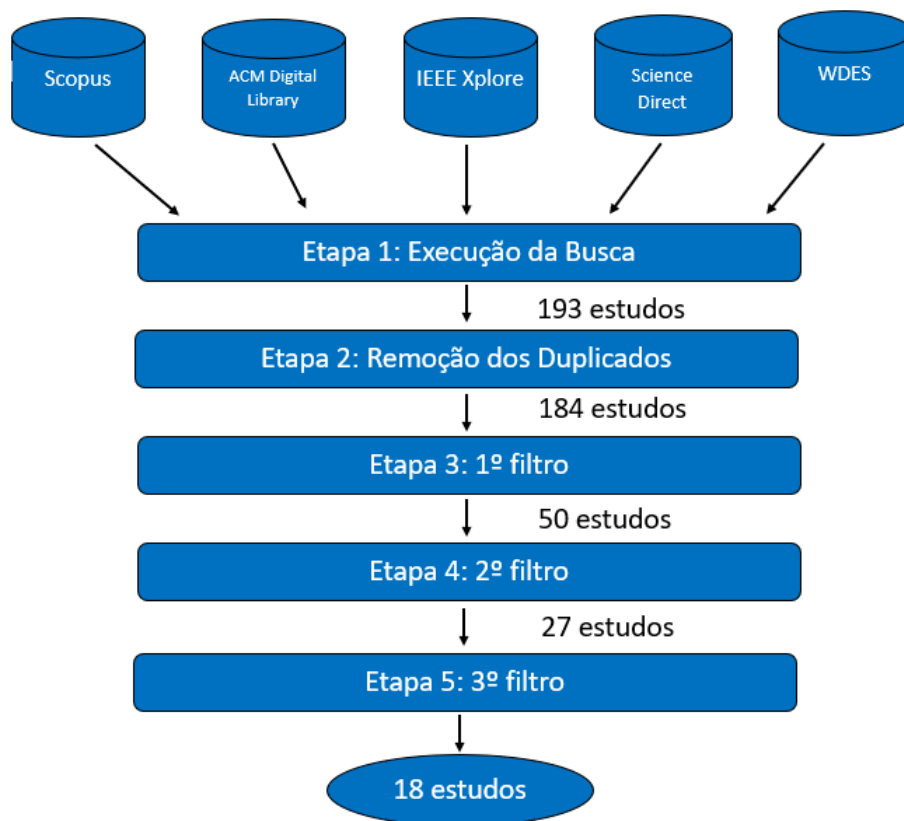


Figura 6: Resultados do processo de seleção de estudos.

estudo de caso, validação com especialista etc.) e (7) fatores para segurança da informação em SoS.

4.2.4 Apresentação dos Resultados

4.2.4.1 Dados Demográficos

Na Figura 7, é apresentada a evolução cronológica dos 18 estudos selecionados. É possível notar que a maioria dos estudos foi publicada nos últimos 10 anos, o que pode sinalizar que a área de pesquisa envolvendo segurança da informação e SoS é recente.

Conforme observado na Figura 8, os estudos primários relevantes foram conduzidos predominantemente nos EUA (6 estudos - 33,3% do total), seguido pelo Reino Unido (5 estudos - 27,8% do total). Os demais países apresentaram somente 1 estudo (5,6% do total para cada um).

A Tabela 3 apresenta a síntese da extração de dados dos estudos selecionados, em ordem decrescente de ano de publicação, de acordo com as seguintes dimensões alinhadas às sub-questões de pesquisa: *tecnologia utilizada para segurança da informação em SoS*, *avaliação da tecnologia apresentada no estudo* e *fatores para segurança da informação*

Tabela 3: Dados extraídos dos estudos selecionados.

ID	Título	Referência	Tecnologia utilizada para segurança da informação em SoS	Avaliação da tecnologia apresentada no estudo	Fatores para segurança da informação em SoS
E1	Identifying and mitigating security risks for secure and robust NGI networks	Lever e Kifayat (2020)	Algoritmo probabilístico	Análise de resultados	Controle de acesso, risco de nós centralizados e distância entre os nós
E2	Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology	Petratos e Faccia (2019)	Análise da superfície de ataque cibernético	Análise sistemática	Pontos de vulnerabilidade
E3	Simulation Trust and the Internet of Things	Loper (2019)	Simulação de ambiente para uso de IoT	Ambiente controlado para medir os resultados sem interferências	Criptografia, latência e privacidade
E4	A systems-of-systems security framework for requirements definition in cloud environment	Carturan e Goya (2019)	<i>Framework</i> para definição de requisitos de segurança em um ambiente de computação em nuvem	Experimento em empresa	Vulnerabilidades e confiabilidade dos componentes, proteção dos dados e carga de trabalho
E5	Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems	Tagarev e Sharkov (2019)	Análise de dados, Monte Carlo e Cadeia de Markov	Análise de dados usando Inteligência Artificial	Predição de ataques ou vulnerabilidades
E6	Assessing System of Systems Security Risk and Requirements with OASoSiS	Ki-Aries et al. (2018)	Abordagem para elicitar, analisar e validar riscos e requisitos de segurança	Estudo de caso	Fatores humanos, ameaças, vulnerabilidades, riscos, confidencialidade, integridade, disponibilidade e responsabilidade
E7	Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach	Ceccarelli et al. (2018)	Ferramenta de apoio	Identificação de ameaças a SoS	Interconexão e vulnerabilidades
E8	Real-time secure communication for Smart City in high-speed Big Data environment	Rathore et al. (2017)	Proposta de novo protocolo de segurança	Análises comparativas	Custo computacional e comunicação segura
E9	Security of communications in connected cars Modeling and safety assessment	Tbatou et al. (2017)	Criptografia, PKI e Hash	Estudo de caso	Latência e poder computacional
E10	System of systems cyber effects simulation ontology	Ormrod et al. (2015)	Modelagem de sistema	Análise comparativa	Risco e impacto de ataques
E11	Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis	Guariniello e De Laurentis (2014)	Ferramenta para avaliar impacto de ciberataques	Experimento real em SoS	Risco e impacto de ataques
E12	On advanced cryptographic techniques for information security of smart grid AMI	Mihaljevic et al. (2011)	Criptografia de chave simétrica	Análise comparativa de métodos criptográficos	Poder computacional e latência
E13	Extracting security control requirements	Hosey e Gamble (2010)	Análise documental	Análise por especialistas	Padrões de referência
E14	System-of-systems boundary check in a public event scenario	Zhou et al. (2010)	Ferramenta de modelagem para destacar possíveis pontos de violação de acesso em comunicação em rede	Cenário simulado	Políticas de segurança de uma organização constituinte e pontos de vulnerabilidade
E15	Modeling the linkage between systems interoperability and security engineering	Neaga e Henshaw (2010)	Modelagem de links entre interoperabilidade e segurança	É apresentada somente uma visão holística	Fatores organizacionais e humanos, como responsabilidades pessoais (políticas e melhores práticas para segurança do sistema) e vulnerabilidades
E16	Model driven security accreditation (MDSA) for agile, interconnected it landscapes	Lang e Schreiner (2009)	MDSA: análise de documentos de forma automática	Validação com especialistas	Documentação completa e precisa
E17	A new schema for security in dynamic uncertain environments	Agrawal (2009)	Esquema de monitoramento para compartilhamento de informação	Exemplos de aplicação	Comportamento do usuário e riscos agregados
E18	System-of-systems security engineering	Bodeau (1994)	Processo para Engenharia de Segurança em SoS	Análise descritiva de cada etapa do processo	Riscos associados ao fluxo de informações, domínios da política de segurança, interfaces entre constituintes e tipo de arquitetura



Figura 7: Estudos publicados no período de 1994 a 2020.

Fonte: Elaborado pelos autor.

em SoS. Os códigos ID apresentados serão utilizados para referenciar os estudos ao longo das próximas seções.

As *tecnologias de segurança da informação* dizem a respeito de modelos, métodos, técnicas ou ferramentas de segurança da informação utilizadas em todo o contexto de SoS. A *avaliação da tecnologia* apresenta como foi testada e/ou validada a tecnologia proposta no estudo (experimento, estudo de caso, cenário simulado, análise comparativa, validação com especialista etc.). Em relação aos *fatores de segurança da informação*, são listados os fatores que influenciaram no contexto da solução aplicada no estudo, de modo a identificar se há algum padrão que se repete nos demais estudos.

4.2.4.2 Análise dos Resultados:

Para responder à QP, os dados coletados foram analisados a partir das respostas das Subquestões:

SQ1 *Que métodos, técnicas, modelos e ferramentas têm sido utilizados para a segurança da informação em SoS?*

A partir dos estudos analisados, é possível perceber que diversas tecnologias são empregadas para segurança da informação em SoS. Em sua maioria, tratam-se de abordagens analíticas, modelagens, esquemas, algoritmos e, em menor número, ferramentas. Dentre as tecnologias, pode-se destacar o uso de **protocolos** para orientar a implementação de medidas de segurança da informação em E8; a aplicação de **criptografia** como forma de proteger os dados que trafegam entre os constituintes em E9 e E12; e o uso de **algoritmo** probabilístico, como Monte Carlo, para mitigar riscos de segurança da informação

Estudos publicados no período de 1994 a 2020.

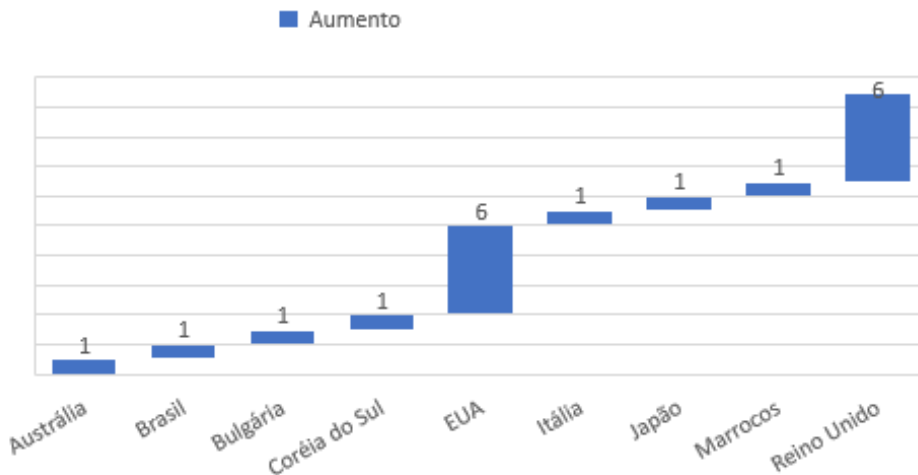


Figura 8: Distribuição dos estudos selecionados por país no período de 1994 a 2020.
Fonte: Elaborado pelo autor.

no ambiente SoS em E1.

Embora não exista uma definição ou padronização do uso de técnicas, modelos, métodos ou ferramentas em segurança de SoS, a análise dos estudos permitiu identificar as seguintes tecnologias aplicadas: **esquemas de monitoramento** constante na troca de informações entre os constituintes em E17; a **simulação de ambiente** para análise de compartilhamento de informações em ambiente controlado em E3 e E14 para compreender os possíveis efeitos de ataques durante tráfego das informações; e a **análise de pontos de vulnerabilidade**, durante a interoperação entre os constituintes em E15, quando é possível mitigar esses pontos assim que mapeados.

***SQ2** Como é feita a avaliação desses métodos, técnicas, modelos e ferramentas?*

A escolha de um método de avaliação depende, principalmente, do tipo de tecnologia e do objetivo. Como metodologia de avaliação aplicada nos estudos, foi possível perceber a recorrência de: **estudos de caso** em E6 e E9, que permite por meio de um cenário real ou realista compreender os efeitos da tecnologia proposta; **análise e validação feita por especialista** em E13 e E16, onde a coleta de dados reais contribui diretamente com soluções para o problema, geralmente aplicadas em casos que envolvem modelagem ou análise de documentação de arquitetura ou requisitos de projeto; e **análise comparativa** em E8 e E10, que buscam referências em situações similares de exposição a riscos e pontos de vulnerabilidade para propor uma solução de segurança.

Outra forma de avaliação que merece atenção é o uso de **Inteligência Artificial (IA)** - *Deep Learning* e *Machine Learning* em E5 para analisar os dados de operação em sistemas distribuídos e verificar a eficácia dos pontos de segurança, assim como a resiliência do sistema em ciberataques. As análises com IA têm sido promissoras, porém requerem amadurecimento para se tornarem propostas viáveis. Também pode-se destacar uma **análise descritiva** dos processos para engenharia de segurança em SoS feita em E18.

***SQ3** Quais fatores mais específicos são considerados no contexto de segurança da informação em SoS?*

Nesta questão, buscou-se identificar que tipos de fatores condicionam as tomadas de decisão em relação a implementação de medidas de segurança da informação em SoS, partindo dos conceitos da tríade CID apresentada na norma ISO/IEC 27002:2013 (ISO, 2013). Foi possível notar que um fator crítico para a maioria das abordagens nos estudos é a análise e identificação dos **pontos de vulnerabilidade** no SoS e em seus constituintes, como pode ser visto em E2, E4, E5, E6, E7, E14 e E15.

Outro fator bastante frequente, e relacionado com o anterior, é análise e identificação de **risco de ataques ou ciberataques**, conforme E1, E5, E6, E10, E11, E17 e E18. O risco está bastante associado ao negócio e missão do SoS, bem como aos tipos de relacionamentos existentes entre os sistemas constituintes. Tanto risco de ataques como pontos de vulnerabilidade são mais considerados como ponto de atenção em soluções de abordagem analíticas, de modelagem e aplicação de ferramentas.

Em menor número de ocorrência, mas também vale destacar como fatores as **políticas de segurança**, presente em E14 e E1, e os **fatores humanos**, presente em E6, E15 e E17. As políticas de segurança (e.g., controle de acesso ou nível de privacidade dos dados) que cada organização dos constituintes adota devem ser consideradas ao planejar o esquema de segurança do SoS. Os fatores humanos também influenciam na decisão, pois os comportamentos de atores ou o tipo de cliente do SoS devem ser previstos para que as funcionalidades do SoS não sejam comprometidas com a implementação da tecnologia de segurança da informação.

4.3 Limitações

Este trabalho apresenta algumas limitações como a quantidade termos sinônimos constantes na *string* de busca, o que pode ter limitado o número de estudos retornados. Além disso, bases como *Web of Science* e *SpringerLink* não foram incluídas nas buscas, embora

as bases selecionadas tenham sido consideradas como principais. Dessa forma, este estudo pode ser expandido no futuro com uma *string* de busca mais ampla e adicionando as bases de dados mencionadas.

4.4 Discussão

Após uma análise dos 18 estudos selecionados, foi possível responder à questão de pesquisa deste trabalho: *[QP] Como as tecnologias de segurança da informação têm sido utilizadas no contexto de um SoS?* De forma geral, os estudos apontam para a tendência de que as técnicas, processos, métodos e abordagens de segurança da informação devem envolver a integração com os mais diversos tipos de sistemas e bases de dados de diferentes organizações.

O que pode incluir a conexão com computação em nuvem para armazenar dados, sistemas de *Big Data Analytics* para colher, inspecionar, tratar e modelá-los com objetivo de obter *insights* e identificar oportunidades para a organização. Também deve incluir ERP (do inglês, *Enterprise Resource Planning*, ou Planejamento de Recursos Empresariais) para acessar todos os dados e processos dos mais diversos departamentos de uma organização. Isto obriga um SoS e seus constituintes a interoperarem com esses sistemas e suas bases de dados.

Graciano Neto et al. (2017) destacam que integrar dados oriundos de diferentes políticas de acesso e visibilidade é um desafio para a interoperabilidade plena de sistemas em um ambiente altamente dinâmico e distribuído. Tal interconexão pode proporcionar o aumento da superfície de ataque e a diminuição da segurança cibernética como é relatado em E2, em cujo estudo os autores utilizam uma metodologia de **análise de superfície de ataque** cibernético para avaliar as ameaças de ciberataques em um SoS que está interconectado a um Sistema de Informação Contábil (SIC).

Assim, seria interessante o *stakeholder* conhecer quantos sistemas estão interconectados ao SoS, qual é a arquitetura desses sistemas e como a integração e/ou interconexão é realizada. Um invasor experiente pode usar com facilidade este tipo de informação para obter acesso e transmitir ataques cibernéticos em pontos de vulnerabilidades específicos, comprometendo a segurança do SoS e obtendo, dessa forma, informações privilegiadas. Por exemplo, em E9, os autores mencionam que *hackers* podem invadir os sistemas de carros inteligentes e acessar sensores que controlam *airbags*, sistemas de desligamento, operações de travamento de portas e até mesmo desabilitar todo o carro. Eles podem usar ataques de negação de serviço para derrubar a rede dos veículos, reprogramar ilegalmente

as unidades de controle eletrônico (UCE) do carro com software malicioso e podem até baixar mapas de navegação incorretos e enganar o motorista.

Os efeitos gerados de ataques direcionados podem vir em cascata e geralmente são amplificados de um sistema específico para outro mais geral na hierarquia, criando falhas sistêmicas e colapsando todo o SoS. Uma solução encontrada para proteger a confidencialidade, autenticidade e integridade da informação que circulam por meio desses veículos conectados é a utilização de **criptografia** e **protocolos** de segurança nas camadas físicas, de *link* de rede ou de aplicativo. Também devem ser utilizadas tecnologias de infraestrutura de chave pública (do inglês, *public key infrastructure*, ou PKI) para proteger os pontos de acesso dos canais de comunicação do veículo e a autenticação pode ser realizada usando códigos de autenticação de mensagens ou assinaturas digitais, e.g., a função *hash*.

Ainda é mencionado em E12 o uso de técnicas de criptografia de chave simétrica, autenticação e gerenciamento de chaves secretas. Elas minimizam a sobrecarga implícita dos requisitos de segurança em um ambiente de medição inteligente de energia elétrica (do inglês, *Advanced Metering Infrastructure* ou AMI).

Em E1, os autores argumentam que os desafios das cidades inteligentes estão relacionados a como os seus sistemas constituintes são conectados e interligados por meio de redes locais e Internet. Como um tema investigado em E2, tais sistemas constituintes estão ficando mais complexos, escalonáveis e a ameaça ao tamanho da superfície da distância dos nós está ficando mais dinâmica. Isso cria uma alta dependência entre os sistemas constituintes com níveis e hierarquias diferentes, aumentando os riscos de avarias massivas, seja através de uma falha acidental ou de um ataque malicioso. Devido ao aumento no número de dispositivos distintos interconectados, tornou-se difícil desenvolver uma solução de segurança dinâmica e confiável que possa proteger o SoS contra todos os riscos de segurança potenciais.

Cabe também ressaltar que E17 considera a importância de **esquemas de monitoramento** de segurança na rede em que o SoS está envolvido. Estes esquemas precisam incorporar explicitamente mecanismos que monitoram o ambiente geral e alimentam suas observações com os requisitos de segurança para compensar a incerteza e o dinamismo do ambiente. Tais esquemas também devem incorporar mecanismos de segurança individuais projetados para fornecer parâmetros de “controle” que podem ser definidos para ajustar as propriedades de segurança do sistema e mantê-los em limites aceitáveis. Isso pode ocorrer mesmo quando o ambiente e o contexto do sistema passam por mudanças como a integração e interconexão com outros sistemas, a atualização do software que executa um

sistema específico ou até mesmo a descontinuação de um constituinte no SoS.

Portanto, é importante analisar e compreender a conectividade de diversos sistemas em diferentes níveis, de modo a identificar vulnerabilidades e mitigá-las. A solução apresentada em E1 considera o uso de **algoritmos** evolutivos e probabilísticos de forma dinâmica para otimizar o nível de segurança nesses ambientes, considerando fatores como controle de acesso, risco de nós centralizados e distância entre os nós. Além disso, é interessante mencionar, em E5, o uso de medidas preditivas de ataques cibernéticos ou de vulnerabilidades por meio de algoritmos de **simulação de ambiente** como Monte Carlo e Cadeia de Markov.

Cabe também destacar a importância da segurança de sistemas legados que, por conta da sua tecnologia antiga, esbarram em códigos antigos e complexos, dificultando a interoperação com outros sistemas, colocando em risco o bom andamento dos negócios, já que impede o crescimento e a expansão do SoS. Uma solução prática encontrada em E13 para interconectar e integrar sistemas legados é formar um conjunto de **requisitos funcionais** abrangentes que governem um SoS nos níveis local, global e de interação. Tal mudança pode reduzir qualquer ambiguidade na determinação se essa interconexão ou integração satisfaz os controles de segurança, i.e., se atende ao princípio da confidencialidade que determina que somente os dados necessários para o compartilhamento da informação estejam disponíveis para acesso autorizado de sistemas.

Ao mesmo tempo, isso reduz a necessidade de reexaminar todos os requisitos quando influências externas forçam esses sistemas, funções ou variáveis computacionais a mudar devido à configuração com novas tecnologias. Em vez disso, apenas os requisitos afetados pela mudança são direcionados para nova verificação. Além disso, é importante que a gestão dos dados entre os constituintes seja provida conforme os padrões acordados pelas diferentes políticas e regras de gerenciamento e controle das diversas organizações proprietárias do SoS. As políticas de segurança dos constituintes (E14 e E15) devem garantir que os dados sejam autênticos e corretos e no formato necessário para a interoperação.

4.5 Considerações Finais

Este mapeamento sistemático teve como objetivo investigar como as tecnologias de segurança da informação são utilizadas no contexto de SoS. A partir disso, o intuito foi caracterizar esse domínio para criar um corpo de conhecimento que possa apoiar pesquisadores e profissionais que atuam no âmbito de SoS no planejamento e desenvolvimento de soluções para problemas de segurança da informação.

Por meio deste MSL, foram retornados 18 estudos que apresentam uma profusão de métodos, técnicas, modelos e ferramentas relacionadas a essas questões de segurança no SoS. Assim, é possível perceber uma tendência, ainda que inicial, dos tipos de abordagens de segurança da informação aplicadas em SoS. Os trabalhos 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.

O MSL também apresentou um panorama sobre a pesquisa na área, ressaltando as tecnologias aplicadas nos estudos (e.g., protocolos, criptografia, algoritmos e simulação de ambiente) de modo que os *stakeholders* possam refletir sobre os riscos cibernéticos e que estes riscos também são riscos tecnológicos e podem gerar impactos no processos de tomada de decisão em suas respectivas organizações. Um programa de gestão de recursos humanos sobre segurança da informação deve ser realizado paralelamente para que todos que interagem com o SoS não gerem acesso a pontos de vulnerabilidades desconhecidos.

Também são apresentados alguns fatores como pontos de vulnerabilidade, a análise de riscos de ataques e as políticas de segurança dos constituintes como os mais críticos para as soluções propostas nos estudos. Como alguns desses fatores são indicadores para a predição de ataques ao SoS, cabe destacar soluções que envolvam algoritmos e IA para antever essas ocorrências. Tal ocorrência pode impulsionar o desenvolvimento de ferramentas para atuar de forma automatizada nesses casos.

5. Pesquisa de Opinião

Este capítulo está organizado da seguinte forma. A Seção 5.1 discute a motivação para a pesquisa de opinião. A Seção 5.2 descreve o planejamento e execução da pesquisa de opinião e o procedimento para a análise qualitativa. A Seção 5.3 apresenta resultados quantitativos e qualitativos explorando o tripé da área: pessoas, processos/organizações e tecnologias. A Seção 5.4 apresenta as limitações encontradas. A Seção 5.5 apresenta as discussões relacionando os resultados do MSL com os resultados da pesquisa de opinião. Por fim, a Seção 5.6 fornece uma visão geral da pesquisa de opinião com algumas considerações finais.

5.1 Introdução

O SoS são compostos por sistemas constituintes independentes, que atuam conjuntamente para realização de um objetivo comum por meio da interação entre eles (NIELSEN et al., 2015). No cenário sociotécnico e organizacional que reconhece a interação entre pessoas e a tecnologia em uma organização, é um desafio manter a transparência das informações e a interoperabilidade entre os sistemas constituintes do SoS.

Isso ocorre em virtude da interconectividade e a interação que devem ser preservadas para o cumprimento de um ou mais objetivos globais (GRACIANO NETO et al., 2017) (FERNANDES et al., 2018). Tal interconectividade e interação permite a conexão com aplicativos, serviços de computação em nuvem e os mais diversos tipos de sistemas em cenários com escala ou complexidade variada, tais como militar, transporte, financeiro, energia, saúde, Internet, entre outros.

Isso faz com que no gerenciamento desses sistemas sejam observadas questões de segurança, principalmente para evitar que ocorram falhas por meio de ataques cibernéticos e acesso não autorizado a dados.

Assim, o objetivo desta pesquisa de opinião é analisar os aspectos de segurança da informação com o propósito de avaliar os resultados obtidos no MSL do Capítulo 4, com respeito à sua aplicabilidade na indústria do ponto de vista de pesquisadores e profissionais no contexto de SoS.

Para isso, foram escolhidos especialistas de comitê de congressos acadêmicos, pois são os eventos de referência das áreas de segurança da informação e SoS. Além disso, muitos desses especialistas também atuam profissionalmente na indústria ou possuem projetos de pesquisa aplicados a cenários reais, conferindo uma visão mais ampla para caracterizar o domínio de segurança da informação e SoS.

5.2 Planejamento

Com o propósito de compreender a necessidade do questionário de pesquisa, buscou-se primeiramente relacionar o tema para justificar a necessidade (WOHLIN et al., 2012). Dessa forma, as questões formuladas serviram para identificar quais aspectos de segurança da informação discutidos na literatura são aplicados no contexto desses sistemas. Para isso, foram formuladas 38 questões, sendo 5 questões demográficas e 33 questões específicas apresentadas no Apêndice I.

As questões específicas foram divididas em três partes seguindo as dimensões de SI na visão de Laudon e Laudon (2004):

- 1) **Tecnologias:** considera a tecnologia da informação como uma ferramenta utilizada pelos gerentes e tomadores de decisão para enfrentar as constantes mudanças nas organizações;
- 2) **Processos/Organizações:** envolve a coordenação do trabalho de uma organização por meio de uma hierarquia estruturada e processos de negócio;
- 3) **Pessoas:** envolve como as pessoas constroem os SI, os mantêm e os utilizam nas organizações.

O tempo de participação na pesquisa foi de 15 a 20 minutos. As questões foram disponibilizadas por meio de formulário eletrônico Google Forms.

A população-alvo foram especialistas de SI, SoS e Segurança da Informação que se encontram no comitê do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021) e *International Workshop on Software Engineering*

for Systems-of-Systems and Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (SESoS/WDES 2021).

Foram escolhidos especialistas desses dois comitês de congressos acadêmicos por esses congressos serem eventos de referência das áreas de segurança da informação e SoS. Além disso, muitos deles também atuam profissionalmente na indústria ou possuem projetos de pesquisa aplicados a cenários reais, conferindo uma visão mais ampla para caracterizar o domínio de segurança da informação e SoS.

5.2.1 Execução

A pesquisa de opinião no Apêndice I foi realizada entre os dias 8 de outubro e 12 de novembro de 2021, foram enviados o total de 117 convites com 32 respostas dos respectivos especialistas, gerando uma taxa de 27,35%, considerada positiva em estudos como este (pesquisa on-line) (NULTY, 2008) e considerando as dificuldades de condução de pesquisas desta natureza em Engenharia de Software e Sistemas de Informação (KITCHENHAM et al., 2015).

A Figura 9 apresenta os dados de tempo de experiência sobre áreas de conhecimento dos respondentes.

Escala:

0 = Menos de 1 ano;

1 = Entre 1 e 5 anos;

2 = Entre 5 e 10 anos;

3 = Entre 10 e 15 anos;

4 = Acima de 15 anos.

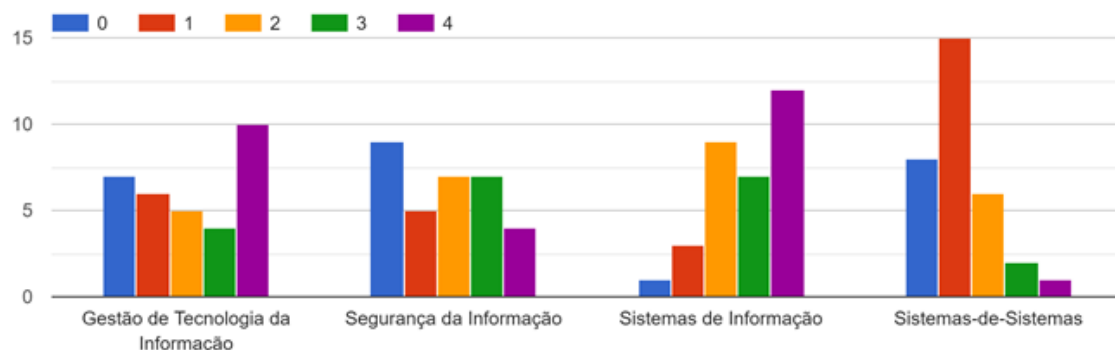


Figura 9: Tempo de experiência sobre as áreas de conhecimento dos respondentes.

5.3 Resultados

A primeira dimensão (tecnologias) da pesquisa relacionada ao nível de concordância dos respondentes em relação a tecnologias relevantes para apoiar segurança da informação em sistemas como SoS. Nesta dimensão, a questão 11 está relacionada ao uso de **análise dos pontos de vulnerabilidades** durante a interoperação entre os sistemas constituintes para mitigá-los assim que mapeados. Esta questão obteve o percentual de 68,8% que representa os especialistas que “concordam totalmente”, conforme apresentado na Figura 10.

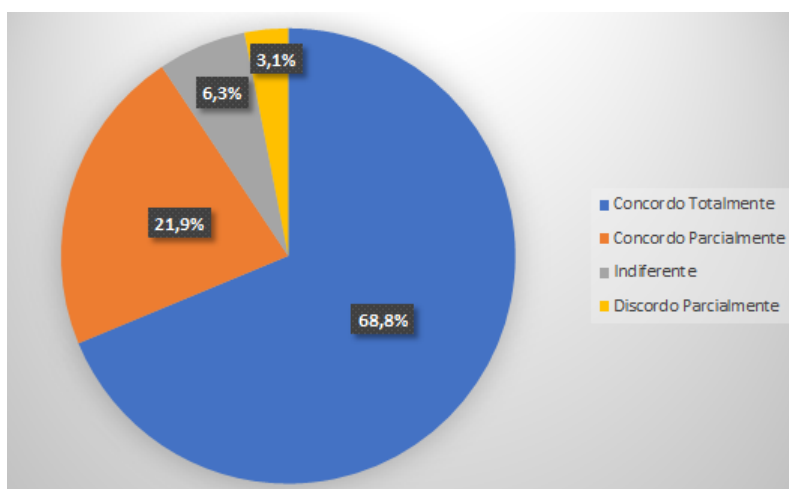


Figura 10: Percentual de concordância da questão 11 relacionada ao uso de análise de pontos de vulnerabilidades durante a interoperação entre os sistemas constituintes.

Outra questão que também recebeu o mesmo percentual de resposta dos especialistas foi a questão 16 que está relacionada ao uso de **protocolos** de segurança seguro e eficiente na transmissão de dados para proteção da comunicação, apresentada na Figura 11. Por exemplo, a comunicação entre um Sistema Remoto Inteligente (SRI) e os usuários de um edifício inteligente contra intrusos externos.

A segunda dimensão (processos) compreende os fatores de segurança da informação que condicionam as tomadas de decisão em relação à implementação de medidas de segurança da informação em SoS. Ela está relacionada ao nível de concordância dos respondentes em relação aos fatores que são mais críticos no contexto de segurança da informação em sistemas como SoS. Nessa dimensão, a questão 29, relacionada ao nível de **privacidade dos dados** que cada organização gestora dos sistemas constituintes adota deve ser considerado ao planejar o esquema de segurança do SoS, obteve o maior percentual de concordância dos especialistas. Os especialistas que responderam “concordam totalmente” foram 87,5%. Isso é evidenciado também na resposta de um dos especialistas:

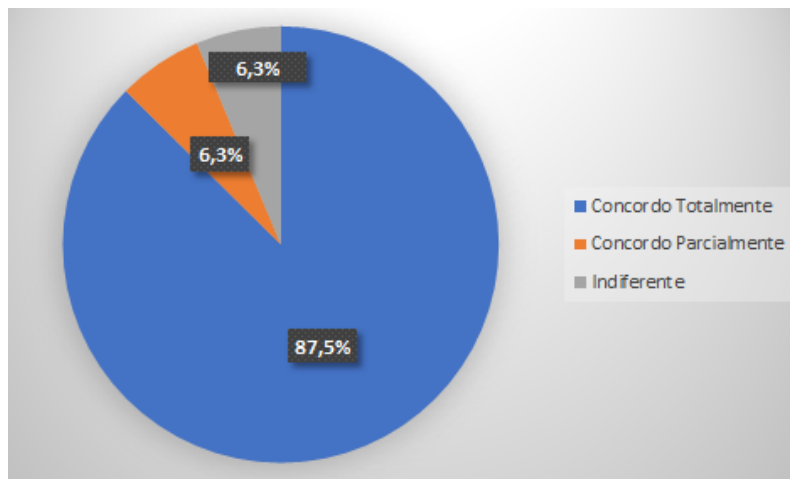


Figura 11: Percentual de concordância da questão 16 relacionada uso de protocolos de segurança seguro e eficiente na transmissão de dados para proteção da comunicação.

“... seria importante fazer uso de técnicas de privacidade como privacidade diferencial e secure multiparty computation para garantir que os dados coletados sejam analisados sem que haja problemas relacionados à privacidade.” [Especialista 13]

Outra questão que também recebeu alto percentual de concordância foi a questão 35 que está relacionada a **falta de padronização** dos métodos de segurança da informação podem gerar falhas que podem levar a vulnerabilidades de segurança da informação, apresentada na Figura 12. Por exemplo, o uso de métodos informais para soluções de problemas pela equipe de tecnologia da informação. Os especialistas que responderam “concordam totalmente” foram 71,9%.

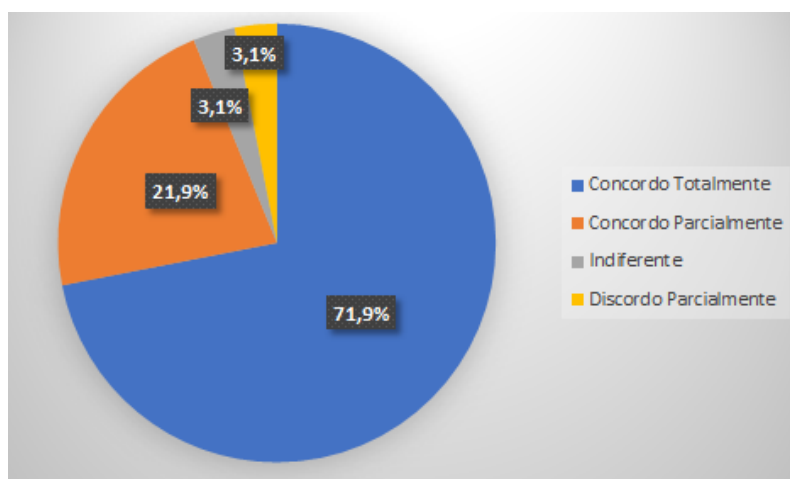


Figura 12: Percentual de concordância da questão 35 que está relacionada à falta de padronização dos métodos de segurança da informação.

Cabe também mencionar a questão 36 que está relacionada a **falta de treinamentos** especializados e na educação em todos os níveis dos colaboradores, desde funcionários

não técnicos até as equipes de tecnologia da informação. O descuido com o uso de uma ferramenta ou a falta de conhecimento dos riscos em sistemas como um SoS pode ser a porta de entrada para cibercriminosos. Os especialistas que responderam “concordam totalmente” foram 65,6%.

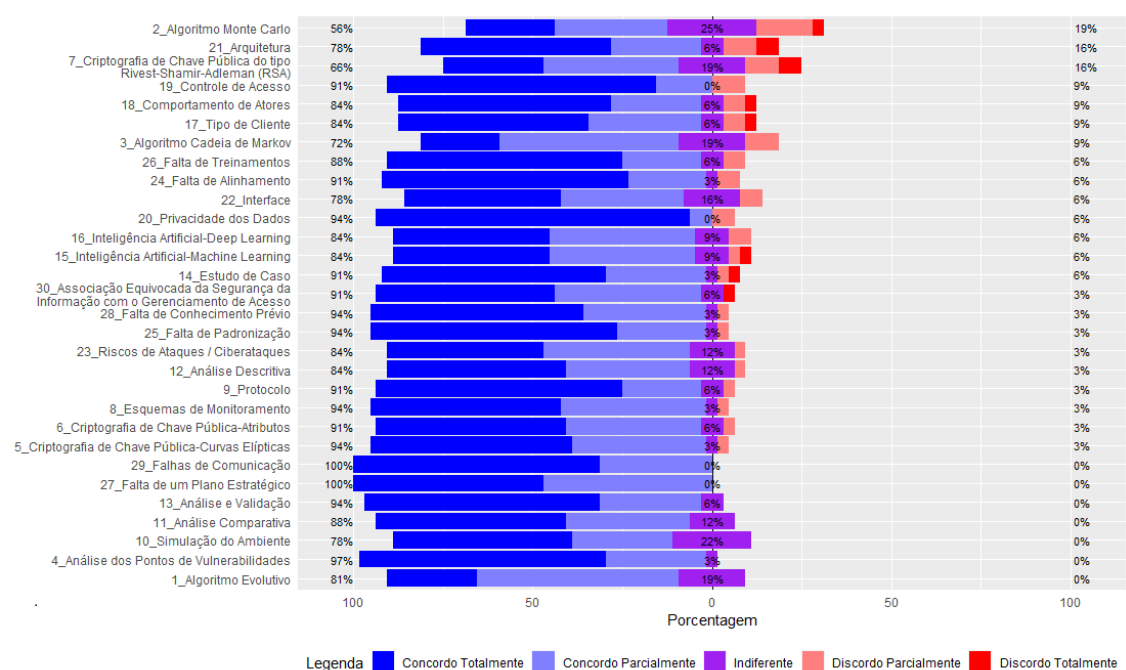


Figura 13: Resultados da pesquisa de opinião com a participação de 32 especialistas.

Já a questão 37 relacionada a **falta de um planejamento estratégico** eficiente com as características da segurança da informação em sistemas como um SoS pode gerar riscos para organização. É responsabilidade do gestor estar atento a essas características e, assim, criar um planejamento eficiente, buscando as tecnologias de segurança da informação que melhor atendam às políticas organizacionais. Os especialistas que responderam que “concordam totalmente” e “concordam parcialmente” foram 53,1% e 46,9%, respectivamente.

A terceira dimensão (pessoas) da pesquisa de opinião compreende nível de concordância dos respondentes em relação a alguns problemas que podem ser encontrar no contexto de segurança da informação em sistemas como SoS ao lidar com pessoas. Nessa dimensão, a questão 40, que está relacionada a falhas de comunicação entre os colaboradores, técnicos e gestores devido à complexidade do SoS, causando dificuldade de refletir a segurança da informação nesses sistemas, obteve o percentual de 53,1% que “concordam totalmente” e 46,9% que “concordam parcialmente”, das respostas dos especialistas, respectivamente.

Cabe destacar, nesse sentido, a importância do uso de tecnologias de criptografia re-

lacionadas as questões 5, 6 e 7 que obtiveram alto percentual de percentagem conforme a Figura 13, também evidenciada pela resposta de um dos especialistas:

“A criptografia simétrica ainda pode ser bastante útil em diversos casos. A criptografia de chave pública é útil para estabelecer canais seguros e realizar outras funções como assinatura digital, ...” [Especialista 13]

Além disso, pode-se destacar que as questões de 27 e 29 relacionadas a falhas de comunicação e a falta de um plano estratégico receberam 100% de concordância dos respondentes. Isso indica a necessidade de uma ferramenta que oriente os gestores de Tecnologia da Informação (TI) na solução desses problemas.

5.4 Limitações

Por não ser um estudo supervisionado, podem ter ocorridos problemas eventuais no processo de resolução do questionário, como falta de compreensão das questões, grande número de questões para serem respondidas e ausência de experiência dos participantes nos temas Segurança da Informação e SoS, respectivamente.

5.5 Discussão

Ao comparar os resultados obtidos do MSL com os da pesquisa de opinião, observam-se concordâncias entre a literatura e a indústria. Nesse sentido, destacam-se os estudos que possuem métodos, técnicas, modelos e ferramentas utilizados para segurança da informação em SoS com maior nível de concordância dos respondentes da pesquisa de opinião apresentados na Tabela 4.

Por exemplo, em E15 é mencionado a **análise de pontos de vulnerabilidades** durante a interoperação entre os sistemas constituintes no SoS. Ela é confirmada na questão 11 da pesquisa de opinião por 68,8% dos especialistas que responderam que “concordam totalmente” com a respectiva questão. Em E8, pode-se destacar o uso de **protocolos** para orientar a implementação de medidas de segurança da informação no SoS e seus sistemas constituintes. Isto é confirmado na questão 16 da pesquisa de opinião por 68,8% dos especialistas que responderam que “concordam totalmente” com a respectiva questão.

Cabe também destacar a avaliação desses métodos, técnicas, modelos e ferramentas com maior nível de concordância dos respondentes da pesquisa de opinião. Por exemplo,

Tabela 4: Estudos que possuem métodos, técnicas, modelos e ferramentas utilizados na segurança da informação em SoS com maior nível de concordância de profissionais e pesquisadores.

ID	Título	Referência	Método, técnica, modelo ou ferramenta	Percentual de especialistas que concordam totalmente
E6	Assessing System of Systems Security Risk and Requirements with OASoSIS	Ki-Aries et al. (2018)	Estudo de Caso	62,5%
E8	Real-time secure communication for Smart City in high-speed Big Data environment	Rathore et al. (2017)	Protocolo	68,8%
E9	Security of communications in connected cars Modeling and safety assessment	Tbatou et al. (2017)	Estudo de Caso	62,5%
E13	Extracting security control requirements	Hosey e Gamble (2010)	Análise e Validação	65,6%
E14	System-of-systems boundary check in a public event scenario	Zhou et al. (2010)	Política de Segurança	75%
E15	Modeling the linkage between systems interoperability and security engineering	Neaga e Henshaw (2010)	Análise de Pontos de Vulnerabilidade	68,8%
E15	Modeling the linkage between systems interoperability and security engineering	Neaga e Henshaw (2010)	Política de Segurança	87,5%
E16	Model driven security accreditation (MDSA) for agile, interconnected it landscapes	Lang e Schreiner (2009)	Análise e Validação	65,6%

a **análise e validação** feita por especialista em E13 e E16, onde a coleta de dados reais contribui diretamente com soluções para o problema, geralmente aplicadas em casos que envolvem modelagem ou análise de documentação de arquitetura, ou requisitos de projeto. Esta resposta é confirmada na questão 21 da pesquisa de opinião por 65,6% dos especialistas que responderam “concordam totalmente” com a respectiva questão. Os **Estudos de caso** em E6 e E9 permitem por meio de um cenário real ou realista compreender os efeitos da tecnologia proposta. Esta resposta é confirmada na questão 22 da pesquisa de opinião por 62,5% dos especialistas que responderam “concordam totalmente” com a respectiva questão.

Também compete destacar que os fatores mais específicos considerados no contexto de segurança da informação em SoS com maior nível de concordância dos respondentes da pesquisa de opinião. Por exemplo, as **políticas de segurança** relacionadas ao controle de acesso e nível de privacidade dos dados no SoS, presentes em E14 e E15. Estas respostas são confirmadas nas questões 28 e 29 da pesquisa de opinião por 75% e 87,5%, respectivamente, que responderam “concordam totalmente” com a questão.

Por fim, conforme pode ser verificado na Figura 13, os dados da pesquisa de opinião confirmam os resultados do MSL. Um dos pontos que podem se destacar para a análise, é

que a opinião dos especialistas que responderam que “concordam totalmente” e “concordam parcialmente” estão com altos índices de porcentagem.

Cabe também ressaltar os resultados das questões 34, 35, 36 e 37 da pesquisa de opinião, em que é abordada a necessidade de que os gestores de TI precisam ter gestão voltada para segurança da informação no SoS. Outro ponto interessante ressaltado nos resultados das questões 39 e 40 da pesquisa de opinião é a necessidade de uma abordagem de segurança da informação que permita aos gestores de TI compreendê-la sem dificuldades. Nesse sentido, o uso de uma ontologia de domínio para segurança da informação em SoS pode apoiar esses gestores na tomada de decisão do dia-a-dia em relação às questões de segurança no SoS.

5.6 Considerações Finais

Neste capítulo, foram reportados os resultados da pesquisa de opinião cujo propósito foi obter a análise de especialistas das áreas de segurança informação e SoS para auferir maior confiabilidade nos resultados encontrados no MSL. Foi utilizada a escala *Likert* para avaliar questões de acordo com o nível de concordância sobre as afirmações apresentadas. Esta pesquisa foi realizada entre os dias 8 de outubro e 12 de novembro de 2021. Para tal, foram enviados o total 117 convites com 32 respostas dos respectivos especialistas, gerando uma taxa de participação de 27,35%.

Destacam-se as tecnologias com maior aplicabilidade na indústria no contexto de SoS como **análise de pontos de vulnerabilidades** durante a interoperação entre os sistemas constituintes no SoS. Também o uso de **protocolos** para orientar a implementação de medidas de segurança da informação no SoS e seus sistemas constituintes.

Destaca-se também a avaliação das tecnologias com maior nível de aplicabilidade como **análise e validação** feita por especialista, onde a coleta de dados reais contribui diretamente com soluções para o problema, geralmente aplicadas em casos que envolvem modelagem ou análise de documentação de arquitetura, ou requisitos de projeto. **Estudos de caso**, que permite por meio de um cenário real ou realista compreender os efeitos da tecnologia proposta.

Também, destacam-se os fatores mais específicos considerados no contexto de segurança da informação em SoS com maior nível de aplicabilidade como, as **políticas de segurança** relacionadas ao controle de acesso e nível de privacidade dos dados no SoS. Por fim, os resultados retratam que gestores de TI precisam ter uma gestão voltada para

segurança da informação no SoS. Como também a necessidade de uma abordagem de segurança da informação que permita que estes gestores de TI possam compreendê-la sem dificuldades.

6. Ontologia SegInfoSoS

Este capítulo está organizado da seguinte forma: a Seção 6.1 traz o objetivo da construção da ontologia. A Seção 6.2 retrata as etapas da construção da ontologia SegInfoSoS. A Seção 6.3 apresenta a ontologia desenvolvida. A Seção 6.4 traz a execução de testes com a ontologia desenvolvida. Por fim, a Seção 6.5 apresenta com algumas considerações finais.

6.1 Introdução

O SoS é uma categoria de sistema complexo onde a interconectividade e a interação devem ser preservadas no comprimento do seus objetivos globais. Assim, torna-se desafiador o gerenciamento da segurança da informação nesses sistemas.

Dessa forma, o objetivo desta pesquisa foi desenvolver uma ontologia de domínio para apoiar gestores de TI no planejamento e desenvolvimento de soluções para problemas de segurança da informação nesses sistemas. Para isso, a Metodologia 101 (do inglês, *Ontology Development 101*) (NOY; MCGUINNESS, 2001) foi utilizada para criação da Ontologia de Gerenciamento de Segurança da Informação em SoS (SegInfoSoS) porque, além de ser a metodologia mais utilizada para a construção de ontologias, também é a mais simples de ser executada (ISOTANI; BITTENCOURT, 2015).

6.2 Processo de construção da ontologia

Esta seção descreve o processo de construção da ontologia proposta neste trabalho. A construção seguiu as etapas definidas pela Metodologia 101, conforme detalhada nas subseções a seguir. Cabe mencionar que esta ontologia não é o produto final deste trabalho, sendo realizado um refinamento na Seção 7.4 do Capítulo 7, após a realização da discussão

com o grupo focal.

6.2.1 Etapa 1 - Determinar o domínio e o escopo da ontologia.

Nesta etapa, procurou-se definir o propósito e os objetivos da ontologia, a quais usuários ela se destina, o tipo de ontologia a ser desenvolvida e a delimitação do seu escopo. Dessa forma, construiu-se um *template*, apresentado na Tabela 5, para especificar tais informações.

Tabela 5: Template de especificação da ontologia SegInfoSoS.

Domínio/escopo geral
A SegInfoSoS é uma ontologia de domínio que representa o conhecimento relativo à segurança da informação em SoS considerando as perspectivas de fatores específicos, metodologias de avaliação e tecnologias.
Propósito geral
A SegInfoSoS tem como propósito geral ser um instrumento de apoio aos gestores de TI das organizações detentoras de um SoS ou por pesquisadores da área, explicitando-lhes as características de segurança da informação por meio de três perspectivas que são fatores específicos, metodologias de avaliação e tecnologias. Esse apoio visa trazer para esses profissionais o entendimento técnico e prático para eles poderem evitar os riscos, as vulnerabilidades e as ameaças sejam exploradas no SoS.
Classes de usuários
A SegInfoSoS é destinada aos gestores de TI e pesquisadores de SoS, segurança da informação e ontologia.
Tipo de ontologia
A SegInfoSoS foi classificada como ontologia de domínio para o gerenciamento de segurança da informação em SoS.
Delimitação do escopo de cobertura
- Ponto de Partida:
A ideia para construção de uma ontologia de domínio para representação da segurança da informação em SoS emergiu da necessidade de abordar a segurança da informação no contexto de SoS de modo que os gestores de TI desses sistemas tenham a capacidade compreendê-la sem dificuldades.

Continua na próxima página.

Tabela 5 – Template de especificação da ontologia SegInfoSoS. *Continuação.*

O domínio coberto pela ontologia SegInfoSoS está relacionado aos resultados da revisão informal da literatura do Capítulo 2 em conjunto com os achados do MSL do Capítulo 4, que foram confirmados pela pesquisa de opinião do Capítulo 5.
- Questões de competência: As questões de competência foram formuladas com base nos objetivos da pesquisa do MSL do Capítulo 4 e, cujo propósito foi investigar a importância, os recursos e as tecnologias para implementação da segurança da informação no contexto de SoS. QC1. Como estão estruturados os conceitos relativos à segurança da informação em SoS? QC2. Quais são as tecnologias, os modelos, as técnicas ou as ferramentas de segurança da informação no SoS? QC3. Quais são os fatores específicos da segurança da informação no SoS? QC4. Quais são os tipos de fatores humanos de segurança da informação no SoS? QC5. Quais são os métodos de avaliação de segurança da informação no SoS? QC6. Quais soluções de criptografia são encontradas atualmente no SoS? QC7. Quais soluções de algoritmo são encontradas atualmente no SoS?

6.2.2 Etapa 2 - Considerar o reuso de outras ontologias.

Não foram encontrados nos repositórios disponíveis na literatura ontologias com o mesmo domínio proposto neste período inicial do trabalho.

6.2.3 Etapas 3 e 4 - Enumerar os termos importantes da ontologia e definir as classes e a hierarquia de classes.

Os termos foram reunidos, definidos e enumerados com base nos resultados de uma revisão informal da literatura apresentados no Capítulo 2 em conjunto com os achados do MSL do Capítulo 4, confirmados pela pesquisa de opinião do Capítulo 5.

Na Tabela 6, tem-se a rastreabilidade dos estudos relacionados a Segurança da informação em SoS selecionados e agrupados em Fator Específico, Metodologia de Avaliação e Tecnologia.

Na Tabela 7, tem-se a rastreabilidade dos estudos relacionados com a definição de SoS agrupados em Característica do constituinte, Classe derivada, Desafio, Serviço, Tipo e Uso.

Tabela 6: Rastreabilidade dos estudos selecionados do MSL.

ID	Título	Referência	Fator de Segurança da Informação em SoS
E1	Identifying and mitigating security risks for secure and robust NGI networks	Lever e Kifayat (2020)	Fator Específico: Risco de ataque ou ciberataque
E2	Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology	Petratos e Faccia (2019)	Fator Específico: Ponto de vulnerabilidade
E4	A systems-of-systems security framework for requirements definition in cloud environment	Carturan e Goya (2019)	Fator Específico: Ponto de vulnerabilidade
E5	Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems	Tagarev e Sharkov (2019)	Fator Específico: Ponto de vulnerabilidade - Risco de ataque ou ciberataque
E6	Assessing System of Systems Security Risk and Requirements with OASoSIS	Ki-Aries et al. (2018)	Fator Específico: Fator humano - Ponto de vulnerabilidade - Risco de ataque ou ciberataque
E7	Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach	Ceccarelli et al. (2018)	Fator Específico: Ponto de vulnerabilidade
10	System of systems cyber effects simulation ontology	Ormrod <i>et al.</i> (2015)	Fator Específico: Risco de ataque ou ciberataque
E11	Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis	Guariniello e De Laurentis (2014)	Fator Específico: Risco de ataque ou ciberataque
E14	System-of-systems boundary check in a public event scenario	Zhou et al. (2010)	Fator Específico: Política de segurança - Ponto de vulnerabilidade
E15	Modeling the linkage between systems interoperability and security engineering	Neaga e Henshaw (2010)	Fator Específico: Fator humano - Política de segurança - Ponto de vulnerabilidade
E17	A new schema for security in dynamic uncertain environments	Agrawal (2009)	Fator Específico: Fator humano - Risco de ataque ou ciberataque
E18	System-of-systems security engineering	Bodeau (1994)	Fator Específico: Risco de ataque ou ciberataque
E5	Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems	Tagarev e Sharkov (2019)	Metodologia de Avaliação: Inteligência artificial - <i>Deep Learning</i> e <i>Machine Learning</i>
E6	Assessing System of Systems Security Risk and Requirements with OASoSIS	Ki-Aries et al. (2018)	Metodologia de Avaliação: Estudo de caso
E8	Real-time secure communication for Smart City in high-speed Big Data environment	Rathore et al. (2017)	Metodologia de Avaliação: Análise comparativa
E9	Security of communications in connected cars Modeling and safety assessment	Tbatou et al. (2017)	Metodologia de Avaliação: Estudo de caso
E10	System of systems cyber effects simulation ontology	Ormrod et al. (2015)	Metodologia de Avaliação: Análise comparativa
E13	Extracting security control requirements	Hosey e Gamble(2010)	Metodologia de Avaliação: Análise e validação de especialista
E16	Model driven security accreditation (MDSA) for agile, interconnected it landscapes	Lang e Schreiner (2009)	Metodologia de Avaliação: Análise e validação feita por especialista
E18	System-of-systems security engineering	Bodeau (1994)	Metodologia de Avaliação: Análise descritiva
E1	Identifying and mitigating security risks for secure and robust NGI networks	Lever e Kifayat (2020)	Tecnologia: Algoritmo probabilístico (Monte Carlo e Cadeia de <i>Markov</i>)
E3	Simulation Trust and the Internet of Things	Loper (2019)	Tecnologia: Simulação de ambiente
E8	Real-time secure communication for Smart City in high-speed Big Data environment	Rathore et al. (2017)	Tecnologia: Protocolo
E9	Security of communications in connected cars Modeling and safety assessment	Tbatou et al. (2017)	Tecnologia: Criptografia
E11	Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis	Guariniello e De Laurentis (2014)	Tecnologia: Criptografia
E14	System-of-systems boundary check in a public event scenario	Zhou et al. (2010)	Tecnologia: Simulação do ambiente
E15	Modeling the linkage between systems interoperability and security engineering	Neaga e Henshaw (2010)	Tecnologia: Análise de ponto de vulnerabilidade
E17	A new schema for security in dynamic uncertain environments	Agrawal (2009)	Tecnologia: Esquema de monitoramento

Tabela 7: Rastreabilidade dos estudos selecionados da revisão informal da literatura.

ID	Título	Referência	Definição de SoS
E19	Architecting principles for systems-of-systems	Maier (1998)	Característica do Constituinte: Comportamento emergente - Desenvolvimento evolucionário - Distribuição geográfica gerencial e operacional
E20	Software Engineering	Sommerville (2016)	Característica do Constituinte: Heterogeneidade - Intensivos em dados
E20	Software Engineering	Sommerville (2016)	Classe derivada: SIF
E21	Oportunidades de KIPO para Gestão em Sistemas de Informação Federados no Caso do Programa Bolsa Família	Dias et al. (2021)	Classe derivada: SIF
E22	Interoperability in systems-of-information system	Fernandes et al. (2018)	Classe derivada: SoIS
E22	Interoperability in systems-of-information system	Fernandes et al. (2018)	Desafio: Transparência - Interoperabilidade
E23	GranDSI-BR Grand Research Challenges in Information Systems in Brazil	Boscarioli et al. (2017)	Desafio: Transparência - Interoperabilidade
E24	Thinking smart cities as systems-of-systems: A perspective study	Cavalcante et al. (2019)	Serviço: Carro autônomo - Controle de tráfego - Gestão de edifício - Integração de transporte - Saúde-Segurança pública
E19	Architecting principles for systems-of-systems	Maier (1998)	Tipo: Dirigido - Virtual - Colaborativo
E20	Software Engineering	Sommerville (2016)	Tipo: Dirigido/ Organizacional - Federado - Coalizão
E24	Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering	Dahmann e Baldwin (2008)	Tipo: Reconhecido
E6	Assessing System of Systems Security Risk and Requirements with OASoSIS	Ki-Aries et al. (2018)	Uso: Cidade inteligente
E10	System of systems cyber effects simulation ontology	Ormrod et al. (2015)	Uso: Militar
E9	Security of communications in connected cars Modeling and safety assessment	Tbatou et al. (2017)	Uso: Transporte

A definição da hierarquia de classes foi realizada pelo processo de desenvolvimento *top-down*.

- **Segurança da Informação:**

- (i) **Fator Específico:**

- (a) Fator humano (E6, E15 e E17)
 - (b) Política de segurança (E14 e E15)
 - (c) Ponto de vulnerabilidade (E2, E4, E5, E6, E7, E14 e E15)
 - (d) Risco de ataque ou ciberataque (E1, E5, E6, E10, E11, E17 e E18)

- (ii) **Metodologia de Avaliação:**

- (a) Análise comparativa (E8 e E10)
 - (b) Análise descritiva (E18)
 - (c) Análise e validação de especialista (E13 e E16)
 - (d) Estudos de caso (E6 e E9)

(e) Inteligência artificial (*Deep Learning* e *Machine Learning*) (E5)

(iii) **Tecnologia:**

(a) Algoritmo probabilístico (Monte Carlo e Cadeia de *Makov*) (E1)

(b) Análise de ponto de vulnerabilidade (E15)

(c) Criptografia (E9 e E12)

(d) Esquema de monitoramento (E17)

(e) Protocolo (E8)

(f) Simulação do ambiente (E3 e E14)

• **SoS:**

1) **Característica do constituinte** (E19, E20):

(a) Comportamento emergente

(b) Desenvolvimento evolucionário

(c) Distribuição geográfica

(d) Heterogeneidade

(e) Independência gerencial e operacional

(f) Intensivo em dados

2) **Classe derivada** (E20, E21):

(a) SIF

(b) SoIS

3) **Desafio** (E22, E23):

(a) Interoperabilidade

(b) Transparência da Informação

4) **Serviço** (E24):

(a) Carro autônomo

(b) Controle de tráfego

(c) Gestão de edifício

(d) Integração de transporte

(e) Saúde

(f) Segurança pública

5) **Tipo** (E19, E20, E24):

(a) Coalizão

- (b) Colaborativo
 - (c) Dirigido/Organizacional
 - (d) Federado
 - (e) Reconhecido
 - (f) Virtual
- 6) **Uso** (E6, E10, E9):
- (a) Cidade inteligente
 - (b) Militar
 - (c) Transporte

6.2.4 Etapa 5 - Definir as propriedades das classes

As classes não possuem informações suficientes para responder às questões de competências. Por isso, após a definição das classes, é preciso descrever as propriedades de objetos e propriedades de dados definidas na quinta e sexta etapas da metodologia 101, conforme apresentado na Tabela 8.

Tabela 8: *Template* de especificação das propriedades da ontologia SegInfoSoS.

Propriedades da ontologia SegInfoSoS:			
A ontologia SegInfoSoS possui 9 propriedade de objetos e 3 propriedades de dados.			
Propriedade de objetos: representam as relações entre as classes.			
Domínio	Range	Características das Propriedades	Propriedades dos Objetos
Uso	SoS	Functional	usoEhTidoPor
Desafio	SoS	Functional	desafioEhTidoPor
SegInfo	SoS	Functional	segInfoEhTidoPor
Servico	SoS	Functional	servicoEhTidoPor
SoS	Desafio	Functional	temDesafio
SoS	SegInfo	Functional	temSegInfo
SoS	Servico	Functional	temServico
SoS	Uso	Functional	temUso
SegurancaDaInformacao	temSeguranca some FatorEspecifico	Functional	temSeguranca
SegurancaDaInformacao	temSeguranca some MetodologiaDeAvaliacao	Functional	temSeguranca
SegurancaDaInformacao	temSeguranca some Tecnologia	Functional	temSeguranca
Propriedade de dados: representam os atributos das classes.			
Domínio	Range	Características das Propriedades	Propriedades dos Dados
Algoritmo	String	Functional	algoritmoProbabilisticoTemNome
Criptografia	String	Functional	criptografiaTemNome

6.2.5 Etapa 6: Criar as instâncias

O último passo proposto pela metodologia 101 é a criação das instâncias das classes, conforme apresentado na Tabela 9. A ontologia SegInfoSoS conta com 50 instâncias. As instâncias foram criadas com base nos resultados da Revisão Informal da Literatura do Capítulo 2 e MSL do Capítulo 4.

Tabela 9: *Template* de especificação das instâncias da ontologia SegInfoSoS.

Ontologia SegInfoSoS
Classe: SegurancaDaInformacao
Instâncias:
◆ FatorEspecifico ◆ MetodologiaDeAvaliacao ◆ Tecnologia
Subclasse: FatorEspecifico
◆ FatorHumano_ComportamentoDeAtor ◆ FatorHumano_TipoDeCliente ◆ PoliticaDeSeguranca_ControlDeAcesso ◆ PoliticaDeSeguranca_NivelDePrivacidadeDeDados ◆ PontoDeVulnerabilidade_Arquitetura ◆ PontoDeVulnerabilidade_InterfaceDoConstituente ◆ RiscoDeAtaque_Ciberataque
Subclasse: MetodologiaDeAvaliacao
Instâncias:
◆ AnaliseComparativa ◆ AnaliseEValidacaoDeEspecialista ◆ AnáliseDescritiva ◆ EstudoDeCaso ◆ InteligenciaArtificial_DeepLearning ◆ InteligenciaArtificial_MachineLearning
Subclasse: Tecnologia
Instâncias:

Continua na próxima página.

Tabela 9 – *Template* de especificação das instâncias da ontologia SegInfoSoS. *Continuação.*

◆ AlgoritmoEvolucionario ◆ AlgoritmoProbabilisticoCadeiaDeMarkov ◆ AlgoritmoProbabilisticoMonteCarlo ◆ AnaliseDePontoDeVulnerabilidade ◆ Criptografia_DeChavePrivada_BaseadaEmAtributos ◆ Criptografia_DeChavePrivada_CurvasElipticas ◆ Criptografia_DeChavePrivada_RSA ◆ EsquemaDeMonitoramento ◆ Protocolo ◆ SimulacaoDeAmbiente
Classe: SoS
Subclasse: CaracteristicaDoConstituente
Instâncias:
◆ ComportamentoEmergente ◆ DesenvolvimentoEvolucionario ◆ DistribuicaoGeografica ◆ Heterogeneidade ◆ IndependenciaGerencial
◆ IndependenciaOperacional ◆ IntensivoEmDados
Subclasse: ClasseDerivada
Instâncias:
◆ SIF ◆ SolS
Subclasse: Desafio
Instâncias:
◆ Interoperabilidade ◆ TransparenciaDaInformacao
Subclasse: Servico
Instâncias:

Continua na próxima página.

Tabela 9 – *Template* de especificação das instâncias da ontologia SegInfoSoS. *Continuação.*

◆ CarroAutonomo ◆ ControleDeTrafego ◆ DistribuicaoDeEnergia ◆ GestaoDeEdificio ◆ IntegracaoDeTransporte ◆ Saude ◆ SegurancaPublica
Subclasse: Tipo
Instâncias:
◆ Coalizao ◆ Colaborativo ◆ Dirigido/Organizacional ◆ Federado ◆ Reconhecido ◆ Virtual
Subclasse: Uso
Instâncias:
◆ CidadesInteligentes ◆ Militar ◆ Transporte

6.3 Representação da ontologia SegInfoSoS

A representação da ontologia SegInfoSoS segue as características definidas pelo modelo conceitual de ontologia de Parkin et al. (2021). As Figuras 14 e 15 apresentam as subclasses SegurançaDaInformacao e SoS da ontologia SegInfoSoS.

6.4 Execução de testes

Após a criação de instâncias, passou-se para execução de testes com a ontologia por meio de processo de *reasoning* no *Protegé* e de um programa em Java desenvolvido em OWL API API¹.

¹<http://owlapi.sourceforge.net/>

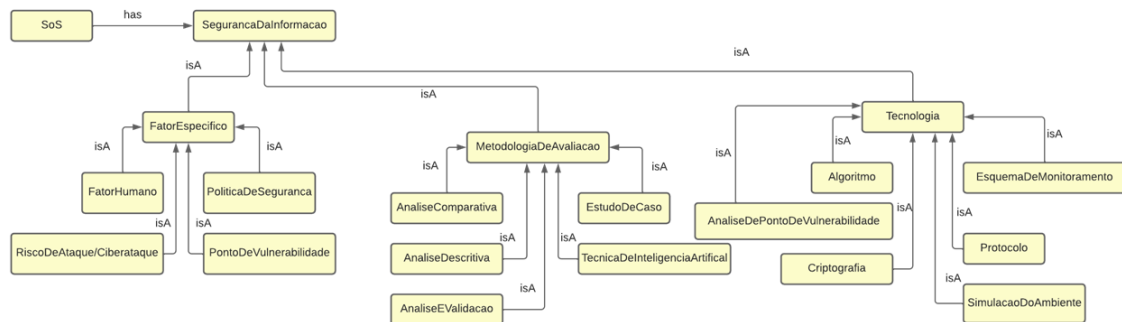


Figura 14: Representação da subclasse SegurancaDaInformacao conforme o modelo conceitual de ontologia definida por Parkin et al. (2021).

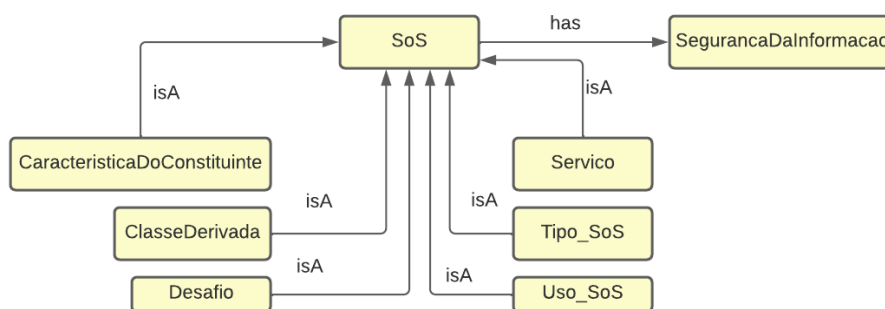


Figura 15: Representação da subclasse SoS na ontologia SegInfoSoS conforme o modelo conceitual de ontologia definida por Parkin et al. (2021).

6.4.0.1 DL Query para consultas na ontologia SegInfoSoS

Para execução de consultas na ontologia SegInfoSoS ², foi usado o *DL Query*, um recurso nativo do *DL Query* do editor de ontologias *Protegé*. *DL Query* usa uma linguagem de consulta baseada em sintaxe *Manchester OWL*, que é uma sintaxe “amigável” para OWL DL. O raciocinador utilizado foi o Pellet. Foram realizadas sete consultas e analisados os resultados esperados, conforme mostram as Tabelas 10 a 16.

Tabela 10: Tabela com a execução de consulta DL Query 1 na ontologia SegInfoSoS.

Query 1: Como estão estruturados os conceitos relativos à segurança da informação em SoS?
Resultado esperado:

Continua na próxima página.

²<https://www.dropbox.com/s/yfq93754goxoz8/SegInfoSoS.owl?dl=0>

Tabela 10 – Tabela com a execução de consulta DL Query 1 na ontologia SegInfoSoS.
Continuação.

• FatorEspecifico • MetodologiaDeAvaliacao • Tecnologia
Código e resultado da <i>DL Query 1</i> .
<i>temSeguranca some FatorEspecifico or temSeguranca some MetodologiaDeAvaliacao or temSeguranca some Tecnologia</i>
Instances (3 of 3) ◆ FatorEspecifico ◆ MetodologiaDeAvaliacao ◆ Tecnologia

Tabela 11: Tabela com a execução de consulta DL Query 2 na ontologia SegInfoSoS.

Query 2: Quais são as tecnologias, os modelos, as técnicas ou as ferramentas de segurança da informação no SoS?
Resultado esperado:
• Algoritmo Evolucionário • Algoritmo Probabilístico Cadeia de <i>Markov</i> • Algoritmo Probabilístico Monte Carlo • Análise Comparativa • Análise de Ponto de Vulnerabilidade • Análise Descritiva • Análise e Validação de Especialista

Continua na próxima página.

Tabela 11 – Tabela com a execução de consulta DL Query 2 na ontologia SegInfoSoS.
Continuação.

• Criptografia de Chave Privada Baseada em Atributos • Criptografia de Chave Privada Curvas Elípticas • Criptografia de Chave Privada RSA • Esquemas de Monitoramento • Estudos de Caso • Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente • Inteligência Artificial - <i>Deep Learning</i> • Inteligência Artificial - <i>Machine Learning</i> • Política de Segurança - Controle de Acesso • Política de Segurança - Nível de Privacidade de Dados • Ponto de Vulnerabilidade - Arquitetura • Ponto de Vulnerabilidade - Interface dos Constituintes • Protocolo • Risco de Ataque / Ciberataque • Simulação de Ambiente
Código e resultado da <i>DL Query 2</i> .
<i>SoS and temSegInfo some</i>

Continua na próxima página.

Tabela 11 – Tabela com a execução de consulta DL Query 2 na ontologia SegInfoSoS.
Continuação.

Instances (23 of 23)
◆ AlgoritmoEvolucionario
◆ AlgoritmoProbabilisticoCadeiaDeMarkov
◆ AlgoritmoProbabilisticoMonteCarlo
◆ AnaliseComparativa
◆ AnaliseDePontoDeVulnerabilidade
◆ AnaliseEValidacao_FeitaPorEspecialista
◆ AnáliseDescritiva
◆ Criptografia_DeChavePrivada_BaseadaEmAtributos
◆ Criptografia_DeChavePrivada_CurvasElípticas
◆ Criptografia_DeChavePrivada_RSA
◆ EsquemaDeMonitoramento
◆ EstudoDeCaso
◆ FatorHumano_ComportamentoDeAtor
◆ FatorHumano_TipoDeCliente
◆ InteligenciaArtificial_DeepLearning
◆ InteligenciaArtificial_MachineLearning
◆ PoliticaDeSeguranca_ControlDeAcesso
◆ PoliticaDeSeguranca_NivelDePrivacidadeDeDados
◆ PontoDeVulnerabilidade_Arquitetura
◆ PontoDeVulnerabilidade_InterfaceDoConstituente
◆ Protocolo
◆ RiscoDeAtaque_Ciberataque
◆ SimulacaoDeAmbiente

Tabela 12: Tabela com a execução de consulta DL Query 3 na ontologia SegInfoSoS.

Query 3: Quais são os fatores específicos da segurança da informação no SoS?
Resultado esperado:
• Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente

Continua na próxima página.

Tabela 12 – Tabela com a execução de consulta DL Query 3 na ontologia SegInfoSoS.
Continuação.

• Política de Segurança - Controle de Acesso • Política de Segurança - Nível de Privacidade de Dados • Ponto de Vulnerabilidade - Arquitetura • Ponto de Vulnerabilidade - Interface do Constituinte • Risco de Ataque / Ciberataque
Código e resultado da <i>DL Query 3</i> .
<i>SoS and temSegInfo some and FatorEspecifico</i>
Instances (7 of 7) ◆ FatorHumano_ComportamentoDeAtor ◆ FatorHumano_TipoDeCliente ◆ PoliticaDeSeguranca_ControlDeAcesso ◆ PoliticaDeSeguranca_NivelDePrivacidadeDeDados ◆ PontoDeVulnerabilidade_Arquitetura ◆ PontoDeVulnerabilidade_InterfaceDoConstituente ◆ RiscoDeAtaque_Ciberataque

Tabela 13: Tabela com a execução de consulta DL Query 4 na ontologia SegInfoSoS.

Query 4: Quais são os tipos de fatores humanos de segurança da informação no SoS?
Resultado esperado:
• Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente

Continua na próxima página.

Tabela 13 – Tabela com a execução de consulta DL Query 4 na ontologia SegInfoSoS.
Continuação.

Código e resultado da <i>DL Query 4</i> .
<i>SoS and temSegInfo some and FatorHumano</i>
Instances (2 of 2) ◆ FatorHumano_ComportamentoDeAtor ◆ FatorHumano_TipoDeCliente

Tabela 14: Tabela com a execução de consulta DL Query 5 na ontologia SegInfoSoS.

Query 5: Quais são os métodos de avaliação de segurança da informação no SoS?
Resultado esperado:
• Análise Comparativa • Análise e Validação de Especialista • Análise Descritiva • Estudo de Caso • Inteligência Artificial - Deep Learning • Inteligência Artificial - Machine Learning
Código e resultado da <i>DL Query 5</i> .
<i>SoS and temSegInfo some and MetodologiaDeAvaliacao</i>
Instances (6 of 6) ◆ AnaliseComparativa ◆ AnaliseEValidacaoDeEspecialista ◆ AnáliseDescritiva ◆ EstudoDeCaso ◆ InteligenciaArtificial_DeepLearning ◆ InteligenciaArtificial_MachineLearning

Tabela 15: Tabela com a execução de consulta DL Query 6 na ontologia SegInfoSoS.

Query 6: Quais soluções de criptografia são encontradas atualmente no SoS?
Resultado esperado:
• Criptografia de Chave Privada Baseada em Atributos • Criptografia de Chave Privada Curvas Elípticas • Criptografia de Chave Privada RSA
Código e resultado da <i>DL Query 6</i> .
<i>SoS and temSegInfo some and Criptografia</i>
Instances (3 of 3) ◆ Criptografia_DeChavePrivada_BaseadaEmAtributos ◆ Criptografia_DeChavePrivada_CurvasElipticas ◆ Criptografia_DeChavePrivada_RSA

Tabela 16: Tabela com a execução de consulta DL Query 7 na ontologia SegInfoSoS.

Query 7: Quais soluções de algoritmos são encontradas atualmente no SoS?
Resultado esperado:
• Algoritmo Evolucionário • Algoritmo Probabilístico Cadeia de Markov • Algoritmo Probabilístico Monte Carlo
Código e resultado da <i>DL Query 7</i> .
<i>SoS and temSegInfo some and Algoritmo</i>
Instances (3 of 3) ◆ AlgoritmoEvolucionario ◆ AlgoritmoProbabilisticoCadeiaDeMarkov ◆ AlgoritmoProbabilisticoMonteCarlo

6.4.1 Programa em Java para consultas na ontologia SegInfoSoS

Um programa em Java com o uso de API OWL foi desenvolvido ³ para execução de consultas na ontologia SegInfoSoS em OWL ⁴ no *prompt* de comando do Windows. A API OWL é uma *interface* de Java e uma implementação da linguagem de ontologias da W3C, utilizada para representar ontologias na Web Semântica. Esta API invoca OWL DL e a versão da OWL 2 e também oferece suporte para utilizar *reasoners* como FaCT++ e Pellet.

O total de seis consultas foram realizadas por meio do programa em Java e analisados os resultados esperados. Estes resultados são apresentados nas Tabelas 17 a 22. O programa em Java é apresentado na Figura 16.

Além disso, na Figura 16, são exibidas algumas questões de competência (1 a 7) definidas preliminarmente para execução de testes com a ontologia SegInfoSoS.

```
*****
SegInfoSoS - Ontologia para Segurança da Informação em SoS
*****
Para obter informações, digite uma opção a seguir:

1 - Como é dividida a segurança da informação do SoS no SegInfoSoS?
2 - Quais são as tecnologias, os modelos, as técnicas ou as ferramentas de segurança da informação no SoS?
3 - Quais são os fatores específicos da segurança da informação no SegInfoSoS?
4 - Quais são os tipos de fatores humanos de segurança da informação no SegInfoSoS?
5 - Quais são os métodos de avaliação de segurança da informação do SoS?
6 - Quais soluções de criptografia são encontradas atualmente no SoS?
7 - Quais soluções de algoritmo são encontradas atualmente no SoS?
8 - Buscar criptografia da segurança da informação no SoS.
9 - Buscar algoritmo da segurança da informação no SoS.
10- Verificar a consistência da ontologia SegInfoSoS.
11- Imprimir as propriedades da ontologia SegInfoSoS.
12- Imprimir a quantidade de propriedades da ontologia SegInfoSoS.
13- Digite 0 para encerrar o programa.
*****
```

Figura 16: Programa em Java com o uso de OWL API no *prompt* de comando do Windows para execução de consultas na ontologia SegInfoSoS.

Tabela 17: Tabela com a execução da questão 1 do programa em Java em OWL API.

Questão 1 - Como estão estruturados os conceitos relativos à segurança da informação em SoS?
Resultado esperado:

Continua na próxima página.

³<http://owlapi.sourceforge.net/>

⁴<https://www.dropbox.com/s/yfq93754goxoz8/SegInfoSoS.owl?dl=0>

Tabela 17 – Tabela com a execução da questão 1 do programa em Java em OWL API.
Continuação.

• Metodologia de Avaliação • Fator Específico • Tecnologia
Resultado da execução da questão 1 do programa em Java em OWL API.
<pre> 1 Os conceitos relativos à segurança da informação em SoS estão estruturados em: 3 classes MetodologiaDeAvaliacao FatorEspecifico Tecnologia </pre>

Tabela 18: Tabela com a execução da questão 2 do programa em Java em OWL API.

Questão 2 - Quais são tecnologias, os modelos, métodos, técnicas ou ferramentas de segurança da informação no SoS?
Resultado esperado:
• Algoritmo Evolucionário • Algoritmo Probabilístico Cadeia de <i>Markov</i> • Algoritmo Probabilístico Monte Carlo • Análise Comparativa • Análise de Ponto de Vulnerabilidade • Análise e Validação de Especialista • Análise Descritiva

Continua na próxima página.

Tabela 18 – Tabela com a execução da questão 2 do programa em Java em OWL API.
Continuação.

• Criptografia de Chave Privada Baseada em Atributos • Criptografia de Chave Privada Curvas Elípticas • Criptografia de Chave Privada RSA • Esquemas de Monitoramento • Estudos de Caso • Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente • Inteligência Artificial - <i>Deep Learning</i> • Inteligência Artificial - <i>Machine Learning</i> • Política de Segurança - Controle de Acesso • Política de Segurança - Nível de Privacidade de Dados • Ponto de Vulnerabilidade - Arquitetura • Ponto de Vulnerabilidade - Interface dos Constituintes • Protocolo • Risco de Ataque / Ciberataque • Simulação de Ambiente
Resultado da execução da questão 2 do programa em Java em OWL API.

Continua na próxima página.

Tabela 18 – Tabela com a execução da questão 2 do programa em Java em OWL API.
Continuação.

<pre> 2 Qtde de Tecnologias : 23 AlgoritmoEvolucionario AlgoritmoProbabilisticoCadeiaDeMarkov AlgoritmoProbabilisticoMonteCarlo AnaliseComparativa AnaliseDePontoDeVulnerabilidade AnaliseEValidacaoDeEspecialista AnáliseDescritiva Criptografia_DeChavePrivada_BaseadaEmAtributos Criptografia_DeChavePrivada_CurvasElípticas Criptografia_DeChavePrivada_RSA EsquemaDeMonitoramento EstudoDeCaso FatorHumano_ComportamentoDeAtor FatorHumano_TipoDeCliente InteligenciaArtificial_DeepLearning InteligenciaArtificial_MachineLearning PoliticaDeSeguranca_ControlDeAcesso PoliticaDeSeguranca_NivelDePrivacidadeDeDados PontoDeVulnerabilidade_Arquitetura PontoDeVulnerabilidade_InterfaceDoConstituinte Protocolo RiscoDeAtaque_Ciberataque SimulacaoDeAmbiente </pre>

Tabela 19: Tabela com a execução da questão 3 do programa em Java em OWL API.

Questão 3 - Quais são os fatores específicos da segurança da informação no SegInfoSoS?
Resultado esperado:
• Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente • Política de Segurança - Controle de Acesso • Política de Segurança - Nível de Privacidade de Dados

Continua na próxima página.

Tabela 19 – Tabela com a execução da questão 3 do programa em Java em OWL API.
Continuação.

• Ponto de Vulnerabilidade - Arquitetura • Ponto de Vulnerabilidade - Interface do Constituinte • Risco de Ataque / Ciberataque
Resultado da execução da questão 3 do programa em Java em OWL API.
<pre> ***** 3 Ciberataque FatorHumano_ComportamentoDeAtor FatorHumano_TipoDeCliente PoliticaDeSeguranca_ControlDeAcesso PoliticaDeSeguranca_NivelDePrivacidadeDeDados PontoDeVulnerabilidade_Arquitetura PontoDeVulnerabilidade_InterfaceDoConstituinte ***** </pre>

Tabela 20: Tabela com a execução da questão 4 do programa em Java em OWL API.

Questão 4 - Quais são os tipos de fatores humanos de segurança da informação no SoS?
Resultado esperado:
• Fator Humano - Comportamento de Ator • Fator Humano - Tipo de Cliente
Resultado da execução da questão 4 do programa em Java em OWL API.
<pre> 4 FatorHumano_ComportamentoDeAtor FatorHumano_TipoDeCliente </pre>

Tabela 21: Tabela com a execução da questão 5 do programa em Java em OWL API.

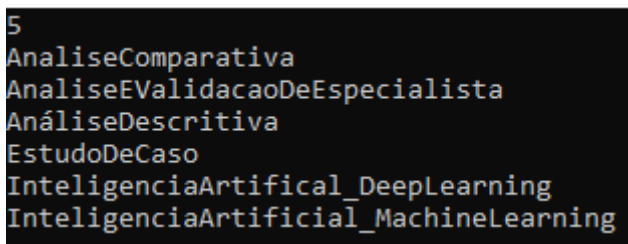
Questão 5 - Quais são os métodos de avaliação de segurança da informação no SoS?
Resultado esperado:
• Análise Comparativa • Análise e Validação de Especialista • Análise Descritiva • Inteligência Artificial - Deep Learning • Inteligência Artificial - Machine Learning
Resultado da execução da questão 5 do programa em Java em OWL API.
 <pre> 5 AnaliseComparativa AnaliseEValidacaoDeEspecialista AnáliseDescritiva EstudoDeCaso InteligenciaArtificial_DeepLearning InteligenciaArtificial_MachineLearning </pre>

Tabela 22: Tabela com a execução da questão 6 do programa em Java em OWL API.

Questão 6 - Quais soluções de criptografia são encontradas atualmente no SoS?
Resultado esperado:
Criptografia de Chave Privada Baseada em Atributos Criptografia de Chave Privada Curvas Elípticas Criptografia de Chave Privada RSA

Continua na próxima página.

Tabela 22 – Tabela com a execução da questão 6 do programa em Java em OWL API.
Continuação.

Resultado da execução da questão 6 do programa em Java em OWL API.
<pre>6 Criptografia_DeChavePrivada_BaseadaEmAtributos Criptografia_DeChavePrivada_CurvasElipticas Criptografia_DeChavePrivada_RSA</pre>

Tabela 23: Tabela com a execução da questão 7 do programa em Java em OWL API.

Questão 7 - Quais soluções de algoritmos são encontradas atualmente no SoS?
Resultado esperado:
Algoritmo Evolucionário Algoritmo Probabilístico Cadeia de Markov Algoritmo Probabilístico Monte Carlo
Resultado da execução da questão 6 do programa em Java em OWL API.
<pre>7 AlgoritmoEvolucionario AlgoritmoProbabilisticoCadeiaDeMarkov AlgoritmoProbabilisticoMonteCarlo</pre>

6.5 Considerações Finais

Este capítulo teve como objetivo definir e descrever as etapas do desenvolvimento da ontologia SegInfoSoS por meio das etapas da Metodologia 101. Com base nas etapas do levantamento de terminologias e suas relações, pode-se perceber que o processo de desenvolvimento de uma ontologia não é tão trivial assim, porém, quando se utiliza uma metodologia de fácil aplicação e entendimento, o processo se torna mais produtivo.

Cabe destacar também a importância de se utilizar uma ferramenta de apoio como o editor de ontologias *Protégé* que facilita desenvolvimento e a manipulação de ontologias.

Como contribuição, os gestores de TI terão à sua disposição uma ontologia de domínio, sendo, portanto, uma ontologia de alto nível, que apresenta um consenso nos termos e linguagem em documentos, na comunicação com as equipes e *stakeholders* envolvidos em questões de segurança da informação em SoS.

7. Avaliação da Ontologia SegInfoSoS

Este capítulo está organizado da seguinte forma: a Seção 7.1 apresenta o objetivo para avaliação da ontologia. A Seção 7.2 detalha a questão de pesquisa para este estudo. A Seção 7.3 apresenta e descreve o método de grupo focal para este estudo. A Seção 7.4 apresenta os ajustes e correções sugeridos na etapa de grupo focal pelos especialistas. A Seção 7.5 procura analisar o site web desenvolvido para a execução da ontologia refinada para avaliar a viabilidade da sua aplicabilidade em um SoS real de uma instituição pública. Por fim, a Seção 7.6 traz algumas considerações finais sobre a avaliação da ontologia.

7.1 Introdução

O gerenciamento da segurança da informação em SoS ainda possui muitos desafios, principalmente com os relacionados a falhas de segurança, como ataques cibernéticos e acesso não autorizados a dados. Assim, é importante caracterizar esse contexto por meio de uma ontologia de domínio para apoiar pesquisadores e profissionais que atuam no âmbito de SoS em questões de segurança da informação.

Dessa forma, o objetivo desta etapa de pesquisa foi avaliar a ontologia SegInfoSoS para verificar a sua aplicabilidade na indústria do ponto de vista de profissionais e pesquisadores no contexto de SoS. Para isso, é proposta as etapas de:

- Aplicação de grupo focal com especialistas para análise de sua sintaxe e semântica;
- Refinamento da ontologia com ajustes e correções sugeridos na aplicação do grupo focal;
- Realização de estudo de viabilidade para verificar o uso da ontologia em um SoS real.

7.2 Questão de Pesquisa

A questão principal da pesquisa para este estudo é:

“Quais são as características necessárias que uma ontologia de domínio precisa ter para apoiar o gerenciamento de segurança da informação em SoS?”

Para responder à questão de pesquisa, o trabalho foi fundamentado em uma abordagem metodológica definida na Seção 1.5 do Capítulo 1.

7.3 Grupo Focal

É uma técnica bastante usada em pesquisa qualitativa para coleta de dados por meio de discussões em grupo organizadas para explorar um conjunto de questões de um determinado domínio (KITZINGER, 1995). Este método de pesquisa se diferencia de uma categoria mais ampla de entrevista em grupo pelo uso explícito da interação do grupo com os dados da pesquisa (KITZINGER, 1995). Esta interação é geralmente realizada pela comunicação entre os participantes que podem ser especialistas de diferentes especialidades com o propósito de gerar dados na exploração de seus conhecimentos e experiências sobre um tema específico, em um determinado período limitado de tempo.

7.3.1 Objetivo do Estudo

O grupo focal foi formado para avaliar o aspecto sintático da ontologia, i.e., o relacionamento entre os termos e a estrutura da ontologia, bem como o aspecto semântico, i.e., o significado adequado do vocabulário utilizado na ontologia.

7.3.2 Subquestão de Pesquisa

Uma subquestão de pesquisa foi definida para apoiar a questão principal da pesquisa (Seção 6.2). A subquestão da pesquisa para este estudo é:

“Como se caracterizam os aspectos sintáticos e semânticos da ontologia na sua aplicabilidade na indústria do ponto de vista de pesquisadores e profissionais no contexto de sistemas-de-sistemas?”

7.3.3 Papéis

Os papéis usados neste estudo foram:

- **Moderador** – O papel é desempenhado pelo pesquisador responsável pela condução do estudo e autor da ontologia de gerenciamento de segurança da informação em sistemas-de-sistemas (SegInfoSoS) com o propósito de avaliar a sua aplicabilidade na indústria do ponto de vista de profissionais no contexto de SoS. O moderador se responsabiliza pela promoção e interação entre os participantes e possibilita que surjam novas ideias com sequência de perguntas e respostas. Ele também é responsável por registrar interações e conclusões durante as discussões do grupo (MORGAN; KRUEGER, 1998);
- **Participante** – É o papel desenvolvido pelos integrantes do grupo focal que irão responder às perguntas do moderador, participar das discussões do grupo e sugerir a realização de modificações e melhorias na ontologia de gerenciamento de segurança da informação em SoS.

7.3.4 Participantes

Foram convidados 5 especialistas com experiência na área de ontologia, SoS e Segurança da Informação. Nos trabalhos acadêmicos com o uso da metodologia de grupo focal, o número de participante pode variar de 3 a 12 participantes e estes participantes não terão a sua identidade identificada sobre as respostas e discussões na dinâmica do grupo. Isso ocorre devido a questões ligadas a confidencialidade e anonimato.

7.3.5 Localidade

O grupo focal foi realizado por meio da ferramenta Google Meet¹ de modo a flexibilizar a agenda dos participantes e respeitar os protocolos de saúde devido à pandemia do COVID-19.

7.3.6 Roteiro

Durante a realização de grupo focal, foram elaboradas várias questões para orientar as discussões. Na condução do estudo, o pesquisador procurou nivelar o conhecimento dos participantes sobre os conceitos abordados, ministrou a palestra, realizou a execução da

¹<https://meet.google.com/>

ontologia SegInfoSoS ² no *DL Query* do editor de ontologias *Protegé* ³ e no programa em Java com o uso da OWL API ⁴ e apresentou as questões a serem respondidas durante a reunião. O convite foi feito por e-mail com os anexos do Termo de Consentimento Livre e Esclarecido. A reunião foi conduzida seguindo o roteiro:

1. Apresentação dos participantes;
2. Esclarecimento sobre o contexto do estudo;
3. Apresentação do Objetivo do Grupo Focal;
4. Demonstração de consultas na ontologia SegInfoSoS ⁵ por meio da *DL Query* do editor de ontologias *Protegé* ⁶ e do programa em Java com o uso da OWL API ⁷ do Capítulo 6;
5. Discussão relacionada às questões de pesquisa.

Ao final da reunião do focal do grupo, os participantes foram convidados a responder a cinco questões, a saber:

- **Q1** - A taxonomia da ontologia SegInfoSoS foi definida corretamente?
- **Q2** - A relação entre as classes e subclasses está coerente?
- **Q3** - A ontologia SegInfoSoS consegue representar os resultados do mapeamento sistemático da literatura (MSL) corretamente?
- **Q4** - A ontologia SegInfoSoS é fácil de compreensão por um especialista da indústria?
- **Q5** - Você considera importante ter uma ontologia de domínio para apoiar os gestores de Tecnologia da Informação (TI) na tomada de decisão em questões de segurança da informação em sistemas-de-sistemas?

Os participantes ficaram à vontade para fazer as sugestões para cada questão.

²<https://doi.org/10.5281/zenodo.6621716>

³<https://protege.stanford.edu/>

⁴<http://owlapi.sourceforge.net/>

⁵<https://doi.org/10.5281/zenodo.6621716>

⁶<https://protege.stanford.edu/>

⁷<http://owlapi.sourceforge.net/>

7.3.7 Execução

O Grupo Focal foi realizado no dia 20 de dezembro de 2021 às 15:30 com a participação de 5 especialistas das áreas de Segurança da Informação, SoS e ontologia. Os participantes do estudo de grupo focal tinham perfis diferentes conforme a experiência e conhecimento técnico. A Tabela 24 resumiu os perfis e habilidades dos participantes grupo focal.

Tabela 24: Perfil dos participantes do grupo focal.

ID Perfil	Áreas de atuação
P1 Doutorado em Informática	Engenharia de Software, Ciência de Dados, Hipertexto e Multimídia
P2 Doutorado em Ciência da Computação	Inteligência Artificial, Engenharia de Ontologias e Aprendizado de Máquina
P3 Doutorado em Ciências da Computação	Engenharia de Software para Sistemas Intensivos de Software e Sistemas-de-Sistemas
P4 Mestrado em Informática	Interoperabilidade em Sistemas-de-Sistemas de Informação.
P5 Mestrado em Sistemas de Engenharia	Engenharia de Software, Segurança da Informação, Sistemas de Informação

7.3.8 Resultado

Em relação aos conceitos da ontologia SegInfoSoS ⁸, verificou-se que a ontologia apresentava problemas relacionados aos aspectos semânticos, evidenciado pela resposta de **P1**:

“...Há problemas de relação semântica entre Fator Específico e Segurança da Informação. Segurança da Informação de quê? Fator Específico de quê? É altamente questionável colocar Fator Específico como subclasse de Segurança da Informação, pois uma instância de Fator Específico não é uma instância de Segurança da Informação.. Não é verdade que todo Fator Específico é uma Segurança da Informação.”

P2 também comentou sobre os problemas relacionados aos aspectos semânticos em relação à taxonomia da ontologia:

“...Fator Específico e Metodologia de Avaliação... não se encaixam bem como sendo um sub-conjunto de Segurança da Informação.”

“...ao invés de Segurança da Informação, seria interessante mudar para Componente de Segurança da Informação.”

⁸<https://doi.org/10.5281/zenodo.6621716>

“ ...também ser mais explicativo com os nomes das classes... ...escrever os termos da ontologia em inglês...porque a abrangência é maior...o objetivo da ontologia é servir como vocabulário comum ...permitir que a máquina interprete esses dados, deduzindo e inferindo novos dados.”

Os comentários dos especialistas **P1** e **P2** demonstraram que a ontologia SegInfoSoS precisa ter sua estrutura taxonômica melhor definida semanticamente. Uma ontologia procura classificar os objetos do mundo real de forma que faça sentido para conceituação dos seres humanos. Assim, o uso de ontologias tem o propósito de viabilizar a interoperabilidade semântica entre seres humanos e sistemas. Tal interoperabilidade permite que tanto os seres humanos como os sistemas compreendam os dados que estão sendo classificados na ontologia com o mesmo entedimento de significado (BURANARACH, 2004). Além do mais, uma ontologia precisa viabilizar os objetivos da Web Semântica, onde os agentes artificiais conseguem manipular automaticamente o conhecimento que está sendo representado por meio de ontologias (BERNERS-LEE et al., 2001).

Cabe também mencionar que **P2** solicitou que fizesse o reuso de ontologias de segurança da de informação do site *Linked Open Vocabularies* (LOV) ⁹ ou de artigos recentemente publicados porque, conforme seu comentário citado abaixo:

“ ...o reuso aumenta a interoperabilidade da ontologia e ainda ganha de presente construções de uma ontologia que está sendo amplamente utilizada.”

Neste contexto, o desenvolvimento de uma nova ontologia por meio da reutilização de ontologias existentes pode ser útil. A reutilização de ontologias permite agilizar o processo de desenvolvimento de ontologias e promove a aplicação de boas práticas.

Também foram encontrados problemas relacionados à taxonomia do SoS, evidenciados pelo comentário de **P3**:

“ ...Já existe uma ontologia de SoS... São conceitos e relações avaliadas... pode-se ter um ganho muito grande no reuso da ontologia... A ontologia de Abdalla possui uma classificação que é mais aceita na literatura...”

Cabe mencionar que **P4** reiterou a necessidade do reuso de ontologias conforme evidenciada em seu comentário:

“ ... deixar muito bem delimitado o escopo do trabalho... Utilizar ontologias já definidas e talvez testadas...”

⁹<http://owlgred.lumii.lv/>

Dessa forma, **P3** e **P4** solicitaram que fizesse o reuso da ontologia OntoSoS de Abdalla (2017).

Com relação à segurança da informação em SoS, **P5** mencionou que poderia incluir a privacidade dos dados como um dos tópicos abordados.

“... No atual momento, é interessante incluir como um dos tópicos, a privacidade dos dados...é um ponto interessante... além do tripé da segurança...”

7.4 Refinamento da Ontologia

No refinamento da ontologia, procurou-se atuar nos ajustes e correções sugeridos na etapa de grupo focal pelos especialistas. Dessa forma, houve o reuso das ontologias *Security Storytelling Ontology*¹⁰ do domínio de segurança da informação organizacional (PARKIN et al., 2021) e OntoSoS do domínio de SoS (ABDALLA, 2017) por meio da compatibilidade entre os vocabulários utilizados de forma *ad hoc* (CAMPOS et al., 2009). A ontologia refinada chama-se *Ontology for Information Security Management in SoS* (InfoSecSoS)¹¹.

As Figuras 17 e 18 apresentam as subclasses *Component__Information__of__Security* e *Component__Systems__of__Systems* da ontologia InfoSecSoS.

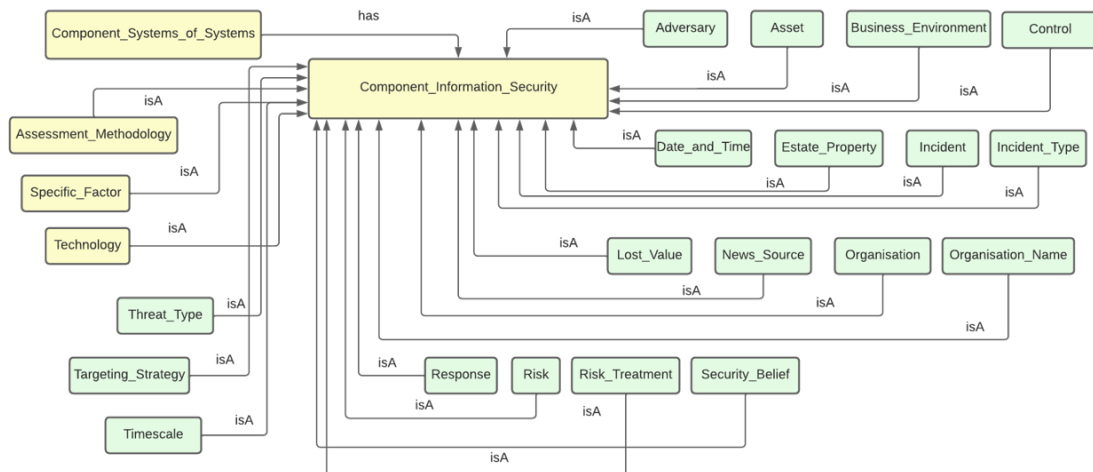


Figura 17: Representação da subclasse *Component__Information__of__Security* da ontologia InfoSecSoS. As subclasses em amarelo são de SegInfoSoS e as subclasses em verde são de *Security Storytelling Ontology*.

A ontologia InfoSecSoS conta com 337 axiomas declarados, distribuídos em 133 clas-

¹⁰<https://github.com/simonarnell/security-storytelling-ontology>

¹¹<https://doi.org/10.5281/zenodo.6621882>

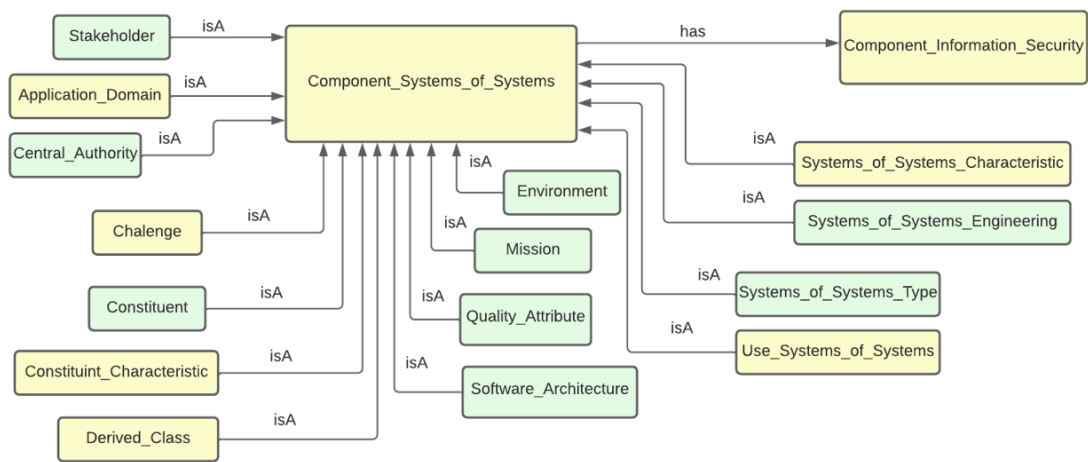


Figura 18: Representação da subclasse *Component_Systems_of_Systems* da ontologia InfoSecSoS. As subclasses em amarelo são de SegInfoSoS e as subclasses em verde são de OntoSoS

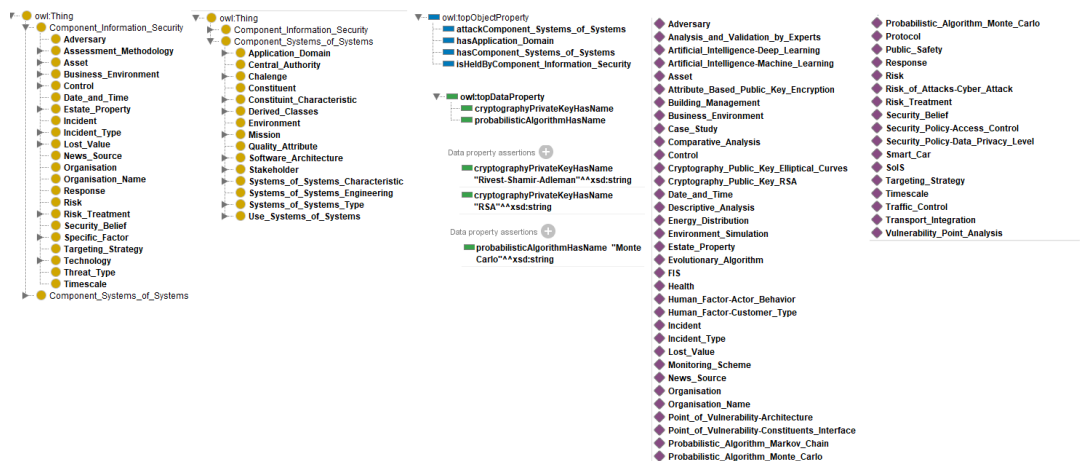


Figura 19: Classes, propriedade de objetos, propriedade de dados e instâncias da ontologia InfoSecSoS no *Protegé*.

ses, 4 propriedades de objetos, 3 propriedades de dados e 50 instâncias, conforme apresentado na Figura 19.

7.5 Estudo de Viabilidade

Foi conduzido ainda um estudo de viabilidade cujo objetivo foi analisar o site web desenvolvido conforme a Figura 20 para a execução da ontologia InfoSecSoS ¹² com o propósito de avaliar a sua viabilidade com respeito a sua aplicabilidade do ponto de vista de profissionais no contexto de SoS. Para isso, foi desenvolvido um cenário hipotético

¹²<https://doi.org/10.5281/zenodo.6621882>

para aplicabilidade da ontologia de gerenciamento em segurança da informação em SoS.

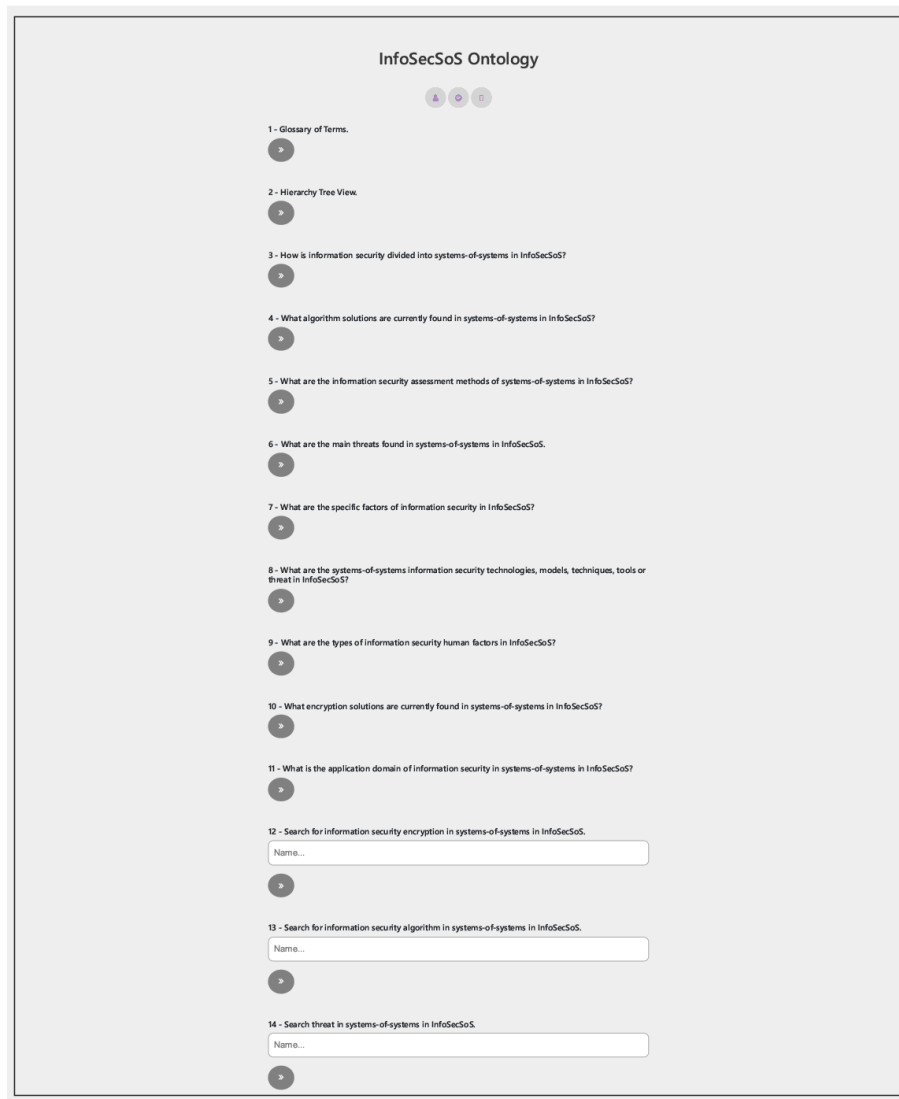


Figura 20: Site Web InfoSecSoS Ontology

7.5.1 Cenário Hipotético

Um *hacker* inseriu um vírus de computador na rede interna do setor X de uma instituição pública federal Y. Este vírus se espalhou pela rede e acessou a arquitetura do sistema operacional (SO) dos equipamentos relacionados à manutenção da infraestrutura do sincronismo da Hora Legal do Brasil. Esse vírus gerou atrasos na geração de fusos horários quebrando todo o sincronismo entre os servidores da instituição Z e a instituição Y. Como as instituições Z e Y são entidades públicas, este problema se repercutiu para as interfaces

dos sistemas SIAFI ¹³, SIAPE ¹⁴, SIASG ¹⁵ e SCDP ¹⁶. Estes sistemas passaram a gerar informações com o horário atrasado.

O Departamento de Tecnologia da Informação (DTI) da instituição Y foi acionado pelos servidores do Serviço Orçamentário, Financeiro e Contábil (SOFC) que estava com dificuldades para acessar os sistemas relacionados acima. Estes sistemas estavam apresentando problemas de acesso com o horário atrasado. Também, ao conseguirem acessar o SIAFI, eles tiveram problemas para realizarem os empenhos e as ordens bancárias (OB) de pagamento da instituição Y. Estes empenhos e OB eram gerados com os horários atrasados. Isto gerou inconsistências na execução de pagamentos nos sistemas do Banco do Brasil. O pessoal do DTI da instituição Y encontrou dificuldades para entender o problema. Uma vez que as redes internas da instituição Y estavam funcionando normalmente.

7.5.1.1 Questões de reflexão do Cenário Hipotético

1. Como a segurança da informação pode ser comprometida nos sistemas relacionados acima?
2. Quais medidas de avaliação de segurança da informação podem ser realizada nos sistemas do cenário hipotético para que o pessoal do DTI não seja surpreendido com esses problemas?
3. Quais as principais tecnologias de segurança da informação executadas nos sistemas do cenário hipotéticos?
4. Como pode ser resolvida as falhas de comunicação entre os colaboradores, técnicos e gestores que ocorre devido à complexidade do SoS, causando dificuldade de refletir a segurança da informação nestes sistemas?
5. No cenário hipotético mencionado acima, todos os controles de nível de privacidade e de acesso estavam sendo executados. Isto não impediu o acesso indevido à rede interna do setor X. Você considera importante ter uma ferramenta que auxilie os gestores de Tecnologia de Informação (TI) em questões de segurança da informação em SoS de modo que eles passem a estar atentos essas questões?

¹³<http://intra.serpro.gov.br/linhas-negocio/catalogo-de-solucoes/solucoes/principais-solucoes/sistema-integrado-de-administracao-financeira-do-governo-federal-siafi>

¹⁴<http://intra.serpro.gov.br/linhas-negocio/catalogo-de-solucoes/solucoes/principais-solucoes/siape-sistema-integrado-de-administracao-de-recursos-humanos>

¹⁵<https://www.gov.br/compras/pt-br/acesso-a-informacao/institucional/siasg>

¹⁶<https://www.gov.br/compras/pt-br/sistemas/diarias-e-passagens-scdp>

7.5.2 Questões de avaliação

Para realização do estudo de viabilidade foram levantadas 5 questões de avaliação da aplicabilidade do site web quanto a facilidade de uso e utilidade na execução da ontologia InfoSecSoS. São elas:

- **Q1** - Foi fácil utilizar o site web *InfoSecSoS Ontology* para responder às questões do cenário hipotético?
- **Q2** - Você teve alguma dúvida ou algum tipo de dificuldade para responder às questões do cenário hipotético por meio da utilização do site web *InfoSecSoS Ontology*?
- **Q3** - O site web *InfoSecSoS Ontology* é útil para o gerenciamento da segurança da informação em SoS no seu dia-a-dia?
- **Q4** - De acordo com a sua opinião, liste os aspectos positivos da utilização do site web *InfoSecSoS Ontology*.
- **Q5** - De acordo com a sua opinião, liste os aspectos negativos da utilização do site web *InfoSecSoS Ontology*.

7.5.3 Execução

O estudo de viabilidade foi realizado no dia 11 de fevereiro de 2021 às 11:30 com a participação dos gestores de Sistema de Informação e Segurança da Informação com mais de 15 anos de experiência de uma instituição pública federal. A Tabela 25 resumiu os perfis e habilidades dos participantes do estudo de viabilidade.

Tabela 25: Perfil dos participantes do estudo de viabilidade.

ID	Perfil	Áreas de atuação
P6	Mestrado Profissional em Novas Tecnologias Aplicadas à Educação	Sistemas de Informação, Gestão de Sistemas Complexos, Redes de Computadores
P7	Técnico em Informática	Sistema Operacional e Segurança da Informação

7.5.4 Resultado

Quanto à análise dos aspectos positivos de utilização do site web *InfoSecSoS Ontology*, os participantes expressaram os seguintes comentários:

P6: *“O site apresentou uma boa árvore de hierarquia e um vasto glossário.”*

P7: *“Concentração de diversos temas relacionados à Segurança da Informação em um único local de consulta.”*

De fato, este site web procurou apresentar, por meio da execução da ontologia InfoSecSoS, um vocabulário comum de entendimento técnico e prático para que os gestores de TI possam evitar que os riscos, as vulnerabilidades e as ameaças sejam explorados no âmbito do SoS.

Quanto a análise dos aspectos negativos de utilização do site web InfoSecSoS Ontology, um participante comentou:

P6: *“Entendo ter faltado metodologias práticas que nos auxiliem na gestão de segurança, links para os termos do glossário”*

Porém, os dois participantes afirmaram que não detectaram aspectos intrinsecamente negativos, mas apenas sugestões de melhorias expressos em seus comentários abaixo:

P6: *“A terminologia escolhida, apesar de abarcar os diversos itens corretos relacionados ao tema, não parece ser idêntica a outras mais difundidas em Segurança da Informação, como a ISO 27000 ou o Glossário de Segurança da Informação do GSI/PR.”*

P7: *“Na Árvore Hierárquica os termos das folhas poderiam possuir hiperlinks para suas definições, ou um texto mouseover/tooltip, evitando com isto o avançar/retroceder da navegação interna.”*

7.6 Considerações Finais

Por meio da avaliação da ontologia, foi possível extrair conhecimentos relevantes sobre segurança da informação em SoS que estavam codificados nas propriedades da ontologia. Isso não seria possível apenas pela análise de uma taxonomia. Uma taxonomia busca organizar a informação e/ou conhecimento em relações hierárquicas entre os termos. No que lhe concerne, a ontologia representa um modelo de dados do conjunto de conceitos de um domínio e os relacionamentos entre estes conceitos. Ela permite realizar inferência sobre os objetos de seu domínio.

Dessa forma, os resultados das avaliações dos especialistas do método de grupo focal e estudo de viabilidade comprovam que o uso da ontologia InfoSecSoS apoia a caracterização e organização do conhecimento do domínio de Segurança da Informação em SoS.

Nesse sentido, tal ontologia se torna uma referência para o planejamento, implementação de estratégias, gerenciamento e soluções de segurança da informação nesses sistemas. Isso facilita automatização da aplicação deste domínio, beneficiando, dessa forma, o trabalho de gestores de TI e equipes das organizações detentoras do SoS ou por pesquisadores da área.

8. Conclusão

Este capítulo apresenta as conclusões da dissertação, a contribuição da pesquisa e as limitações do estudo. Também discute os trabalhos futuros.

8.1 Epílogo

SoS é uma classe de sistemas complexos caracterizados pela união de sistemas independentes gerencialmente e operacionalmente que colaboram para cumprir uma missão global. O SoS é formado por um arranjo ou conjunto de sistemas constituintes que possuem objetivos estabelecidos para serem cumpridos. Cada constituinte realiza sua missão de forma individual e contribui para a realização da missão global.

No cenário sociotécnico e organizacional que reconhece a interação entre as pessoas e a tecnologia em uma organização, é desafiador manter a transparência e interoperabilidade entre os sistemas constituintes. Tais sistemas constituintes podem se interconectar com computação em nuvem, principalmente para armazenar dados, e sistemas de *Big Data Analytics* para colher, inspecionar, tratar e modelar esses dados para obter *insights* e identificar oportunidades para a organização. *Big data* e computação em nuvem são recursos importantes em estratégias de negócios principalmente em sistemas financeiros e bancários. Muitas organizações atualmente usam um link para acessar os seus dados em plataformas de nuvem, enquanto outras grandes corporações desenvolveram data centers com nuvem privada ou nuvem híbrida. Além disso, pode-se utilizar ERP para acessar todos os dados e processos dos mais diversos departamentos de uma organização.

Isso faz com que um SoS e seus sistemas constituintes interoperarem com esses sistemas e suas bases de dados e sejam também aplicados nos variados cenários com escala ou complexidade variada de sistemas interconectados, tais como militar, transporte, financeiro, energia, saúde, Internet, entre outros. Nesse sentido, 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 o SoS como um todo e acarretar diversos problemas para o negócio. Por exemplo, nas cidades inteligentes, as falhas podem comprometer a segurança de pessoas e bens patrimoniais, além de causar impacto na economia e até mesmo a insolvência dos sistemas constituintes.

Cabe também destacar a ocorrência do aumento contínuo no número e no impacto de ataques cibernéticos. A segurança cibernética está afetando cada vez mais os sistemas, o que pode atingir uma infraestrutura crítica, como, por exemplo, um SoS que cuida da contabilidade de uma organização.

Em vista disso, foi possível responder questão principal da pesquisa (QPP) por meio do desenvolvimento de 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, foram levantadas uma questão da pesquisa (QP) e sub-questões (SQ1, SQ2 e SQ3) à QP na condução do MSL.

Em resposta a SQ1, as tecnologias mais empregadas em SoS são:

- **Algoritmo** probabilístico, como Monte Carlo e Cadeia de *Markov*;
- **Análise de pontos de vulnerabilidade**;
- **Criptografia**;
- **Esquemas de monitoramento**;
- **Simulação de ambiente**;
- **Protocolos**.

Em relação à SQ2, o MSL permitiu identificar:

- **Análise comparativa**;
- **Análise e validação feita por especialista**;
- **Estudos de caso**;
- **Inteligência Artificial (IA)**, *Deep Learning* e *Machine Learning*.

No que se refere a SQ3, foi possível identificar:

- Análise e identificação dos **pontos de vulnerabilidade** no SoS e em seus sistemas constituintes;
- Análise e identificação de **risco de ataques ou ciberataques**;
- **Políticas de segurança** como controle de acesso ou nível de privacidade dos dados;
- **Fatores humanos** como comportamentos de atores ou o tipo de cliente do SoS.

Para identificar aspectos de segurança da informação discutidos na literatura são aplicados no contexto de SoS, foi executada uma pesquisa de opinião no período de 8 de outubro a 12 de novembro de 2021. A população-alvo foram especialistas de SI, SoS e Segurança da Informação que se encontram no comitê do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021), e *International Workshop on Software Engineering for Systems-of-Systems and Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems* (SESoS/WDES 2021).

Ao comparar os resultados obtidos do MSL com os da pesquisa de opinião, foram observadas concordâncias entre a literatura e a aplicabilidade do SoS. Com os resultados do MSL e da pesquisa de opinião, foi possível propor uma ontologia de domínio para apoiar gestores de TI na tomada de decisão em questões de segurança da informação em SoS, avaliado por 5 especialistas por meio de um grupo focal, que permitiu o seu refinamento. Um estudo de viabilidade foi realizado com a participação de dois gestores (um de TI e o outro, de segurança da informação) de uma instituição pública federal para verificar a aplicabilidade do site web quanto a facilidade de uso e utilidade na execução da ontologia refinada.

Por fim, é importante destacar a importância de uma ontologia de domínio para o gerenciamento da segurança da informação em sistemas complexos como SoS. O uso de tal ontologia é uma forma de garantir a compreensão e entendimento dos elementos da segurança da informação na comunicação entre os gestores de TI, equipes e *stakeholders* envolvidos no gerenciamento desses sistemas.

8.2 Contribuições

Esta dissertação contribui para:

- 1) Fundamentação da segurança da informação em SoS com a caracterização desse domínio e criação de um corpo de conhecimento que apoie pesquisadores e profis-

sionais que atuam no âmbito de SoS no planejamento e desenvolvimento de soluções para problemas de segurança da informação;

- 2) Identificação do cenário de segurança da informação em SoS, mapeando um conjunto de abordagens aplicadas bem como a identificação dos fatores que afetam a escolha dos mecanismos de segurança para o gerenciamento deste sistema;
- 3) Caracterização dos aspectos de segurança da informação aplicados no SoS por meio de pesquisa de opinião para avaliar os resultados obtidos no MSL com respeito à sua aplicabilidade na indústria sob o ponto de vista de pesquisadores e profissionais no contexto de SoS;
- 4) Elaboração de uma ontologia de domínio para apoiar gestores de TI na tomada de decisão em questões de segurança da informação no contexto de SoS.

As atividades realizadas durante o mestrado viabilizaram as seguintes publicações:

- **Oportunidades de KIPO para Gestão em Sistemas de Informação Federados no Caso do Programa Bolsa Família** - Este artigo foi produzido na fase inicial da pesquisa com o objetivo de demonstrar 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. Os gestores de TI podem encontrar muitas dificuldades para gerenciar esses SI (JAY, 2013; SMITH; LEWIS, 2011) com foco na segurança da informação (WHITMAN; MATTORD, 2009). Uma categoria de sistema complexo, como SIF que é uma classe derivada de SoS, está sujeita a diversas políticas e regras de gerenciamento e controle (SOMMERVILLE, 2016). O estudo foi publicado no Seminário de Pesquisa em Ontologias no Brasil (ONTOBRAS) 2020 (DIAS et al., 2020);
- **Ontologia para o Gerenciamento de Segurança da Informação em Sistemas-de-Sistemas** - Este artigo teve como objetivo definir a metodologia a ser utilizada para a elaboração da ontologia de domínio. O estudo foi publicado no Workshop de Teses e Dissertações (WTD0) do ONTOBRAS 2021 (DIAS et al., 2021);
- *Investigating information security in systems-of-systems* - Este artigo tem o objetivo de apresentar os resultados do mapeamento em conjunto com resultados da pesquisa de opinião. O estudo foi publicado na trilha principal do Simpósio Brasileiro de Sistemas de Informação (SBSI) 2022.

8.3 Limitações

Este trabalho se limitou aos conceitos de segurança da informação em SoS encontrados nos resultados do MSL e confirmados na pesquisa de opinião por especialistas que atuam profissionalmente na indústria ou possuem projetos de pesquisa aplicados a cenários reais. Conceitos relacionados aos tipos de ataques cibernéticos e boas práticas para proteger o SoS destes ataques não foram adicionados na ontologia. Além disso, os testes e consultas realizados na ontologia ficaram limitados a apenas ao respectivo domínio de conhecimento.

Como segurança da informação é uma em constante inovação e desenvolvimento, seria interessante que novos mapeamentos sistemáticos e pesquisas de opinião mais específicos encontrados nos tópicos da taxonomia da ontologia sejam conduzidos. Isso permitirá a inserção de novos conceitos e aspectos relevantes para a ontologia.

Outro ponto de limitação foi a restrição do COVID-19 que impôs restrições a interações pessoais. Um estudo de caso participativo poderia ser realizado, por exemplo, para avaliar o site web na execução da ontologia InfoSecSoS. Isso permitiria que ele fosse acompanhada mais de perto por dois ou mais de especialistas em organizações que trabalham com um SoS real. No entanto, mesmo com fim das restrições sanitárias da pandemia da COVID-19, pode ser difícil encontrar organizações que se disponham a avaliar o site web com o propósito de propor melhorias práticas e que os administradores concordem em participar de estudos em conjunto com a academia.

8.4 Trabalhos Futuros

Como trabalhos futuros, é possível destacar:

- **Executar outros MSL** - é importante que novos mapeamentos sejam realizados, para abordar os tipos de ataques que podem ocorrer em SoS, a questão da privacidade entre os sistemas constituintes, a integração com aplicativos e sistemas em nuvem, a segurança de sistemas legados que, por conta da sua tecnologia antiga, esbarram em códigos antigos e complexos, dificultando a interoperação com os sistemas constituintes recentemente inseridos no SoS, entre outros;
- **Executar outras pesquisas de opinião** - realizar um processo contínuo de coleta de dados de modo a criar um repositório histórico de Segurança da Informação em SoS e incluir contextos de negócios similares (e.g., militar, segurança pública, cidades

inteligentes, sistemas bancários, categorias de SIF, categorias de SoIS, entre outros) que possam identificar aspectos importantes para a pesquisa;

- **Evoluir a ontologia** - expandir a ontologia nos subdomínios de sua taxonomia, tipos de ataques, privacidade dos dados, sistemas em nuvem, entre outros. As ontologias SegInfoSoS ¹ e InfoSecSoS ² estão disponíveis para download;
- **Comparar com outras ontologias existentes** - comparar a InfoSecSoS com outras ontologias desenvolvidas pelo mundo para permitir um vocabulário compartilhado sobre segurança da informação entre diferentes organizações;
- **Realizar operações de inserção, atualização e exclusão de classes, subclasses e instâncias na ontologia de forma controlada no site web** - isso permitirá uma economia para as pequenas empresas que não precisariam pagar para ter um SGBD controlando suas aplicações além de proporcionar adaptação às especificidades do domínio de seu negócio, escalabilidade que possibilita estender relacionamentos e correspondências de conceitos às outras ontologias existentes e a capacidade de evolução do modelo com novas demandas emergentes.

¹<https://doi.org/10.5281/zenodo.6621716>

²<https://doi.org/10.5281/zenodo.6621882>

Referências

- ABDALLA, Gabriel. Establishment of an Ontology for Systems-of-Systems. Master's Thesis. University of São Paulo, São Carlos, Brazil, 2017.
- AGRAWAL, Dakshi. A New Schema for Security in Dynamic Uncertain Environments. **IEEE Sarnoff Symposium**, p. 1–5, 2009. DOI: <10.1109/SARNOF.2009.4850378>.
- ALMEIDA, Mauricio B; BAX, Marcello P. Uma visão geral sobre ontologias: pesquisa sobre definições, tipos, aplicações, métodos de avaliação e de construção. **Ciência da informação**, SciELO Brasil, v. 32, n. 3, p. 7–20, 2003.
- ALMEIDA, NAC. Modelagens sobre gestão organizacional em uma perspectiva multidisciplinar e sistêmica: proposições para a Rede Federal de Educação Profissional, Científica e Tecnológica–RFEPCT. Tese. Universidade Federal da Bahia, Salvador, Brasil, 2013.
- KI-ARIES, Duncan; FAILY, Shamal; DOGAN, Huseyin; WILLIAMS, Christopher. Assessing System of Systems Security Risk and Requirements with OASoSIS. **2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE)**, p. 14–20, 2018. DOI: <10.1109/ESPRE.2018.00009>.
- B. ALMEIDA, Mauricio; R. FELIPE, Eduardo; BARCELOS, Renata. Toward a document-centered ontological theory for information architecture in corporations. **Journal of the Association for Information Science and Technology**, v. 71, n. 11, p. 1308–1326, 2020. DOI: <<https://doi.org/10.1002/asi.24337>>. eprint: <<https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/asi.24337>>. Disponível em: <<<https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.24337>>>.
- BERNERS-LEE, Tim; HENDLER, James; LASSILA, Ora. The semantic web. **Scientific american**, JSTOR, v. 284, n. 5, p. 34–43, 2001.

- BODEAU, D.J. System-of-systems security engineering. **Tenth Annual Computer Security Applications Conference**, p. 228–235, 1994. DOI: <10.1109/CSAC.1994.367304>.
- BOSCARIOLI, Clodis; ARAUJO, Renata Mendes; MACIEL, Rita Suzana Pitangueira. I GrandSI-BR Grand Research Challenges in Information Systems in Brazil 2016-2026. **Special Committee on Information Systems (CE-SI). Brazilian Computer Society (SBC)**, p. 12–40, 2017.
- BREITMAN, KK. **Web Semântica - A Internet do Futuro**. VitalSource Bookshelf, Grupo GEN., 2005. ISBN 9788521617808. Disponível em: <<<https://bookshelf.vitalsource.com/books/9788521617808>>>.
- BURANARACH, Marut. **A framework for the organization and discovery of information resources in a www environment using association, classification and deduction**. University of Pittsburgh, 2004.
- CAMPOS, Maria Luiza de Almeida; CAMPOS, Maria Luiza Machado; DÁVILA, Alberto MR; GOMES, Hagar Espanha; CAMPOS, Linair Maria; LIRA, Laura. Aspectos metodológicos no reuso de ontologias: um estudo a partir das anotações genômicas no domínio dos tripanosomatídeos. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 3, n. 1, 2009.
- CARTURAN, S. B. O. G.; GOYA, D. H. A Systems-of-Systems Security Framework for Requirements Definition in Cloud Environment. In: **PROCEEDINGS of the 13th European Conference on Software Architecture - Volume 2**. Paris, France: Association for Computing Machinery, 2019. (ECSA '19), p. 235–240. ISBN 9781450371421. DOI: <10.1145/3344948.3344977>. Disponível em: <<<https://doi.org/10.1145/3344948.3344977>>>.
- CASOLA, Valentina; CATELLI, Rosario; DE BENEDICTIS, Alessandra. A First Step Towards an ISO-Based Information Security Domain Ontology. **2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)**, p. 334–339, 2019. DOI: <10.1109/WETICE.2019.00075>.
- CECCARELLI, A.; ZOPPI, T.; VASENEV, A.; MORI, M.; IONITA, D.; MONTOYA, L.; BONDAVALLI, A. Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach. **ACM Trans. Cyber-Phys. Syst.**, Association for Computing Machinery, New York, NY, USA, v. 3, n. 2, out. 2018. ISSN 2378-962X. DOI: <10.1145/3234513>. Disponível em: <<<https://doi.org/10.1145/3234513>>>.

- CHANDRASEKAN, B; JOSEPHSON, J; BENJAMINS, V. The Ontology of Tasks and Methods. In: WORKSHOP. KNOWLEDGE Acquisition Modeling and Mngt. Banff., 1998.
- DAHMAN, J. S.; BALDWIN, K. J. Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering. In: 2008 2nd Annual IEEE Systems Conference. 2008. p. 1–7. DOI: <10.1109/SYSTEMS.2008.4518994>.
- DHILLON, Gurpreet; KOLKOWSKA, Ella. Can a Cloud Be Really Secure? A Socratic Dialogue. In: **Computers, Privacy and Data Protection: an Element of Choice**. Edição: Serge Gutwirth, Yves Poulet, Paul De Hert e Ronald Leenes. Dordrecht: Springer Netherlands, 2011. p. 345–360. ISBN 978-94-007-0641-5. DOI: <10.1007/978-94-007-0641-5_16>. Disponível em: <<https://doi.org/10.1007/978-94-007-0641-5_16>>.
- DIAS, Roberto Monteiro; ANTÔNIO, Nadja Piedade de; HORITA, Flávio E. A.; SANTOS, Rodrigo Pereira dos. Oportunidades de KIPO para Gestão em Sistemas de Informação Federados no Caso do Programa Bolsa Família (KIPO Opportunities for Management of Federated Information Systems in the Case of the "Bolsa Família" Program). 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**. CEUR-WS.org, 2020. v. 2728. (CEUR Workshop Proceedings), p. 227–234. Disponível em: <<<http://ceur-ws.org/Vol-2728/short4.pdf>>>.
- DIAS, Roberto Monteiro; ZACARIAS, Rodrigo Oliveira; SANTOS, Rodrigo Pereira dos. Ontologia para o Gerenciamento de Segurança da Informação em Sistemas-de-Sistemas (Ontology for management of information security in systems-of-systems). In: _____. **Proceedings of the XIV Seminar on Ontology Research in Brazil (ONTOBRAS 2021) and V Doctoral and Masters Consortium on Ontologies (WTDO 2021), Online, Brazil, November 16-19, 2021**. CEUR-WS.org, 2021. v. 3050. (CEUR Workshop Proceedings), p. 273–278. Disponível em: <<<http://ceur-ws.org/Vol-3050/master2.pdf>>>.
- DYBA, T.; DINGSOYR, T.; HANSEN, G. K. Applying Systematic Reviews to Diverse Study Types: An Experience Report. In: ESEM 2007. 2007. p. 225–234.
- ELMAGHRABY, Adel S.; LOSAVIO, Michael M. Cyber security challenges in Smart Cities: Safety, security and privacy. **Journal of Advanced Research**, v. 5, n. 4, p. 491–497, 2014. Cyber Security. ISSN 2090-1232. DOI: <https://doi.org/10.1007/978-94-007-0641-5_16>.

1016/j.jare.2014.02.006>. Disponível em: <<<https://www.sciencedirect.com/science/article/pii/S2090123214000290>>>.

FENSEL, Dieter. **Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce**. 2. ed. Berlin, Heidelberg: Springer-Verlag, 2003. ISBN 3540003029.

FERNANDES, Juliana Costa; BAIÃO, Fernanda; SANTOS, Rodrigo Pereira dos. KIPO Opportunities for Interoperability Decisions in Systems-of-Information Systems in the Domain of Environmental Management. In: _____. **Software Ecosystems, Sustainability and Human Values in the Social Web**. Cham: Springer International Publishing, 2020. p. 21–41. ISBN 978-3-030-46130-0.

FERNANDES, Juliana Costa; FERREIRA, Francisco; CORDEIRO, Felipe; NETO, Valdemar Vicente Graciano; SANTOS, Rodrigo Pereira dos. A conceptual model for systems-of-information systems. In: IEEE. PROCEEDINGS of the International Conference on Information Reuse and Integration for Data Science (IRI). Los Angeles, USA, 2019. p. 364–371.

FERNANDES, Juliana Costa; GRACIANO NETO, Valdemar Vicente; SANTOS, Rodrigo Pereira dos. Interoperability in Systems-of-Information Systems: A Systematic Mapping Study. In: PROCEEDINGS of the 17th Brazilian Symposium on Software Quality. Curitiba, Brazil: Association for Computing Machinery, 2018. (SBQS), p. 131–140. ISBN 9781450365659. DOI: <10.1145/3275245.3275259>. Disponível em: <<<https://doi.org/10.1145/3275245.3275259>>>.

FERREIRA, Francisco Henrique Cerdeira; SANTOS, Rodrigo Pereira dos. Arquitetura para Prevenção e Tolerância a Falhas em Sistemas-de-sistemas Virtuais. In: ANAIS Estendidos do XV Simpósio Brasileiro de Sistemas de Informação. Aracaju: SBC, 2019. p. 75–80. DOI: <10.5753/sbsi.2019.7444>. Disponível em: <<https://sol.sbc.org.br/index.php/sbsi_estendido/article/view/7444>>.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008.

GRACIANO NETO, Valdemar Vicente; OQUENDO, Flavio; NAKAGAWA, Elisa Yumi. Smart systems-of-information systems: Foundations and an assessment model for research development. **Sociedade Brasileira de Computação**, 2017.

GRUBER, Thomas R. Toward Principles for the Design of Ontologies Used for Knowledge Sharing. **Int. J. Hum.-Comput. Stud.**, Academic Press, Inc., USA, v. 43, n. 5–6, p. 907–928, dez. 1995. ISSN 1071-5819. DOI: <10.1006/ijhc.1995.1081>. Disponível em: <<<https://doi.org/10.1006/ijhc.1995.1081>>>.

- GUARINIELLO, C.; DELAURENTIS, D. Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. **Procedia Computer Science**, v. 28, p. 720–727, 2014. DOI: <10.1016/j.procs.2014.03.086>.
- GUARINO, N. **Formal Ontology in Information Systems: Proceedings of the 1st International Conference June 6-8, 1998, Trento, Italy**. 1st. NLD: IOS Press, 1998. ISBN 9051993994.
- GUIZZARDI, Giancarlo. Desenvolvimento para e com reuso: Um estudo de caso no domínio de Vídeo sob Demanda. **Universidade Federal do Espírito Santo, Centro Tecnológico**, v. 11, 2000.
- HOSEY, J.; GAMBLE, R. Extracting Security Control Requirements. In: PROCEEDINGS of the CSIIRW '10. Oak Ridge, Tennessee, USA: Association for Computing Machinery, 2010. ISBN 9781450300179. DOI: <10.1145/1852666.1852715>. Disponível em: <<<https://doi.org/10.1145/1852666.1852715>>>.
- INOCÊNCIO, Thiago J.; GONZALES, Gustavo R.; CAVALCANTE, Everton; HORITA, Flávio E. A. Emergent Behavior in System-of-Systems: A Systematic Mapping Study. In _____. **Proceedings of the XXXIII Brazilian Symposium on Software Engineering, SBES 2019, Salvador, Brazil, September 23-27, 2019**. ACM, 2019. p. 140–149. DOI: <10.1145/3350768.3350779>. Disponível em: <<<https://doi.org/10.1145/3350768.3350779>>>.
- ISO. **ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls**. 2013.
- ISOTANI, S.; BITTENCOURT, I. I. **Dados abertos conectados: em busca da web do conhecimento**. Novatec, 2015. Disponível em: <<<https://ceweb.br/livros/dados-abertos-conectados/>>>.
- JAY, Jason. Navigating Paradox as a Mechanism of a Change and Innovation in Hybrid Organizations. **The Academy of Management Journal**, v. 56, n. 1, p. 137–159, 2013. DOI: <10.2307/23414348>.
- KITCHENHAM, Barbara; CHARTERS, Stuart. Guidelines for performing Systematic Literature Reviews in Software Engineering. Citeseer, 2007.
- KITCHENHAM, Barbara Ann; BUDGEN, David; BRERETON, Pearl. **Evidence-Based Software Engineering and Systematic Reviews**. Chapman Hall/CRC, 2015. ISBN 1482228653.
- KITZINGER, Jenny. Qualitative Research: Introducing Focus Groups. **BMJ (Clinical research ed.)**, v. 311, p. 299–302, ago. 1995. DOI: <10.1136/bmj.311.7000.299>.

- LANG, U.; SCHREINER, R. Model Driven Security Accreditation (MDSA) for Agile, Interconnected It Landscapes. In: PROCEEDINGS of the First ACM Workshop on Information Security Governance. Chicago, Illinois, USA: Association for Computing Machinery, 2009. (WISG '09), p. 13–22. ISBN 9781605587875. DOI: <10.1145/1655168.1655173>. Disponível em: <<<https://doi.org/10.1145/1655168.1655173>>>.
- LAUDON, Kenneth C; LAUDON, Jane P. **Sistemas de informação gerenciais. 5ª Edição**. São Paulo: Pearson, 2004.
- LEUNG, Nelson KY; LAU, Sim Kim; FAN, Joshua. An ontology-based collaborative knowledge management network to enhance the reusability of inter-organizational knowledge. **Communications of the IIMA**, v. 9, n. 1, p. 5, 2009.
- LEVER, K. E.; KIFAYAT, K. Identifying and mitigating security risks for secure and robust NGI networks. **Sustainable Cities and Society**, v. 59, p. 102098, 2020.
- LOPER, M. L. Simulation Trust and the Internet of Things. In: 2019 Winter Simulation Conference (WSC). 2019. p. 2–16.
- MAIER, M. W. Architecting principles for systems-of-systems. **Systems Engineering: The Journal of the International Council on Systems Engineering**, Wiley Online Library, v. 1, n. 4, p. 267–284, 1998.
- MALAGUTTI, Marcelo Antônio Osller. O papel da dissuasão no tocante a ofensas cibernéticas. **Doutrina Militar Terrestre em Revista**, v. 4, n. 9, p. 18–27, 2016.
- MERIAH, Ines; RABAI, Latifa Ben Arfa; KHEDRI, Ridha. 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). 2021. p. 1–8. DOI: <10.1109/RDAAPS48126.2021.9452006>.
- MIHALJEVIC, M.; IMAI, H.; DAVID, M.; KOBARA, K.; WATANABE, H. On Advanced Cryptographic Techniques for Information Security of Smart Grid AMI. In: PROCEEDINGS of the CSIIRW '11. Oak Ridge, Tennessee, USA: Association for Computing Machinery, 2011. ISBN 9781450309455. DOI: <10.1145/2179298.2179371>. Disponível em: <<<https://doi.org/10.1145/2179298.2179371>>>.
- MORGAN, David L; KRUEGER, Richard A. **The focus group guidebook**. Sage, 1998.
- NEAGA, E. I.; HENSHAW, M. J. C. Modeling the linkage between systems interoperability and security engineering. In: 2010 5th International Conference on System of Systems Engineering. 2010. p. 1–6.

- NIELSEN, Claus Ballegaard; LARSEN, Peter Gorm; FITZGERALD, John; WOODCOCK, Jim; PELESKA, Jan. Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions. **ACM Comput. Surv.**, Association for Computing Machinery, New York, NY, USA, v. 48, n. 2, set. 2015. ISSN 0360-0300. DOI: <10.1145/2794381>. Disponível em: <<<https://doi.org/10.1145/2794381>>>.
- NOY, N.; MCGUINNESS, Deborah. Ontology Development 101: A Guide to Creating Your First Ontology. **Knowledge Systems Laboratory**, v. 32, jan. 2001.
- NULTY, Duncan. The adequacy of response rates to online and paper surveys: what can be done? **Assessment & Evaluation in Higher Education**, Routledge, v. 33, n. 3, p. 301–314, 2008. DOI: <10.1080/02602930701293231>. eprint: <<https://doi.org/10.1080/02602930701293231>>. Disponível em: <<<https://doi.org/10.1080/02602930701293231>>>.
- ORMROD, D.; TURNBULL, B.; O’SULLIVAN, K. System of systems cyber effects simulation ontology. In: 2015 Winter Simulation Conference (WSC). 2015. p. 2475–2486.
- OUEDRAOGO, W. F.; BIENNIER, F.; MERLE, P. Optimizing service protection with model driven security@ run. time. In: IEEE. 2015 IEEE Symposium on Service-Oriented System Engineering. 2015. p. 50–58.
- PARKIN, Simon; ARNELL, Simon; WARD, Jeremy. Change That Respects Business Expertise: Stories as Prompts for a Conversation about Organisation Security. In: NEW Security Paradigms Workshop. Virtual Event, USA: Association for Computing Machinery, 2021. (NSPW ’21), p. 28–42. ISBN 9781450385732. DOI: <10.1145/3498891.3498895>. Disponível em: <<<https://doi.org/10.1145/3498891.3498895>>>.
- PETRATOS, P.; FACCIA, A. Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology. In: PROCEEDINGS of the 2019 3rd International Conference on Cloud and Big Data Computing. Oxford, United Kingdom: Association for Computing Machinery, 2019. (ICCBDC 2019), p. 100–105. ISBN 9781450371650. DOI: <10.1145/3358505.3358513>. Disponível em: <<<https://doi.org/10.1145/3358505.3358513>>>.
- RATHORE, M. M.; PAUL, A.; CHILAMKURTHI, N.; HONG, W.; SEO, H. Real-time secure communication for Smart City in high-speed Big Data environment. **Future Generation Computer Systems**, v. 83, nov. 2017. DOI: <10.1016/j.future.2017.08.006>.

- SMITH, Wendy; LEWIS, Marianne. Toward a Theory of Paradox: A Dynamic Equilibrium Model of Organizing. **Academy of Management Review**, v. 36, n. 2, p. 381–403, 2011. DOI: <10.5465/AMR.2011.59330958>.
- SOMMERVILLE, Ian. **Software Engineering**. 10th Edition: Pearson, 2016.
- STUDER, Rudi; BENJAMINS, V Richard; FENSEL, Dieter. Knowledge engineering: principles and methods. **Data & knowledge engineering**, Elsevier, v. 25, n. 1-2, p. 161–197, 1998.
- TAGAREV, T.; SHARKOV, G. Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems. In: PROCEEDINGS of the 20th International Conference on Computer Systems and Technologies. Ruse, Bulgaria: Association for Computing Machinery, 2019. (CompSysTech '19), p. 8–18. ISBN 9781450371490. DOI: <10.1145/3345252.3345255>. Disponível em: <<<https://doi.org/10.1145/3345252.3345255>>>.
- TBATOU, S.; RAMRAMI, A.; TABII, Y. Security of Communications in Connected Cars Modeling and Safety Assessment. In: PROCEEDINGS of the BDCA'17. Tetouan, Morocco: Association for Computing Machinery, 2017. ISBN 9781450348522. DOI: <10.1145/3090354.3090412>. Disponível em: <<<https://doi.org/10.1145/3090354.3090412>>>.
- USCHOLD, Mike; GRUNINGER, Michael. Ontologies: Principles, methods and applications. **Knowledge Engineering Review**, v. 11, p. 93–136, 1996.
- WHITMAN, M. E.; MATTORD, H. J. **Principles of information security**. 3. ed.: Thompson Course Technology, 2009.
- WOHLIN, Claes; RUNESON, Per; HÖST, Martin; OHLSSON, Magnus C.; REGNELL, Björn; WESSLÉN, Anders. Analysis and Interpretation. In: EXPERIMENTATION in Software Engineering. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. p. 123–151. ISBN 978-3-642-29044-2. DOI: <10.1007/978-3-642-29044-2_10>. Disponível em: <<https://doi.org/10.1007/978-3-642-29044-2_10>>.
- ZHOU, B. et al. System-of-systems boundary check in a public event scenario. In: SOSE 2010. 2010. p. 1–8.

Apêndice I. Formulário da Pesquisa de Opinião

- Formulário de pesquisa de opinião sobre segurança da informação em SoS.

Pesquisa de opinião sobre segurança da informação em sistemas-de-sistemas (SoS)

Esta pesquisa de opinião pretende analisar aspectos de segurança da informação com o propósito de avaliar a sua aplicabilidade na indústria do ponto de vista de pesquisadores e profissionais no contexto de sistemas-de-sistemas.

Esta pesquisa de opinião é conduzida por Roberto Dias (UNIRIO) com colaboração de Rodrigo Zacarias (UNIRIO), sob orientação do prof. Rodrigo Santos (UNIRIO).

Estima-se que o tempo para completar esta entrevista é de 15 a 20 minutos.

Aceitando participar desta pesquisa de opinião, você concorda com os termos descritos abaixo.

DECLARAÇÃO DE CONSENTIMENTO

Eu estou ciente que os dados obtidos por meio deste estudo serão mantidos sob confidencialidade e os resultados serão posteriormente apresentados de forma agregada, de modo que o participante não seja associado a um dado específico, garantindo seu anonimato durante a divulgação dos resultados.

Tenho ciência de que os dados coletados nesta pesquisa serão utilizados para fins acadêmicos, podendo os resultados serem publicados em meios de comunicação científicos, tais como congressos e periódicos. Dessa forma, comprometo-me a não comunicar meus resultados enquanto o estudo não for concluído, bem como manter sigilo das técnicas e documentos apresentados e fazem parte do estudo.

CONDIÇÕES

1. Eu entendo que toda a informação é confidencial. Eu não serei pessoalmente identificado. Eu concordo em preencher o questionário para fins de pesquisa e que os dados derivados desta pesquisa de opinião serão processados de forma anônima antes de ser publicado em periódicos, conferências e postagens em "blogs".
2. Eu entendo que a minha participação nesta pesquisa de opinião é totalmente voluntária e que me recusar a participar não envolverá nenhuma penalização ou perda de benefícios. Se eu escolher, eu posso desistir de participar a qualquer momento.
3. Eu entendo que posso contactar os pesquisadores se eu tiver qualquer dúvida sobre quaisquer questões do questionário. Eu estou ciente que meu consentimento não me beneficiará diretamente. Eu também estou ciente que os autores manterão os dados perpetuamente e poderão utilizá-los para futuros trabalhos acadêmicos.
4. Clicando com o "sim" na questão abaixo, eu livremente dou meu consentimento e reconheço meus direitos como um participante voluntário de pesquisa como exposto acima e dou meu consentimento aos pesquisadores para utilizarem minhas informações ao conduzirem pesquisas nos assuntos mencionados acima.

Em caso de dúvidas, por favor escrever para: roberto.dias@edu.unirio.br e, rodrigo.zacarias@edu.unirio.br e rps@uniriotec.br

*Obrigatório

1. E-mail *

2. Você concorda como o termo de consentimento? *

Marcar apenas uma oval.

- ☐ Sim
☐ Não

Questões demográficas

3. Qual é o seu nível de formação? *

Marcar apenas uma oval.

- ☐ Pós-Doutorado
☐ Doutorado
☐ Mestrado
☐ Especialização
☐ Graduação
☐ Técnico

4. Qual é o seu segmento de atuação? *

Marque todas que se aplicam.

- ☐ Pesquisadores ou profissionais da academia
☐ Pesquisadores ou profissionais da indústria

5. Em que setor você atua? *

Marcar apenas uma oval.

- ☐ Público
☐ Privado
☐ Terceiro Setor (por exemplo: Organizações Não Governamentais, Associações, Entidades sem fins lucrativos)

6. Qual o seu tempo de experiência nas seguintes áreas de conhecimento? *

Escala 0 = Menos de 1 ano; 1 = Entre 1 e 5 anos; 2 = Entre 5 e 10 anos; 3 = Entre 10 e 15 anos; 4 = Acima de 15 anos.

Marcar apenas uma oval por linha.

	0	1	2	3	4
Gestão de Tecnologia da Informação	☐	☐	☐	☐	☐
Segurança da Informação	☐	☐	☐	☐	☐
Sistemas de Informação	☐	☐	☐	☐	☐
Sistemas-de-Sistemas	☐	☐	☐	☐	☐

7. Qual o seu nível de experiência nas seguintes áreas de conhecimento? *

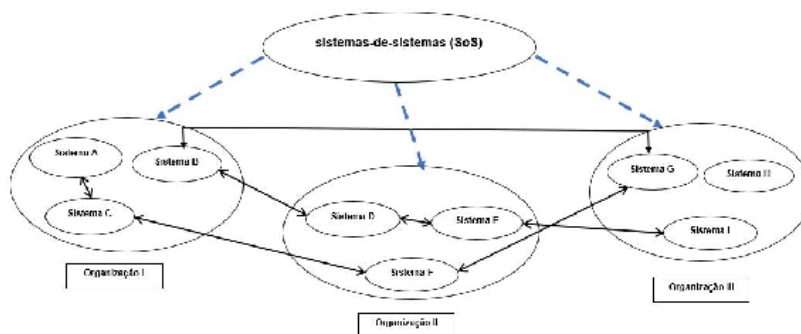
Escala: 0 = nenhum (nunca participou de atividades deste tipo); 1 = estudei em aula ou em livro (possui conhecimento teórico apenas); 2 = pratiquei em projetos em sala de aula (possui conhecimento teórico aplicado apenas no contexto acadêmico); 3 = usei em projetos pessoais (possui conhecimento teórico somado de experiências práticas individuais); 4 = usei em poucos projetos na indústria (possui conhecimento teórico somado de poucas experiências práticas reais); e 5 = usei em muitos projetos na indústria (possui conhecimento teórico somado de muitas experiências práticas reais).

Marcar apenas uma oval por linha.

	0	1	2	3	4	5
Gestão de Tecnologia da Informação	☐	☐	☐	☐	☐	☐
Segurança da Informação	☐	☐	☐	☐	☐	☐
Sistemas de Informação	☐	☐	☐	☐	☐	☐
Sistemas-de-Sistemas	☐	☐	☐	☐	☐	☐

Segurança da informação em sistemas-de-sistemas (SoS)

Visão conceitual de sistemas-de-sistemas (SoS):



Leia o texto abaixo sobre "Segurança da informação em SoS" para compreensão do contexto da área apresentada:

Os sistemas-de-sistemas (SoS) são uma classe de sistemas complexos caracterizados pela união de sistemas independentes gerencialmente e operacionalmente que colaboram para cumprir uma missão global. O SoS é formado por um arranjo ou conjunto de sistemas constituintes que possuem objetivos estabelecidos para serem cumpridos. Cada constituinte realiza sua missão de forma individual e contribui para a realização da missão global. Pode-se destacar como um exemplo clássico desses sistemas as cidades inteligentes, onde diferentes dispositivos e sistemas de informação atuam para oferecer serviços à população por meio da colaboração de diferentes organizações públicas e/ou privadas proprietárias desses sistemas. Considere, como exemplo de colaboração em uma cidade inteligente, um sistema de previsão de tempo que se comunica com o sistema de controle de trânsito para liberar as ruas que não tenham pontos de alagamentos sofridos pela cidade em uma tempestade. Tal colaboração diminui o trânsito nas ruas alagadas e direciona os veículos e pessoas para as ruas que estão livres destes pontos de alagamentos. Isso permite que as pessoas e os veículos sejam movidos para caminhos alternativos mais facilmente.

No cenário sociotécnico e organizacional que reconhece a interação entre as pessoas e a tecnologia em uma organização, é um desafio manter a transparência de como os dados são visualizados no SoS e a interoperabilidade de como os seus sistemas constituintes se comunicam. Isso faz com um SoS e seus sistemas constituintes possam interoperar com os mais diferentes tipos de sistemas e suas bases de dados, em variados cenários com escala ou complexidade diversificada, tais como militar, transporte, financeiro, energia, saúde, internet, entre outros.

Nesse sentido, 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 o SoS como um todo e acarretar diversos problemas para o negócio. Por exemplo, nas cidades inteligentes, as falhas podem comprometer a segurança de pessoas e bens patrimoniais, além de causar impacto na economia e até mesmo a insolvência dos sistemas constituintes.

Cabe também destacar a ocorrência do aumento contínuo no número e no impacto de ataques cibernéticos. A segurança cibernética está afetando cada vez mais os sistemas, o que pode atingir uma infraestrutura crítica, como, por exemplo, um SoS que cuida da contabilidade de uma organização.

Dimensão Tecnologias:

Indique abaixo o seu nível de concordância em relação a algumas tecnologias relevantes para apoiar segurança da informação em sistemas como SoS:

8. Uso de **algoritmo evolutivo** de forma dinâmica para otimizar o nível de segurança em ambientes de interconexão do SoS, considerando fatores como controle de acesso, risco de nós centralizados e distância entre os nós. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

9. Uso do **algoritmo Monte Carlo** na predição de ataques e vulnerabilidades. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

10. Uso do **algoritmo Cadeia de Markov** na abordagem de simulação de um método de pós-auditoria para medir a eficácia dos investimentos realizados em segurança da informação em uma organização. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

11. Uso de **análise de pontos de vulnerabilidades** durante a interoperação entre os sistemas constituintes para mitigá-los assim que mapeados. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

12. Uso de **criptografia de chave pública baseada em curvas elípticas** para garantir a confidencialidade, autenticidade e o não-repúdio de comunicações eletrônicas e de armazenamento de dados, como, por exemplo, em um ambiente de medição inteligente de energia elétrica (do inglês, smart grid advanced metering infrastructure ou AMI). *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

13. Uso de **criptografia de chave pública baseada em atributos** (do inglês attribute-based encryption ou ABE) para descrever quais usuários são autorizados a codificar/descodificar os dados de pacientes que trafegam entre os sistemas constituintes de um sistema de saúde pública, como por exemplo, o sistema único de saúde (SuS). *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

14. Uso de **criptografia de chave pública do tipo Rivest-Shamir-Adleman (RSA)** para permitir a transmissão segura dos dados, como, por exemplo, entre gateways ou pontos de acesso de canais de comunicação de um veículo em uma rede de internet veicular (IOV). *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

15. Uso de **esquemas de monitoramento** que se utilizam de mecanismos de segurança individuais com fornecimento de parâmetros de controle para ajustar as propriedades de segurança e mantê-los dentro dos limites aceitáveis em um SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

16. Uso de **protocolo** de segurança seguro e eficiente na transmissão de dados para proteção da comunicação, por exemplo, a comunicação entre um sistema remoto inteligente (SRI) e os usuários de um edifício inteligente contra intrusos externos. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

17. Uso de **simulação de ambiente** para análise de compartilhamento de informações em ambiente controlado para compreender os possíveis efeitos de ataques durante tráfego das informações. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

18. Há outras tecnologias que você utiliza para apoiar segurança da informação em sistemas como SoS?

Indique abaixo o seu nível de concordância em relação a algumas metodologias de avaliação relevantes para apoiar segurança da informação em sistemas como SoS:

19. Uso de **análise comparativa** para buscar referências em situações similares de exposição a riscos e pontos de vulnerabilidade para propor uma solução de segurança. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

20. Uso de **análise descritiva** em cada etapa do processo em engenharia de segurança em SoS para verificar os riscos associados ao fluxo de informações, aos domínios da política de segurança, a interfaces entre constituintes e tipo de arquitetura. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

21. Uso de **análise e validação** com especialista por meio de coleta de dados reais contribuindo diretamente para soluções de problema de segurança, geralmente aplicadas em casos que envolvem modelagem ou análise de documentação de arquitetura, ou requisitos de projeto. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

22. Uso do **estudo de caso** por meio de um cenário real ou realista para elicitar, analisar e validar riscos e requisitos de segurança em SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

23. Uso de **Inteligência artificial** por meio de **Machine Learning** para analisar os dados de operação nos sistemas constituintes, verificar a eficácia dos pontos de segurança e a resiliência do sistema em ciberataques por meio da predição desses ataques ou vulnerabilidades. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

24. Uso de **Inteligência artificial** por meio de **Deep Learning** para analisar os dados de operação nos sistemas constituintes, verificar a eficácia dos pontos de segurança e a resiliência do sistema em ciberataques por meio da predição desses ataques ou vulnerabilidades. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

25. Há outras metodologias de avaliação que você utiliza para apoiar segurança da informação em sistemas como SoS?

**Dimensão
Processos:**

Compreende-se que os fatores de segurança da informação condicionam as tomadas de decisão em relação à implementação de medidas de segurança da informação em SoS, partindo dos conceitos da preservação da confidencialidade, integridade e disponibilidade de informações (tríade CID) apresentada na ISO/IEC 27002:2013.
Indique abaixo o seu nível de concordância em relação aos fatores que são mais críticos no contexto de segurança da informação em sistemas como SoS:

26. O **tipo de cliente** deve ser previsto para que as funcionalidades do SoS não sejam comprometidas com a implementação de tecnologia que não está prevista na sua política de segurança. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

27. O **comportamento de atores** deve ser previsto para que as funcionalidades do SoS não sejam comprometidas com a implementação de tecnologia que não está prevista na sua política de segurança. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

28. O **controle de acesso** que cada organização dos constituintes adota deve ser considerado ao planejar o esquema de segurança do SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

29. O nível de **privacidade dos dados** que cada organização dos constituintes adota deve ser considerado ao planejar o esquema de segurança do SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

30. A **arquitetura** dos sistemas constituintes de um SoS deve ser conhecida. Um invasor experiente pode usar com facilidade este tipo de informação para obter acesso e transmitir ataques cibernéticos em pontos de vulnerabilidades específicos, comprometendo a segurança e obtendo informações privilegiadas. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

31. A alta dependência na **interface** de cada sistema constituinte de um SoS aumenta os riscos de avarias massivas, seja por meio de uma falha acidental ou um ataque malicioso. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

32. **Riscos de ataques/Ciberataques** por meio de hackers que se utilizam de ataques de negação de serviço para derrubar a rede dos veículos inteligentes, reprogramar ilegalmente as unidades de controle eletrônico (UCEs) desses veículos com software malicioso. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

33. Há outros fatores que você queira destacar no contexto de segurança da informação em sistemas como SoS?

Indique abaixo o seu nível de concordância em relação a alguns problemas que podemos encontrar no contexto de segurança da informação em sistemas como SoS:

34. **Falta de alinhamento** nos modelos, métodos, técnicas e/ou ferramentas de segurança da informação podem gerar incidentes de segurança da informação. As escolhas de soluções e medidas de segurança devem estar alinhadas com os objetivos do SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

35. **Falta de padronização** dos métodos de segurança da informação podem gerar falhas que podem levar a vulnerabilidades de segurança da informação. Por exemplo, o uso de métodos informais para soluções de problemas pela equipe de tecnologia da informação. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

36. **Falta de treinamentos** especializados e na educação em todos os níveis dos colaboradores, desde funcionários não técnicos até as equipes de tecnologia da informação. O descuido com o uso de uma ferramenta ou a falta de conhecimento dos riscos em sistemas como um SoS pode ser a porta de entrada para cibercriminosos. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

37. **Falta de um plano estratégico** eficiente com as características da segurança da informação em sistemas como um SoS pode gerar riscos para organização. É responsabilidade do gestor estar atento a essas características e, assim, criar um planejamento eficiente, buscando as tecnologias de segurança da informação que melhor atendam às políticas organizacionais. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

38. Há outros problemas que você queira destacar no contexto de segurança da informação em sistemas como SoS?

**Dimensão
Pessoas:**

Indique abaixo o seu nível de concordância em relação a alguns problemas que podemos encontrar no contexto de segurança da informação em sistemas como SoS ao lidar com pessoas:

39. Gestores indecisos ou com dificuldades na tomada de decisão devido à **falta de conhecimento prévio** de segurança da informação no SoS. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

40. **Falhas de comunicação** entre os colaboradores, técnicos e gestores devido à complexidade do SoS, causando dificuldade de refletir a segurança da informação nesses sistemas. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
☐ Concordo Parcialmente
☐ Indiferente
☐ Discordo Parcialmente
☐ Discordo Totalmente

41. A associação equivocada da segurança da informação com o gerenciamento de acesso na percepção dos colaboradores, técnicos e gestores no SoS. Por exemplo, colaboradores, técnicos e gestores podem associar a segurança da informação com esconder a informação dificultando o seu acesso. *

Marcar apenas uma oval.

- ☐ Concordo Totalmente
- ☐ Concordo Parcialmente
- ☐ Indiferente
- ☐ Discordo Parcialmente
- ☐ Discordo Totalmente

42. Há outros problemas que você queira destacar no contexto de segurança da informação em sistemas como SoS ao lidar com pessoas?

Dúvidas e Sugestões

43. Alguma dúvida ou dificuldade em responder às questões? Você tem alguma sugestão? Por favor, compartilhe conosco a resposta abaixo.

Este conteúdo não foi criado nem aprovado pelo Google.

Google Formulários