
**UNIVERSIDADE ESTADUAL DE CAMPINAS**
**FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO**

**FERRUCIO DE FRANCO ROSA**

# HCAPP-SEC: SELEÇÃO E ANÁLISE DE ITENS DE AVALIAÇÃO DE SEGURANÇA BASEADAS EM HEURÍSTICAS E CRITÉRIOS

# *HCAPP-SEC: SELECTION AND ANALYSIS OF SECURITY ASSESSMENT ITEMS BASED ON HEURISTICS AND CRITERIA*

**CAMPINAS**
**2018**

**FERRUCIO DE FRANCO ROSA**

# HCAPP-SEC: SELEÇÃO E ANÁLISE DE ITENS DE AVALIAÇÃO DE SEGURANÇA BASEADAS EM HEURÍSTICAS E CRITÉRIOS

## *HCAPP-SEC: SELECTION AND ANALYSIS OF SECURITY ASSESSMENT ITEMS BASED ON HEURISTICS AND CRITERIA*

Tese submetida à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Doutor em Engenharia Elétrica, na área de Engenharia de Computação.

*Dissertation submited to the School of Electrical and Computer Engineering, University of Campinas, in partial fulfillment of the requirements to obtain the Doctorate degree in Electrical Engineering, in the area of Computer Engineering.*

Orientador: Prof. Dr. Mario Jino

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO FERRUCIO DE FRANCO ROSA E ORIENTADA PELO PROF. DR. MARIO JINO

_____
Assinatura do Orientador

**CAMPINAS**
**2018**

**Agência(s) de fomento e no(s) de processo(s):** Não se aplica.
**ORCID:** http://orcid.org/0000-0001-9504-496X

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Luciana Pietrosanto Milla - CRB 8/8129

R71h

Rosa, Ferrucio de Franco, 1973-
HCAPP-SEC : seleção e análise de itens de avaliação de segurança baseadas em heurísticas e critérios / Ferrucio de Franco Rosa. – Campinas, SP : [s.n.], 2018.

Orientador: Mario Jino.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Avaliação. 2. Segurança. 3. Heurística. I. Jino, Mario, 1943-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações para Biblioteca Digital

**Título em outro idioma:** HCAPP-SEC : selection and analysis of security assessment items based on heuristics and criteria

**Palavras-chave em inglês:**

Assessment

Security

Heuristics

**Área de concentração:** Engenharia de Computação

**Titulação:** Doutor em Engenharia Elétrica

**Banca examinadora:**

Mario Jino [Orientador]

Romis Ribeiro de Faissol Attux

Ivan Luiz Marques Ricarte

Carla Merkle Westphall

Edgar Toshiro Yano

**Data de defesa:** 21-05-2018

**Programa de Pós-Graduação:** Engenharia Elétrica

# COMISSÃO EXAMINADORA – TESE DE DOUTORADO

**Candidato:** Ferrucio de Franco Rosa  RA: 098962

**Data da Defesa:** 21 de maio de 2018

**Título da Tese:** “HCApp-Sec: Seleção e análise de itens de avaliação de segurança baseadas em heurísticas e critérios” (*HCApp-Sec: Selection and analysis of security assessment items based on heuristics and criteria*)

Prof. Dr. Mario Jino (Presidente, FEEC-UNICAMP)

Prof. Dr. Romis Ribeiro de Faissol Attux (FEEC-UNICAMP)

Prof. Dr. Ivan Luiz Marques Ricarte (FT-UNICAMP)

Profa. Dra. Carla Merkle Westphall (UFSC)

Prof. Dr. Edgar Toshiro Yano (ITA)

A ata de defesa, com as respectivas assinaturas dos membros da Comissão Examinadora, encontra-se no processo de vida acadêmica do aluno.

# DEDICATÓRIA

*Dedico este trabalho de maneira muito especial à minha esposa Luiza e à minha filha Isabela, que se privaram de vários momentos para que eu pudesse desenvolver este trabalho. Após tantas dificuldades, ao final, o meu maior motivador para a conclusão deste trabalho foi a certeza de que este feito servirá de exemplo de superação para a minha filha. Ela verá no futuro que qualquer obstáculo, seja ele físico, intelectual ou emocional, não podem servir de desculpa para desistir dos seus sonhos. Também devo dedicar este trabalho aos meus pais e irmãos que durante toda vida, apesar das dificuldades, me deram condições, apoio e incentivo para que eu pudesse progredir.*

# AGRADECIMENTOS

Agradeço ao meu orientador, professor Dr. Mario Jino, pela oportunidade, pelos ensinamentos, pela amizade e pela confiança atribuída a mim na elaboração deste trabalho. Foi uma grande honra para mim ser orientado por uma pessoa tão especial, uma referência na área de Engenharia de Software do nosso país.

Aos membros da banca examinadora, professores Romis Ribeiro de Faissol Attux, Ivan Luiz Marques Ricarte, Carla Merkle Westphall e Edgar Toshiro Yano, pelas importantes sugestões de melhoria.

Agradeço aos professores e funcionários da UNICAMP, que sempre nos atenderam prontamente, com cortesia e muita competência.

Agradeço ao Centro de Tecnologia da Informação Renato Archer (CTI) e a todos os colegas servidores pela oportunidade e pelo apoio que me foram dados para que eu pudesse desenvolver este trabalho concomitantemente com minhas atividades de pesquisador e servidor público. Em especial, aos amigos Amândio Balcão, Antônio Montes, Luiz Otávio Duarte, Antônio Theóphilo, Rodrigo Bonacin, Miguel Argollo, Luiz Antonio Teixeira, Paulo Bueno, Guilherme Ruppert, Walcir Cardoso e Rogério Winter, que foram fundamentais no campo profissional, mas principalmente no pessoal.

Agradeço a todos os meus amigos do DCTA, pelo apoio, pelo estímulo, e pelos ensinamentos. Em especial, José Parente, Jorge Tadano, Luiz Guarino, Bruno Silva, André Kusumoto, Nelson Leite, Alexandre Barreto, José Bernardo e Fernando Mauro.

Enfim, agradeço a todos que contribuíram direta ou indiretamente com este trabalho.

E sobretudo a Deus que nos orienta e mostra os caminhos que devemos seguir.

*“There is no such thing as perfect security, only varying levels of insecurity. “*

*Salman Rushdie*

# RESUMO

Nos dias atuais, o software tem papel importante na maioria das indústrias e áreas de atividade. Os aspectos relacionados à segurança da informação são críticos, com forte impacto na qualidade dos sistemas. Como saber se uma determinada avaliação de segurança foi boa ou suficiente? Por meio de critérios e heurísticas é possível determinar a suficiência da avaliação de segurança e, consequentemente, analisar sua qualidade. Fontes de conhecimento (normas, padrões, conjuntos de casos de teste) e seus itens de avaliação são instrumentos essenciais para avaliar a segurança dos sistemas. Para criar projetos de avaliação de segurança mais efetivos, é necessário saber as propriedades de segurança e as dimensões de avaliação abordadas em cada item de uma fonte de conhecimento de segurança. Nesta tese, uma abordagem para selecionar e analisar itens de avaliação de segurança (HCApp-Sec) é proposta; suas bases provêm de critérios e heurísticas de avaliação e visam a aumentar a cobertura das dimensões de avaliação e propriedades de segurança dos projetos de avaliação. A abordagem centra-se em selecionar itens de avaliação de forma sistemática. Sistematiza-se o processo de avaliação de segurança por meio da formalização conceitual da área de avaliação de segurança; uma ontologia (SecAOnto) é usada para explicitar os conceitos principais. HCApp-Sec pode ser aplicada a qualquer fonte de conhecimento de segurança para selecionar ou analisar itens de avaliação em relação a 11 propriedades de segurança e 6 dimensões de avaliação. A abordagem é flexível e permite que outras dimensões e propriedades sejam incorporadas. Nossa proposta visa a apoiar: (i) a geração de projetos de avaliação de segurança de alta cobertura que incluam itens mais abrangentes e com cobertura assegurada das principais características de segurança e (ii) a avaliação de fontes de conhecimento de segurança em relação à cobertura de aspectos de segurança. Em uma prova de conceito, um mapeamento de fontes de conhecimento de segurança é apresentado. Então, aplica-se a proposta a uma fonte de conhecimento de segurança bem conhecida (ISO/IEC 27001); seus itens são analisados.

**Palavras-chave**: Avaliação. Segurança. Dimensão de Avaliação. Propriedade de Segurança. Heurística. Critério. Cobertura. Ontologia.

# ABSTRACT

*Nowadays, software plays an important role in most industries and application domains. The aspects related to information security are critical, with a strong impact on systems quality. How to know whether a particular security assessment was good or sufficient? By means of criteria and heuristics it is possible to determine the sufficiency of the security assessment and consequently to analyze its quality. Knowledge sources (standards, patterns, sets of test cases) and their assessment items are essential instruments for evaluation of systems security. To create security assessment designs with suitable assessment items we need to know which security properties and assessment dimensions are covered by each knowledge source. We propose an approach for selecting and analyzing security assessment items (HCApp-Sec); its foundations come from assessment criteria and heuristics and it aims to increase the coverage of assessment dimensions and security properties in assessment designs. Our proposal focuses on the selection of better assessment items in a systematic manner. We systematize the security assessment process by means of a conceptual formalization of the security assessment area; an ontology of security assessment makes explicit the main concepts. HCApp-Sec can be applied to any security knowledge source to select or analyze assessment items with respect to 11 security properties and 6 assessment dimensions. The approach is flexible and allows other dimensions and properties to be incorporated. Our proposal is meant to support: (i) the generation of high-coverage assessment designs which includes security assessment items with assured coverage of the main security characteristics and (ii) evaluation of security standards with respect to coverage of security aspects. We have applied our proposal to a well known security knowledge source (ISO/IEC 27001); their assessment items were analyzed.*

***Keywords**: Assessment. Security. Assessment Dimension. Security Property. Heuristics. Criteria. Coverage. Ontology.*

# LISTA DE ILUSTRAÇÕES

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ACM | *Association for Computing Machinery* |
| AD | *Assessment Design* – Projeto de Avaliação |
| AI | *Assessment Item* – Item de Avaliação |
| BACEN | Banco Central do Brasil |
| BLA | *Business Logic Attack* |
| BSI | *British Standards Institution* |
| BSIMM | *Building Security In Maturity Model* |
| CovDM | *Coverage of Assessment Dimensions* – Cobertura de Dimensões de Avaliação |
| CovPP | *Coverage of Security Properties* – Cobertura de Propriedades de Segurança |
| CovLOC | *Local Coverage of Assessment Item* – Cobertura Local de um Item de Avaliação |
| CovGLO | *Local Coverage of Knowledge Source* – Cobertura Global de uma Fonte de Conhecimento |
| CovTOT | *Total Coverage of Assessment Design* – Cobertura Total de um Projeto de Avaliação |
| CSA | *Cloud Security Alliance* |
| C-All-AD | *All Assessment Designs Criterion* – Critério Todos os Projetos de Avaliação |
| C-All-AI-KS | *All Assessment Items of Knowledge Source Criterion* – Critério Todos os Itens de Avaliação de uma Fonte de Conhecimento |
| C-All-DM | *All Assessment Dimensions Criterion* – Critério Todas as Dimensões de Avaliação |
| C-All-DM-PP | *All Assessment Dimensions and All Security Properties Criterion* – Critério Todas as Dimensões de Avaliação e Todas as Propriedades de Segurança |
| C-All-KS | *All Knowledge Sources Criterion* – Critério Todas as Fontes de Conhecimento |
| C-All-PP | *All Security Properties Criterion* – Critério Todas as Propriedades de Segurança |
| C-CombDM | *Combination of Assessment Dimensions Criterion* – Critério Combinação de Dimensões de Avaliação |
| C-CombPP | *Combination of Security Properties Criterion* – Critério Combinação de Propriedades de Segurança |

| | |
|---|---|
| C-CombDM-PP | *Combination of Assessment Dimensions and Security Properties Criterion* – Critério Combinação de Dimensões de Avaliação e Propriedades de Segurança |
| DCSSI | *Direction Centrale de la Sécurité des Systémes d'Information, Secrétariat Général de la Défense Nationale, France* |
| DM | *Assessment Dimension* – Dimensão de Avaliação |
| ENISA | *European Union Agency for Network and Information Security* |
| HCApp-Sec | *Approach for Selecting and Analyzing Security Assessment Items based on Heuristics and Criteria* (Abordagem para Seleção e Análise de Itens de Avaliação de Segurança baseada em Heurísticas e Critérios) |
| H-AboveAvg | *Above Average Heuristics* – Heurística Acima da Média |
| H-CovDM | *Coverage of Assessment Dimensions Heuristics* – Heurística Cobertura de Dimensões de Avaliação |
| H-CovPP | *Coverage of Security Properties Heuristics* – Heurística Cobertura de Propriedades de Segurança |
| H-CovLOC | *Local Coverage Heuristics* – Heurística Cobertura Local |
| H-CovGLO | *Global Coverage Heuristics* – Heurística Cobertura Global |
| H-CovTOT | *Total Coverage Heuristics* – Heurística Cobertura Total |
| H-ParetoPercentage | *Pareto Percentage Heuristics* – Heurística Pareto Porcentagem |
| H-ParetoFrontier | *Pareto Frontier Heuristics* – Heurística Fronteira de Pareto |
| HIPAA | *Health Insurance Portability and Accountability Act* |
| IEC | *International Electrotechnical Commission* |
| IEEE | *Institute of Electrical and Electronics Engineers* |
| INPI | Instituto Nacional de Propriedade Industrial |
| IoE | *Internet of Everything* (Internet de Tudo) |
| IoT | *Internet of Things* (Internet das Coisas) |
| ISACA | *Information Systems Audit and Control Association* |
| ISECON | *Institute for Security and Open Methodologies* |
| ISO | *International Organization for Standardization* |
| ISSA | *Information Systems Security Association* |
| KS | *Knowledge Source* – Fonte de Conhecimento |
| MITRE | *The MITRE Corporation* |
| NeOn | *NeOn Foundation* |
| NIST | *National Institute of Standards and Technology (USA)* |

| | |
|---|---|
| NSA | *National Security Agency (USA)* |
| OSSTMM | *Open Source Security Testing Methodology Manual* |
| OSVDB | *Open Source Vulnerability Database* |
| OWASP | *Open Web Application Security Project* |
| OWL | *Web Ontology Language (Linguagem de Ontologia da Web)* |
| PIPEDA | *Personal Information Protection and Electronic Documents Act* |
| PP | *Security Property* – Propriedade de Segurança |
| SecAOnto | *Security Assessment Ontology* – Ontologia de Avaliação de Segurança |
| SEI/CMU | *Software Engineering Institute at Carnegie Mellon University* |
| SE | *Social Engineering* |
| SOX | *Sarbanes Oxley Act* – Lei Sarbanes Oxley |
| UML | *Unified Modeling Language* |
| W3C | *World Wide Web Consortium* |

# SUMÁRIO

# 1 INTRODUÇÃO

*"Corporations understand the value of security because the leakage of their competitive information could be the end of the corporation."*

*John McAfee*

Nos dias atuais, um carro não é mais um carro, mas um computador sobre rodas. Um smartphone tornou-se uma agência bancária, onde o seu ambiente operacional muda a qualquer momento. Atualmente, podemos ver sérios ataques a importantes infraestruturas governamentais usando dispositivos inteligentes. (BBC News, 2016a, 2016b; Mertl, 2016; The New York Times, 2012; The Tesla Team, 2016). Os aspectos relacionados à segurança da informação (por exemplo, confidencialidade, integridade, disponibilidade, autenticidade) estão se tornando cada vez mais críticos na área de engenharia de software.

Violações e fraudes relacionadas à segurança de informação são comuns e não costuma haver por parte dos desenvolvedores de software a necessária preocupação com segurança ao longo do processo de desenvolvimento. Geralmente, a segurança é objeto de mais atenção apenas após o software já ter sido desenvolvido, ou até mesmo disponibilizado (Barros, Rosa, & Balcão Filho, 2013; Rosa, Jino, Bonacin, & Teixeira-Junior, 2018).

O crescente número de vulnerabilidades encontradas em software mostra a necessidade de pesquisa e desenvolvimento de metodologias para assegurar níveis de segurança adequados aos sistemas (Colombo, 2014; Meier et al., 2003). Defeitos conhecidos estão presentes em sistemas já em operação, causando problemas ou aguardando para serem ativados. Defeitos desconhecidos são ainda mais graves e praticamente desconsiderados nas avaliações. As vulnerabilidades *Zero-Day*[1] e ataques

[1] *Zero-Day* se refere a um defeito crítico, por vezes chamado de "vulnerabilidade" ou "ataque", que pode ser conhecido e estar sendo explorado há algum tempo por uma classe restrita de atacantes (Bilge & Dumitras, 2012; Li, Sanghi, Chen, Kao, & Chavez, 2006; Portokalidis, Slowinska, & Bos, 2006). Em outra perspectiva, *Zero-Day* pode ser entendido como o momento em que um defeito importante é divulgado amplamente; o "Dia Zero" é onde se inicia por parte dos defensores a corrida pela correção do problema e pela atualização dos sistemas dos usuários. Enquanto as atualizações não acontecem, os sistemas se

mais sofisticados (por exemplo, APT – *Advanced Persistent Threat*) são difíceis de detectar usando abordagens tradicionais baseadas em vulnerabilidades conhecidas (Razzaq et al., 2014).

*Cyber War, Cyber Defense, Cyber Security* e termos relacionados têm sido usados para descrever a importância do tema, apresentando um contexto onde o software é usado como arma e as infraestruturas críticas dos países estão em risco constante. *Cyber Armies* (Exércitos Cibernéticos) foram criados e ataques cibernéticos já são considerados convencionais pelas grandes potências (Aschmann, Jansen van Vuuren, & Leenen, 2015; Barreto, 2013).

No contexto de *e-Commerce*, vazamentos de informação e todos os tipos de fraudes eletrônicas causam diariamente enormes prejuízos financeiros e de credibilidade às empresas (Mundie & Mcintire, 2013; Obrst, Chase, & Markeloff, 2012; Razzaq, Hur, Ahmad, & Masood, 2013).

Segurança da informação afeta diretamente a economia e a qualidade de vida das pessoas. Desenvolver sistemas de informação onde aspectos de segurança são críticos é muito difícil (Bialas, 2017; Mellado, Fernández-Medina, & Piattini, 2007). Uma razão pela qual a segurança é tão difícil de avaliar é que alguns requisitos de segurança são do tipo "*shall not*", ou seja, especificam o que não deveria acontecer em detrimento de funcionalidades de sistema ou comportamentos esperados (Sommerville, 2007). Assim, a segurança não deve simplesmente ser testada durante o desenvolvimento, mas idealmente deve ser assegurada durante todo o ciclo de vida do sistema.

É necessário que haja preocupação com segurança da informação desde as etapas iniciais do ciclo de vida de um software, para que os requisitos de segurança sejam bem elaborados e que seja feita uma verificação cuidadosa do atendimento a esses requisitos. Mas, nem sempre isso é possível. A verificação de requisitos de segurança precisa ser feita pela sistematização de avaliações de segurança de software, com projetos especificamente elaborados para o contexto de segurança da informação (Chikh, Abulaish, Nabi, & Alghathbar, 2011; Daramola, Sindre, & Stalhane, 2012; Elahi, 2009; Massacci, Mylopoulos, Paci, Yu, & Tun, 2011; Mellado, Blanco, Sánchez, & Fernández-Medina, 2010; Mellado et al., 2007; Salini & Kanmani, 2012, 2013; Souag,

---

tornam ainda mais sujeitos a ataques, pois todas as classes de atacantes podem explorar a falha para obtenção de vantagem indevida.

2012; Souag, Salinesi, Wattiau, & Mouratidis, 2013; Souag, Salinesi, Mazo, & Comyn-Wattiau, 2015).

Instituições das áreas de segurança da informação e defesa cibernética demandam ferramentas (métodos, processos, técnicas, sistemas etc.) que auxiliem na avaliação sistemática de segurança da informação. Existem aplicativos voltados exclusivamente a testar vulnerabilidades conhecidas (*scanners* de vulnerabilidades), mas nenhum com critérios considerando pontos de observação que possibilitem descoberta de defeitos desconhecidos nos sistemas (*Zero-Day*, por exemplo). Esses aplicativos por vezes apresentam grande quantidade de falsos-positivos, diminuindo sua credibilidade ou sua utilidade (Barreto, 2013; Basso, Moraes, & Jino, 2010; Ficco & Romano, 2010; Hu, Bertok, & Tari, 2008; Khairkar, Kshirsagar, & Kumar, 2013; Kotenko, Polubelova, Saenko, & Doynikova, 2013; OWASP, 2008; Razzaq et al., 2014; Shahriar & Zulkernine, 2011; Zhang, Caragea, & Ou, 2011).

Detectar vulnerabilidades de software e distinguir unidades de código vulneráveis de unidades não-vulneráveis (por exemplo, função ou arquivo) não é trivial; consequentemente o software é frequentemente implantado com fragilidades que podem ser exploradas por atacantes. A baixa eficácia (ou seja, alta taxa de falsos positivos e baixa cobertura) das ferramentas de detecção de vulnerabilidades é uma evidência clara deste fato (Medeiros, Ivaki, Costa, & Vieira, 2017; Vieira, Antunes, & Madeira, 2009).

A indústria de software tem utilizado técnicas e ferramentas como testes de invasão, análise de risco, análises e revisões estáticas de código-fonte, auditorias de segurança, desenvolvimento seguro, etc., que de fato contribuem para a verificação de aspectos de segurança, mas não foram suficientes para assegurar altos níveis de segurança das aplicações. Essas técnicas geralmente são baseadas em ferramentas de mercado, sem maiores preocupações com formalização conceitual e gestão sistemática das avaliações que permitiriam reuso de conhecimento (Barros et al., 2013; OWASP, 2008, 2015; Pumvarapruek & Senivongse, 2014; Savola, Pentikäinen, & Ouedraogo, 2010; Stanford, Bau, Bursztein, Gupta, & Mitchell, 2010).

Observa-se em ambiente operacional que existe a possibilidade de utilização de ontologias para prover suporte a: (i) gestão de avaliações de segurança (projeto, execução, etc.); (ii) geração (via critérios específicos para segurança) e gestão de casos de teste ou cenários de avaliação de segurança; (iii) identificação e garantia de

atendimento dos requisitos de segurança; (iv) à conformidade com políticas e normas de segurança; (v) aplicação de melhores práticas de segurança; e (vi) gestão da segurança (em sentido amplo).

Há conhecimento teórico e experiência prática em relação a mecanismos e técnicas para se aprimorar a segurança da informação, criados ou adquiridos tanto na academia (estado-da-arte) como na indústria de software (estado-da-prática), mas de forma dispersa, não estruturada, não sistematizada ou formalizada. Por exemplo, frequentemente atividades visando a testar a segurança de sistemas de informação dependem fortemente da capacitação e da experiência dos profissionais envolvidos nessas atividades; defeitos de segurança antigos, de correção já conhecida e divulgada, continuam a ser introduzidos em novos sistemas, ou se encontram instalados em sistemas em operação – é difícil localizá-los e corrigi-los de forma sistemática (Barros et al., 2013; Gartner, Ruhroth, Burger, Schneider, & Jurjens, 2014; MITRE, 2015; NIST, 2015b; OSVDB, 2015; Salini & Kanmani, 2012; Stanford et al., 2010; Tsoumas & Gritzalis, 2006; Wita, Jiamnapanon, & Teng-amnuay, 2010).

Para facilitar a proteção efetiva da informação, uma melhor identificação, compreensão e avaliação da ameaça à segurança e suas características são cruciais para os gestores de segurança (Jouini, Rabai, & Khedri, 2015). *Frameworks* baseados em um modelo conceitual com recursos para descrever de forma conceitualmente rica múltiplos recursos de segurança são avanços importantes em comparação com os *Frameworks* atuais, que tratam de forma restrita os problemas de segurança (Pereira & Santos, 2012).

Neste contexto, surgem algumas questões: Como projetar e executar avaliações de segurança efetivas e que encontrem defeitos desconhecidos? Como avaliar a cobertura dessas avaliações? Quais recursos de sistematização de conhecimento da avaliação (por exemplo, ontologias de avaliação de segurança) devem ser usados? Como identificar defeitos de segurança no software já em uso com critérios factíveis? Como saber se uma determinada avaliação de segurança foi boa ou suficiente? Aplicação de critérios torna possível determinar a suficiência da avaliação de segurança e, consequentemente, analisar sua qualidade.

Não há uma contramedida específica para problemas mais complexos; técnicas, modelos, processos e ferramentas devem ser definidos e utilizados de forma sistemática para tentar minimizar o problema e propor defesas efetivas. São necessários

métodos e processos para auxiliar de forma sistemática na geração de projetos de avaliação mais eficientes. Métodos devem ter como objetivo melhorar a cobertura das características de segurança nas avaliações de sistemas; as propriedades de segurança a serem cobertas em uma avaliação devem ser claras e formalizadas.

## 1.1 PROBLEMA, HIPÓTESES E OBJETIVOS

Para melhor entendimento da seção, são descritos alguns conceitos essenciais que são detalhados no capítulo de conceituação. Fontes de Conhecimento (*Knowledge Source* – KS) são padrões de segurança ou outros documentos que possam ser usados em avaliações de segurança. Uma KS é composta de Itens de Avaliação (*Assessment Items* – AI), tais como casos de teste e itens de verificação. São consideradas 11 Propriedades de Segurança (*Security Properties* – PP): Disponibilidade (*Availability*); Integridade (*Integrity*); Confidencialidade (*Confidentiality*); Autenticidade (*Authenticity*); Não-repúdio (*Non-repudiation*); Rastreabilidade (*Traceability*); Privacidade (*Privacy*); Auditabilidade (*Auditability*); Legalidade (*Legality*); Resiliência (*Resilience*); Não-retroatividade (*Non-retroactivity*). São consideradas 6 Dimensões de Avaliação (*Assessment Dimensions* – DM): Lógica de Negócios (*Business Logic*); Arquitetura de Sistema (*System Architecture*); Processo (*Process*); Sistema em Execução (*System in Runtime*); Estrutura do Código-fonte (*Source-code Structure*); e Ambiente Operacional (*Operating Environment*).

Considerando o contexto e a reflexão postos, e com base na revisão bibliográfica, algumas questões surgem: Quais fontes de conhecimento de segurança (por exemplo, *checklists*, normas e padrões de segurança, conjuntos de casos de teste etc.) são adequadas para os requisitos? Quais itens de avaliação de segurança abordam certas dimensões de avaliação e propriedades de segurança? Qual item de avaliação de segurança aborda a verificação das regras de negócios? Qual item de avaliação de segurança aborda a característica disponibilidade? Como criar previamente um conjunto de critérios de avaliação, com base na cobertura de aspectos de segurança? Quais foram os critérios usados para selecionar os itens de avaliação? De posse dos itens de avaliação, quais priorizar? É possível gerar estratégias de avaliação? Após a avaliação, qual foi a cobertura? O que foi e o que não foi avaliado e porquê?

Avaliação sistemática de segurança depende da obtenção de respostas consistentes para as questões acima. Encontrar itens de avaliação relevantes e que cubram uma grande variedade de problemas de segurança é uma tarefa difícil. São necessários critérios de avaliação diversificados e que mostrem quais propriedades de segurança e dimensões de avaliação são abordados em cada item de avaliação. Por exemplo, uma pequena quantidade de itens de avaliação pode abranger a quantidade apropriada de propriedades de segurança bem como cobrir um escopo adequado de dimensões de avaliação.

O seguinte **Problema** de Pesquisa é tratado nesta tese: "***Como selecionar e analisar sistematicamente itens de avaliação de segurança?***".

O Problema de Pesquisa pode ser decomposto nas seguintes **Deficiências**:

(i) Formalização Conceitual – Há necessidade de consenso quanto à formalização conceitual de termos importantes em Avaliação de Segurança, tais como Avaliação, Defeito, Falha, Erro, Risco, Vulnerabilidade, Ataque, Ameaça, Dimensões de Avaliação, Propriedades de Segurança, entre outros. Existe ambiguidade na definição desses termos.

(ii) Diversidade na Avaliação – Não foram identificadas na literatura abordagens que considerem diversas fontes de conhecimento ao mesmo tempo.

(iii) Critérios de Avaliação – Não foram identificados na literatura critérios de avaliação baseados em cobertura de características de segurança que apoiem a seleção e a avaliação sistemáticas de itens de avaliação.

Para abordar as deficiências, as seguintes **Hipóteses** são adotadas:

(i) Sistematização – Ontologias podem auxiliar no aprimoramento da precisão conceitual do modelo, diminuindo ambiguidades e possibilitando formalização conceitual.

(ii) Critérios de Cobertura – O aumento da diversidade de características de segurança avaliadas e a provisão de critérios para seleção ou priorização que considerem essa diversidade pode melhorar a cobertura

do projeto de avaliação; em estágios futuros pode levar à identificação de mais defeitos ou de tipos adicionais de defeitos (classes).

Baseado no exposto anteriormente, os seguintes **Objetivos** são propostos:

### Objetivo Geral

- Elaborar uma abordagem sistemática para seleção e análise de itens de avaliação de segurança mais efetivos, com base em critérios.

### Objetivos Específicos

- Arquitetura Conceitual que proporcione uma visão geral da abordagem.
- Ontologia de Aplicação para a área de Avaliação de Segurança de Sistemas, que formalize os conceitos principais.
- Abordagem para apoiar a atividade de Avaliação de Segurança, que busque aumentar a cobertura de propriedades de segurança por meio da seleção de itens baseada em critérios claros e efetivos.
- Base de Conhecimento, que contenha informação de fontes de conhecimento e seus itens de avaliação, além de informação sobre projetos de avaliação.
- Protótipo de Software para demonstração da abordagem.
- Prova de Conceito, aplicando a abordagem proposta a uma fonte de conhecimento de segurança; uma avaliação dos resultados obtidos deve ser conduzida.

## 1.2 CONTRIBUIÇÕES RELACIONADAS COM A TESE

A Figura 1.1 apresenta uma visão geral dos resultados da tese. No **Apêndice D** apresentam-se os resultados obtidos com a pesquisa no que diz respeito a artigos e outros trabalhos desenvolvidos, listando os títulos e resumos dos artigos.

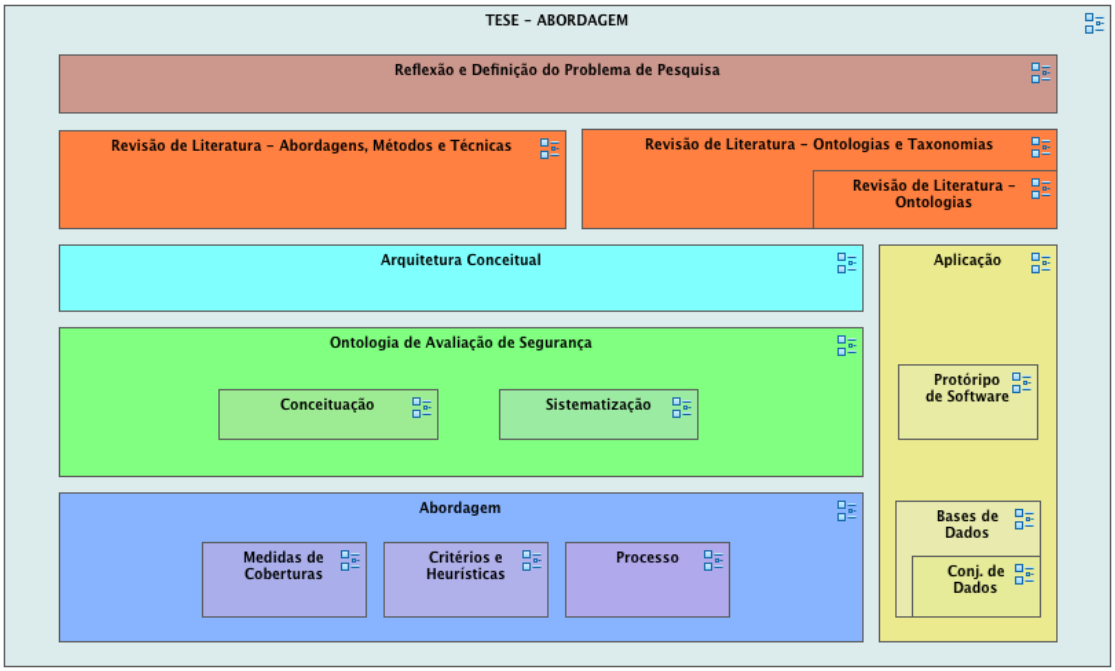


**Figura 1.1.** Visão geral dos resultados da Tese

A seguir apresenta-se uma breve descrição das contribuições mais relevantes conforme segue: 1) Abordagem para apoiar a Avaliação de Segurança; 2) Ontologia de Avaliação de Segurança; e 3) Programa de Computador.

### 1) Abordagem para apoiar a avaliação de segurança

Uma abordagem para selecionar e analisar itens de avaliação de segurança (HCApp-Sec) é proposta; suas bases provêm de critérios e heurísticas de avaliação e visam a apoiar a geração de projetos de avaliação de segurança mais efetivos. Nossa proposta centra-se em usar critérios e heurísticas de avaliação para selecionar melhores itens de avaliação de forma sistemática. Como produtos desta tese, os seguintes artigos foram produzidos: uma descrição resumida da abordagem, bem como uma prova de conceito, são apresentados por Rosa, Jino, & Bonacin (2018a); uma contextualização e uma reflexão sobre a necessidade de abordagens voltadas a possibilitar avaliações de

segurança de sistemas de forma sistemática são apresentadas por Barros et al. (2013) e por Rosa & Jino (2016); partes do levantamento bibliográfico são apresentados por Rosa, Jino, & Bonacin (2017) e por Rosa & Jino (2017), uma arquitetura conceitual para avaliação de segurança é proposta por Rosa & Jino (2016); Rosa et al. (2018) descrevem a conceituação da área de Avaliação de Segurança. Rosa et al. (2018) apresentam as heurísticas propostas.

2) Ontologia de Avaliação de Segurança

A formalização conceitual em avaliação de segurança, na qual este trabalho se baseia, foi expressa por meio de uma Ontologia de Avaliação de Segurança (*Security Assessment Ontology* – SecAOnto), que está disponível no GitHub (Rosa, Jino, & Teixeira Junior, 2017c). Uma ontologia pode ser classificada segundo seu grau de abstração ou generalização; as ontologias de aplicação descrevem conceitos que consideram contexto de domínio e contexto de tarefa (Guarino, 1998), (Guizzardi, Falbo, & Guizzardi, 2008). A ontologia proposta é uma ontologia de aplicação, expressa em OWL, que fornece conceitos e uma terminologia comum a ser usada na atividade de avaliação de segurança de sistemas de informação. Na conceituação, por Rosa et al. (2018), conceitos inspirados nas referências são utilizados, mas a maioria deles é definida a partir de uma nova perspectiva, devido às particularidades do contexto da avaliação de segurança.

3) Programa de Computador

Foi desenvolvido um Protótipo de Software para apoiar a criação de projetos de avaliação de segurança de forma estruturada. O protótipo pode ser usado na fase de planejamento da avaliação para os cálculos de coberturas (*Back-end*) e na seleção dos itens de avaliação (*Front-end*); está disponível no GitHub (Rosa, Jino, Teixeira Junior, & Balcão Filho, 2016b) e, como apresentação de prova de conceito (Rosa, Jino, Teixeira Junior, & Balcão Filho, 2016a). Os diagramas de classes e de dados do protótipo podem ser encontrados nos Apêndices A e B, respectivamente. Após finalização da versão 1.0, o sistema foi registrado no INPI, conforme Processo: BR 51 2016 001707-4.

## 1.3 ESTRUTURA DA TESE

Projetos de avaliação de segurança devem ser compostos por itens de avaliação com cobertura assegurada das principais características de segurança; ou seja, precisamos saber quais propriedades de segurança e quais dimensões de avaliação são cobertas pelos itens das fontes de conhecimento para selecionar os melhores itens com base em critérios efetivos. Visando este objetivo, este trabalho está organizado como descrito a seguir.

***Capítulo 2.*** A revisão da literatura busca levantar esforços de criação de abordagens sistemáticas para avaliação de segurança. Os trabalhos selecionados são sintetizados e uma visão geral da área de avaliação sistemática de segurança é apresentada. Trabalhos relacionados são discutidos.

***Capítulo 3.*** A conceituação da área de avaliação de segurança, incluídos o processo de avaliação e os conceitos básicos, é expressa por meio de uma Ontologia de Avaliação de Segurança (*Security Assessment Ontology* – SecAOnto). A ontologia é um esforço incial para a criação de um vocabulário comum a ser usado tanto na abordagem deste trabalho bem como para apoiar outras propostas em que é útil ou necessária a formalização conceitual.

***Capítulo 4.*** A abordagem para seleção e análise de itens de avaliação de segurança (HCApp-Sec) é composta por: uma arquitetura conceitual; algoritmos para medição de cobertura de avaliação; e critérios e heurísticas de avaliação de segurança. A Arquitetura Conceitual é uma visão geral da proposta. A Cobertura de Avaliação visa a quantificar as propriedades de segurança e as dimensões de avaliação tratadas pelos itens de avaliação. São propostos um conjunto de critérios de avaliação de segurança e um conjunto de heurísticas de avaliação de segurança. O protótipo de software implementa o cálculo das coberturas de avaliação.

***Capítulo 5.*** Na prova de conceito, a abordagem (HCApp-Sec) é aplicada a uma fonte de conhecimento de segurança (ISO/IEC 27001); a fonte de

conhecimento é caracterizada e os itens de avaliação são selecionados e analisados a partir de critérios e heurísticas propostos.

*Capítulo 6.* As conclusões sumarizam os resultados da tese; aspectos de aplicabilidade e limitações são discutidos bem como trabalhos futuros.

*Apêndices.* Apêndice A: Diagrama de Classes do Protótipo de Software; Apêndice B: Modelo Entidade-Relacionamento do Protótipo de Software; Apêndice C: *dataset* completo da fonte de conhecimento usada na prova de conceito; Apêndice D: os resultados deste trabalho e os resumos das publicações produzidas; Apêndice E: o mapeamento das fontes de conhecimento de segurança.

*Anexos.* Anexo A: os itens de avaliação da Fonte de Conhecimento KS1 (ISO/IEC 27001).

# 2 LEVANTAMENTO BIBLIOGRÁFICO

*"Sanity is only that which is within the frame of reference of conventional thought."*

*Erich Fromm*

O conhecimento disponível na literatura para apoiar a realização de avaliações de segurança, tanto pela indústria de software como por comunidades acadêmicas e de pesquisa, não possui estruturação suficiente para que as técnicas disponíveis sejam aplicadas de forma ampla e bem sucedida (Barros et al., 2013; Rosa & Jino, 2017). Abordagens baseadas em conhecimento por meio de ontologias construídas para o contexto de segurança da informação podem contribuir para a estruturação de conhecimento.

O levantamento bibliográfico em "Avaliação de Segurança de Sistemas de Informação" visa a apoiar o direcionamento da pesquisa nessa área de aplicação, ou seja, levantar problemas em aberto, contribuições principais, limitações, características principais, objetivos e resultados dos trabalhos.

Mais especificamente, buscam-se na literatura trabalhos que representem o estado-da-arte em três frentes de pesquisa. A primeira frente é voltada a identificar trabalhos que buscam sistematizar e formalizar conceitos do domínio "Segurança de Sistemas de Informação", por meio de taxonomias e ontologias. A segunda frente incorpora à primeira frente palavras-chave (termos de busca) da área de "Teste e Avaliação de Sistemas" para identificar trabalhos que abordam os dois domínios. Por fim, a terceira frente busca selecionar trabalhos que apresentem métodos, processos, *frameworks*, arquiteturas, ferramentas e outras abordagens para avaliação sistemática de segurança de sistemas de informação.

Este capítulo apresenta:

2.1) A base metodológica para o protocolo de revisão utilizado no levantamento;

2.2) A execução do protocolo de revisão, composto por palavras-chave e frases de busca, critérios de inclusão e exclusão, bases e indexadores;

2.3) A revisão bibliográfica resumida sobre abordagens usadas para apoiar a avaliação sistemática de segurança. O objetivo é apresentar uma visão geral da área de avaliação de segurança;

2.4) Uma síntese dos trabalhos relacionados à abordagem proposta; e

2.5) Discussão sobre os trabalhos relacionados e um quadro comparativo desses trabalhos com a abordagem proposta.

## 2.1 METODOLOGIA

O levantamento bibliográfico baseia-se, com adaptações, nos procedimentos para execução de revisão sistemática de literatura propostos por Biolchini et al. (2005) e por Kitchenham (2004).

O processo de revisão sistemática pode ser entendido como uma abordagem de três fases (Biolchini et al., 2005): a primeira se inicia a partir dos conceitos que explícita e formalmente representam o problema em questão e prossegue com o estudo de trabalhos que possam prover evidências sobre o tópico específico de investigação; a segunda fase parte desse estudo, onde os trabalhos são detalhados ou categorizados de acordo com seus conteúdos e comparados entre si, para identificar resultados que representem um novo tipo de evidência; a terceira fase inicia-se com os resultados da fase anterior e segue para a análise e síntese em direção às conclusões.

As informações principais a serem extraídas dos trabalhos são: problemas em aberto, contribuições principais, limitações, características principais, objetivos e resultados obtidos.

O levantamento bibliográfico segue um protocolo de revisão controlada de literatura, para levantar trabalhos relevantes no contexto do problema em questão e outros relacionados à proposta de solução. Neste trabalho não se espera obter uma revisão sistemática de todos os domínios envolvidos no processo de avaliação de segurança.

## 2.2 O PROCESSO DE LEVANTAMENTO BIBLIOGRÁFICO

O protocolo de revisão utilizado compõe-se de: bases e indexadores; frases de busca, critérios de inclusão e de exclusão, síntese e análise preliminar dos trabalhos estudados. Para que as frases de busca sejam construídas é necessário definir questões

de pesquisa que fornecem as palavras-chave. Nesta revisão, questões motivadoras (mais genéricas) dão origem a questões secundárias (mais específicas) divididas em frentes de busca, que posteriormente se aglutinam na questão principal. O levantamento não consegue obter respostas para todas as questões motivadoras, mas estas servem para, além de derivar questões mais específicas, contextualizar a complexidade e necessidade do tema e para apresentar questões de pesquisa que a abordagem proposta poderia apoiar.

As questões motivadoras relacionadas à formalização conceitual na área de avaliação de segurança são:

- Quais técnicas e ferramentas de modelagem conceitual ou de gestão do conhecimento podem ser utilizadas na formalização conceitual e na definição de uma terminologia comum no contexto de avaliação de segurança?
- Como reusar conhecimento no processo de avaliação de segurança de sistemas?
- Como diminuir a ambiguidade conceitual em métodos e técnicas voltados a avaliar a segurança em sistemas?
- Como diminuir a dependência na habilidade e na experiência do avaliador?
- Como utilizar ferramentas de formalização conceitual, tais como taxonomias e ontologias de segurança da informação, em abordagens de apoio à avaliação de segurança?

As questões motivadoras relacionadas a teste e avaliação de sistemas são:

- Que critérios e técnicas podem ser aplicados nas avaliações de segurança?
- Existem critérios e técnicas específicos para apoiar a fase de projeto de teste ou avaliação de segurança de sistemas?
- Como selecionar e utilizar casos de teste ou itens de avaliação mais efetivos?
- Como aumentar a cobertura das avaliações de segurança sem comprometer fortemente custo ou prazo?

As questões motivadoras relacionadas a avaliação sistemática de segurança de sistemas são:

- Como sistematizar critérios de avaliação que levem em consideração as possibilidades de ataques e fraudes?
- Existem outras metodologias de teste de segurança, além das chamadas técnicas de "*penetration testing*" ou "teste exploratório"?
- Como utilizar fontes de conhecimento de segurança, tais como técnicas, métodos, normas, melhores práticas, para evitar a introdução de defeitos já conhecidos?
- Como identificar vulnerabilidades desconhecidas em sistemas?
- Como especificar itens de avaliação de modo a aumentar a cobertura e possibilitar a identificação de defeitos de segurança em sistemas?
- Como identificar quais características de segurança foram cobertas pela avaliação?
- Como relacionar e atribuir pesos às características de segurança para priorizar e aumentar a efetividade de avaliações?
- Como considerar requisitos e ambientes operacionais em constante modificação?
- Como diminuir a insegurança dos sistemas, por meio de métodos e técnicas de avaliação factíveis e minimamente mensuráveis?
- Como quantificar o nível de segurança ou de insegurança de um determinado sistema?

A partir das questões motivadoras, questões secundárias foram derivadas por meio da identificação de termos relacionadas a domínios (ex.: segurança, teste), problemas de pesquisa (ex.: medidas, formalização) e resultados (ex.: métodos, abordagens, critérios, ontologias) contidos nas questões motivadoras.

A seguir apresentamos as questões secundárias a serem abordadas em três frentes de busca, como segue:

**Frente 1** – Contribuições relacionadas à formalização conceitual da área de segurança de sistemas de informação. Para que se definam bases conceituais consistentes, busca-se identificar trabalhos que apresentem

vocabulários controlados, terminologias, taxonomias, ontologias e outras formas de representação de conhecimento na área de segurança de sistemas de informação.

*Q1 – Quais trabalhos são voltados a apoiar a sistematização e formalização de conhecimento na área de segurança de sistemas de informação?*

**Frente 2** – Contribuições relacionadas a critérios de avaliação de segurança de sistemas. Busca-se identificar trabalhos que apresentem critérios de avaliação e teste de sistemas com ênfase em encontrar defeitos de segurança.

*Q2 – Quais trabalhos são voltados a avaliar ou testar a segurança de sistemas de informação usando critérios ou medidas de cobertura?*

**Frente 3** – Contribuições relacionadas a abordagens de avaliação de segurança de sistemas. Busca-se identificar, mais especificamente, trabalhos que apresentem métodos, processos e técnicas para avaliação e teste de segurança de sistemas de informação voltados a aumentar a cobertura de características de segurança.

*Q3 – Quais trabalhos são voltados a aumentar a cobertura de características de segurança em avaliações de segurança de sistemas de informação?*

Como questão principal para este levantamento bibliográfico propõe-se a seguinte: *"Quais são as abordagens (técnicas, métodos, processos etc.) voltadas a aumentar a cobertura de características de segurança de sistemas de informação de forma sistemática?"*

Para cada questão proposta (1 a 3) foram definidas palavras-chave e frases de busca, apresentados na Tabela 2.1. O idioma utilizado na definição das palavras-chave é o inglês.

**Tabela 2.1.** Palavras-chave e frases de busca

| *Questão* | *Palavras-chave* | *Frases de busca* |
|---|---|---|
| *Q1* | *Security; Privacy; Dependability; Assurance; Reliability; Ontology; Taxonomy.* | *(Security OR Privacy OR Dependability OR Assurance OR Reliability) AND (Ontology OR Taxonomy)* |
| *Q2* | *Security; Privacy; Dependability; Assurance; Reliability; Ontology; Taxonomy; Test; Testing; Assessment; Criterion; Criteria; Evaluation; Coverage.* | *((Security OR Privacy OR Dependability OR Assurance OR Reliability) AND (Ontology OR Taxonomy)) AND (Test OR Testing OR Assessment OR Criterion OR Criteria OR Evaluation OR Coverage)* |
| *Q3* | *Security; Privacy; Dependability; Assurance; Reliability; Ontology; Taxonomy; Knowledge; Test; Testing; Assessment; Criterion; Criteria; Evaluation; Coverage; Method; Process; Framework; Architecture.* | *((Security OR Privacy OR Dependability OR Assurance OR Reliability) AND (Ontology OR Taxonomy OR Knowledge)) AND (Test OR Testing OR Assessment OR Criterion OR Criteria OR Evaluation OR Coverage) AND (Method OR Process OR Framework OR Architecture)* |

Por representarem uma amostra importante das publicações de qualidade reconhecida nas áreas de Engenharia e Computação, as bases e indexadores escolhidos para a busca são os seguintes:

- IEEE Xplore – http://ieeexplore.ieee.org/
- ACM Digital Library – http://www.acm.org/
- Scielo – http://www.scielo.org/php/index.php
- Proquest – http://www.proquest.com
- ScienceDirect – Elsevier – http://www.sciencedirect.com/
- SpringerLink – http://link.springer.com/
- Wiley Interscience Journal Finder – http://onlinelibrary.wiley.com/
- ISI Web of Science – Thomson Reuters – http://www.webofknowledge.com/
- Engineering Village – http://www.engineeringvillage.com/
- Google Scholar – http://scholar.google.com.br/
- Researchgate – https://www.researchgate.net

Na busca e seleção dos trabalhos, os seguintes critérios foram utilizados:

(i) Critérios de Inclusão – Trabalhos mais recentes; trabalhos que contêm conceitos julgados importantes; trabalhos que se enquadram nas questões de pesquisa definidas.

(ii) Critérios de Exclusão – Trabalhos que não se enquadram nas questões de pesquisa definidas.

Nas bases e indexadores selecionados foram considerados na busca avançada os campos "título", "resumo", "documento completo" e suas combinações, de acordo com a disponibilidade. Foram identificados mais de 160 trabalhos de interesse. Após uma leitura rápida, passando pelo resumo, tópicos principais e pela conclusão, os trabalhos foram selecionados e resumidos.

A análise resumida dos trabalhos estudados contém caracterização e categorização, comparação e inferências sobre os trabalhos. Além de trabalhos contendo contribuições diversas, tais como arquiteturas, métodos, frameworks, taxonomias, ontologias, etc., também foram identificados outros trabalhos de revisão bibliográfica, cujos resultados foram chamados de levantamento (*survey)*, revisão sistemática (*systematic review*) ou mapeamento sistemático (*systematic mapping*).

Também foram considerados trabalhos derivados das referências; esse passo complementar é conhecido como "*snowballing*" (referências de referências) (Greenhalgh, Robert, Macfarlane, Bate, & Kyriakidou, 2004). Ao final do trabalho, outra iteração do levantamento foi feita, para identificar trabalhos relacionados que no momento da revisão anterior ainda não tinham sido indexados.

A revisão final pode ser considerada uma revisão controlada de literatura, baseada em um protocolo de levantamento bibliográfico. A Figura 2.1 apresenta uma síntese do processo de revisão da literatura.

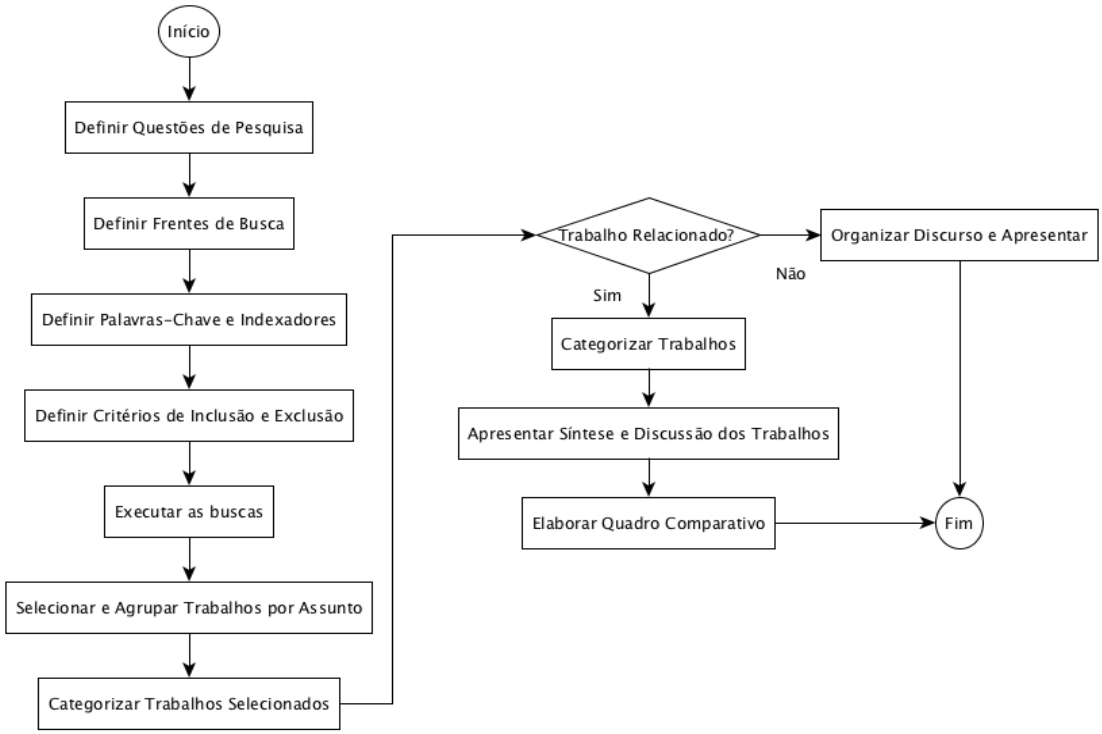


**Figura 2.1.** Síntese do processo de revisão da literatura

Os trabalhos selecionados foram divididos em categorias, de acordo com suas contribuições principais e problemas de pesquisa, da seguinte forma: (i) abordagens que apoiam a avaliação sistemática de segurança (Seção 2.3) e (ii) trabalhos relacionados (Seção 2.4). A Figura 2.2 apresenta como o levantamento bibliográfico foi dividido.

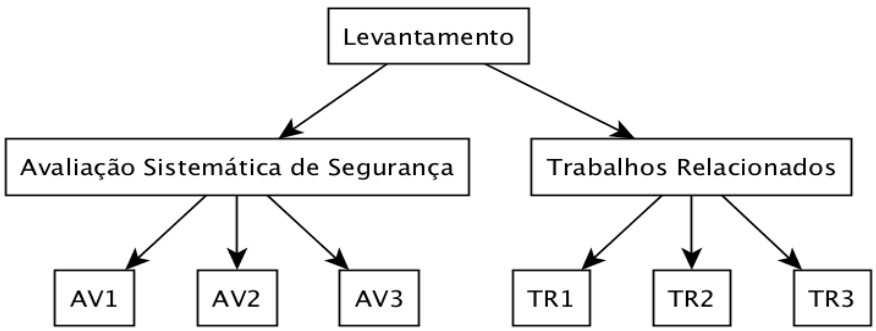


**Figura 2.2.** Estruturação da apresentação do levantamento bibliográfico

Conforme apresentado na Figura 2.2, o levantamento bibliográfico foi dividido em duas frentes: (i) AV – Avaliação Sistemática de Segurança e (ii) TR – Trabalhos Relacionados, como segue:

- AV1 – Abordagens baseadas em ontologia: trabalhos que se apoiam em ontologias na resolução de problemas de pesquisa na área de segurança da informação.
- AV2 – Abordagens direcionadas a avaliação de risco e conformidade: trabalhos que buscam avaliar riscos e conformidade de segurança.
- AV3 – Ontologias para apoio à avaliação de segurança: trabalhos que apresentam ontologias voltadas a formalizar conceitualmente as áreas de avaliação de sistemas e de segurança da informação.
- TR1 – Apoiam a avaliação de segurança de maneira sistemática: trabalhos voltados a apoiar o processo de avaliação de segurança com uso de formalização conceitual.
- TR2 – Apresentam contribuições similares às da tese: trabalhos que apresentam métricas, critérios, heurísticas, ontologia, programa, na área de segurança da informação.
- TR3 – Possuem objetivos similares aos da tese: trabalhos que visam a geração, seleção ou priorização de itens de avaliação de segurança.

Os trabalhos relacionados devem ser classificados também como sendo de avaliação sistemática de segurança, como mostrado na seção 2.4.

## 2.3 ABORDAGENS USADAS PARA APOIAR A AVALIAÇÃO SISTEMÁTICA DE SEGURANÇA

Os trabalhos apresentados nesta seção representam iniciativas de pesquisa que buscam aprimorar a avaliação de segurança da informação de forma sistemática. Nesta seção apresenta-se uma visão global, excetuando-se os trabalhos relacionados, apresentados na seção seguinte (2.4). Para isso, conforme mostrado na Figura 2.2, dividimos a apresentação desta seção em:

2.3.1) AV1 – Abordagens baseadas em ontologia.

2.3.2) AV2 – Abordagens direcionadas a avaliação de risco e conformidade.

2.3.3) AV3 – Ontologias para apoio à avaliação de segurança.

### 2.3.1 Abordagens baseadas em ontologia

Nesta seção são apresentadas sínteses de trabalhos que se apoiam em ontologias na resolução de problemas em segurança da informação.

Um método para detectar e classificar ataques a aplicativos Web baseado em ontologia é proposto por Razzaq et al. (2014); o método é capaz de detectar ataques analisando a parte especificada de uma solicitação de usuário onde os ataques são possíveis. Regras semânticas ajudam a capturar o contexto da aplicação, possíveis ataques e o protocolo que foi usado. Essas regras também permitem que a inferência seja executada sobre os modelos ontológicos para avaliar a segurança do ambiente e detectar variações de ataques de aplicativos na Web. Em contraste com os métodos atuais de segurança baseados em assinatura, esta proposta é uma técnica baseada em ontologia; o método proposto especifica ataques a aplicativos da Web usando regras semânticas, o contexto das consequências e especificações dos protocolos de aplicação. O modelo ontológico foi desenvolvido usando lógica de descrição com base em OWL.

Formalização e gestão de conhecimento de segurança da informação são cruciais para desenvolver métodos e processos sistemáticos para avaliar os sistemas com respeito às propriedades de segurança. Um método para construir ontologias relacionadas à segurança cibernética é apresentado por Wali, Chun, & Geller (2013). A abordagem utiliza um glossário de termos fundamentais de segurança da informação proposto pelo relatório NISTIR (NIST, 2015a) e definições importadas de conceitos de segurança foram incluídas na ontologia. A abordagem combina os seguintes trabalhos: (Herzog, Shahmehri, & Duma, 2007), (NIST, 2015a), e (Goodrich & Tamassia, 2010). Souag (2012) apresenta um processo de engenharia de requisitos aprimorado com ontologias com o objetivo de melhorar a definição de requisitos de segurança. Este trabalho situa-se na interseção de três domínios científicos principais (engenharia de requisitos, engenharia de conhecimento e engenharia de segurança) e as ontologias estão incluídas no processo de engenharia de requisitos.

Definir os requisitos de segurança é um passo importante no processo de desenvolvimento. Um método para análise de requisitos com base em *Security Targets* (ST) do padrão *Common Criteria* (ISO/IEC, 2008a, 2008b, 2009) é proposto por Saeki, Hayashi, & Kaiya (2013). O conhecimento derivado do ST contribui para levantar requisitos de segurança. GOORE (*goal-oriented and ontology-driven requirements*

*elicitation method*) e SOAD (*security ontology for an application domain*) foram combinados visando a usar o método proposto como ferramenta de apoio. Em GOORE, os termos e os relacionamentos em uma ontologia de domínio desempenham um papel importante no processamento semântico, como o refinamento de metas e a identificação de conflitos. Um método baseado em ontologia para definir requisitos é apresentado por Souag et al. (2013) com o objetivo de responder à seguinte pergunta: como combinar o uso de ontologias de segurança e ontologias de domínio para orientar a elicitação de requisitos de maneira eficiente e efetiva?

Uma arquitetura para fornecer interoperabilidade entre redes heterogêneas (*Machine-to-Machine area networks*) é apresentada por Gyrard, Bonnet, & Boudaoud (2013). As redes heterogêneas possuem diferentes protocolos e formatos de dados, tais como *smart home area, health area, weather forecasting area, vehicular area* etc. Na arquitetura proposta são utilizados recursos semânticos (ontologia de domínio) visando a ajudar os não-especialistas a proteger suas aplicações por meio de sugestões de contramedidas, tais como algoritmos criptográficos, protocolos de segurança etc. Uma ontologia de alto nível é apresentada; esta define relações entre ataques, contramedidas e propriedades de segurança (por exemplo, autenticação). Os seguintes domínios classificam ataques e contramedidas: aplicações web, redes móveis (2G, 3G, 4G), redes sem fio e gerenciamento de rede.

Vasilevskaya (2013), com base em uma ontologia, propõe um método chamado *Asset Elicitation Technique*, que analisa o projeto do sistema para obter requisitos de segurança. Uma ontologia de avaliação (*top-level*) foi desenvolvida para capturar os resultados da avaliação de desempenho. Foi definido um processo que auxilia um engenheiro de sistema embarcado na seleção de um conjunto relevante de soluções de segurança. Neste processo são usados: o conhecimento de segurança anterior, a identificação de problemas de segurança em um projeto de sistema e a análise de restrições de recursos de soluções de segurança disponíveis.

### 2.3.2 Abordagens para avaliação de risco e de conformidade

Nesta seção são apresentadas sínteses de trabalhos que buscam avaliar riscos e conformidade de segurança.

Uma abordagem de identificação de ameaça em que é construído um modelo quantitativo de risco de segurança para sistemas de informação é proposta por Jouini et al. (2015) com o objetivo de ajudar os gerentes a avaliar com precisão as ameaças de segurança. Um método para complementar o processo de seleção de serviços, derivando quantitativamente o grau de conformidade com o CCM (*Cloud Controls Matrix*) para diferentes serviços da nuvem é proposto por Pumvarapruek & Senivongse (2014). O objetivo principal é aplicar a classificação de texto na classificação de informações publicadas nas páginas Web dos provedores para determinar quais práticas e diretrizes de segurança os provedores seguiram ao fornecer seus serviços. As melhores práticas e diretrizes de segurança do CCM e do CAIQ (*Consensus Assessments Initiative Questionnaire*) (CSA, 2015) são usadas como base para classificar por nível de conformidade as páginas Web dos provedores. Um Processo de Certificação (SBIS-CFM) para Sistemas de Registro Eletrônico em Saúde (S-RES) é proposto por Leão, Giulliano, Lúcio, & Galvão (2013); o processo destina-se a avaliar sistemas que coletam, armazenam, apresentam, transmitem ou imprimem informações pessoais sobre a saúde de pacientes. A certificação possui 2 manuais, a saber: Manual de Certificação S-RES (CM); Manual Operacional de Testes e Análises para Certificação S-RES (OM) (Giulliano, Lúcio, & Galvão, 2014). OM apresenta um método para avaliar a conformidade com requisitos de segurança, por meio de um conjunto de casos de teste (chamados de *scripts*); os *scripts* são divididos em níveis de segurança.

No que diz respeito ao gerenciamento de riscos, métodos e modelos conceituais visam a aprimorar a segurança. Um método para gerenciamento de risco e um modelo conceitual expresso por meio de ontologia são apresentados por Pereira & Santos (2010); o trabalho baseia-se numa abordagem ontológica para estruturar e organizar informações de segurança. O modelo conceitual definido é composto de 8 conceitos, com base nos padrões de segurança ISO/IEC_JCT1, e é representado em uma estrutura de ontologia. Os 8 conceitos descritos são: (i) Incidente; (ii) Evento de Segurança; (iii) Ativo; (iv) CIA (confidencialidade, integridade e autenticidade); (v) Ameaça; (vi) Ataque; (vii) Controle; e (viii) Vulnerabilidade.

Processos e padrões de segurança para desenvolvimento de software com o objetivo de minimizar riscos e apoiar engenheiros no processo de desenvolvimento são propostos por Moradian, Håkansson, & Andersson (2012). O projeto dos padrões de software baseia-se em ontologias, que fornecem conhecimento estruturado que pode ser

reutilizado e combinado. Além disso, é apresentada uma visão geral da ontologia de segurança proposta. Um processo baseado em reuso e centrado no padrão *Common Criteria* (ISO/IEC, 2008a, 2008b, 2009) é apresentado por Mellado et al. (2007); este trabalho trata dos requisitos de segurança nos estágios iniciais do desenvolvimento de software de forma sistemática. A principal contribuição é fornecer um repositório de recursos de segurança no ciclo de vida do software, além da integração de *Common Criteria* e SSE-CMM (ISO/IEC, 2008c).

Uma abordagem orientada por modelo para avaliar e medir os sistemas de segurança é apresentada por Rieke, Schütte, & Hutchison (2012) com o objetivo de fornecer um modelo extensível para todas as partes do processo de monitoramento e suporte à decisão, a saber: (i) detectar eventos ameaçadores; (ii) inserir eventos ameaçadores no contexto do estado atual do sistema; (iii) explicar o seu potencial impacto; e (iv) tomar as ações apropriadas. Os autores definem como "Arquitetura" a proposta de um Meta-Modelo (*Security Information Meta-Model – SIMM – and Security Strategy Meta-Model – SSMM*) e um *Framework* (*Security Strategy Processing Components – components of conceptual framework*). Segundo os autores, o SSMM fornece uma maneira de modelar políticas de segurança em nível abstrato, e pode ser compilado em regras específicas para monitoramento, suporte a decisão e imposição de aplicação (*enforcement*). O modelo de implantação proposto abrange todas as partes do processo de gerenciamento de segurança em tempo de execução, que geralmente são fornecidos por diferentes sistemas, tais como IDS/IPS, SIEM, e sistemas de gerenciamento de risco e conformidade. A estrutura fornece um mecanismo para coletar informações sobre sistemas operacionais para verificar se o sistema atinge os objetivos de segurança.

Diretrizes para a criação de uma política de avaliação de segurança são propostas no Guia para Avaliação de Segurança do NIST (NIST, 2008). A metodologia proposta apresenta requisitos mínimos e melhores práticas para o processo de avaliação de segurança. As recomendações são apresentadas nas seguintes fases: planejamento, teste e pós-teste. É apresentada uma lista de verificação para selecionar o melhor método ou abordagem para realizar a avaliação de segurança. Não é objetivo apresentar um programa abrangente de avaliação ou teste de segurança da informação, mas sim uma visão geral dos elementos-chave dos testes e avaliações de segurança com ênfase em técnicas específicas, seus benefícios, limitações e recomendações para seu

uso. Este trabalho não propõe métricas ou medidas para seleção ou priorização de controles durante a fase de planejamento.

O estudo apresentado por Vibhandik & Bose (2015) busca mostrar como a combinação de ferramentas (ou técnicas), pode aumentar a cobertura de testes de vulnerabilidade para aplicações Web, considerando a modelagem de ameaças baseada em OWASP Top 10 (OWASP, 2015). Neste trabalho, foram combinados dois *scanners* de vulnerabilidades conhecidas (W3AF (W3AF.ORG, 2017) e Nikto (CIRT.NET, 2017)) para apoiar a avaliação na fase de execução. Não são apontados no trabalho quais os critérios usados para selecionar os casos de teste nas ferramentas.

Um modelo de medição para avaliação dos níveis de implementação da segurança da informação em organizações é proposto por Stambul & Razali (2011). O modelo consiste em três níveis de maturidade que determinam os graus em que a segurança da informação é abordada em uma organização. Os níveis contêm vários fatores que são necessários para garantir a segurança da informação. O estudo utilizou revisão sistemática de literatura como instrumento para determinar os parâmetros de medição apropriados. Os parâmetros identificados foram combinados com modelos gerais e padrões de medição de segurança da informação. O modelo pode ser usado por organizações para determinar seus níveis de maturidade para garantir a segurança de suas informações.

### 2.3.3 Ontologias para apoio à avaliação de segurança

Para o desenvolvimento de abordagens que buscam avaliar a segurança de maneira sistemática faz-se necessária a formalização conceitual da área de avaliação de segurança; ontologias são importantes instrumentos de apoio para essa tarefa. Nesta seção são apresentadas sínteses de trabalhos que apresentam ontologias voltadas a formalizar conceitualmente as áreas de avaliação de sistemas e de segurança da informação, que podem apoiar o desenvolvimento de abordagens sistemáticas de avaliação de segurança.

A maioria dos trabalhos analisados tem por objetivo descrever domínios ou subdomínios de “segurança da informação” e “teste de software”, incluindo seus vários subdomínios (por exemplo: gerenciamento de riscos, políticas de segurança, análise de

incidentes, padrões de ataque, testes de desempenho, testes de sistemas especialistas, etc.).

Em geral, propostas mais genéricas ou abstratas (ontologias de alto nível) podem ser encontradas no trabalhos de Souag et al. (2015), Salini & Kanmani (2012), Grobler, van Vuuren, & Leenen (2012), Liu & Lee (2010), Zhu & Huo (2005) e Jutla & Xu (2004). Propostas específicas (ontologias de tarefa ou de aplicação) podem ser encontradas nos trabalhos de Khairkar et al. (2013) e de Viljanen (2005).

A formalização do conhecimento é uma questão-chave abordada pelos trabalhos. O estudo apresentado por Raskjn, Hempelmann, Nirenburg, & Lafayette (2002) propõe um modelo para conceitos-chave do domínio da segurança da informação. Ele explica como as ontologias podem ser usadas para fornecer uma base teórica para a segurança da informação, enquanto Feledi & Fenz (2012) apresentam uma formalização do conhecimento de segurança da informação interpretável por máquina. Herzog et al. (2007) têm o objetivo de modelar os principais conceitos do domínio da segurança da informação usando OWL; são descritos conteúdo, modo de uso, possibilidade de extensão, implementação técnica e ferramentas para tratar a ontologia.

Várias questões são levantadas sobre como representar o conhecimento no campo de segurança da informação. As seguintes questões são abordadas por Souag et al. (2015): (1) Quais conceitos e relacionamentos são necessários para uma ontologia de segurança? (2) Como tornar esta ontologia fácil de ser usada pelos engenheiros de requisitos? Os autores apresentam os seguintes requisitos para se construir ontologias de segurança: (a) Criar uma plataforma genérica de conceitos diferentes (ameaças, riscos, requisitos etc.); (b) Criar uma fonte de reutilização do conhecimento para a coleta de requisitos em vários projetos.

Outros estudos se concentram na formalização de aspectos específicos da segurança da informação, tais como o software malicioso e a gestão de riscos. Liu & Lee (2010) propõem uma ontologia de domínio para formalizar conhecimento sobre gestão de riscos; o objetivo é adotar ontologias para fazer uso do conhecimento de especialistas em detecção de intrusão, segurança de rede, políticas de segurança etc., para modelagem, armazenamento, compartilhamento e consulta. Uma ontologia e um vocabulário comum são propostos por Viljanen (2005) para descrever fatos que devem ser considerados no cálculo da confiança; foca-se nos aspectos de confiança e interoperabilidade. Uma ontologia do domínio da segurança da informação, focada na

gestão de riscos é apresentada por Fenz, Pruckner, & Manutscheri (2009). Neste trabalho, *The German IT Grundschutz Manual* (BSI, 2008) e o *NIST Handbook* (Bowen, Hash, & Wilson, 2006) são utilizados como referências. Os conceitos de ameaça, vulnerabilidade e controle são usados para representar o conhecimento no domínio. De acordo com os autores, as ontologias de Herzog et al. (2007) e de Fenz & Ekelhart (2009) representam uma visão geral da área de segurança.

A segurança da Web é um aspecto-chave nos dias atuais. Uma ontologia dos requisitos de segurança para aplicações Web é proposta por Salini & Kanmani (2013). De acordo com os autores, faltam ontologias de requisitos de segurança para uso na fase de especificação de requisitos. Este trabalho tem como objetivo permitir a reutilização do conhecimento sobre os requisitos de segurança no desenvolvimento de diferentes aplicativos da Web. Uma ontologia para detectar ataques em sistemas da Web é apresentada por Khairkar et al. (2013). Os autores utilizam conceitos de web semântica e ontologias para analisar registros (*logs*) de segurança, buscando identificar potenciais problemas de segurança. Este trabalho destina-se a extrair relações semânticas entre ataques e intrusões em um Sistema de Detecção de Intrusão (IDS). A privacidade é outra questão importante no ambiente da Web; Uma ontologia de alto nível para modelar conceitos relacionados aos aspectos de privacidade é apresentada por Raskjn et al. (2002). O estudo propôs uma ontologia de alto nível para apoiar leis, guias e padrões. Inclui-se também um fragmento da ontologia contendo o modelo PIPEDA (lei de privacidade para empresas no Canadá) como prova de conceito.

Domínios de aplicação específicos são abordados, tais como *e-Voting* e *e-Gov*. Uma ontologia de alto nível de requisitos de segurança é apresentada por Salini & Kanmani (2012). Com base nesta ontologia, pode-se conceber e desenvolver requisitos para sistemas de votação eletrônica (*e-Voting*). O objetivo principal é propor padrões de segurança para facilitar o processo de determinação de requisitos de segurança para sistemas de votação eletrônica. Propriedades específicas de segurança são apresentadas para sistemas de votação eletrônica, a saber: *anonymity* (anonimato), *disclosability* (divulgação), *uniqueness* (unicidade ou singularidade), *accuracy* (precisão), *transparency* (transparência), e *non-coercibility* (não-coerção). Um esboço de uma ontologia de segurança de alto nível para aplicações de *e-Gov* do governo sul-africano é proposta por Grobler et al. (2012). Apresenta-se uma breve discussão sobre o uso de ontologias de segurança em um ambiente governamental. O trabalho é focado no uso de

uma metodologia baseada em ontologia para identificar e propor uma descrição, formalmente codificada, do ambiente de segurança cibernética. A ontologia visa a identificar e representar os atores e seus papéis em um ambiente de segurança cibernética do governo sul-africano.

Su & Biennier (2010) propõem uma ontologia de segurança para formalizar conceitos importantes no contexto de sistemas colaborativos e apoiar a política de segurança em diferentes níveis de detalhe. Os fatores que afetam a segurança dos sistemas colaborativos são analisados. O padrão para apoiar a gestão de riscos OCTAVE (SEI/CMU, 2015) é usado como referência. São apresentados conceitos importantes, tais como políticas, reputação de serviços, credenciais, evidências, conformidade.

Os trabalhos selecionados também incluem preocupações sobre métricas de segurança (Evesti, Savola, Ovaska, & Kuusijarvi, 2011; Kotenko et al., 2013), padrões (Koinig, Tjoa, & Ryoo, 2015; Ramanauskaite, Olifer, Goranin, & Čenys, 2013) e processos de desenvolvimento de software (Kang & Liang, 2013). Uma ontologia de métricas de segurança é apresentada por Kotenko et al. (2013), especificamente construídas para o domínio SIEM; SIEM (*Security Information and Event Management*) é uma solução de software que combina SIM (*Security Information Management*) e SEM (*Security Event Manager*). O estudo apresentado por Evesti et al. (2011) propõe uma ontologia para apoiar o processo de medição da segurança da informação (*Information Security Measuring Ontology* – ISMO). Uma ontologia de segurança baseada em padrões é proposta por Ramanauskaite et al. (2013). Após avaliar as ontologias de segurança, os autores concluem que as ontologias não cobrem mais que um terço dos padrões. Assim, eles propõem uma nova ontologia destinada a cobrir um maior número de padrões. Os autores mapearam os trabalhos de Herzog et al. (2007) e de Fenz et al. (2009) com os padrões ISO 27001 (ISO/IEC, 2013a), PCI DSS (PCI Security Standards Council, 2015), ISSA 5173 (ISSA-UK, 2015), e NISTIR 7621 (NIST, 2015a). O estudo apresentado por Koinig et al. (2015) utilizou como referência os requisitos regulatórios contidos em padrões, tais como HIPAA (U.S. Department of Health & Human Services, 2015), SOX (Addison-Hewitt Associates, 2015), e ISO/IEC 27001 (ISO/IEC, 2013a) para construir uma ontologia de segurança para computação em nuvem.

O processo de desenvolvimento de software é outro aspecto que afeta a segurança do sistema. A falta de conceituação e sistematização de conceitos de segurança é enfatizada por Kang & Liang (2013). De acordo com os autores, a ontologia

proposta no seu trabalho pode ser usada para identificar os requisitos de segurança no processo de desenvolvimento como base prática e teórica. STACK (*Security Toolbox: Attacks & Countermeasures ontology*) é proposta por Gyrard et al. (2014) com o objetivo de auxiliar os desenvolvedores no projeto de aplicativos seguros. STACK define conceitos de segurança como ataques, contramedidas, propriedades de segurança e seus relacionamentos. As contramedidas podem ser conceitos criptográficos (algoritmo de criptografia, gerenciamento de chaves, assinatura digital, função *hash*), ferramentas de segurança ou protocolos de segurança.

## 2.4 TRABALHOS RELACIONADOS

Nesta seção apresenta-se um breve resumo dos trabalhos relacionados. Como critério de inclusão nesta seção, consideram-se trabalhos relacionados às abordagens (métodos, técnicas, arquiteturas etc.), conforme mostrado na Figura 2.2.

- [TR1] – Apoiam a avaliação de segurança de maneira sistemática.
- [TR2] – Apresentam contribuições similares às da tese.
- [TR3] – Possuem objetivos similares aos da tese.

Apesar de não terem sido descritos na seção anterior, todos os trabalhos relacionados (classificados como TR) são classificados também como AV, pois buscam aprimorar a avaliação de segurança da informação de forma sistemática.

[TR1/AV3] Um método para mapear o conhecimento de segurança da informação dos padrões EBIOS (DCSSI, 2016) e Grundschutz (BSI, 2008) para uma ontologia de segurança é apresentado por Fenz et al. (2009). O conhecimento fornecido por esses padrões é transformado em código OWL. O método proposto permite reutilizar bases de conhecimento de segurança de informação e mapeá-las para estruturas de dados abertas e padronizadas. Segundo os autores, embora existam ontologias de segurança da informação, nenhum método foi proposto para mapear diretrizes de melhores práticas ou padrões de segurança da informação para uma ontologia. A abordagem proposta baseia-se no NIST *Handbook* (Bowen et al., 2006). Para simplificar o processo de mapeamento, foram definidas ameaças de nível superior

(por exemplo, divulgação de dados, adulteração de dados e perda de dados), que afetam atributos de segurança (confidencialidade, integridade e disponibilidade).

[TR1;TR3/AV1] Uma abordagem para melhorar os testes de regressão com base em ontologias de requisitos não-funcionais é proposta por Kassab, Ormandjieva, & Daneva (2011). Os testes são selecionados com base na análise de mudanças e impactos de requisitos não-funcionais, tais como segurança, desempenho ou confiabilidade. Cada teste vinculado a um requisito alterado ou modificado é selecionado para testes de regressão. Uma conceituação de Requisitos Não-Funcionais (NFRs) é proposta por meio de uma ontologia.

[TR2/AV1] Uma metodologia para desenvolver métricas de segurança é apresentada por Savola et al. (2010); esta pode ser usada para garantir corretude de controles de segurança. A metodologia baseia-se na análise de ameaças e vulnerabilidades, na decomposição da arquitetura do sistema e dos requisitos de segurança, e foi aplicada em um estudo de caso: um serviço de correio eletrônico. Segundo os autores, medições e métricas de segurança são necessárias para quantificar e analisar a qualidade de avaliações de segurança; abordagens sistemáticas para quantificar a segurança nas atividades de avaliação são desejáveis, mas são raras; e faltam taxonomias, modelos, metodologias e ferramentas amplamente aceitos.

[TR2/AV1] Um modelo de conhecimento de segurança e um método heurístico são apresentados por Gartner et al. (2014). Um método baseado na análise da linguagem natural é proposto para refinar e adaptar o conhecimento de segurança. A abordagem visa a identificar vulnerabilidades em requisitos de linguagem natural com base em incidentes de segurança relatados. A abordagem consiste em duas partes: (1) Avaliação de segurança e (2) Extração de conhecimento de segurança. Este trabalho foca na identificação de vulnerabilidades conhecidas (e suas variações) em requisitos de linguagem natural. Embora o foco seja nos aspectos técnicos da segurança, a abordagem também é capaz de incorporar aspectos relacionados a humanos. Como limitação, o sucesso da abordagem de avaliação depende da qualidade do conhecimento de segurança. O trabalho apresenta estudos primários e seus conceitos de segurança principais.

[TR2;TR3/AV2] Colombo (2014) apresenta um método quantitativo para avaliar e priorizar a segurança. AHP (*Analytic Hierarchy Process*) é usado como uma ferramenta matemática para transformar medidas intangíveis em medidas tangíveis. O

objetivo principal é avaliar um aspecto de segurança específico (Autenticidade) para controle de acesso em aplicações Web, ou seja, avaliar o processo de autenticação de um sistema em testes de tempo de execução. O método não considera outras dimensões de avaliação ou problemas de segurança, como o ambiente operacional, a rede, as regras de negócios, a análise do código fonte, a disponibilidade, a integridade, etc. Os requisitos de segurança para controle de acesso são apresentados por meio de uma lista de verificação e podem ser usados como fonte de conhecimento para avaliação de segurança de sistemas críticos, tais como sistemas que fornecem serviços bancários pela Internet.

[TR2/AV2] Fenz (2010) apresenta uma metodologia para geração automática de métricas de segurança de TI baseadas em ISO 27001. O objetivo principal é permitir que as organizações avaliem sua conformidade com os padrões de segurança da informação e a eficácia das implementações de controles. A metodologia é baseada na ontologia de segurança apresentada por Fenz & Ekelhart (2009).

[TR2/AV2] Uma metodologia para auditoria de segurança (*Open Source Security Testing Methodology Manual* – OSSTMM) é proposta no manual do ISECON (ISECON, 2010) com o objetivo de fornecer uma abordagem científica para a caracterização da segurança operacional por meio do exame e da correlação dos resultados dos testes de forma consistente. Uma auditoria OSSTMM é uma medida de segurança no nível operacional. Um objetivo secundário é fornecer diretrizes que permitam assegurar que: (i) o teste foi conduzido completamente; (ii) o teste incluiu todos os canais necessários; (iii) o teste obedeceu à lei; (iv) os resultados são mensuráveis; (v) os resultados são consistentes e repetíveis; e (vi) os resultados contêm apenas fatos derivados dos próprios testes. O rav (*risk assessment value*) é uma medida de escala de uma superfície de ataque; é calculado pelo equilíbrio quantitativo entre porosidade, limitações e controles. Nesta escala, 100 rav é um equilíbrio perfeito e qualquer coisa a menos representa falta de controles (ou contramedidas) e, portanto, uma maior superfície de ataque. Mais de 100 rav mostra mais controles do que são necessários, o que pode ser um problema, pois controles geralmente adicionam interações dentro de um escopo, além de problemas de complexidade e manutenção.

[TR2;TR3/AV2] Uma abordagem para o teste de segurança (chamada de Teste de Vulnerabilidade Baseado em Risco) é apresentada por Botella et al. (2014); este teste é orientado pela avaliação e cobertura de risco para executar e automatizar

testes de vulnerabilidade para aplicações web. O teste de vulnerabilidade baseado em risco adapta técnicas de teste baseadas em modelos usando uma abordagem baseada em padrões para a geração de casos de teste de acordo com riscos previamente identificados. A integração de informações de atividades de análise de risco com a abordagem de geração de teste baseada em modelo é realizada por uma linguagem de propósito de teste. A abordagem é aplicada ao teste de segurança de uma aplicação web.

[TR3/AV2] Um método para gerar testes de um conjunto de regras contidas em uma política de segurança é proposto por Darmaillacq et al. (2006) com o objetivo de habilitar a geração automática de casos de teste a partir de regras da política de segurança da rede. Segundo os autores, verificar se uma política de segurança foi implementada corretamente em uma rede é um problema-chave para os administradores de sistema. Embora alguns estudos tenham sido publicados sobre a análise de consistência de regras de *firewall* (geralmente para detectar conflitos), esses trabalhos ainda estão limitados a pontos específicos de políticas de segurança.

[TR3/AV2] Zech et al. (2014) propõem um método para gerar testes de segurança negativos (o que o sistema não deve fazer) para testes de segurança não-funcionais de aplicações web por meio de programação lógica e engenharia de conhecimento. Gerenciar a quantidade quase infinita de casos de teste negativos, que resultam de possíveis riscos de segurança é uma tarefa difícil. Com base em um modelo declarativo do sistema em teste, uma análise de risco é realizada e utilizada para derivação de casos de teste.

[TR2;TR3/AV2] Uma técnica de priorização para testes de regressão para casos de teste de segurança é proposta por Huang, Peng, & Huang (2012). Sua técnica reúne registros históricos, cuja ordem de execução mais efetiva é determinada por um algoritmo genético. Geralmente, a ordem de reexecução é a mesma da execução ou aleatória. Os autores reúnem os registros históricos dos últimos testes de regressão e, em seguida, propõem um algoritmo genético para determinar a ordem mais efetiva.

[TR2;TR3/AV2] Uma abordagem para seleção de teste de regressão é proposta por Hwang et al. (2012). Cada caso de teste do sistema que pode revelar falhas causadas por mudanças na política de segurança é selecionado. São propostas três técnicas de seleção baseadas em cobertura para testar a evolução das políticas de segurança, cada uma das quais inclui uma sequência de regras para especificar quais assuntos são permitidos ou negados para acessar quais recursos em quais condições. As

três técnicas baseiam-se em dois critérios de cobertura: (1) cobertura de regras alteradas na política e (2) cobertura de diferentes decisões do programa para a política evoluída e original.

[TR2;TR3/AV2] Yu & Lau (2012) propõem uma abordagem para priorização baseada em falhas de casos de teste. A priorização baseada em falhas utiliza diretamente o conhecimento teórico de sua capacidade de detecção de falhas e as relações entre os casos de teste e as falhas no modelo de falha prescrito, com base nos quais os casos de teste são gerados. Aplica-se a abordagem ao teste da implementação de expressões lógicas em relação às suas especificações. A proposta é validada por um estudo empírico que avalia a eficácia das técnicas de priorização usando duas métricas diferentes.

[TR1;TR2/AV2] Kiesling, Strausß, & Stummer (2012) propõem uma abordagem de avaliação de risco de segurança de informação baseada em simulação e otimização multi-objetivo de investimento em controles de segurança. Um quadro metodológico é descrito, explicando as características da organização, a sua infraestrutura de informação, os bens a serem protegidos, as fontes específicas de ameaças e as preferências de risco dos gestores. Esta estrutura compreende (i) modelagem ontológica de conhecimento de segurança, (ii) técnicas de geração de grafos de ataque dinâmico, (iii) simulação probabilística de ataques por agentes de ameaça orientados por objetivos, (iv) identificação meta-heurística de portfólios eficientes de controles de segurança da informação, e (v) suporte a decisões interativas. O objetivo é inferir possíveis rotas de ataques e gerar gráficos de ataque com base na motivação, objetivos, capacidades e modos de entrada disponíveis dos invasores e para usar esse conhecimento inferido para simular ataques à infraestrutura modelada de uma organização. Neste trabalho o termo “critério” é usado em referência a risco, custo e benefício; o termo “controle” é usado para descrever medidas para detectar, prevenir ou corrigir vulnerabilidades. O trabalho faz uso de um modelo conceitual, expresso em uma ontologia, que apresenta os conceitos principais, tais como ativo, vulnerabilidade, ataque, controle, ameaça, acesso, entre outros. Segundo os autores, a abordagem é conceitual e carece de avaliação por meio de estudos de caso.

[TR1;TR2/AV1;AV3] Neubauer, Ekelhart, & Fenz (2008) apresentam uma abordagem para apoiar gestores de segurança na definição do conjunto ideal de controles de segurança para atender o padrão ISO 27001. Dados de entrada de uma ontologia de segurança (sub-ontologias a partir de (BSI, 2008; Ekelhart, Fenz, Klemen, &

Weippl, 2006, 2007)) são usados, permitindo a integração padronizada de regras que são necessárias para modelar combinações de contramedidas potenciais (ex.: sistema de acesso, porta de segurança, extintor de incêndio, guardas etc.), chamados de "controles mais granulares", baseadas nos controles do padrão ISO 27001. A abordagem foi implementada em uma ferramenta e testada por meio de um prova de conceito. O objetivo é subsidiar os tomadores de decisão na definição dos controles necessários para a certificação, e também fornecer informações sobre a eficiência dos controles escolhidos em relação a objetivos definíveis (efetividade, manutenibilidade, confiabilidade, custos iniciais, custos de manutenção), chamados de "critérios de seleção".

[TR2/AV2] Otero, Otero, & Qureshi (2010) propõem uma abordagem para avaliar os controles de segurança da informação para ajudar os gestores a selecionar os mais eficazes em ambientes com recursos limitados. O objetivo principal é apoiar gestores na tarefa de selecionar mecanismos de proteção em ambientes com restrições de recursos (financeiros, humanos, tempo etc.). Segundo os autores, métodos de seleção de controles de segurança da informação não levam em consideração restrições específicas da organização, como custos de implementação, cronograma e disponibilidade de recursos ao determinar o melhor conjunto de controles; além disso, esses métodos podem não garantir a inclusão de controles necessários ou a exclusão de controles desnecessários. A abordagem utiliza *Desirability Functions* (DF – técnica para juntar medidas em um valor unificado) para quantificar a conveniência de cada controle de segurança da informação levando em consideração *Quality Attributes* (QA), que são benefícios e penalidades (restrições) associadas à implementação do controle; o objetivo é fornecer uma medida única que é representativa da qualidade geral de cada controle com base em objetivos organizacionais.

[TR2;TR3/AV2] Diéguez, Cares, & Cachero (2017) propõem o uso de técnicas e metodologias da área de pesquisa operacional, utilizadas na resolução de problemas de otimização, para apoiar a seleção de controles em padrões, tais como ISO/IEC 27001. Apesar de publicado, este trabalho é um projeto de doutorado apresentado em workshop de teses de conferência IEEE e ainda não foi concluído.

[TR2;TR3/AV2] Botella et al. (2018) apresentam uma abordagem de MBT (Teste Baseado em Modelo) para validação de componentes de segurança. Apresenta-se uma combinação de três critérios de seleção de teste (*structural, TOCL, and Test*

*Purpose*) aplicados ao teste de requisitos de segurança de componentes, tais como módulos de segurança de hardware. Essa combinação se baseia no uso de critérios de seleção de testes estáticos (cobertura de modelos estruturais), complementada por critérios de seleção de testes dinâmicos (com base em cenários de testes abstratos ou propriedades temporais), destinados a casos-chave de requisitos funcionais de segurança. A abordagem é implementada em uma ferramenta de MBT (*Model-based Testing*) industrial e foi aplicada em três componentes de segurança. Os resultados mostram que os três critérios de seleção de testes são complementares (visam tipos distintos de erros no software) e são capazes de revelar inconsistências na especificação.

[TR2;TR3/AV2] Maheswari & Mala (2018) propõem uma abordagem heurística para priorização de caso de teste multi-critério e ciente de tempo (HTMCTCP); consideram-se vários alvos simultaneamente e escolhem-se os melhores casos de teste dentro do orçamento de tempo estipulado. Essa técnica alterna entre a busca de vizinhança (*neighbourhood search*) e a busca global (*global search*) no enorme espaço de busca do problema para evitar ficar preso em ótimos locais e também garante convergência rápida para a melhor solução. A eficácia da técnica é comparada com abordagens de otimização existentes, como algoritmo genético (GA) e algoritmo de recozimento simulado (SA).

## 2.5 DISCUSSÃO SOBRE OS TRABALHOS RELACIONADOS

Depreende-se da análise dos trabalhos relacionados que falta uma visão sistêmica ou holística sobre o processo de avaliação de segurança; uma abordagem sistêmica deve abordar vários aspectos e incorporar vários pontos de vista. Conceituação uniforme e um vocabulário comum da área de avaliação de segurança são necessários.

É importante escolher itens de avaliação mais diversos, robustos e orientados para encontrar defeitos de uma ampla gama de possibilidades. Testes altamente repetitivos podem minimizar a chance de descobrir problemas importantes, pelo mesmo motivo que pisar nas pegadas de outra pessoa minimiza a chance de ser explodido por uma mina terrestre (J. M. Bach, 2003; Paulo Marcos Siqueira Bueno, 2012).

Algumas abordagens são fortemente baseadas ou dependentes da experiência dos avaliadores. O método proposto por Colombo (2014) não considera outras dimensões de avaliação ou propriedades de segurança, tais como, ambiente operacional, rede, regras de negócios, análise de código fonte, disponibilidade, integridade etc. O *checklist* resultante do trabalho não faz uso de critérios de cobertura na geração do conjunto proposto de itens de avaliação. No trabalho de Gartner et al. (2014), embora o foco esteja nos aspectos técnicos da segurança, a abordagem também é capaz de incorporar aspectos relacionados a humanos. O trabalho apresenta estudos primários e seus principais conceitos de segurança. Como limitação, o sucesso da abordagem depende muito da qualidade do conhecimento de segurança. As limitações do método desenvolvido por Fenz et al. (2009) são: (i) requer um alto grau de intervenção manual; (ii) requer uma intervenção manual substancial para mapear uma nova base de conhecimento em uma base de conhecimento existente.

O foco do manual do ISECON (ISECON, 2010) é na realização de avaliações de segurança da informação na fase de execução, mas não na fase de planejamento. O resultado é um relatório de auditoria de teste de segurança e uma lista de verificação de conformidade e não um projeto de avaliação com base em critérios de cobertura de segurança. A medida proposta (rav – *risk assessment value*) é diferente de outras medidas de segurança porque só pode ser derivada de testes de segurança operacional, não medindo o risco de uma superfície de ataque, mas sim a medida desta superfície (ambiente); ou seja, não pode inferir se um alvo específico será atacado. No entanto, ele pode inferir onde (superfície), em um alvo, poderá ser atacado, de quais tipos de ataques o alvo pode ser defendido com sucesso, quão fundo um atacante pode chegar e qual dano pode causar. Assim, o rav não é uma medida de cobertura, mas sim uma medida de nível de segurança de ativos. Com relação ao escopo, define-se a superfície de ataque e não as dimensões da avaliação. No que diz respeito à segurança, define-se uma métrica de segurança resultante de uma auditoria e não uma medida de cobertura de avaliação de segurança a ser usada no planejamento da avaliação.

Trabalhos com foco em geração, seleção e priorização de casos de teste foram identificados. A abordagem apresentada por Botella et al. (2014) integra técnicas de identificação de teste baseada em risco e de priorização de teste para apoiar o processo de teste baseado em modelo. Os requisitos do sistema são usados para escrever o modelo de teste UML, enquanto o modelo de segurança CORAS (em relação ao catálogo

de padrões de teste genéricos associados) permite definir os objetivos de teste selecionados e priorizá-los em relação à avaliação de risco. O método apresentado por Zech et al. (2014) é voltado a gerar um conjunto de casos de teste executáveis para testes de segurança não funcionais (casos de teste negativos) com base em programação lógica. Kassab et al. (2011) apresenta uma abordagem para selecionar casos de teste voltada a melhorar os testes de regressão; uma ontologia de requisitos não-funcionais é usada para a conceituação de Requisitos Não-Funcionais (NFRs). Huang et al. (2012) apresentam uma técnica baseada em algoritmos genéticos para determinar a ordem de reexecução para testes de regressão. No trabalho de Hwang et al. (2012) são propostas técnicas de seleção de teste para políticas de controle de acesso. Yu & Lau (2012) propõem uma abordagem de priorização de conjunto de teste baseada em falhas. Maheswari & Mala (2018) propõem uma abordagem para priorização de caso de teste multi-critério com base em tempo.

A conformidade com o padrão internacional ISO/IEC 27001 (ISO/IEC, 2013a) não diz muito sobre a qualidade do sistema de gestão implementado; o certificado de conformidade garante que o sistema foi implementado, mas não que os controles operacionais e técnicos foram auditados ou que uma avaliação de segurança foi feita (Bachlechner et al., 2011). Segundo Nespoli et al. (2017), não há consenso na literatura sobre o termo “contramedida”. O termo contramedida é usado como sinônimo de “controle” ou “salvaguarda” no padrão ISO/IEC 27002 (ISO/IEC, 2013b) e significa administrar riscos (tratar – mitigar, aceitar) de um ativo, incluindo políticas, procedimentos, diretrizes, estruturas organizacionais ou práticas, que podem ser de natureza administrativa, técnica, de gestão ou legal. Kiesling et al. (2012) selecionam controles com base em simulação, considerando risco, custo e benefício; ou seja, buscam responder uma questão de gestão: qual será o investimento financeiro necessário para implementar um conjunto de controles de segurança e qual seria o retorno para a organização? Este trabalho apresenta também um modelo ontológico de conhecimento de segurança (modelo conceitual apoiado por ontologia). O objetivo principal é apoiar gestores na tomada de decisão sobre ações de investimento financeiro e não apoiar engenheiros na seleção de insumos para avaliação de segurança. O objetivo principal de Neubauer et al. (2008) é definir controles necessários para certificar conformidade com o padrão 27001 (ISO/IEC, 2013a) e sua eficiência (dos controles) com relação a objetivos definidos, enquanto A abordagem apresentada por Botella et al. (2018) pode

ser aplicada em um contexto mais geral em sistemas que apoiam avalidação de conformidade com especificações ou auditorias. Otero et al. (2010) busca avaliar os controles usando atributos de qualidade.

Nota-se a falta de métodos para avaliar sistematicamente a cobertura de aspectos de segurança. São necessários métodos que possuam as seguintes características: (i) utilizem conhecimento sistematizado formalizado por meio de vocabulários comuns, taxonomias ou ontologias; (ii) mapeiem os itens de avaliação de normas ou padrões de segurança para propriedades de segurança; (iii) forneçam medidas de cobertura das propriedades de segurança em fontes de conhecimento; (iv) apoiem a aplicação de critérios de avaliação de forma sistemática. O método proposto neste trabalho destina-se a preencher essas lacunas.

A Tabela 2.2 apresenta uma síntese dos trabalhos relacionados apontando particularidades e diferenças, domínios de aplicação e contribuições mais importantes. Apresentamos na comparação métodos e abordagens como "contribuições principais" e também outros resultados como "outras contribuições". As atribuições da Tabela 2.2 são baseadas na descrição ou inferência dos autores, devido a ser difusa a forma como os autores definem seus próprios trabalhos e contribuições. Por exemplo, alguns autores definem seus resultados como "*Architectural Framework*", "*Ontological Framework*", "*Ontology-based Method*", entre outras definições. Como critério de inclusão, consideram-se trabalhos relacionados às abordagens (métodos, técnicas, arquiteturas, ontologias etc.) que: TR1) apoiam a avaliação de segurança de maneira sistemática: trabalhos voltados a apoiar o processo de avaliação de segurança com uso de formalização conceitual; TR2) Apresentam contribuições similares às da tese: trabalhos que apresentam métricas, critérios, heurísticas, ontologia, programa, na área de segurança da informação; TR3) Possuem objetivos similares aos da tese: trabalhos que visam a geração, seleção ou priorização de itens de avaliação de segurança.

**Tabela 2.2.** Síntese dos trabalhos relacionados

| *Referência* | *Foco em* | *Domínio de Aplicação* | *Contribuição Principal* | *Outras Contribuições* | *Critério de Inclusão* |
|---|---|---|---|---|---|
| (Gartner et al., 2014) | Identificar vulnerabilidades | Segurança da Informação | Método para detectar vulnerabilidades em requisitos | | TR2 |
| (Colombo, 2014) | Avaliar segurança | Métricas de Segurança | Método para avaliar e priorizar segurança | *Checklist* para avaliar autenticação em sistemas Web | TR2/TR3 |
| (Fenz, 2010) | Medir segurança | Métricas de Segurança da Informação | Método para gerar métricas de segurança | | TR2 |
| (Fenz et al., 2009) | Gerir conhecimento | Gestão de riscos de Segurança da Informação | Método para mapear conhecimento de segurança | | TR1 |
| (ISECON, 2010) | Avaliar segurança | Avaliação de Segurança | Método para auditar segurança | *Checklist*; Medida de nível de segurança operacional | TR2 |
| (Kassab et al., 2011) | Avaliar segurança | Avaliação de Segurança | Abordagem para melhorar testes de regressão | Ontologia de NFRs | TR1/TR3 |
| (Savola et al., 2010) | Desenvolver métricas de segurança | Métricas de Segurança | Método para gerar métricas | | TR2 |
| (Botella et al., 2014) | Gerar casos de teste | Teste de Segurança | Abordagem para teste de segurança | | TR2/TR3 |
| (Darmaillacq et al., 2006) | Gerar casos de teste | Teste de Segurança | Método para gerar testes de segurança | | TR3 |
| (Zech et al., 2014) | Gerar casos de teste negativos. | Teste de Segurança | Método para gerar testes de segurança negativos | | TR3 |
| (Huang et al., 2012) | Priorizar reexecução de testes | Teste de Segurança | Abordagem para priorização para testes de regressão | | TR2/TR3 |
| (Hwang et al., 2012) | Selecionar testes para reexecução | Teste de Segurança | Abordagem para seleção de teste de regressão | | TR2/TR3 |
| (Yu & Lau, 2012) | Gerar casos de teste | Teste de Segurança | Abordagem para priorização baseada em falhas de casos de teste | | TR2/TR3 |
| (Kiesling et al., 2012) | Selecionar controles de segurança | Avaliação de Segurança | Abordagem para apoiar a avaliação de riscos de segurança da informação | | TR1/TR2 |
| (Neubauer et al., 2008) | Selecionar controles de segurança | Avaliação de Segurança | Abordagem para seleção de controles para atender ao padrão ISO 27001 | Sub-ontologias com controles mais granulares | TR1/TR2 |
| (Otero et al., 2010) | Avaliar controles de segurança | Avaliação de Segurança | Abordagem para seleção de controles mais eficazes para | | TR2 |

| *Referência* | *Foco em* | *Domínio de Aplicação* | *Contribuição Principal* | *Outras Contribuições* | *Critério de Inclusão* |
|---|---|---|---|---|---|
| | | | uma organização | | |
| (Diéguez et al., 2017) | Selecionar controles de segurança | Avaliação de Segurança | Abordagem para seleção de controles em padrões de segurança | | TR2/TR3 |
| (Botella et al., 2018) | Teste de Requisitos com base em modelos | Teste de Segurança | Abordagem para avaliação de conformidade com especificações | Protótipo de Software | TR2/TR3 |
| (Maheswari & Mala, 2018) | Priorizar reexecução de testes | Teste de Segurança | Abordagem para priorização para testes de regressão | | TR2/TR3 |
| (Diéguez et al., 2017) | Selecionar controles de segurança | Avaliação de Segurança | Abordagem para seleção de controles em padrões de segurança | | TR2/TR3 |

## 2.6 CONSIDERAÇÕES FINAIS

Neste capítulo, foi apresentada a revisão de literatura, incluindo os trabalhos relacionados. Ao final do trabalho, mais de 300 referências compõem a base do projeto no Mendeley (software de gestão de referências). Mais de 200 trabalhos foram selecionados nas principais bases e indexadores, de acordo com um protocolo de revisão controlada. Destes, 17 trabalhos foram considerados relacionados por conterem características ou objetivos similares em relação ao todo ou a partes da abordagem proposta. Adicionalmente às referências apresentadas na tese, uma análise de outras classes de trabalhos (ontologias e taxonomias) é apresentada por Rosa & Jino (2017) e por Rosa, Jino, & Bonacin (2017); esses trabalhos compõem parte da revisão apresentada por Rosa et al. (2018). De forma complementar ao processo de revisão proposto, também foram considerados trabalhos derivados das referências (*snowballing*). Deve ser considerado que nem todas as bases pesquisadas permitiram acesso completo e aberto aos trabalhos; por essa razão, alguns trabalhos citados foram descritos com base em informações contidas em seus resumos. Depreende-se da análise dos trabalhos que a avaliação de segurança é uma questão complexa e transversal. Os trabalhos têm buscado resolver o problema por meio de uma combinação de técnicas, formalização conceitual e uso de padrões e guias de melhores práticas. Os objetivos variam desde a definição conceitual até seleção de casos de teste para avaliações de conformidade. Os trabalhos são aplicados em vários novos domínios ainda em consolidação, tais como, *Cloud Computing, Service-Oriented Architecture, Mobile, e-Voting,* etc.

No próximo capítulo, apresenta-se a conceituação da área de avaliação de segurança por meio de uma ontologia, provendo as bases conceituais da abordagem proposta neste trabalho.

# 3 CONCEITUAÇÃO DA ÁREA DE AVALIAÇÃO DE SEGURANÇA

*"The art and science of asking questions is the source of all knowledge. Why do writers write? Because it isn't there."*

*Thomas Berger*

A formalização do conhecimento em avaliação de segurança é uma tarefa difícil mas importante para os pesquisadores que precisam formalizar o conhecimento em seus sistemas, métodos e técnicas. Existe sobreposição de domínios e conceitos relacionados são frequentemente tratados de forma isolada. Em outras palavras, os principais conceitos em alguns contextos são considerados como sinônimos, em outros são tratados como tendo diferentes significados. Por exemplo: Segurança e Confiabilidade; Privacidade e Segurança; Teste e Avaliação; Rastreabilidade e Não-Repúdio; Vulnerabilidade e Risco; Auditabilidade e Transparência; entre outros conflitos conceituais. Com relação aos padrões de segurança, por exemplo, o *IT Grundschutz Manual* (BSI, 2008) não está orientado para o conceito de vulnerabilidade, ao contrário do *NIST Handbook* (Bowen et al., 2006); as primeiras versões do *Top Ten Privacy Risks* do OWASP (OWASP, 2015), eram chamadas de *Top Ten Vulnerabilities*. Portanto, é crucial estabelecer a conceituação formal em avaliação de segurança; ontologias podem ser usadas para esta tarefa.

Neste capítulo apresenta-se como o processo de avaliação de segurança normalmente é conduzido, uma proposta de processo de avaliação de segurança e uma conceituação da avaliação de segurança por meio de uma ontologia.

Este capítulo está dividido conforme segue:

3.1) O processo de avaliação de segurança;

3.2) Conceituação da avaliação de segurança por meio da Ontologia de Avaliação de Segurança (*Security Assessment Ontology* – SecAOnto): classificação e processo de engenharia da ontologia; conceituação e discussão.

## 3.1 PROCESSO DE AVALIAÇÃO DE SEGURANÇA

A avaliação de segurança pode ser definida como um processo projetado para avaliar aspectos de segurança identificáveis de sistemas em um domínio de aplicação, classificando o sistema avaliado em inaceitável ou aceitável (Vecchiato, 2017). Na prática, a avaliação da segurança deve considerar duas perspectivas: 1) a busca ativa de vulnerabilidades e de problemas de segurança; e 2) a caracterização da propensão da existência de outros problemas ocultos ou não identificados (Neto, 2012; Vecchiato, 2017).

O processo de avaliação de segurança inclui regras que definem como realizar a avaliação, com ênfase na busca de defeitos de segurança. Por exemplo: quais dimensões de avaliação (escopo, cobertura) ou domínios de aplicação serão abordados, quais fontes de conhecimento e propriedades de segurança serão abordadas na avaliação.

A atividade de avaliar a segurança de um dispositivo pode não estar cercada de regras ou critérios, mas geralmente possui duas importantes particularidades: a) Avaliação contínua, devido à incerteza quanto à completude dos requisitos (por exemplo, vulnerabilidades desconhecidas); b) O usuário e os sistemas interoperáveis são sempre considerados mal-intencionados (atacantes). A avaliação de segurança também tem os objetivos de: (i) medir o nível de segurança ou insegurança de um sistema ou processo; (ii) atribuir grau de maturidade em segurança a uma organização; (iii) verificar a conformidade com normas ou padrões; (iv) encontrar defeitos ou vulnerabilidades em aplicações.

Ressaltam-se alguns problemas quanto à forma como o processo de avaliação de segurança é geralmente conduzido, a saber:

- Sistema em uso: a segurança não é abordada durante o processo de desenvolvimento. Frequentemente, o sistema ou dispositivo a ser avaliado já está concluído ou até mesmo em uso.
- Teste exploratório: não há padrão, nenhuma formalização conceitual, nem medidas de cobertura. A fase de planejamento é negligenciada, partindo-se diretamente para a execução da avaliação com base na experiência do testador.

- Com base em vulnerabilidades: a cobertura é baseada em vulnerabilidades conhecidas e não em características de segurança desejadas. Vulnerabilidades específicas são pesquisadas em determinados pontos do sistema ao invés de uma busca mais abrangente. Como resultado da avaliação tem-se um relatório contendo as vulnerabilidades conhecidas que foram testadas no sistema.
- Orientado a ferramentas de software: avaliadores usam ferramentas de exploração de vulnerabilidades conhecidas, disponíveis ou usadas anteriormente. Por exemplo, após executar um *scanner* em modo "*all*" 400 pontos vulneráveis foram identificados no código ou no sistema em uso.
- As expectativas são altas: a avaliação de segurança precisa ser boa, rápida, barata e, além disso, certificar a segurança do sistema.
- Baixa reutilização do conhecimento: a reutilização é observada somente quando o mesmo avaliador é designado. Quanto mais criativo e experiente no uso das ferramentas, mais valorizado é o avaliador.

Neste contexto, surge a questão: Como selecionar os melhores itens de avaliação de uma fonte de conhecimento de segurança da informação? No processo de criação de um projeto de avaliação de segurança, precisamos escolher normas (27001, 15408 etc.), conjuntos de casos de teste, padrões de segurança, entre outras fontes de conhecimento, ainda na fase de planejamento da avaliação, com base em critérios bem definidos.

Como cada fonte de conhecimento possui vários itens de avaliação e cada item de avaliação aborda uma ou mais propriedades de segurança (por exemplo, disponibilidade, integridade, confidencialidade, autenticidade, etc.), questiona-se especificamente: Existe uma abordagem voltada a aumentar a cobertura de características de segurança, que apoie a seleção dos melhores itens de avaliação de segurança em uma fonte de conhecimento?

Com essa questão em mente, propõe-se um processo de avaliação de segurança definido por uma sequência de etapas da seguinte maneira: 1) construção da semântica das fontes de conhecimento, 2) construção do projeto de avaliação, e 3) execução da avaliação de segurança com base nos conjuntos de critérios propostos.

Na Figura 3.1, apresenta-se uma visão geral do processo de avaliação de segurança proposto por meio de um diagrama de atividades UML.

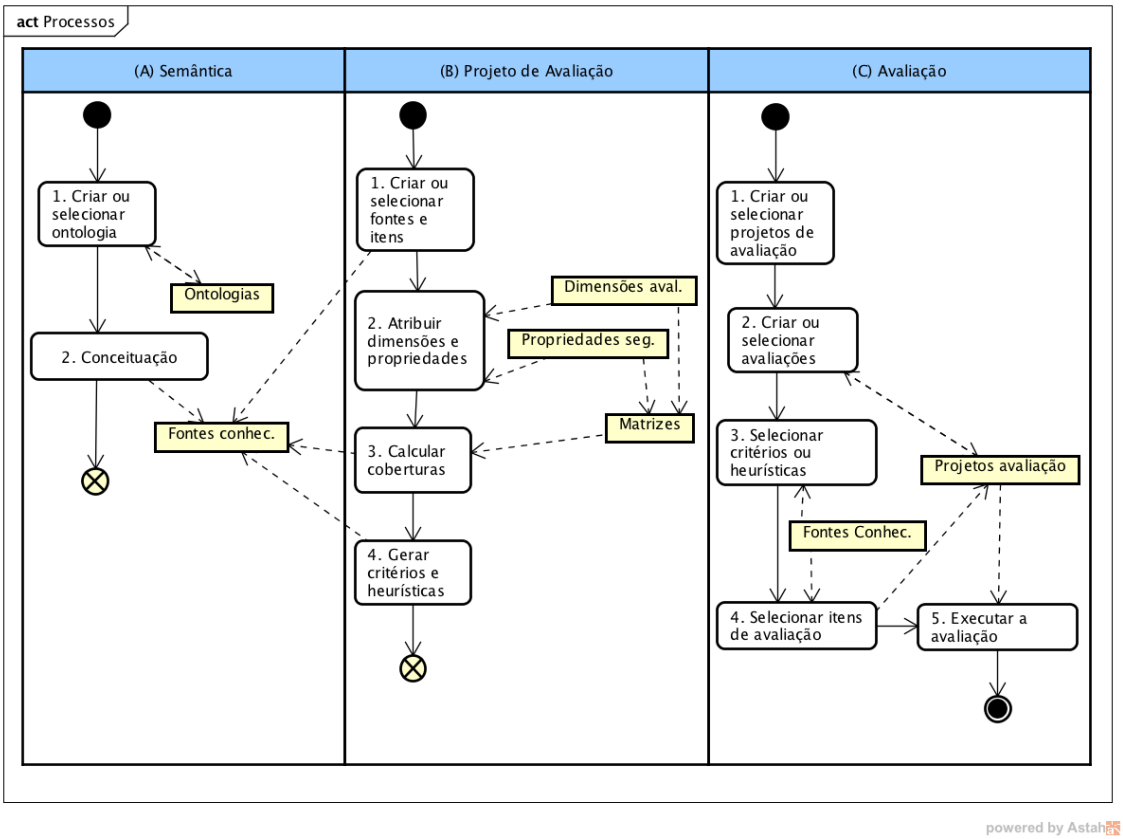


**Figura 3.1.** Visão geral do processo de avaliação de segurança

Primeiro, uma ontologia é criada para apoiar a conceituação, descrevendo os conceitos principais de avaliação de segurança e seus relacionamentos. As fontes de conhecimento são propostas para fornecer os itens de avaliação. A cobertura das características de segurança nos itens de avaliação é calculada. Os critérios para a seleção dos itens de avaliação são propostos com base em medidas de cobertura. Em seguida, os itens de avaliação são selecionados com base em critérios escolhidos; determina-se e explicita-se uma medida de cobertura para os itens selecionados. Finalmente, o projeto de avaliação é gerado e a avaliação de segurança é realizada.

A abordagem é bastante útil na fase de planejamento da avaliação de segurança, por propor critérios claros para gerar melhores projetos de avaliação; estes provavelmente encontrarão mais defeitos ou novas classes de defeitos de segurança na fase de execução. Nada impede que a abordagem seja usada em outras fases, inclusive fora do contexto de uma avaliação; por exemplo, para avaliar uma determinada fonte de conhecimento e seus itens de avaliação com respeito à cobertura de características de segurança.

## 3.2 CONCEITUAÇÃO DA ÁREA DE AVALIAÇÃO DE SEGURANÇA POR MEIO DE UMA ONTOLOGIA

Uma ontologia pode ser usada para representar e estruturar formalmente o conhecimento em avaliação de segurança. Com este propósito, propomos a SecAOnto (*Security Assessment Ontology*). Primeiro, classificamos a ontologia proposta, então o processo de engenharia de ontologia utilizado na construção é descrito e os principais conceitos de SecAOnto são detalhados. A proposta de conceituação é dividida em: (i) Avaliação de Sistemas, (ii) Segurança da Informação e (iii) Avaliação de Segurança.

### 3.2.1 Classificação da Ontologia

Segundo Guarino (1998), ontologias podem ser classificadas de acordo com seu grau de abstração ou generalização, da seguinte forma: *Top-level Ontologies* (Ontologias de Topo, ou Fundamentais, ou de Alto Nível ou de Base), definindo conceitos genéricos que são independentes de domínios específicos (Guizzardi et al., 2008); *Domain Ontologies* (Ontologias de Domínio), descrevendo um domínio específico, especificando conceitos, propriedades e restrições; *Task Ontologies* (Ontologias de Tarefa), descrevendo conceitos de uma tarefa (ou uma ação) e *Application Ontologies* (Ontologias de Aplicação), descrevendo conceitos que consideram o contexto do domínio e o contexto da tarefa.

A ontologia proposta (SecAOnto) é uma ontologia de aplicação e fornece os principais conceitos e uma terminologia comum a ser usada em avaliação de segurança de sistemas de informação. Outras perspectivas de classificação e uma discussão adicional podem ser encontradas nos trabalhos de Obrst (2010) e de Semy, Pulvermacher, & Obrst (2004). Na Figura 3.2 apresentamos a classificação de SecAOnto.

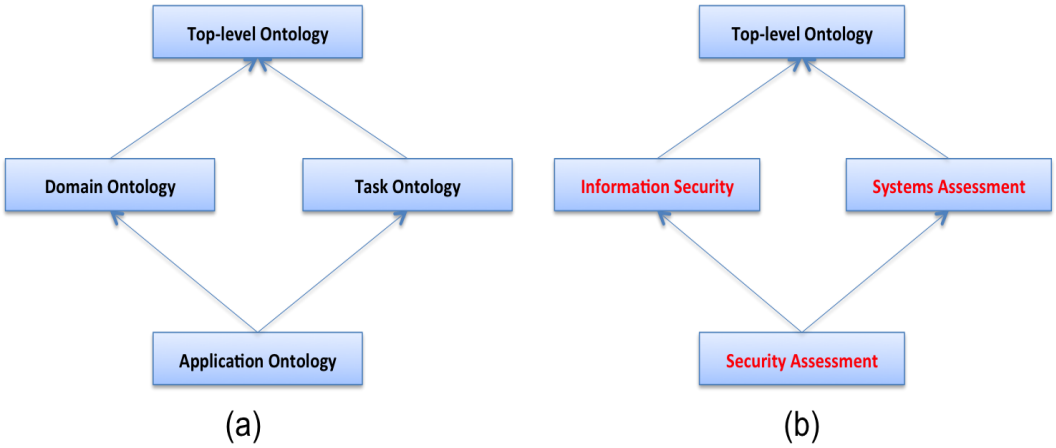


**Figura 3.2.** Classificação de SecAOnto

A Figura 3.2 (a) representa a classificação de Guarino e a Figura 3.2 (b) representa o enquadramento de SecAOnto como uma ontologia de aplicação segundo a classificação de Guarino. Em (b), *Security Assessment* (Avaliação de Segurança) herda do domínio *Information Security* (Segurança da Informação) e da tarefa *Systems Assessment* (Avaliação de Sistemas).

### 3.2.2 Processo de Engenharia da Ontologia

Como sugerido por Bermejo (2007) e por Barbosa, Nakagawa, & Maldonado (2006), a criação de uma ontologia pode ser feita por meio das seguintes atividades: planejamento, especificação de requisitos, captura de conhecimento, criação, integração, implementação, desenvolvimento, documentação e manutenção. Considerando também a metodologia proposta por Obrst et al. (2012) (Reutilizar, coletar e manter), adotamos na construção de SecAOnto as seguintes etapas:

(i) **Coleta, especificação de requisitos e captura de conhecimento.** Aqui, foca-se na captura e formalização do conhecimento, explicando como as referências são usadas ou são integradas na ontologia proposta.

(ii) **Criação, integração, implementação e desenvolvimento.** As principais fontes de conhecimento da ontologia são conceitos oriundos de glossários e vocabulários (ISACA, 2015; MITRE, 2015; NIST, 2015b), taxonomias e ontologias sobre segurança da informação (Azevedo et al., 2008; Fenz & Ekelhart, 2009; Herzog et al., 2007; Massacci et al., 2011; Nabil & Mohamed,

2012; Ramanauskaite et al., 2013; Souag et al., 2015; Viljanen, 2005), avaliação de sistemas (Paulo M S Bueno, Jino, & Wong, 2011; Paydar & Kahani, 2010; E. F. de Souza & de Souza, 2014; Zhu & Huo, 2005), regulamentos governamentais e guias de prática do mercado destinados a avaliar a segurança de sistemas (ISO/IEC, 2008a, 2013a; OWASP, 2008). Também são utilizados conceitos a partir de referências, mas a maioria dos conceitos propostos e sua inter-relação é definida a partir de uma perspectiva nova, devido às particularidades do contexto de avaliação de segurança. Alguns conceitos propostos por Herzog et al. (2007) foram reutilizados com adaptações; especificamente, conceitos relacionados a contramedidas, ativos e ataques.

(iii) **Aplicação e compartilhamento.** Aplicar para validar conceitos e documentar para compartilhar. Aplicamos os principais conceitos na formalização da abordagem e no desenvolvimento do algoritmo de cálculo de cobertura (matriz de adjacências expressa e instanciada na ontologia) e compartilhamos a conceituação no Repositório GitHub (Rosa, Jino, & Teixeira Junior, 2017c).

SecAOnto foi desenvolvida em *Web Ontology Language* (OWL) (Bechhofer et al., 2004; W3C, 2015) usando a ferramenta Protégé (Stanford University, 2015). A ontologia foi desenvolvida com a participação de um especialista sênior em segurança da informação e um especialista sênior em avaliação de software e foi revisada por outros três especialistas em segurança da informação e teste de software. No total, cerca de dez versões da ontologia foram produzidas em dois anos por meio de um processo de revisão iterativa.

### 3.2.3 Formalização conceitual – *Security Assessment Ontology (SecAOnto*)

Avaliação de segurança herda conceitos de avaliação de sistemas (inclui teste e verificação) e de segurança da informação. Por isso, é importante apontar as definições específicas, com base nas opiniões dos principais autores, e propor um vocabulário comum para o processo de avaliação de segurança.

A Figura 3.3 apresenta os conceitos principais de *Security Assessment Ontology* (SecAOnto), incluindo conceitos relacionados a: 1) Avaliação de Sistemas (Paulo Marcos Siqueira Bueno, 2012; Delamaro, Maldonado, Barbosa, Vicenzi, & Jino, 2007; É. F. de Souza, Falbo, & Vijaykumar, 2017); 2) Segurança da Informação (Fenz & Ekelhart, 2009; Herzog et al., 2007; ISACA, 2015; OWASP, 2008; Pereira & Santos, 2012; Savola, 2007); 3) Avaliação de Segurança (Bowen et al., 2006; Duarte, Montes Filho, Guerra, & Rosa, 2010; ISACA, 2015). Nas próximas subseções, detalhamos a conceituação dessas áreas.

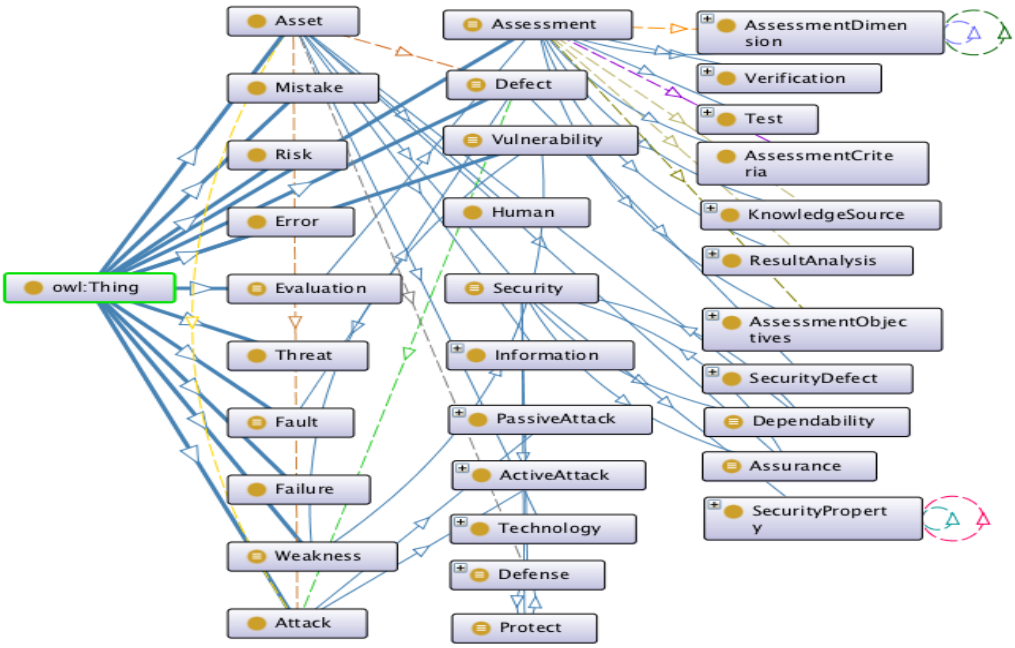


**Figura 3.3.** Classes principais de SecAOnto

### 3.2.3.1 Conceituando Avaliação de Sistemas

Inicia-se a conceituação definindo os conceitos de avaliação principais: Teste (*Test*), Verificação (*Verification*) e Avaliação (*Assessment*). Classes são descritas na ontologia em inglês e identificadas por itálico, com a primeira letra maiúscula.

Teste (*Test*) é a atividade dinâmica voltada para a execução de um programa ou modelo de forma controlada, usando entradas específicas e verificando se o comportamento está de acordo com as especificações para identificar defeitos ou para

garantir sua confiabilidade. Existem vários tipos de testes, por exemplo, Funcional, Invasão, Injeção de Defeitos, Exploratório etc.

Verificação (*Verification*) é a atividade que visa a constatar se um requisito está presente. Existem vários tipos de verificação, por exemplo, conformidade (com regras ou regulamentos), métodos formais, análise de vulnerabilidade, engenharia reversa, engenharia social, regras de negócio, etc.

O termo avaliação (*Assessment*) é mais genérico e inclui as atividades de testes (É. F. de Souza et al., 2017) e de verificação. Consideram-se sinônimos os termos em inglês *Evaluation* e *Assessment* neste contexto.

A Figura 3.4 apresenta uma síntese da conceituação de Avaliação, Teste e Verificação.

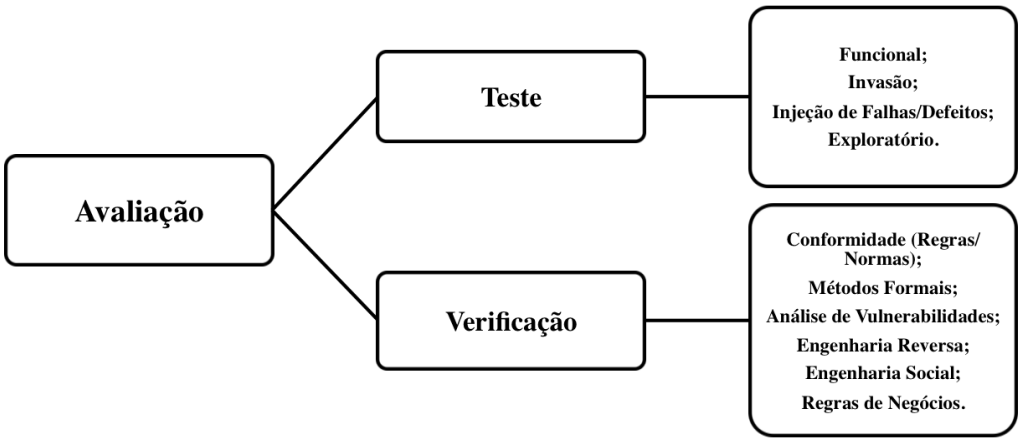


**Figura 3.4.** Síntese da conceituação de Avaliação, Teste e Verificação

A Figura 3.5 apresenta o ramo da Classe Avaliação (*Assessment*), que também inclui as Classes *AssessmentDimension*, *AssessmentObjectives*, *AssessmentItem, AssessmentCriteria* e *AssessmentHeuristics*.

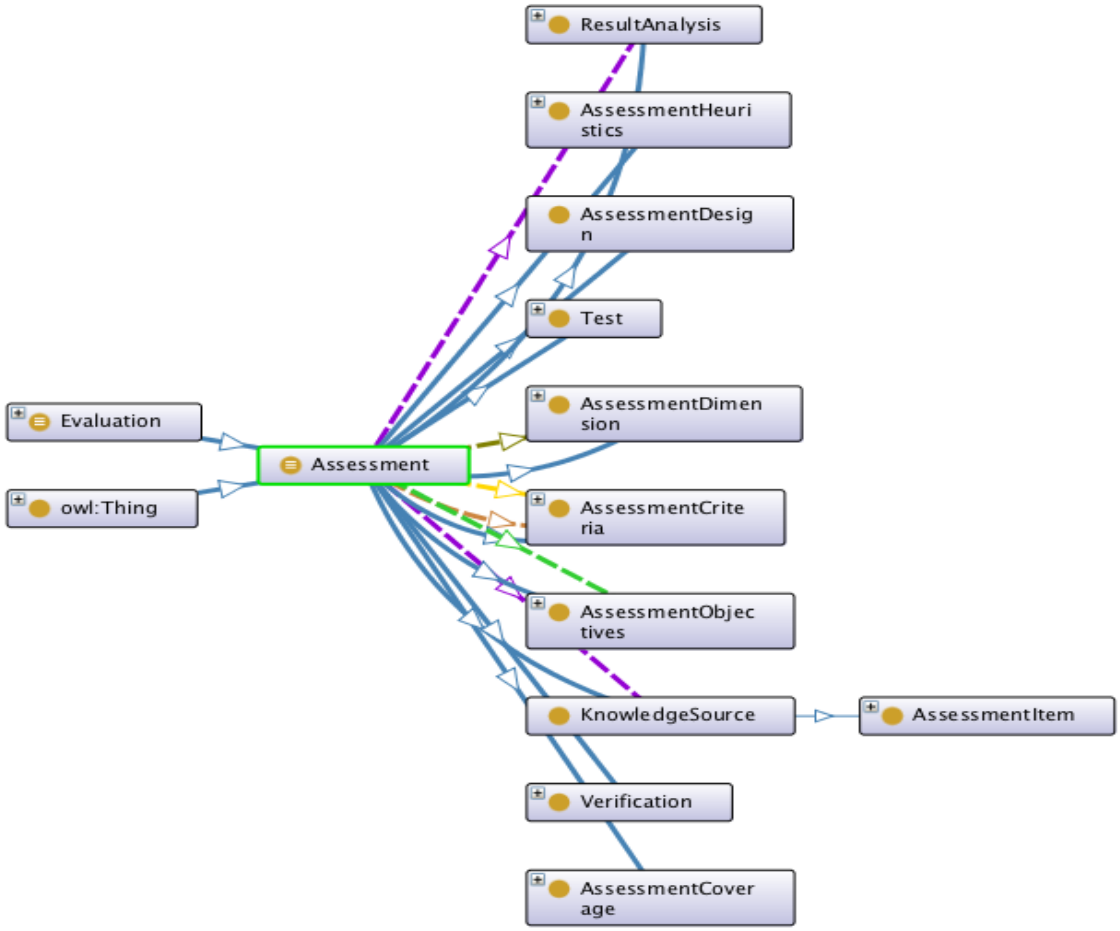


**Figura 3.5.** Ramo da Classe Avaliação (*Assessment*)

As Fontes de Conhecimento (Classe *KnowledgeSource*) representam referências ou padrões usados no processo de avaliação; em outras palavras, são instrumentos que fornecem um conjunto de Itens de Avaliação (Classe *AssessmentItem*). Por exemplo: padrões, normas, listas de verificação, conjuntos de casos de teste, conjuntos de itens de verificação, etc. Na Tabela 3.1 são apresentados exemplos de fontes de conhecimento.

**Tabela 3.1.** Exemplos de Fontes de Conhecimento

| *Fonte* | *Objetivo* |
|---|---|
| ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components* (ISO/IEC, 2008a, 2008b, 2009) | Avaliação de Segurança de dispositivos ou produtos (Hardware e Software). |
| SANS *Critical Security Controls for Effective Cyber Defense* (The SANS Institute, 2015) | Avaliação de Segurança de Software. |
| ISO/IEC 27001 (ISO/IEC, 2013a) | Avaliação de Segurança de serviços e processos em ambientes organizacionais. |
| SBIS/CFM MOEA Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) (Giulliano et al., 2014) | Avaliação de Software Médico (Registro Eletrônico de dados de pacientes) |
| FIPS (NIST) *Security Requirements For Cryptographic Modules* (140-2) (NIST, 2017a) | Avaliação de segurança de dispositivos que usam módulos criptográficos. |
| CSA/CAIQ *Consensus Assessments Initiative Questionnaire* (CSA, 2015) | Avaliação de Segurança em ambientes de *Cloud Computing* |

Itens de Avaliação (Classe *AssessmentItem*) são requisitos de avaliação destinados a encontrar defeitos ou provocar falhas em um sistema sob avaliação. Por exemplo: casos de teste, itens de verificação de um padrão. Os itens de avaliação geralmente têm um resultado esperado e um procedimento (*script*) para executá-los. Um Projeto de Avaliação (*Assessment Design – AD*) é composto por *n* Itens de Avaliação Selecionados (*Selected Assessment Items – SAI*).

Na Tabela 3.2 apresentamos exemplos de itens de avaliação (AIs). Especificamente, os AIs da fonte usada no exemplo são Itens de Verificação, mas em outras fontes poderiam ser encontrados casos de teste ou outras formas de representação.

**Tabela 3.2.** Exemplos de Itens de Avaliação

| *AI* | *Descrição* |
|---|---|
| 6.1.5 | *Whether the organizations need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed. Does this address the requirement to protect the confidential information using legal enforceable terms?* |
| 7.2.1 | *Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.* |
| 9.1.4 | *Whether the physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster should be designed and applied. Whether there is any potential threat from neighbouring premises.* |
| 10.9.1 | *Whether the information involved in electronic commerce passing over the public network is protected from fraudulent activity, contract dispute, and any unauthorized access or modification. Whether Security control such as application of cryptographic controls are taken into consideration. Whether electronic commerce arrangements between trading partners include a documented agreement, which commits both parties to the agreed terms of trading, including details of security issues.* |
| 10.10.1 | *Whether audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring. Whether appropriate Privacy protection measures are considered in Audit log maintenance.* |
| 11.5.3 | *Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.,* |
| 12.2.3 | *Whether requirements for ensuring and protecting message integrity in applications are identified, and appropriate controls identified and implemented. Whether an security risk assessment was carried out to determine if message integrity is required, and to identify the most appropriate method of implementation.* |
| 14.1.2 | *Whether events that cause interruption to business process is identified along with the probability and impact of such interruptions and their consequence for information security.* |
| 15.1.4 | *Whether data protection and privacy is ensured as per relevant legislation, regulations and if applicable as per the contractual clauses.* |
| 15.1.6 | *Whether the cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.* |

Fonte: (ISO/IEC, 2013a)

Um macro-processo de avaliação que considere as fontes de conhecimento e seus itens de avaliação é considerado. Este apresenta de maneira resumida as fases contidas na atividade de avaliação, a saber: Análise de Riscos, Definição de Critérios, Avaliação e Análise de Resultados. A Figura 3.6 apresenta uma síntese do macro-processo de avaliação. Existem outras propostas de processo genérico de avaliação para sistemas, por exemplo, ISO/IEC 25040 (ISO/IEC, 2011). As fases de definição dos critérios e de avaliação são o foco da abordagem, enquanto que as outras são abstraídas, devido a demandarem novos estudos para expansão da proposta.

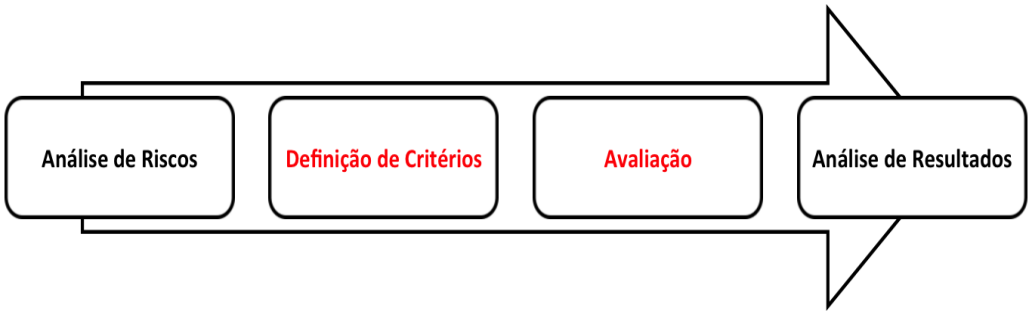


**Figura 3.6.** Macro-processo de Avaliação

Conforme apresentado na Figura 3.6, pressupomos que uma análise de riscos foi feita *a priori* para selecionar o dispositivo ou sistema a ser avaliado, ou seja, definiu-se um escopo geral. O escopo mais detalhado da avaliação do dispositivo se dá por meio das dimensões de avaliação, que são identificadas posteriormente nos itens de avaliação. De posse do ativo a ser avaliado, seguimos para a aplicação da abordagem, ou seja, a definição dos critérios a partir das coberturas e a proposta do projeto de avaliação com os melhores itens de acordo com os critérios. Após a avaliação, análises dos resultados são conduzidas. Apesar da apresentação em formato sequencial, geralmente as avaliações seguem um modelo cíclico.

Critérios de Avaliação (Classe *AssessmentCriteria*) representam regras ou requisitos a serem satisfeitos pela atividade de avaliação. Os critérios de avaliação são usados para: selecionar itens de avaliação; verificar a qualidade da atividade de avaliação; e definir a suficiência dos requisitos para o final das atividades de avaliação. A Figura 3.7 apresenta uma síntese dos insumos que podem ser usados na definição de critérios de avaliação.

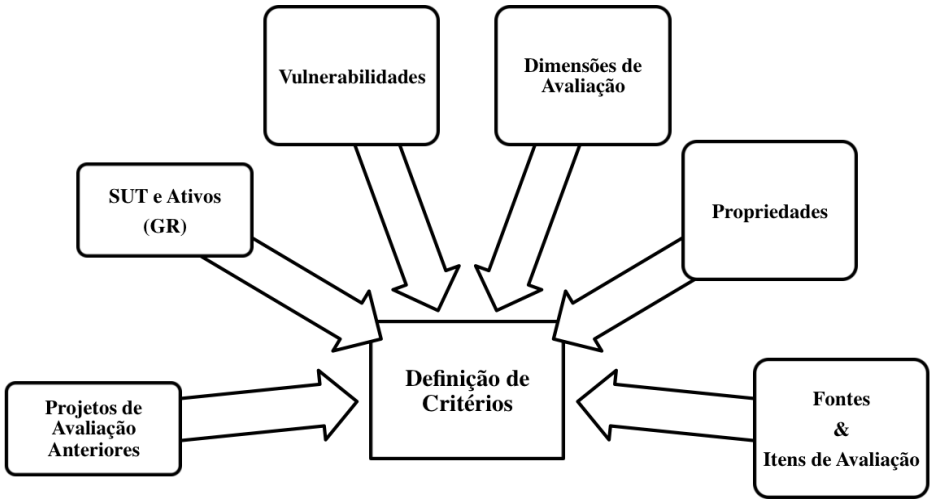


**Figura 3.7.** Síntese dos insumos para definição de critérios de avaliação

Heurísticas de Avaliação (Classe *AssessmentHeuristics*) são regras que definem como executar a atividade de avaliação, levando em consideração que cobrir as melhores condições requer uma análise rigorosa; são conjuntos de escolhas, pois pode haver muitas opções. Nenhuma heurística é aplicável em todas as situações; uma heurística que funcionou muito bem em uma situação pode não funcionar em outra. É necessário avaliar as heurísticas aplicáveis para escolher uma heurística apropriada para cada situação. Heurísticas são aproximações de critérios; não garantem que as melhores condições estão satisfeitas.

Uma análise de resultados da avaliação faz-se necessária e pode ser classificada como Homologação ou Certificação. A Homologação está relacionada a "ratificar", "afirmar", "confirmar" e "aprovar". Os produtos de homologação são relatórios de avaliação, de análise e de testes. Geralmente, uma homologação possui as seguintes características: possivelmente não divulgada; está sujeita a apelação, contestação ou recurso; está vinculada a uma versão específica do sistema ou software. Já a Certificação está relacionada a "certificar", "prover uma concessão formal" e "submissão à regulamentação". Os produtos de certificação são: certificados de conformidade com um padrão; e declaração formal por meio de um certificado ou documento equivalente. Geralmente, a certificação possui as seguintes características: possivelmente divulgada; baixa probabilidade de contestação ou recurso; está vinculada a uma versão específica de um sistema ou software, ou também a um determinado período de tempo; pode envolver a obtenção de prerrogativas e direitos. A Figura 3.8

apresenta uma síntese da conceituação da análise de resultados (Homologação/Certificação).

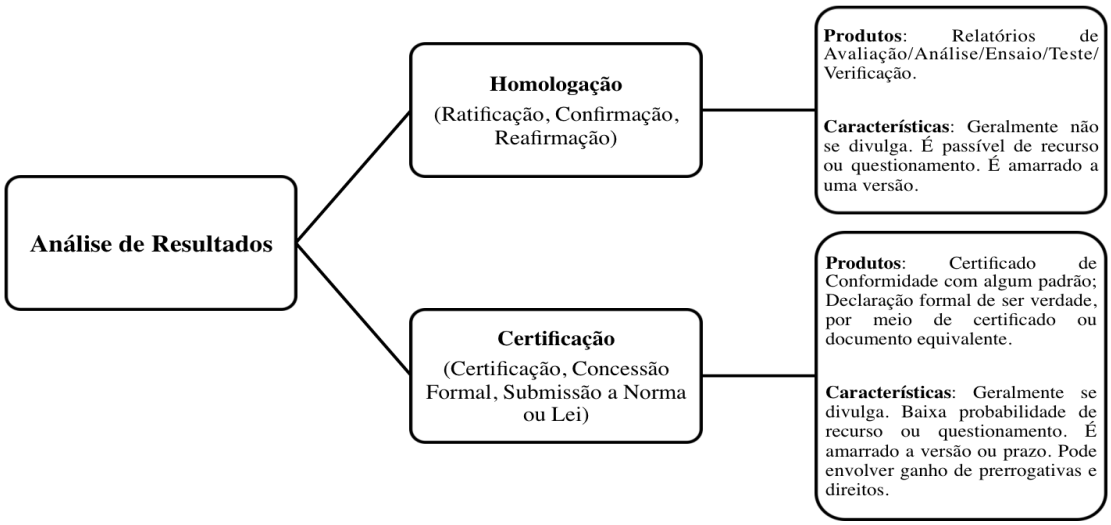


**Figura 3.8.** Síntese da conceituação da análise de resultados

Uma parte importante da formalização em avaliação de sistemas é conceituação da cadeia de falha (*Engano, Defeito, Erro, Falha*). Um Engano (*Mistake*) refere-se a uma ação humana que pode produzir um Defeito (*Defect* ou *Fault*). Programadores (na fase de desenvolvimento), Engenheiros (na fase de projeto) ou Operadores (na fase de implantação) cometem Enganos por várias razões (esquecimento, falta de conhecimento etc.). O Defeito representa uma deficiência ou uma ausência em um passo, processo ou em definições de dados. Se estiver presente em um programa, um Defeito pode causar um Erro (*Error*) quando executado. A Figura 3.9 expande o ramo do Defeito (*Defect*).

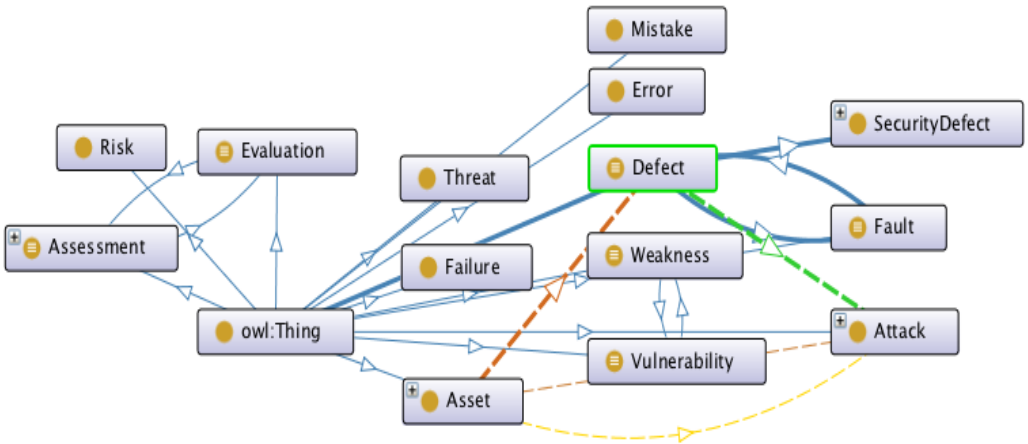


**Figura 3.9.** Ramo da Classe *Defect*

Um Erro (*Error*) representa uma condição inconsistente ou inesperada do programa ou sistema, ou seja, é um valor incorreto ou uma sequência incorreta em um determinado estado do programa. Pode ser causado pela execução de um Defeito. A Falha (*Failure*) ocorre pela propagação de um Erro, quando o resultado produzido é diferente do resultado esperado.

A Figura 3.10 apresenta uma síntese da conceituação da cadeia de falha (*Engano, Defeito, Erro, Falha*). Na primeira sequência da Figura 3.11 apresenta-se a visão de Avaliação de Sistemas e na segunda sequência apresenta-se uma analogia na visão da Avaliação de Segurança.

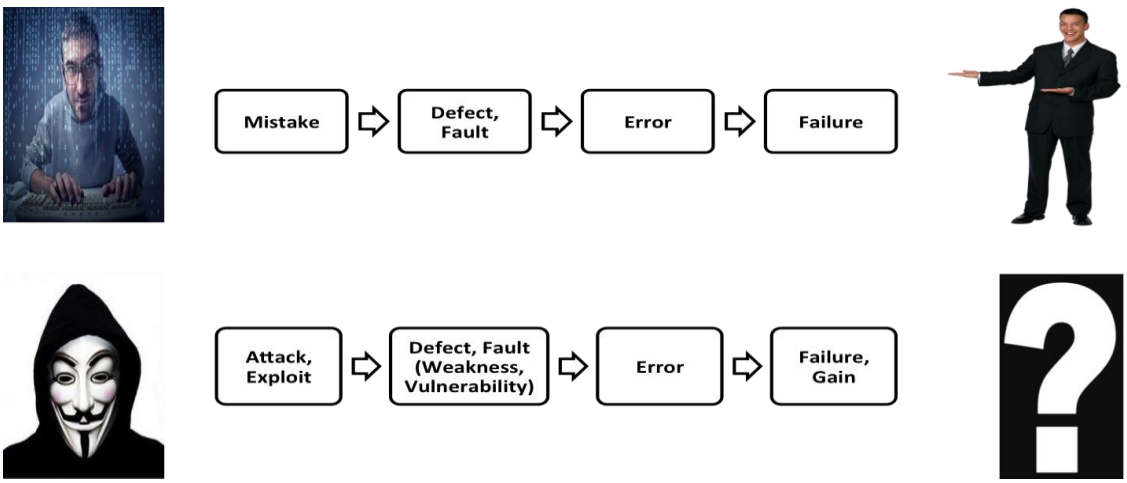


**Figura 3.10.** Síntese da conceituação da cadeia de falha

Conforme mostrado na Figura 3.10:

(i) Na primeira sequência, um Programador (ou Operador, por exemplo) comete um *Engano* (*Mistake*) e introduz um *Defeito* (*Defect*); o *Defeito*, quando exercitado, pode causar um *Erro* (*Error*), que pode ser propagado até uma *Falha* (*Failure*), se percebido. Um *Erro* pode não ser percebido.

(ii) De forma análoga, na segunda sequência, um Atacante executa um *Ataque* (*Attack*) tentando explorar um *Defeito* (ou Vulnerabilidade), para causar um *Erro*, que pode levar a uma *Falha* (Ganho). O objetivo do Atacante é que o Ganho obtido (legalmente ou não) nunca seja percebido. Podem ser citados como exemplos de ganhos (ou motivações): político, financeiro, aprendizado, diversão, ostentação etc.

Um aspecto importante em avaliação de sistemas é sob quais perspectivas o sistema será avaliado. Estas perspectivas são abordadas na literatura tradicional de avaliação de sistemas (ex.: caixa-preta, caixa-branca, caixa-cinza), mas não de forma estruturada. Entendemos que para avaliação de sistemas com ênfase em encontrar defeitos de segurança outras perspectivas são necessárias e estas precisam ser relacionadas conceitualmente. Assim, propomos a estruturação destas perspectivas definindo conceitualmente e relacionando-as, chamadas de Dimensões de Avaliação. Dimensões de Avaliação (Classe *AssessmentDimension*) representam o escopo da avaliação, ou seja, definem sob qual visão ou perspectiva o sistema (ou dispositivo) deve ser avaliado. As dimensões de avaliação são uma proposta conceitual. Incialmente, são propostas as seguintes dimensões de avaliação: Lógica de Negócios (Classe *BusinessLogic)*; Arquitetura do sistema (Classe *SystemArchitecture)*; Processo (Classe *Process*); Sistema em tempo de execução (Classe *System in Runtime* (*BlackBox*)); Estrutura do código-fonte (Classe *Source-code Structure* (*WhiteBox*)); e Ambiente Operacional (Classe *Operating Environment*). Outras dimensões podem ser incluídas em trabalhos futuros.

A seguir conceituamos cada uma das dimensões propostas e apresentamos termos que podem identificar a dimensão em itens de avaliação. À medida que outras fontes vão sendo incorporadas, novos termos podem ser incluídos, enriquecendo a expressividade da ontologia.

**DM 1.** A dimensão da lógica de negócios (*BusinessLogic*) visa a avaliar os requisitos do sistema, buscando pontos vulneráveis ou ausências na especificação do sistema que possam ser legitimamente exploradas. Defeitos na Lógica de Negócios não podem ser detectados com revisão do código-fonte. Termos que identificam a dimensão: "*information; business; requirement; profile; role; rule; module; method; function; algorithm; evidence; measure*".

**DM 2.** A dimensão da arquitetura do sistema (*SystemArchitecture*) visa a avaliar o *design* do sistema, procurando pontos vulneráveis ou ausências que possam fazer com que o sistema funcione incorretamente. Por exemplo: protocolos vulneráveis, interoperabilidade insegura, problemas de mobilidade etc. Termos que identificam a dimensão: "*architecture; layer; integration; exchange; transfer; protocol*".

**DM 3.** A dimensão do processo (*Process*) visa a avaliar processos e procedimentos do sistema, procurando pontos vulneráveis ou ausências que possam interferir no funcionamento correto do sistema. Esta dimensão destina-se a avaliar o contexto geral, tentando identificar os pontos de processo onde o sistema está inserido, mas que estão além do escopo dos requisitos de software. Por exemplo: autorização de acesso e atribuição de perfis, horários de uso e operação, critérios de acesso físico a recursos ou instalações, entre outros. Termos que identificam a dimensão: "*process; documentation; relation; service; date; hour; time; store; identify; user; responsibility; profile; rule; policy; management; organization; commitment; assignment; responsibility; role; asset; agreement; legal; enforce; procedure; incident; law; enforcement; review; change; implementation*".

**DM 4.** A dimensão de sistema em execução (ou em uso) (*System in Runtime (BlackBox))* visa a avaliar a execução do sistema, procurando por vulnerabilidades ou ausências que possam ser exploradas em caso de configuração incorreta ou uso incorreto, deliberadamente ou não. Esta dimensão, no contexto do teste de software pode ser definida como teste caixa-preta, onde não é possível ou viável instrumentar e analisar o código-fonte da solução. Termos que identificam a dimensão: "*system; black box; run; verify; runtime; execution; interface*".

**DM 5.** A dimensão da estrutura de código-fonte (*Source-code Structure (WhiteBox))* visa a avaliar o código-fonte, procurando por vulnerabilidades ou ausências que possam ser exploradas. Por exemplo, bibliotecas vulneráveis, algoritmos incorretos, funções não seguras, parâmetros frágeis etc. Esta dimensão, no contexto do teste de software pode ser definida como teste caixa-branca, onde é possível ou viável instrumentar e analisar o código-fonte da solução. Termos que identificam a dimensão: "*source-code; code; white box; function; variable; structure; input; output; constant*".

**DM 6.** A dimensão do ambiente operacional (*Operating Environment*) visa a avaliar o ambiente operacional do sistema, procurando por vulnerabilidades ou ausências que possam ser exploradas. Por exemplo, versões não seguras, protocolos, configurações etc. Os ambientes operacionais são sistemas operacionais, sistemas de suporte, armazenamento ou de infraestrutura de rede onde o sistema em avaliação irá operar. Termos que identificam a dimensão: "*operating system; environment; operator; administrator; user; network; database; SGBD; support; monitoring; infraestructure; communication; configuration*".

Na Figura 3.11, apresentam-se as Subclasses da Classe *AssessmentDimension*.

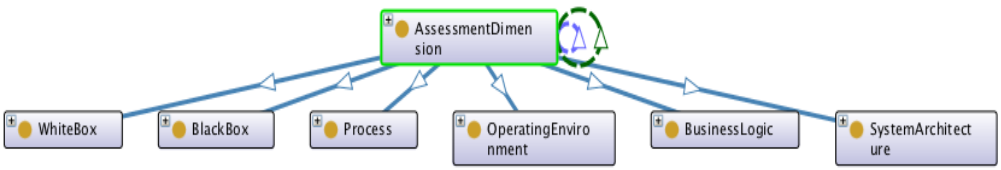


**Figura 3.11.** Ramo da Classe *AssessmentDimension*

A classe cobertura de avaliação (*AssessmentCoverage*) representa uma medida que quantifica a qualidade da avaliação. Bueno (2012) define a cobertura do teste como a porcentagem dos elementos requeridos exercitados pela execução de um conjunto de casos de teste. Por exemplo, a porcentagem de comandos executados durante um teste seria uma medida de cobertura do critério "Todos os Comandos". É razoável assumir que um conjunto de testes que executa 90% dos comandos é melhor

do que outro conjunto de testes que executa apenas 50% dos comandos. Quando um conjunto de casos de teste exercita todos os elementos exigidos pelo critério, dizemos que este conjunto satisfaz o critério. Deste modo, pode-se afirmar que a medida de cobertura quantifica, sob certa perspectiva, a qualidade de uma avaliação.

### 3.2.3.2 Conceituando Segurança da Informação

Segurança (Classe *Security*) é a classe básica na conceituação de segurança da informação e é entendida como um objetivo, isto é, proteger o ativo (Classe *Asset*) contra uso indevido. A segurança é detalhada em subclasses que se referem a propriedades de segurança (Classe *SecurityProperty*). Os termos *Dependability* e *Assurance* são consideradas sinônimos do termo *Security* neste contexto. Na Figura 3.12 apresentam-se as subclasses da classe *Security*.

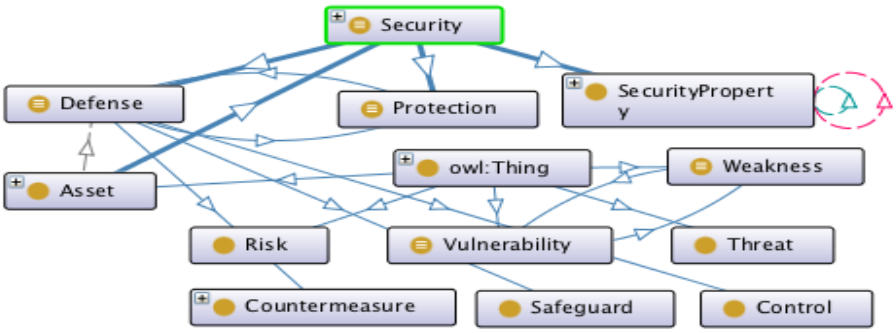


**Figura 3.12.** Ramo da Classe *Security*

Ativo (*Asset*), Vulnerabilidade (*Vulnerability*), Fraqueza (*Weakness*), Risco (*Risk*) e Ameaça (*Threat*) são conceitos de alto nível (subclasses de *Thing*). A Classe *Asset* representa informações ou qualquer componente de sistema que tenha valor para a instituição, por exemplo, dados, dispositivos ou outros componentes do ambiente operacional. A Classe *Vulnerability* representa uma fragilidade ou incapacidade de um sistema que pode ser explorado por atacantes.

O Risco (*Risk*) é a probabilidade de ocorrência de eventos adversos que possam afetar um Ativo (*Asset*). A Classe *Threat* representa uma Ameaça para um Ativo, ou seja, o Ativo está sob risco (ameaçado) de ser atacado. Um Ataque (*Attack*) é uma tentativa de acessar indevidamente um recurso com propósito malicioso, por exemplo,

para destruir, expor, alterar, desativar, roubar ou obter qualquer ganho não autorizado. Os Ataques buscam explorar Vulnerabilidades (ou Fraquezas) dos sistemas. Os atacantes são agentes de ameaça.

Defesa (*Defense*) e Proteção (*Protection*) (subclasses de *Security*) são métodos, processos ou mecanismos destinados a proteger um Ativo (*Asset*). Contramedida (*Countermeasure*), Salvaguarda (*Safeguard*) e Controle (*Control*) são exemplos de ações (processos, métodos) ou mecanismos (software, hardware) de defesa. A Auditoria (*Auditing*) é uma revisão independente de registros e processos para avaliar a conformidade com processos, procedimentos, requisitos, controles de padrões ou políticas de segurança. Um processo de auditoria depende de geração de evidência e uma correta rastreabilidade (*Traceability*).

Em segurança da informação certas características ou objetivos são cruciais e devem ser observados no desenvolvimento de sistemas seguros. Estas características são abordadas na literatura tradicional de segurança da informação, mas não de forma estruturada. Entendemos que para avaliação de sistemas com ênfase em encontrar defeitos de segurança as características principais precisam estar definidas claramente e devem ser relacionadas conceitualmente. Assim, propomos a estruturação destas características definindo conceitualmente e relacionando-as, chamadas de Propriedades de Segurança. Propriedades de Segurança (Classe *SecurityProperty*) são princípios ou características de segurança específicas de informações ou sistemas. As propriedades de segurança são uma proposta conceitual. Incialmente, são propostas as seguintes propriedades de segurança: Disponibilidade (*Availability*); Integridade (*Integrity*); Confidencialidade (*Confidentiality*); Autenticidade (*Authenticity*); Não-repúdio (*Non-repudiation*); Rastreabilidade (*Traceability*); Privacidade (*Privacy*); Auditabilidade (*Auditability*); Legalidade (*Legality*); Resiliência (*Resilience*); Não-retroatividade (*Non-retroactivity*).

A seguir conceituamos cada uma das propriedades de segurança propostas e apresentamos termos que podem identificar a propriedade em itens de avaliação.

**PP1.** Disponibilidade (*Availability*): informação ou sistema é acessível e utilizável quando demandado. Termos que identificam a propriedade: "*availability; available; usable; run; operating; environment; network; work; perform; performance; stress*".

**PP2.** Integridade (*Integrity*): informação ou sistema não foram modificados ou destruídos de forma não autorizada ou acidental. Esta propriedade diz respeito a se a informação está correta ou o sistema fornece dados corretos. Termos que identificam a propriedade: "*integrity; create; modify; edit; delete; destroy; correct; data; backup*".

**PP3.** Confidencialidade (*Confidentiality*): a informação é acessível e utilizável apenas por usuários ou sistemas autorizados. Geralmente, perfis, níveis de acesso ou graus de sigilo são definidos. Termos que identificam a propriedade: "*confidentiality; secrecy; confidential; classified; reserved; secret; top-secret; permission; allow; clearance; disclosure; protect; access; authorize; profile; role; level*".

**PP4.** Autenticidade (*Authenticity*): o sistema permite verificar se atos ou documentos são verdadeiros (autênticos) ou falsos. Os processos de autenticação visam a provar que os componentes de um sistema ou seus usuários são quem eles afirmam ser por meio de mecanismos como senhas, *tokens* etc. O processo de autenticação é um mecanismo para atestar, por exemplo, que uma assinatura em um documento é autêntica, ou que uma pessoa é quem diz ser com base em informações biométricas. Termos que identificam a propriedade: "*authenticity; authentic; authentication; identify; biometric; factor; originality; origin; veracity; truth; true; false; valid; unique; account*".

**PP5.** Não-repúdio (*Non-repudiation*): o sistema registra evidências de atos importantes, de modo que os usuários ou outros sistemas não podem negar a autoria das ações realizadas. Termos que identificam a propriedade: "*non-repudiation; evidence; proof; record; act; action; user; author; authorship; perform; refuse; reject; discard; refuse; decline; deny; repudiate; repudiation; responsibility, commitment; duty; incumbency; identify; unique; biometric*".

**PP6.** Rastreabilidade (*Traceability*): o sistema registra informações sobre ações críticas, permitindo a recuperação do histórico de ações, se necessário. Em outras palavras, a rastreabilidade significa monitorar e registrar atividades em um sistema, para acompanhar as ações de usuários ou componentes de software. Termos que identificam a propriedade:

"*traceability; trace; record; register; report; memory; raw data; account; accounting; accountability; log; evidence; history; origin; action*".

**PP7.** Privacidade (*Privacy*): o sistema não divulga indiscriminadamente, ou sem permissão específica, informações sobre intimidade pessoal (informações pessoais). Essa intimidade tem vários níveis de percepção. Esta propriedade pode ser entendida como sendo a confidencialidade de informações íntimas ou pessoais. Mais detalhes sobre a percepção da privacidade podem ser encontrados no trabalho de Bostwick (1976). Termos que identificam a propriedade: "*privacy; confidential; classified; secrecy; disclosure; private; personal; individual; particular; specific; single; proper; own*".

**PP8.** Auditabilidade (*Auditability*): o sistema tem a capacidade de gerar e fornecer evidências a terceiro confiável de que os requisitos de segurança foram alcançados. Termos que identificam a propriedade: "*auditability; audit; evidence; compliance; requirement; certification; homologation*".

**PP9.** Legalidade (*Legality*): o sistema e o processo em que este está inserido estão de acordo com as leis ou regulamentos aplicáveis. Termos que identificam a propriedade: "*legality; law; standard; regulation; governance; rule; ordinance; statute; legal; licit; valid; legitimate; compliance; submission; observance; agreement; claim; accounting; accountability; contract; enforce*".

**PP10.** Resiliência (*Resilience*): o sistema pode continuar operando mesmo em condições adversas, tais como, problemas de ambiente operacional ou falhas causadas por ataques cibernéticos. Termos que identificam a propriedade: "*resilience; resist; withstand; endure; ensure; preserve; keep; bear; tolerate; oppose; detain; stop; block; defend; protect; survival; adverse; attack; operation; failures; resilient; strong; hard; robust; durable*".

**PP11.** Não-retroatividade (*Non-retroactivity*): o sistema não permite que ações sejam realizadas ou documentos sejam gerados retroativamente no tempo. Termos que identificam a propriedade: "*retroactivity; retroactive; date; period; term; action; time; expiration; backward*".

Outras propriedades podem ser incluídas, especialmente quando domínios de aplicação específicos são abordados. Por exemplo, em *e-Voting*, as seguintes

propriedades de segurança específicas são propostas: Anonimato (*Anonymity*), Divulgação ou Exposição (*Disclosability*), Unicidade ou Singularidade (*Uniqueness*), Precisão (*Accuracy*), Transparência (*Transparency*), Não-coerção (*Non-coercibility*) (Salini & Kanmani, 2012). Adicionalmente, em outros domínios, podem ser identificadas outras propriedades de segurança, como Irrevogabilidade ou Impossibilidade de Reversão (*Irrevocability* ou *Irreversibility*), Capacidade de Sobrevivência e Manutenção (*Survivability* e *Maintainability*) (Avizienis, Laprie, & Randell, 2004).

Na Figura 3.13, apresenta-se o ramo da Classe *SecurityProperty*

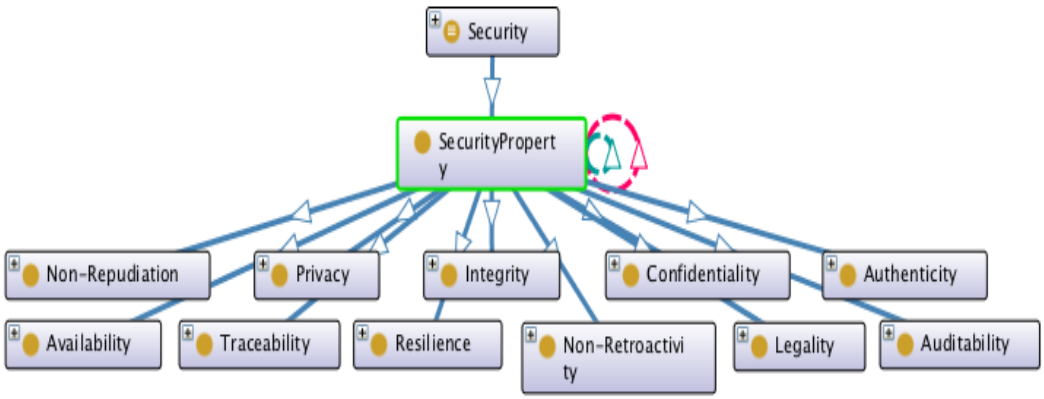


**Figura 3.13.** Ramo da Classe *SecurityProperty*

Com relação ao termo "Propriedade de Segurança", a literatura também considera termos relacionados com o mesmo sentido. Em alguns momentos o conceito está relacionado com o termo "Segurança" em outros com o termo "Informação". Por exemplo, características como CIA (Confidencialidade, Integridade e Autenticidade) são citadas como propriedades da informação a serem asseguradas (Pereira & Santos, 2010), aspectos de segurança (Colombo, 2014), atributos de segurança (Fenz & Ekelhart, 2009), objetivos de segurança (Rieke et al., 2012), propriedades de segurança (Felderer et al., 2016; Gyrard et al., 2013; Kiesling et al., 2012), controles de processo (ISECON, 2010) ou métricas de resiliência (ENISA, 2011).

### 3.2.3.3 Conceituando Avaliação de Segurança da Informação

Avaliar a Segurança da Informação significa testar ou verificar o sistema com ênfase em encontrar defeitos de segurança; o foco é em avaliar se os aspectos de segurança estão presentes no sistema. O processo de Avaliação de Segurança (*SecurityAssessment*) herda conceitos das áreas de Avaliação de Sistemas e Segurança da Informação. Na Figura 3.14 apresenta-se o ramo da Classe *SecurityAssessment*.

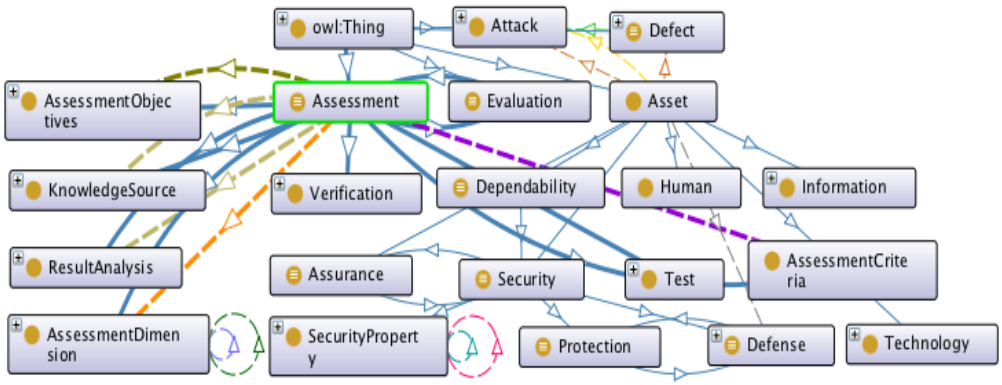


**Figura 3.14.** Ramo da Classe *SecurityAssessment*

Os Defeitos de segurança (Classe *SecurityDefect*) são defeitos que afetam, direta ou indiretamente, o nível de segurança de um sistema. Existem três subclasses de Defeitos de Segurança, a saber: Defeito de Projeto (*DesignDefect*), Defeito de Desenvolvimento (*DevelopmentDefect*), e Defeito de Operação (*OperationDefect*).

Um Defeito de Projeto (*DesignDefect*) é uma especificação incorreta da lógica de negócios, tais como regras, requisitos, arquitetura, recursos etc. As subclasses de *DesignDefect* são:

- Funcionalidade (*Functionality*) – O sistema não faz algo que deveria fazer;
- Interoperabilidade (*Interoperability*) – O sistema não troca informações adequadamente com outros sistemas;
- Desempenho (*Performance* e *Availability*) – O sistema não opera e processa informações dentro do tempo esperado.

Um Defeito de Desenvolvimento (*DevelopmentDefect*) é uma codificação incorreta de uma funcionalidade. As subclasses de *DevelopmentDefect* são:

- Saída (*Output*) – O sistema não produz o resultado esperado, ou produz resultados não esperados;
- Validação (*Validation*) – O sistema não valida parâmetros ou dados de entrada;
- Tratamento de Erros (*TreatmentOfErrors*) – O sistema não detecta ou não manipula devidamente erros inesperados;
- Limite (*Limit*) – O sistema não trata corretamente os valores extremos;
- Cálculo (*Calculus*) – O sistema calcula incorretamente. Por exemplo: operador matemático errado, como "+" em vez de "-";
- Condição de Concorrência (*RaceCondition*) – O sistema não trata as condições de concorrência. Por exemplo: duas aplicações tentando obter o mesmo recurso computacional;
- Condição de Estresse (*StressCondition*) – O sistema não suporta sobrecarga por um tempo especificado;
- Ambiente Operacional (*OperationalEnvironment*) – O sistema não considera incompatibilidade ou falhas no ambiente operacional (por exemplo, hardware, sistemas operacionais, energia etc.).

Um Defeito de Operação (*OperationDefect*) é a representação de um ambiente operacional inadequado ou do uso incorreto de recursos do sistema; falta de manutenção adequada (corretiva e preventiva) e evolução constante do sistema. As subclasses *OperationDefect* são:

- Atualização (*Update*) - O sistema não considera falhas no processo de gerenciamento de configuração. Por exemplo: falha na revisão periódica e atualização de versões de sistemas operacionais, bibliotecas e componentes de software, sistemas de apoio e redes etc.
- Humanos (*ByHuman*) - O sistema não considera problemas na operação, devido a enganos cometidos por humanos nas configurações ou uso de sistema;
- Processos Externos (*ExternalProcesses*) - O sistema não considera o uso inadequado ou malicioso por humanos ou outros sistemas.

Na Figura 3.15 apresenta-se o ramo da Classe *SecurityDefect*.

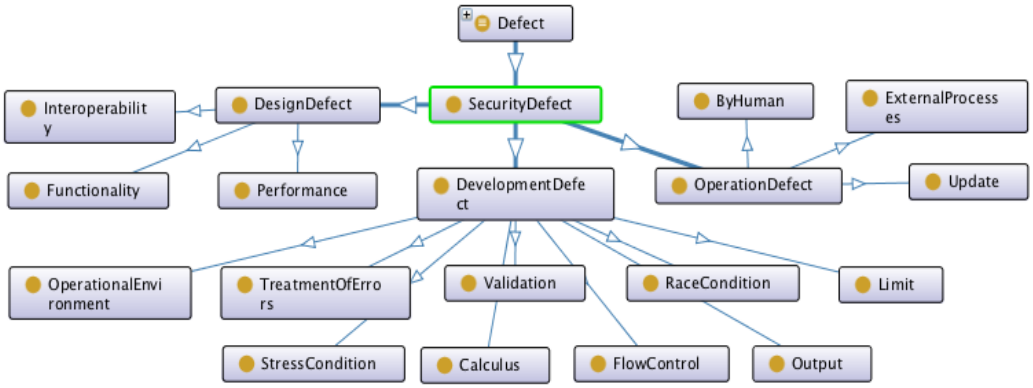


**Figura 3.15.** Ramo da Classe *SecurityDefect*

### 3.2.4 Como SecAOnto é usada na abordagem

Neste tópico apresenta-se como SecAOnto (*Security Assessment Ontology*) (Rosa, Jino, & Bonacin, 2018b; Rosa, Jino, Bonacin, et al., 2018) é usada na abordagem.

A ontologia é aplicada para: (i) a descrição dos conceitos do campo de pesquisa de avaliação de segurança (como mostrado em 3.2.3), e (ii) apoio a um algoritmo de cálculo de cobertura no processo de geração dos critérios e heurísticas de avaliação de segurança.

SecAOnto apoia o desenvolvimento do algoritmo de cálculo das coberturas de propriedades de segurança e de dimensões de avaliação pela identificação de conceitos nas descrições de itens de avaliação.

Com a incorporação dos conceitos e com fontes adicionais mapeadas na base de conhecimento, podemos estender o algoritmo de cálculo de cobertura para percorrer a ontologia buscando nas fontes de conhecimento os termos que identificam as propriedades e dimensões nos itens de avaliação; após essa identificação, as distâncias entre propriedades e entre dimensões, contidas nas matrizes de adjacências, são lidas e as coberturas são calculadas. Dessa forma, utilizando o JENA Framework (The Apache Software Foundation, 2017), podemos ler o OWL (padrão XML), buscar os conceitos representados na Fonte de Conhecimento e depois atribuímos Dimensões de Avaliação e Propriedades de Segurança com suas Distâncias para cada item de avaliação. As

distâncias são usadas para calcular as coberturas, um passo importante para a geração de critérios de avaliação de segurança.

Maiores detalhes sobre como as distâncias são usadas o algoritmo de cálculo de cobertura será detalhado no Capítulo 4.

A proposta de se utilizar ontologia como elemento de uma nova arquitetura conceitual para avaliação de segurança foi apresentada por Rosa & Jino (2016) e por Rosa et al. (2016a); os valores atuais expressos na ontologia foram usados nos cálculos da prova de conceito (Rosa, Jino, & Teixeira Junior, 2017b) demonstrando sua viabilidade; e seus valores de distâncias são tratados adiante neste trabalho.

### 3.2.5 Discussão sobre SecAOnto

SecAOnto é focada na área de aplicação de avaliação de segurança em vez do domínio de segurança da informação em geral ou em subdomínios, como a maioria das ontologias avaliadas.

Devido à complexidade da formalização de avaliação de segurança, faz-se necessário continuar aprimorando SecAOnto. Espera-se continuar evoluindo sua expressividade, por meio da inclusão de detalhes técnicos em alguns ramos de conceitos e criando instâncias próximas de condições do mundo real. As diversas fontes de conhecimento de segurança, ainda por inserir na base de conhecimento, são ricas em conceitos e em uma terminologia que podem contribuir para essa evolução.

A metodologia OntoMetrics permite um julgamento mais preciso das ontologias de segurança em vez da comparação geral, pois permite uma avaliação do conteúdo das ontologias comparadas. No entanto, as considerações de avaliação são muito dependentes da opinião do avaliador e nos requisitos para a ontologia (Ramanauskaite et al., 2013). A avaliação baseada em OntoMetrics a partir da ferramenta Protégé (Lozano-Tello & Gomez-Perez, 2004; Ramanauskaite et al., 2013; Stanford University, 2015) mostra que SecAOnto é uma ontologia *ALCHIQ(D)* com 758 axiomas, 290 axiomas lógicos, 156 classes, 37 propriedades de objetos, e 56 indivíduos. *ALCHIQ(D)* significa lógica de descrição básica (*ALC*) com adição de hierarquia de propriedade (*H*), Propriedades inversas (*I*), Restrições de cardinalidade (*Q*) e Tipos de

dados (*D*). Mais detalhes sobre expressividade de lógicas de descrição são apresentados por Hustadt, Motik, & Sattler (2005) e por Krötzsch, Simančík, & Horrocks (2012).

SecAOnto, cujo OWL é disponibilizado por Rosa, Jino, & Teixeira Junior (2017c), é uma proposta de conceituação de uma área importante de pesquisa aplicada cujos conceitos são geralmente considerados separadamente e de forma ambígua. Uma síntese de diversos conceitos e referências sobre segurança da informação pode ser encontrada no trabalho de Souag et al. (2015); tabelas de referência cruzada entre conceitos e autores pode ser útil para apresentar outras visões dos conceitos, com seus respectivos domínios.

SecAOnto é limitada ao contexto de avaliação de segurança e não tem a pretensão de descrever todo o campo de avaliação de sistemas ou o domínio completo de segurança da informação. Por exemplo, SecAOnto não entra em detalhes do processo de gestão de riscos, classificação e comportamento de software malicioso, análise e descrição de vulnerabilidades, entre outros tópicos.

SecAOnto pode ser aplicada sempre que a formalização conceitual da área de avaliação de segurança for requerida; assim, a proposta pode ser útil para pesquisadores de segurança que precisem conceituar seus métodos e técnicas.

## 3.3 CONSIDERAÇÕES FINAIS

Neste capítulo bases conceituais para a área de avaliação de segurança foram propostas e expressas por meio de uma ontologia, considerando o contexto de um processo de avaliação de segurança proposto. Mais detalhes são apresentados por Rosa et al. (2018); este trabalho apresenta uma ontologia para avaliação de segurança (SecAOnto) e sua aplicação como insumo para o cálculo de coberturas. Os conceitos-chave da abordagem proposta foram descritos em forma de classes de SecAOnto, a saber: fontes de conhecimento, itens de avaliação, coberturas, critérios e heurísticas de avaliação, dimensões de avaliação, e propriedades de segurança. Uma discussão sobre SecAOnto e a conceituação proposta foi apresentada. Devido à complexidade e transversalidade do tema, conceituar a área de avaliação de segurança propondo uma ontologia para formalizar essa conceituação com razoável expressividade é uma tarefa difícil. Isso pode estar ligado ao fato dos trabalhos que se propõem a formalizar conceitualmente a área de segurança geralmente partem dos termos “vulnerabilidade”

ou “ataque”; não que isso seja ruim, mas é um complicador quando se deseja avaliar o sistema como um todo de forma mais holística com ênfase em encontrar defeitos de segurança conhecidos e desconhecidos. Para citar um exemplo, alguns ataques de regras de negócios ou engenharia social não exploram vulnerabilidades, mas sim *features* (boas características de usabilidade) especificadas nos requisitos do sistema. Apesar da descrição resumida do processo de avaliação de segurança apresentar a fase de execução da avaliação, até o momento considera-se a aplicação da abordagem na fase de planejamento da avaliação e em sistemas prontos. Não se pretende propor uma abordagem para avaliação de segurança considerando todo o ciclo de vida de aplicações, ou todo o ciclo de desenvolvimento seguro de software.

No próximo capítulo apresenta-se a abordagem para seleção e análise de itens de avaliação de segurança baseada em critérios e heurísticas de avaliação (HCApp-Sec). HCApp-Sec é composta de uma arquitetura conceitual, algoritmos para fornecer medidas de cobertura de avaliação e conjuntos de critérios e heurísticas de avaliação de segurança. Uma visão geral da proposta é apresentada abordando o problema da necessidade de abordagens sistemáticas para avaliação de segurança. Medidas para o cálculo da cobertura de avaliação são propostas para quantificar propriedades de segurança e dimensões de avaliação abordadas em itens de avaliação. Conjuntos de critérios e heurísticas de avaliação de segurança são propostos usando as medidas de cobertura. E, por fim, os algoritmos principais com partes de código-fonte são descritos e o protótipo de software desenvolvido (*front-end* e *back-end*) é brevemente apresentado.

# 4 HCAPP-SEC – UMA ABORDAGEM PARA SELECIONAR E ANALISAR ITENS DE AVALIAÇÃO DE SEGURANÇA BASEADA EM HEURÍSTICAS E CRITÉRIOS

*"Good tests kill flawed theories; we remain alive to guess again."*

*Karl Popper*

Técnicas para avaliação de segurança foram propostas em diferentes domínios de aplicação (Colombo, 2014; Fenz, 2010; Pereira & Santos, 2010; Zech et al., 2014). De maneira geral, os trabalhos estudados apontam para uma necessidade crescente de abordagens em que o processo de avaliação seja baseado não somente em "vulnerabilidades conhecidas" ou em "conformidade com padrões".

É importante incorporar conhecimentos especializados em segurança, tais como vulnerabilidades conhecidas, explorações e ataques, no processo de avaliação de segurança. Abordagens bem conhecidas de teste de segurança (ex., testes de invasão) não possuem procedimentos sistemáticos quanto à ordem de execução dos casos de teste, o que torna o teste de segurança uma tarefa incômoda (Zech et al., 2014).

Quando se tem uma quantidade grande de itens de avaliação a serem executados, a avaliação poderá se tornar custosa. São necessários critérios para a seleção e priorização de itens de avaliação de acordo com os requisitos de avaliação. Assim, abordagens multi-técnicas, com base em critérios claros de cobertura, são necessárias.

Neste capítulo, apresenta-se uma abordagem para seleção e análise de itens de avaliação de segurança baseada em heurísticas e critérios de avaliação (HCApp-Sec). O processo de avaliação da segurança foi sistematizado por meio da formalização conceitual e da proposta de um conjunto de critérios e heurísticas de avaliação.

HCApp-Sec é composta de uma arquitetura conceitual, algoritmos para fornecer medidas de cobertura de avaliação e conjuntos de critérios e heurísticas de avaliação de segurança.

Apresenta-se a descrição da abordagem nas seguintes seções:

4.1. Arquitetura Conceitual: uma visão geral da proposta cujo objetivo é sistematizar a avaliação de segurança;

4.2. Cobertura de Avaliação: medidas propostas para o cálculo da cobertura de avaliação visam a quantificar propriedades de segurança e dimensões de avaliação presentes em itens de avaliação;

4.3. Critérios de Avaliação de Segurança: o conjunto proposto de critérios de avaliação de segurança visa a selecionar e analisar itens de avaliação de segurança;

4.4. Heurísticas de Avaliação de Segurança: o conjunto proposto de heurísticas de avaliação de segurança faz uso das medidas de cobertura; o objetivo das heurísticas é selecionar itens de avaliação de segurança usando medidas de cobertura para elaborar projetos de avaliação mais efetivos; e

4.5. Algoritmos e Protótipo de Software: algoritmos principais, com partes de código-fonte, e o protótipo de software desenvolvido (*front-end* e *back-end*) são brevemente descritos.

## 4.1 ARQUITETURA CONCEITUAL

Fatores internos e externos (fora de controle) são importantes para estabelecer a confiança entre serviços de software (ex., Web Services). Novas arquiteturas de segurança devem ser propostas para que a proteção seja constante para todo o ciclo de vida da colaboração entre serviços. Novos modelos de avaliação devem considerar a evolução dos sistemas, sempre que houver interação entre serviços (Bai, Dong, Tsai, & Chen, 2005; Dürbeck, Fritsch, Pernul, & Schillinger, 2010; Su & Biennier, 2010).

Nesta seção apresenta-se uma visão geral da abordagem proposta, por meio de uma arquitetura conceitual em camadas. A proposta de arquitetura conceitual visa a abordar o problema da falta de sistematização na avaliação de segurança. As seguintes camadas compõem essa arquitetura: Papéis, Serviços, Processos, Componentes e Bases de Conhecimento.

Na Figura 4.1 apresenta-se a arquitetura conceitual. Uma reflexão sobre a necessidade de uma arquitetura conceitual destinada a realizar avaliações de segurança de sistemas de forma sistemática e mais detalhes sobre esta questão são apresentados por Rosa & Jino (2016). A notação utilizada na Figura segue o padrão Archimate (Beauvoir, 2015; The Open Group, 2018), que é um método para modelagem de arquiteturas de sistemas.

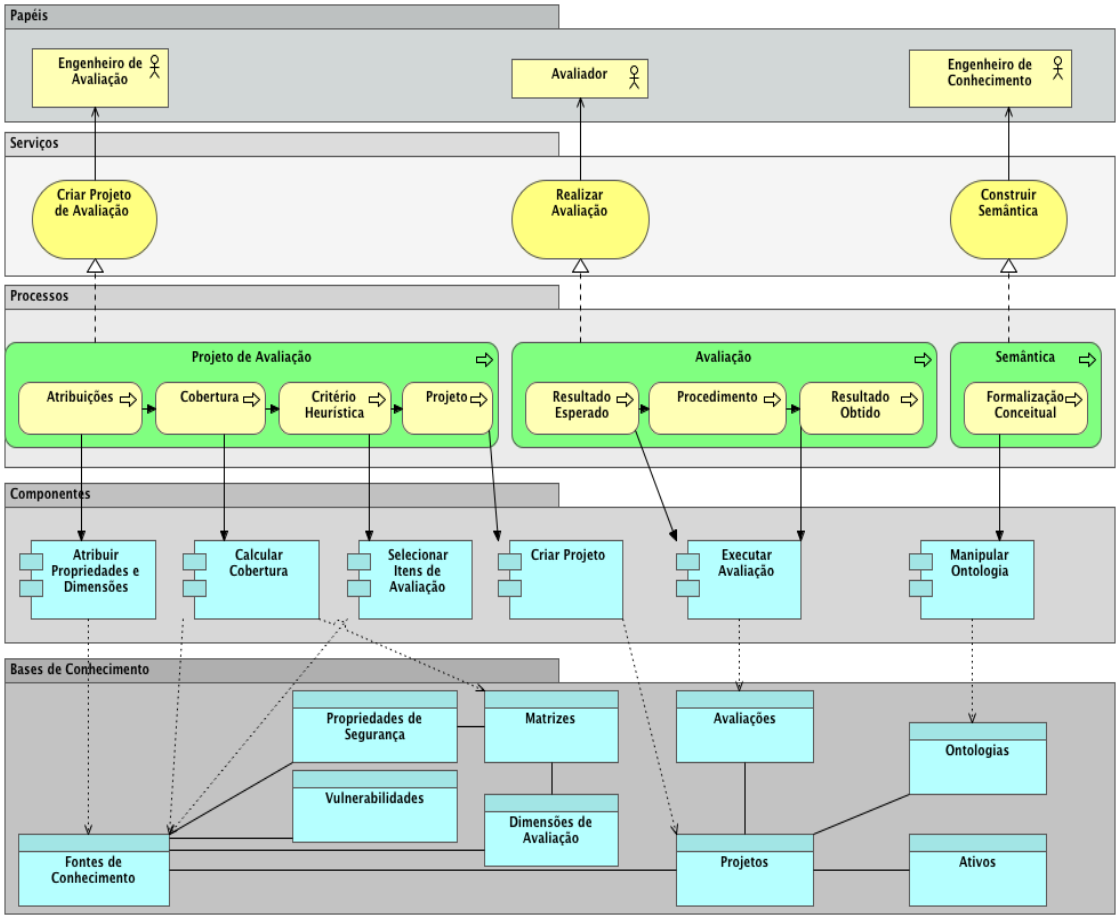


**Figura 4.1.** Arquitetura Conceitual (Rosa & Jino, 2016)

Conforme apresentado na Figura 4.1, as camadas da Arquitetura Conceitual são definidas da seguinte forma:

- *Papéis e Serviços* – (i) O Engenheiro de Conhecimento formaliza o conhecimento, por meio da criação ou manipulação de ontologias; (ii) o Engenheiro de Avaliação de Segurança cria projetos de avaliação, selecionando fontes de conhecimento e itens de avaliação; e (iii) o Avaliador aplica os itens de avaliação selecionados dos projetos de avaliação.
- *Processos* – (i) Semântica: Estamos construindo e mantendo uma ontologia de avaliação de segurança para fornecer conhecimento formalizado para nossa abordagem; Os principais conceitos da ontologia são utilizados nas bases de conhecimento para tornar o conhecimento formalizado e explícito. (ii) Projeto de Avaliação: primeiramente, selecionamos as fontes de conhecimento disponíveis; então, realizamos a atribuição conceitual de cada item de avaliação da fonte de conhecimento, calculamos as coberturas e os

critérios e heurísticas são aplicados; Por fim, construímos o projeto de avaliação contendo os itens de avaliação selecionados. (ii) Avaliação: Definimos os resultados esperados de acordo com os itens de avaliação selecionados, seus procedimentos e realizamos a avaliação.

- *Componentes* – (i) Atribuições: Atribuir as dimensões e propriedades a cada item de avaliação. (ii) Cobertura, Critérios e Heurísticas: Coberturas são calculadas e conjuntos de critérios e heurísticas são aplicados. (iii) Projeto: Depois de selecionar as fontes de conhecimento disponíveis e aplicar os critérios e heurísticas, selecionamos o conjunto efetivo de itens de avaliação para compor o projeto de avaliação. (iv) Avaliação: Uma interface é usada para gerenciar a execução da avaliação com resultados esperados, procedimentos e resultados obtidos para os itens de avaliação. (v) Formalização Conceitual: as atividades de criar e manter ontologias podem ser realizadas usando ferramentas externas, como Protégé (Stanford University, 2015) e Neon (NeOn, 2015). Utilizou-se o software Protégé para gerar e manter a ontologia proposta (SecAOnto).
- *Bases de Conhecimento* – (i) A base de fontes de conhecimento armazena as fontes de conhecimento e seus itens de avaliação; (ii) A base de Dimensões de Avaliação armazena as dimensões de avaliação propostas; (iii) A base de Propriedades de Segurança armazena as propriedades de segurança propostas; (iv) A base de Vulnerabilidades armazena defeitos de segurança conhecidos (e seus *xploits*, se disponíveis) que podem ser usadas em projetos de avaliação. *Xploits* ou outras ferramentas podem ser usadas como insumos para execução dos procedimentos de teste dos itens de avaliação; (v) A base de Matrizes armazena as matrizes de adjacência propostas; (vi) A base de Projetos armazena informações de gestão sobre os projetos de avaliação; (vii) As bases de Avaliações armazenam as informações técnicas sobre as avaliações; (viii) A base de Ativos armazena uma lista de categorias de ativos para classificar sistemas sob avaliação; (ix) A base de Ontologias armazena a ontologia proposta e outras ontologias mapeadas, se necessário.

## 4.2 COBERTURA DE AVALIAÇÃO

Nesta seção propõe-se uma maneira de assegurar a cobertura de propriedades de segurança e dimensões de avaliação em itens de avaliação de fontes de conhecimento de segurança. Essa cobertura será usada como insumo base para definir critérios e heurísticas de avaliação de segurança.

Medidas para o cálculo das coberturas para uso nos critérios e heurísticas de avaliação são propostas com o objetivo de quantificar propriedades de segurança e dimensões de avaliação abordadas em cada item de avaliação de cada fonte de conhecimento.

Resultados de avaliações indicam que, na maioria das situações, os conjuntos de alta diversidade proporcionam eficiência e maior cobertura do que as obtidas por conjuntos do mesmo tamanho gerados aleatoriamente (Bueno, 2012). As medidas propostas são baseadas na diversidade do escopo de avaliação (Dimensões de Avaliação) e na diversidade dos aspectos de segurança (Propriedades de Segurança).

### 4.2.1 Diversidade na Avaliação

Propomos uma medida de diversidade a partir da identificação de dimensões de avaliação e propriedades de segurança em cada item de avaliação de segurança.

Primeiramente, as Dimensões de Avaliação (DM) e Propriedades de Segurança (PP) são identificadas em cada item de avaliação da fonte de conhecimento, no seguinte formato: "*010111*" (palavra de seis caracteres – DM) e "*01011101001*" (palavra de onze caracteres – PP). Cada caractere (*0* ou *1*) significa se o AI aborda (*1*) ou não (*0*) uma DM ou uma PP específica. Por exemplo, "*100110*" significa que as Dimensões de Avaliação (DMs) *1*, *4*, e *5* são abordadas pelo Item de Avaliação (AI); "*01101001011*" significa que as Propriedades de Segurança (PPs) *2*, *3*, *5*, *8*, *10*, e *11* são abordados pelo AI. As atribuições das DMs e das PPs para os AIs são feitas por meio da anotação *IsIdentifiedBy* de SecAOnto. É neste campo que são identificados os termos (sintaxe) que são usados nos AIs que fazem referência aos conceitos (semântica) das DMs e das PPs contidas na ontologia.

Por exemplo, na Tabela 4.1 apresentamos as entradas de dois itens de avaliação (*6.1.5* e *11.5.2*). O AI 6.1.5 destina-se a verificar se a organização sob avaliação

exige Acordos de Confidencialidade ou de Não-Divulgação (*Non-Disclosure Agreement* – NDA) para proteção de informações e se estes são claramente definidos e regularmente revisados. Questiona-se se os NDAs abordam o requisito de proteger as informações confidenciais usando termos legais exigíveis. O AI 11.5.2 destina-se a verificar se o identificador exclusivo (ID do usuário) é fornecido a todos os usuários, tais como operadores, administradores de sistema e todos os outros funcionários, incluindo técnicos. Se a técnica de autenticação adequada é escolhida para fundamentar a identidade reivindicada do usuário. Se contas de usuários genéricas são fornecidas apenas em circunstâncias excepcionais, onde há um benefício comercial claro. Podem ser necessários controles adicionais para manter a responsabilidade.

**Tabela 4.1.** Exemplos de Entradas e Atribuições (DM e PP)

| *AI Descrição* | *AI ID* | *Entrada DM / PP* | *Atribuições DM / PP* |
|---|---|---|---|
| *Whether the organizations need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed. Does this address the requirement to protect the confidential information using legal enforceable terms?* | *6.1.5* | *101000 / 00100010100* | *DM: 1,3 / PP: 3,7,9* |
| *Whether unique identifier (user ID) is provided to every user such as operators, system administrators and all other staff including technical. Whether suitable authentication technique is chosen to substantiate the claimed identity of user. Whether generic user accounts are supplied only under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.* | *11.5.2* | *101101 / 00011100100* | *DM: 1,3,4,6 / PP: 4,5,6,9* |

Conforme mostrado na Tabela 4.1, na descrição do item de avaliação *6.1.5* foram identificados termos que representam as dimensões de avaliação "Lógica de Negócios" (DM 1) e "Processo" (DM 3) e as propriedades de segurança

"Confidencialidade" (PP 3), "Privacidade" (PP 7) e "Legalidade" (PP 9). A mesma sistemática vale para o exemplo do item 11.5.2.

Nota-se que as atribuições das DMs e das PPs para os AIs são feitas por meio da identificação dos termos (sintaxe) que são usados nos AIs que fazem referência aos conceitos (semântica) das DMs e das PPs contidas na ontologia.

### 4.2.2 Matrizes de Adjacência

A medida de diversidade é expressada por meio de valores que representam distâncias conceituais (graus de diversidade) entre dimensões de avaliação e entre propriedades de segurança. Os valores das distâncias são propostos em duas matrizes de adjacência, a saber: Distâncias entre Dimensões de Avaliação (Matriz 1) e Distâncias entre Propriedades de Segurança (Matriz 2). Os valores de distâncias variam de 0,0 a 1,0.

| | **DM1** | **DM2** | **DM3** | **DM4** | **DM5** | **DM6** |
|---|---|---|---|---|---|---|
| **DM1** | 0.0 | 0.5 | 0.2 | 0.6 | 0.7 | 0.9 |
| **DM2** | – | 0.0 | 0.9 | 0.7 | 0.6 | 0.8 |
| **DM3** | – | – | 0.0 | 0.4 | 0.2 | 0.6 |
| **DM4** | – | – | – | 0.0 | 0.5 | 0.2 |
| **DM5** | – | – | – | – | 0.0 | 0.8 |
| **DM6** | – | – | – | – | – | 0.0 |

(1)

| | **PP1** | **PP2** | **PP3** | **PP4** | **PP5** | **PP6** | **PP7** | **PP8** | **PP9** | **PP10** | **PP11** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PP1** | 0.0 | 0.9 | 0.9 | 0.9 | 0.8 | 0.8 | 0.8 | 0.8 | 0.5 | 0.2 | 0.8 |
| **PP2** | – | 0.0 | 0.9 | 0.9 | 0.8 | 0.8 | 0.8 | 0.8 | 0.5 | 0.2 | 0.2 |
| **PP3** | – | – | 0.0 | 0.9 | 0.8 | 0.8 | 0.2 | 0.8 | 0.5 | 0.8 | 0.8 |
| **PP4** | – | – | – | 0.0 | 0.2 | 0.2 | 0.8 | 0.6 | 0.5 | 0.8 | 0.4 |
| **PP5** | – | – | – | – | 0.0 | 0.2 | 0.4 | 0.6 | 0.5 | 0.8 | 0.2 |
| **PP6** | – | – | – | – | – | 0.0 | 0.5 | 0.2 | 0.5 | 0.8 | 0.2 |
| **PP7** | – | – | – | – | – | – | 0.0 | 0.8 | 0.5 | 0.2 | 0.8 |
| **PP8** | – | – | – | – | – | – | – | 0.0 | 0.5 | 0.2 | 0.2 |
| **PP9** | – | – | – | – | – | – | – | – | 0.0 | 0.5 | 0.5 |
| **PP10** | – | – | – | – | – | – | – | – | – | 0.0 | 0.2 |
| **PP11** | – | – | – | – | – | – | – | – | – | – | 0.0 |

(2)

A Matriz (1) representa as seguintes informações em suas linhas e colunas: 1) Regras de Negócios (*Business Logic*); 2) Arquitetura do sistema (*System Architecture*); 3) Processo (*Process*); 4) Sistema em tempo de execução (*System in Runtime*); 5) Estrutura do código-fonte (*Source-code Structure*); 6) Ambiente operacional (*Operating Environment*). A constante Alpha ($\alpha$) representa o número de

dimensões de avaliação que podem ser identificadas no item de avaliação (atualmente 6); Alpha é usada no cálculo da cobertura de dimensões de avaliação (CovDM).

A Matriz (2) representa as seguintes informações em suas linhas e colunas: 1) Disponibilidade (*Availability*); 2) Integridade (*Integrity*); 3) Confidencialidade (*Confidentiality*); 4) Autenticidade (*Authenticity*); 5) Não-repúdio (*Non-repudiation*); 6) Rastreabilidade (*Traceability*); 7) Privacidade (*Privacy*); 8) Auditabilidade (*Auditability*); 9) Legalidade (*Legality*); 10) Resiliência (*Resilience*); 11) Não-retroatividade (*Non-retroactivity*). A constante Beta ($\beta$) representa o número de propriedades de segurança que podem ser identificadas no item de avaliação (atualmente 11); Beta é usada no cálculo da cobertura de propriedades de segurança (CovPP).

Cada ponto representa a distância entre dimensões de avaliação (Matriz 1) ou propriedades de segurança (Matriz 2). O valor é definido entre *0,0* (sem distância) e *1,0* (sem relação). Assim, se uma propriedade de segurança (PP) estiver relacionada com outra PP, o valor será menor, enquanto que se uma PP não estiver relacionada a outra PP, o valor será maior e próximo a *1,0*; isso também se aplica às Dimensões da Avaliação (Matriz 1). Por exemplo, a propriedade de segurança "Privacidade", no contexto deste trabalho, resumidamente é definida como a "Confidencialidade" de informações pessoais; portanto, essas propriedades estão relacionadas e recebem um valor menor (*0,2*). Em contraste, "Autenticidade" e "Resiliência" são quase não relacionados, portanto, estas recebem um valor maior (*0,8*).

As distâncias entre Dimensões de Avaliação e entre Propriedades de Segurança foram expressas por meio da criação de anotações em instâncias das classes de cada propriedade e de cada dimensão. A Figura 4.2 apresenta a representação da matriz de adjacências na ontologia. Outras formas de representar as matrizes foram pensadas, como, por exemplo, criar conceitos *SecurityPropertyAdjacencyMatrix* e *AssessmentDimensionAdjacencyMatrix* e inserir abaixo os conceitos das propriedades e das dimensões.

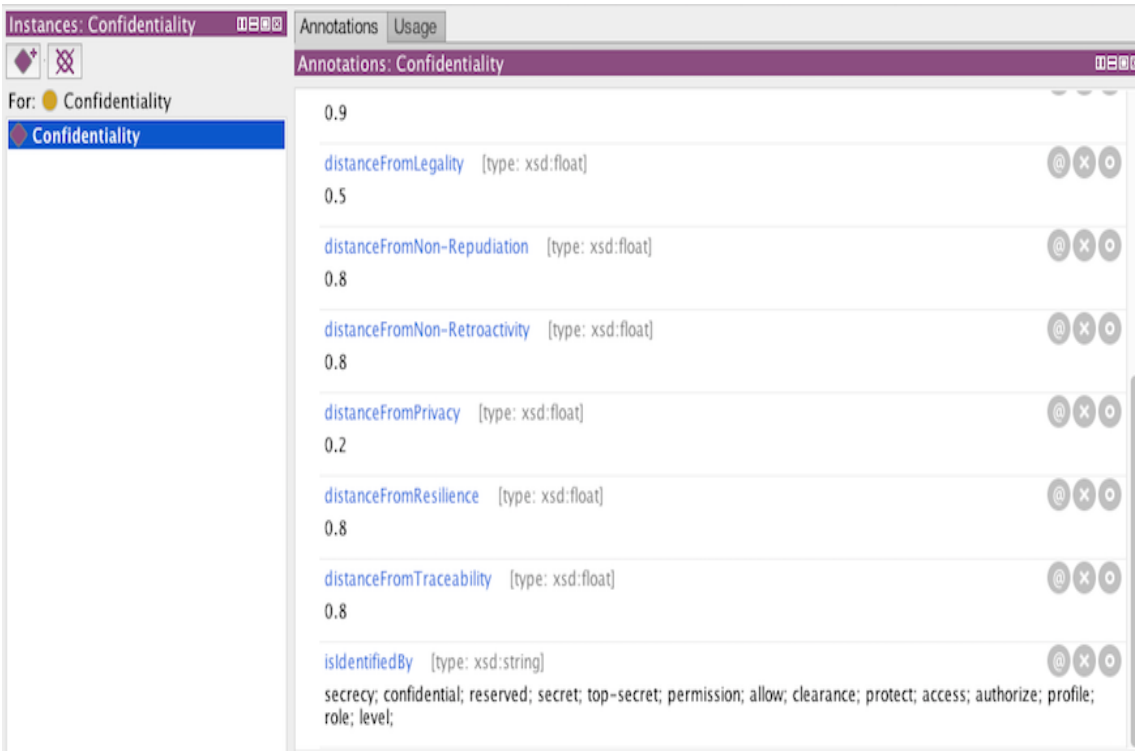


**Figura 4.2.** Representação da matriz de adjacências em SecAOnto

As atribuições das Dimensões de Avaliação (DMs) e das Propriedades de Segurança (PPs) para os Itens de Avaliação (AIs) são feitas por meio da anotação *IsIdentifiedBy*. É neste campo que são identificados os termos (sintaxe) que são usados nos AIs que fazem referência aos conceitos (semântica) das DMs e das PPs contidas na ontologia.

Com respeito à metodologia de geração das matrizes, seus valores de distâncias conceituais foram propostos por um especialista sênior em segurança da informação e por um especialista sênior em avaliação de software e foram revisados por outros três especialistas em segurança da informação e teste de software. Com outras aplicações da abordagem e com o aprimoramento de SecAOnto, os valores podem sofrer ajustes e outras propriedades e dimensões podem ser inseridas. A implementação de algoritmo para gerar automaticamente as matrizes a partir de medidas de similaridade sintática é proposta em trabalho futuro.

Na Tabela 4.2 apresenta-se um trecho de código que mostra como a matriz de adjacências (distâncias) das propriedades de segurança é representada em OWL; uma breve explicação pode ser vista na coluna de comentários.

**Tabela 4.2.** Propriedades de Segurança expressas em SecAOnto (Código OWL)

| *Parte* | *Código OWL* | *Comentários* |
|---|---|---|
| 1 | <!-- http://www.NewOnto1.org/SecAOnto_V1#hasDistance --> <owl:ObjectProperty rdf:about="http://www.NewOnto1.org/SecAOnto_V1#hasDistance"/> | *Security Property has distance.* |
| 2 | <!-- http://www.NewOnto1.org/SecAOnto_V1#hasDistanceFromSecurityProperty --><br><owl:ObjectProperty<br>rdf:about="http://www.NewOnto1.org/SecAOnto_V1#hasDistanceFromSecurityProperty"><br><rdf:type rdf:resource="&owl;SymmetricProperty"/><br><rdfs:range<br>rdf:resource="http://www.NewOnto1.org/SecAOnto_V1#SecurityProperty"/><br><rdfs:domain<br>rdf:resource="http://www.NewOnto1.org/SecAOnto_V1#SecurityProperty"/><br><rdfs:subPropertyOf<br>rdf:resource="http://www.NewOnto1.org/SecAOnto_V1#hasDistance"/><br><owl:inverseOf<br>rdf:resource="http://www.NewOnto1.org/SecAOnto_V1#hasDistanceFromSecurityProperty"<br>/><br></owl:ObjectProperty> | *Security Property has distance from Security Property; #hasDistanceFromSecurityProperty is symmetric; #hasDistanceFromSecurityProperty is subproperty of #hasDistance; #hasDistanceFromSecurityProperty is an object property.* |
| 3 | <rdf:Description rdf:about="http://www.NewOnto1.org/SecAOnto_V1#Authenticity"><br><rdfs:comment rdf:datatype="&xsd;string">"Authenticity – System allows prove the veracity of a particular act or document. This property is regarding whether information or documents are true (authentic) or false."</rdfs:comment><br><distanceFromAuthenticity rdf:datatype="&xsd;float">0.0</distanceFromAuthenticity><br><distanceFromTraceability rdf:datatype="&xsd;float">0.2</distanceFromTraceability><br><distanceFromNon-Repudiation rdf:datatype="&xsd;float">0.2</distanceFromNon-Repudiation><br><distanceFromNon-Retroactivity rdf:datatype="&xsd;float">0.4</distanceFromNon-Retroactivity><br><distanceFromLegality rdf:datatype="&xsd;float">0.5</distanceFromLegality><br><distanceFromAuditability rdf:datatype="&xsd;float">0.6</distanceFromAuditability><br><distanceFromResilience rdf:datatype="&xsd;float">0.8</distanceFromResilience><br><distanceFromPrivacy rdf:datatype="&xsd;float">0.8</distanceFromPrivacy><br><distanceFromConfidentiality<br>rdf:datatype="&xsd;float">0.9</distanceFromConfidentiality><br><distanceFromAvailability rdf:datatype="&xsd;float">0.9</distanceFromAvailability> | *Description of Security Property #Authenticity;*<br>*Distance from #Authenticity = 0.0;*<br>*Distance from #Traceability = 0.2;*<br>*...*<br>*...*<br>*Distance from #Resilience = 0.8;*<br>*...* |
| 4 | <distanceFromIntegrity rdf:datatype="&xsd;float">0.9</distanceFromIntegrity><br><isIdentifiedBy rdf:datatype="&xsd;string">authentic; originality; origin; veracity; truth; true; false;</isIdentifiedBy><br></rdf:Description> | *Distance from #Integrity = 0.9.*<br>*#Authenticity is identified by specific terms.* |

### 4.2.3 Coberturas propostas

Com base nas distâncias entre propriedades de segurança e entre dimensões de avaliação, propõem-se as seguintes coberturas de avaliação:

(i) **CovDM** – Cobertura de Dimensões de Avaliação (*Coverage of Assessment Dimensions*): é uma medida da cobertura das dimensões de avaliação que são abordadas pelo item de avaliação.

(ii) **CovPP** – Cobertura de Propriedades de Segurança (*Coverage of Security Properties*): é uma medida da cobertura das propriedades de segurança que são abordadas pelo item de avaliação.

(iii) **CovLOC** – Cobertura Local dos Itens de Avaliação (*Local Coverage of Assessment Items*): é uma medida da cobertura do item de avaliação, considerando a média de CovDM e CovPP.

(iv) **CovGLO** – Cobertura Global de uma Fonte de Conhecimento (*Global Coverage of Knowledge Source*): é uma medida da cobertura da fonte de conhecimento, considerando a média de CovLOC de todos os itens de avaliação (AI) da fonte de conhecimento.

(v) **CovTOT** – Cobertura Total de um Projeto de Avaliação (*Total Coverage of Assessment Design*): é uma medida da cobertura do projeto de avaliação, considerando a média de CovLOC de todos os itens de avaliação selecionados (SAI) das fontes de conhecimento.

Para cada item de avaliação (AI), as matrizes de adjacências são lidas; as distâncias entre pares de DM e PP são selecionadas; a soma das distâncias é calculada; a média das distâncias é calculada; CovDM e CovPP são calculadas; a soma de CovDM e CovPP é calculada e sua média é obtida; e CovLOC para o AI é calculada.

A seguir o cálculo de cada uma dessas coberturas é definido precisamente.

### (i) CovDM – *Coverage of Assessment Dimensions* (Cobertura de Dimensões de Avaliação)

O cálculo de CovDM de um item de avaliação considera a diversidade das dimensões e as distâncias identificadas no item de avaliação. Primeiramente, identifica-se quais dimensões são abordadas pelo item de avaliação por meio de busca sintática de termos definidos na ontologia SecAOnto. Considere duas dimensões de avaliação *da* e *db*: D(*da, db*) representa a distância conceitual entre as dimensões de avaliação *da* e *db.* As distâncias são lidas diretamente da matriz de distâncias entre dimensões de avaliação (Matriz 1). Então, coleta-se as distâncias entre as dimensões da avaliação.

Considere um conjunto de dimensões de avaliação DM composto de *c* dimensões de avaliação cobertas pelo item de avaliação *dm*: DM = $dm_1$, $dm_2$, ..., $dm_c$. D($dm_i$, $dm_j$) retorna a distância entre $dm_i$ e $dm_j$. CovDM é definida da seguinte forma:

$$\mathrm{CovDM(DM)} = \frac{\sum_{i=1}^{c-1}\sum_{j=(i+1)}^{c}\mathrm{D}(dm_i, dm_j)}{\alpha} \quad (1)$$

O valor da cobertura de dimensões de avaliação CovDM(DM(D)) é a soma das distâncias conceituais entre pares de dimensões de avaliação, dividida pela quantidade de dimensões de avaliação que podem ser identificadas no item de avaliação.

CovDM(DM) $\in \mathbb{R} \mid 0 \leq$ CovDM (DM) $\leq 1$. CovDM = *0* significa que o item de avaliação não cobre nenhuma ou cobre apenas uma dimensão de avaliação.

Um exemplo do cálculo de CovDM é apresentado na Tabela 4.3 (AI *11.5.2*), resultando no valor *0,483*.

**Tabela 4.3.** Exemplo de cálculo de CovDM

| *Matriz DM (1)* | *AI* | *Entrada DM* | *Cálculos* |
|---|---|---|---|
| $\begin{bmatrix} 0.0 & 0.5 & 0.2 & 0.6 & 0.7 & 0.9 \\ - & 0.0 & 0.9 & 0.7 & 0.6 & 0.8 \\ - & - & 0.0 & 0.4 & 0.2 & 0.6 \\ - & - & - & 0.0 & 0.5 & 0.2 \\ - & - & - & - & 0.0 & 0.8 \\ - & - & - & - & - & 0.0 \end{bmatrix}$ (1) | *11.5.2* | *101101* | *DM: 1,3,4,6*<br><br>*CovDM = 0,2 (1-3) + 0,6 (1-4) + 0,9 (1-6) + 0,4 (3-4) + 0,6 (3-6) + 0,2 (4-6) = 2,9 / 6 = 0,483* |

### (ii) CovPP – *Coverage of Security Properties* (Cobertura de Propriedades de Segurança)

O cálculo de CovPP de um item de avaliação considera a diversidade das propriedades de segurança e suas distâncias identificadas no item de avaliação. Primeiramente, identifica-se quais propriedades de segurança são abordadas pelo item de avaliação por meio de busca sintática de termos definidos na ontologia SecAOnto. Considere duas propriedades de segurança *pa* e *pb*: D(*pa, pb*) representa a distância conceitual entre as propriedades de segurança *pa* e *pb.* As distâncias são lidas diretamente na matriz de distâncias entre propriedades de segurança (Matriz 2). Então, coleta-se as distâncias entre as propriedades de segurança.

Considere um conjunto de propriedades de segurança PP composto por *c* propriedades de segurança cobertas pelo item de avaliação *pp*: PP = $pp_1, pp_2, ..., pp_c$. P($pp_i, pp_j$) retorna a distância entre $pp_i$ e $pp_j$. CovPP é definida da seguinte forma:

$$\text{CovPP(PP)} = \frac{\sum_{i=1}^{c-1} \sum_{j=(i+1)}^{c} \text{P}(pp_i, pp_j)}{\beta} \quad (2)$$

O valor da cobertura de propriedades de segurança CovPP(PP(P)) é a soma das distâncias conceituais entre pares de propriedades de segurança, dividida pela quantidade de propriedades de segurança que podem ser identificadas no item de avaliação. $\text{CovPP(PP)} \in \mathbb{R} \mid 0 \leq \text{CovPP(PP)} \leq 1$. CovPP = *0* significa que o item de avaliação não cobre nenhuma ou cobre apenas uma propriedade de segurança. Um exemplo do cálculo de CovPP é apresentado na Tabela 4.4 (AI *11.5.2*), resultando no valor *0,101*.

**Tabela 4.4.** Exemplo de cálculo de CovPP

| *Matriz PP (2)* | *AI* | *Entrada PP* | *Cálculos* |
|---|---|---|---|
| $\begin{bmatrix} 0.0 & 0.9 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & 0.0 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.2 \\ - & - & 0.0 & 0.9 & 0.8 & 0.8 & 0.2 & 0.8 & 0.5 & 0.8 & 0.8 \\ - & - & - & 0.0 & 0.2 & 0.2 & 0.8 & 0.6 & 0.5 & 0.8 & 0.4 \\ - & - & - & - & 0.0 & 0.2 & 0.4 & 0.6 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & - & 0.0 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & - & - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.2 \\ - & - & - & - & - & - & - & - & 0.0 & 0.5 & 0.5 \\ - & - & - & - & - & - & - & - & - & 0.0 & 0.2 \\ - & - & - & - & - & - & - & - & - & - & 0.0 \end{bmatrix}$ (2) | *11.5.2* | *00011100100* | *PP: 4,5,6,9*<br><br>*CovPP = 0,2 (4-5) + 0,2 (4-6) + 0,5 (4-9) + 0,2 (5-6) + 0,5 (5-9) + 0,5 (6-9) = 1,2 / 11 = 0,101* |

### (iii) CovLOC – *Local Coverage of Assessment Items* (Cobertura Local de Itens de Avaliação)

O cálculo de CovLOC de um item de avaliação leva em consideração CovDM e CovPP. Considere um item de avaliação AI; CovLOC de AI é definida da seguinte forma:

$$\text{CovLOC(AI)} = \frac{(\text{CovDM} + \text{CovPP})}{2} \tag{3}$$

O valor da Cobertura Local do Item de Avaliação CovLOC (AI) é a média aritmética da soma da Cobertura de Dimensões de Avaliação (CovDM) e da Cobertura de Propriedades de Segurança (CovPP). $\text{CovLOC(AI)} \in \mathbb{R} \mid 0 \leq \text{CovLOC(AI)} \leq 1$. Se $\text{CovDM} = 0$ e $\text{CovPP} = 0$, $\text{CovLOC} = 0$. Um exemplo do cálculo de CovLOC é apresentado na Tabela 4.5 (AI *11.5.2*), resultando no valor *0,337*.

**Tabela 4.5.** Exemplo de cálculo de CovLOC

| *AI* | *Entradas CovDM / CovPP* | *Cálculos* |
|---|---|---|
| *11.5.2* | *CovDM = 0,2 (1-3) + 0,6 (1-4) + 0,9 (1-6) + 0,4 (3-4) + 0,6 (3-6) + 0,2 (4-6) = 2,9 / 6 = 0,483*<br>*CovPP = 0,2 (4-5) + 0,2 (4-6) + 0,5 (4-9) + 0,2 (5-6) + 0,5 (5-9) + 0,5 (6-9) = 1,2 / 11 = 0,101* | *CovLOC = 0,483 + 0,101 = 0,674 / 2 = 0,337* |

### (iv) CovGLO – *Global Coverage of Knowledge Source* (Cobertura Global de uma Fonte de Conhecimento)

Considere uma fonte de conhecimento KS, composta de um conjunto de $n$ itens de avaliação AI; CovGLO de KS é definida da seguinte forma:

$$\text{CovGLO(KS)} = \frac{\sum_{i=1}^{n} \text{CovLOC}(AI)}{n} \tag{4}$$

O valor da Cobertura Global da Fonte de Conhecimento CovGLO(KS) é a média aritmética da soma das coberturas locais (CovLOC) de todos os itens de avaliação da fonte de conhecimento KS. $\text{CovGLO(KS)} \in \mathbb{R} \mid 0 \leq \text{CovGLO(KS)} \leq 1$.

Um exemplo do cálculo de CovGLO é apresentado na Tabela 4.6; são somadas as CovLOCs de todos os AIs de uma KS e o resultado é dividido pela quantidade total de AIs da KS, resultando no valor *0,443*.

**Tabela 4.6.** Exemplo de cálculo de CovGLO

| *KS* | *ID* | *CovLOC* | *CovGLO Cálculos* |
|---|---|---|---|
| *3* | *10.10.1* | *0,742* | |
| *3* | *15.1.3* | *0,742* | CovTOT = Soma AIs = |
| *3* | *13.2.3* | *0,642* | 5,314 / 12 = 0,443 |
| *3* | *15.1.5* | *0,642* | |
| *3* | *9.2.4* | *0,633* | |
| *3* | *14.1.3* | *0,692* | |
| *3* | *15.3.2* | *0,592* | |
| *3* | *10.3.1* | *0,334* | |
| *3* | *13.1.1* | *0,151* | |
| *3* | *7.1.1* | *0,059* | |
| *3* | *10.10.2* | *0,059* | |
| *3* | *10.8.4* | *0,026* | |
| | ***CovGLO*** | ***0,443*** | |

### (v) CovTOT – *Total Coverage of Assessment Design* (Cobertura Total de um Projeto de Avaliação)

Considere um projeto de avaliação (*Assessment Design*) AD, composto por $n$ itens de avaliação selecionados (*Selected Assessment Items*) *SAI*; CovTOT de AD é definida da seguinte forma:

$$\text{CovTOT(AD)} = \frac{\sum_{i=1}^{n} \text{CovLOC}(SAI)}{n} \tag{5}$$

O valor da cobertura total de um projeto de avaliação CovTOT(AD) é a média aritmética da soma das coberturas locais de todos os *SAI* a partir de qualquer das fontes de conhecimento disponíveis na base. $\text{CovTOT(AD)} \in \mathbb{R} \mid 0 \leq \text{CovTOT(AD)} \leq 1$.

Na Tabela 4.7, um exemplo do cálculo de CovTOT é apresentado; são somadas as CovLOCs de todos os AIs de um AD e o resultado é dividido pela quantidade total de AIs do AD, resultando na CovTOT de AD1 = *0,528.*

**Tabela 4.7.** Exemplo de cálculo de CovTOT

| *AD* | *AI* | *KS* | *CovLOC* | *CovTOT Cálculos* |
|---|---|---|---|---|
| 1 | 11.6.2 | 1 | 0,652 | |
| 1 | 12.3.2 | 1 | 0,761 | $\text{CovTOT} = 0{,}652 + 0{,}761 + 0{,}484 +$ |
| 1 | 11.7.1 | 1 | 0,484 | $0{,}411 + 0{,}334 = 2{,}642 \,/\, 5 = 0{,}528$ |
| 1 | 11.5.6 | 1 | 0,411 | |
| 1 | 10.3.1 | 1 | 0,334 | |

## 4.3 CRITÉRIOS DE AVALIAÇÃO DE SEGURANÇA

Critérios de avaliação efetivos são cruciais para avaliar a segurança de forma sistemática. Critérios incluem regras que definem vários aspectos, tais como: como a avaliação de segurança será executada; como selecionar dados de avaliação de segurança; como verificar a qualidade da atividade de avaliação de segurança; e como definir a suficiência dos requisitos de segurança para determinar o final das atividades de avaliação.

A conceituação de critérios de avaliação de segurança se inspira na definição de critérios de teste de software; definições de critérios de teste são encontradas na literatura, tais como parada (Copeland, 2003; Lewis, 2000; Ryber, 2007), adequação (ou de cobertura) (J. Bach, 1997; Burnstein, 2002; Delamaro et al., 2007), seleção (ou geração) (Fantinato, 2002). No contexto deste trabalho, ampliamos o conceito de "critérios de teste" para "critérios de avaliação", incorporando itens de avaliação que não são "testáveis", mas são "verificáveis" ou há a possibilidade de provas formais para eles.

Segundo Ryber (2007), não há uma forma simples de decidir quando um sistema está completamente testado. É consenso na literatura que não existe um único critério que pode ser usado para determinar quando o teste terminou. Para Copeland (2003), há cinco critérios elementares que, juntos, são geralmente usados para decidir quando parar o teste: 1) Atingimos a cobertura definida no projeto; 2) O número de defeitos descobertos é maior que o número definido como meta; 3) O custo de encontrar mais defeitos é maior que a perda estimada causada pelos possíveis defeitos remanescentes; 4) A equipe de projeto chegou à conclusão coletivamente que a versão atual está pronta para ser disponibilizada; e 5) O tomador de decisão deu a ordem para colocar em produção. Lewis (2000) apresenta 4 critérios de parada: 1) O tempo de teste

programado terminou; 2) O número de defeitos programado foi encontrado; 3) Foram executados todos os testes especificados sem detectar qualquer defeito; e 4) Qualquer combinação dos anteriores.

Para Burnstein (2002) os critérios de adequação representam um padrão mínimo para testar um programa. Bach (1997) descreve uma abordagem chamada *Good-Enough Quality*, onde 4 pontos devem ser considerados; alguma coisa é suficientemente de boa qualidade se: 1) Tem benefícios suficientes; 2) Não tem problemas críticos; 3) Os benefícios superam as desvantagens; 4) Na situação em questão, com todas as coisas consideradas, mais testes e melhorias fariam mais mal do que bem.

Existem duas maneiras de selecionar elementos de cada subdomínio de teste: o primeiro é chamado de "teste aleatório" (*random test*) no qual uma grande quantidade de casos de teste é selecionada aleatoriamente, de modo que, probabilisticamente, tem-se uma boa chance de que todos os subdomínios estejam representados no conjunto de teste *T*. O segundo é o "teste de particionamento" (ou "teste de subdomínios"), em que são definidos quais subdomínios serão usados e, em seguida, selecionamos os casos de teste em cada subdomínio. Quanto ao teste de subdomínios, uma questão-chave é como identificar os subdomínios para, então, fazer a seleção de casos de teste. Na prática, certas "regras" são definidas para identificar quando os dados do teste estão ou não no mesmo subdomínio. Em geral, "requisitos de teste" são definidos, por exemplo, para executar uma determinada estrutura de programa. Os dados de teste que satisfazem este requisito pertencem ao mesmo subdomínio. Assim, dependendo da regra, são obtidos diferentes subdomínios, bem como diferentes conjuntos de teste. Essas regras são chamadas de "critério de teste". Um conjunto de testes que satisfaça todos os requisitos de um critério de teste *C*, ou seja, tendo pelo menos um caso de teste para cada subdomínio dado por *C*, dizemos "adequado" para *C* ou "*C*-adequado" (Delamaro et al., 2007).

De um modo geral, um critério de teste é um método ou diretriz que serve para direcionar a atividade de teste ou tomar decisões relativas ao teste; um critério define um conjunto de condições que devem ser utilizadas na atividade de teste. Um critério de teste pode ser utilizado de duas maneiras: i) Critério de seleção (ou de geração) de um conjunto de dados de teste; ii) Critério de adequação (ou de cobertura) para avaliar a qualidade de um conjunto de dados de teste (Fantinato, 2002).

A seleção de itens de avaliação (AIs) de forma não sistemática coloca em questão a qualidade do conjunto de AIs. Um conjunto de AIs selecionados deve revelar a maior quantidade de defeitos do sistema sob avaliação. Para este fim, o conjunto de AIs deve ser selecionado de modo a cobrir o maior número de condições do sistema. Os critérios de avaliação definem os conjuntos de condições que devem ser satisfeitas durante a atividade de avaliação. Para este conjunto de condições a serem verificadas, damos o nome de requisitos de avaliação do critério. Em outras palavras, os critérios de avaliação definem os elementos necessários (requisitos) a serem aplicados na avaliação (Carniello, 2003).

Um critério de avaliação pode ser usado tanto para selecionar AIs quanto para avaliar a qualidade de um conjunto de AIs. A atividade de avaliação da qualidade de um conjunto de AIs consiste em verificar o quanto este conjunto satisfaz determinado critério de avaliação. Portanto, ao usar os critérios de avaliação é possível quantificar a atividade de avaliação e, consequentemente, definir quando terminar essa atividade (Carniello, 2003).

Critérios de avaliação isolados, tais como, "Todos os itens de avaliação de uma norma ou padrão", podem ser adequados para avaliações de conformidade, mas podem ser irrelevantes para encontrar defeitos de segurança importantes em sistemas críticos. Os padrões e normas de segurança disponíveis têm diferentes granulosidades, objetivos, escopos e domínios de aplicação. Portanto, para uma avaliação efetiva é necessário definir novos conjuntos de critérios com alta diversidade e cobertura adequada de características de segurança.

A relação de inclusão estabelece uma ordem parcial entre os critérios, caracterizando uma hierarquia entre eles. Diz-se que um critério $C_1$ inclui um critério $C_2$ se para qualquer programa $P$ e qualquer conjunto de casos de teste $T_1$ $C_1$-adequado, $T_1$ for também $C_2$-adequado e existir um programa $P$ e um conjunto $T_2$ $C_2$-adequado que não seja $C_1$-adequado. Critérios são incomparáveis quando não há parâmetros para comparação ou não seja possível estabelecer relação de inclusão (Rapps & Weyuker, 1985; Weyuker, 1984).

O conjunto de critérios de avaliação de segurança é proposto visando a selecionar ou priorizar AIs para satisfazer um dado requisito de projeto.

Cada critério possui um ou mais dos seguintes objetivos: Escopo de Avaliação, Segurança, Conformidade, e Reuso de Conhecimento. Os principais objetivos

são descritos da seguinte forma: (i) Escopo de Avaliação: obtenção de maior abrangência de avaliação; (ii) Segurança: a maior diversidade das características de segurança; (iii) Conformidade: verificação de todos os itens de avaliação de uma fonte de conhecimento; (iv) Reuso de conhecimento: usar os melhores projetos de avaliação construídos anteriormente. Com estes objetivos em mente, propõem-se os seguintes Critérios de Avaliação de Segurança:

**C-All-KS** – Critério Todas as Fontes de Conhecimento (*All Knowledge Sources Criterion*). Significa selecionar todos os itens de avaliação (AI) de todas as fontes de conhecimento (KS) disponíveis na base. Notar que C-All-KS é o critério mais abrangente, considerando as KSs que estão na base de conhecimento pois, se requer todos os AIs, inclui necessariamente todas as DMs e todas as PPs; pode haver repetição de DMs e de PPs. Todos os outros critérios relacionados a fontes estão incluídos neste critério, ou seja, se C-All-KS é satisfeito, todos os demais critérios são satisfeitos. Este critério é o mais completo, mas requer muito tempo e alto custo de avaliação**.** Quando se tem várias KSs na base de conhecimento, pode-se ter problemas para satisfazer esse critério devido à grande quantidade de AIs. Por exemplo, se a base possui 10 KSs e um projeto de avaliação utiliza 8 KSs, 80% do critério foi satisfeito.

**C-All-AD** – Critério Todos os Projetos de Avaliação (*All Assessment Designs Criterion*). Significa selecionar todas as avaliações (projetos de avaliação – ADs) criadas anteriormente. O principal objetivo deste critério é proporcionar reutilização do conhecimento, usando ADs melhores que revelaram mais defeitos em condições semelhantes. Por exemplo, podemos reutilizar todos os AIs de um AD anterior, que foi bem sucedido em um cenário específico ou adaptá-los para encontrar outras classes de defeito. Dessa forma, se forem usados todos os ADs em um novo projeto de avaliação, o critério foi satisfeito.

**C-All-AI-KS** – Critério Todos os Itens de Avaliação de uma Fonte de Conhecimento (*All Assessment Items of Knowledge Source Criterion*). Significa selecionar todos os itens de avaliação (AIs) de uma fonte de conhecimento (KS) específica. O principal objetivo deste critério é fornecer elementos para verificar a conformidade com uma KS específica. Por exemplo, para verificar a conformidade com ISO/IEC 27001, precisamos usar todos os AIs fornecidos por esta KS.

**C-All-DM-PP** – Critério Todas as Dimensões de Avaliação e Todas as Propriedades de Segurança (*All Assessment Dimensions and Security Properties*

*Criterion*). Significa selecionar fontes de conhecimento (KSs) que, conjuntamente, abordem todas as dimensões de avaliação (DMs) e todas as propriedades de segurança (PPs). Este critério visa a selecionar ou priorizar KSs com AIs que possuam maior escopo de avaliação, abordando todos as dimensões (DMs); e, adicionalmente, tratem de todas as características de segurança (PPs). Por exemplo, se uma KS, considerando seu conjunto de AIs, aborda todas as DMs e todas as PPs, então esta satisfaz o critério; se uma KS, considerando seu conjunto de AIs, aborda 4 de 6 DMs e 7 de 11 PPs, então 64,7% (11/17) do critério foi satisfeito.

**C-All-DM** – Critério Todas as Dimensões de Avaliação (*All Assessment Dimensions Criterion*). Significa selecionar fontes de conhecimento (KSs) de modo que todas as dimensões de avaliação (DMs) sejam abordadas. Por exemplo, se uma KS, considerando seu conjunto de AIs, aborda todas as DMs, então esta satisfaz o critério; se uma KS, considerando seu conjunto de AIs, aborda 5 de 6 DMs, então 83% do critério foi satisfeito.

**C-All-PP** – Critério Todas as Propriedades de Segurança (*All Security Properties Criterion*). Significa selecionar fontes de conhecimento (KSs) de modo que abordem todas as propriedades de segurança (PPs). Por exemplo, se uma KS, considerando seu conjunto de AIs, aborda todas as PPs, então ela satisfaz o critério; se uma KS, considerando seu conjunto de AIs, aborda 4 de 11 PPs, então 36% do critério foi satisfeito.

**C-CombDM** – Critério Combinação de Dimensões de Avaliação (*Combination of Assessment Dimensions Criterion*). Significa selecionar itens de avaliação (AIs) que possuam características específicas relacionadas às dimensões de avaliação (DMs) em combinações k a k (para k variando de 2 a 6). Por exemplo, para k=2, considerando que são 6 dimensões e que suas combinações par a par resultariam em 15 possibilidades, se selecionarmos todas as combinações então o critério foi satisfeito para k=2; se selecionarmos o conjunto de AIs da combinação DM4-DM6, então 6,7% (1/15) do critério foi satisfeito.

**C-CombPP** – Critério Combinação de Propriedades de Segurança (*Combination of Security Properties Criterion*). Significa selecionar itens de avaliação (AIs) que possuam características específicas relacionadas às propriedades de segurança (PPs) em combinações k a k (para k variando de 2 a 11). Por exemplo, para k=2, considerando que são 11 propriedades e que suas combinações par a par

resultariam em 55 possibilidades, se selecionarmos todas as combinações então o critério foi satisfeito para k=2; se selecionarmos o conjunto de AIs da combinação PP4-PP7, então 1,8% (1/55) do critério foi satisfeito.

**C-CombDM-PP** – Critério Combinação de Dimensões de Avaliação e Propriedades de Segurança (*Combination of Assessment Dimensions and Security Properties Criterion*). Significa selecionar itens de avaliação (AIs) que possuam características específicas relacionadas às dimensões de avaliação (DMs) e às propriedades de segurança (PPs) em combinações k a k (para k variando de 2 a 17). Por exemplo, para k=2, considerando que são 6 dimensões e 11 propriedades (17 no total) e que suas combinações par a par resultariam em 136 possibilidades, se selecionarmos todas as combinações então o critério foi satisfeito para k=2; se selecionarmos o conjunto de AIs da combinação DM4-PP7, então 0,73% (1/136) do critério foi satisfeito.

Um critério pode incluir outros critérios; critérios podem ser incomparáveis. Os critérios podem ser divididos em dois grupos: (i) critérios dependentes de fonte: se referem somente a dimensões de avaliação e propriedades de segurança que são abordadas pelas fontes contidas na base; (ii) critérios independentes de fonte: se referem a qualquer dimensão de avaliação e propriedade de segurança, mesmo que estas não sejam abordadas por nenhuma fonte da base. A divisão em dois grupos proporciona independência conceitual, possibilitando a inserção de dimensões de avaliação e propriedades de segurança sem depender dos conteúdos das fontes contidas na base. Na Figura 4.3 apresenta-se a hierarquia de inclusão dos critérios dependentes de fonte propostos.

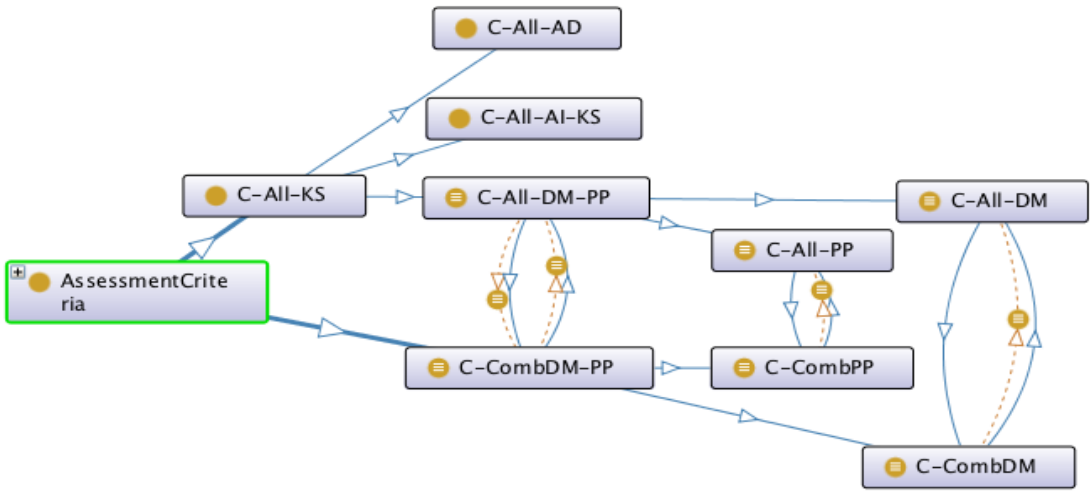


**Figura 4.3.** Hierarquia de inclusão dos critérios dependentes de fonte

Segundo a Figura 4.3, pela própria definição, todos os critérios dependentes de fonte estão incluídos em C-All-KS; se este é satisfeito, C-All-DM-PP é satisfeito, ou seja, todas as KSs da base são usadas e estas abordam todas as DMs e todas as PPs. C-All-KS inclui C-All-AD e C-All-AI-KS. Com relação a C-All-AD, como ADs são compostos de AIs selecionados de KSs, todos os AIs de todos os ADs estão incluídos nas KSs. C-All-KS inclui C-All-AI-KS pois todos os AIs estão incluídos em uma KS e todas as KSs se incluem em C-All-KS. C-All-DM-PP (todas as dimensões e propriedades) inclui C-All-DM (todas as dimensões) e C-All-PP (todas as propriedades). É possível selecionar um conjunto de AIs que aborde todas as dimensões e todas as propriedades sem que seja necessário selecionar todas as KSs. C-All-DM e C-All-PP são incomparáveis pois os elementos requeridos são distintos.

Na Figura 4.4 apresenta-se a hierarquia de inclusão dos critérios independentes de fonte.

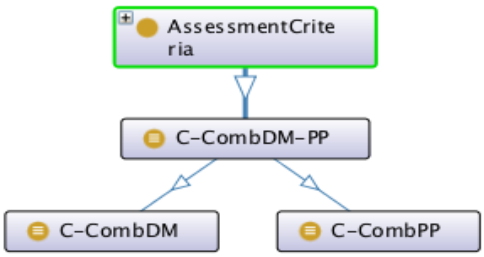


**Figura 4.4.** Hierarquia de inclusão dos critérios independentes de fonte

Segundo a Figura 4.4, pela própria definição, todos os critérios independentes de fonte estão incluídos em C-CombDM-PP; se este é satisfeito, C-CombDM e C-CombPP são satisfeitos, ou seja, todas as combinações de DMs e todas as combinações de PPs são satisfeitas. C-CombDM e C-CombPP são incomparáveis pois os elementos requeridos são distintos. Notar que C-CombDM-PP é equivalente a C-All-DM-PP, ou seja, essa mesma hierarquia de inclusão da Figura 4.4 pode ser inserida na hierarquia dependente de fonte (Figura 4.3), quando são consideradas somente as dimensões e propriedades da base. A mesma observação vale para C-All-DM e C-CombDM, e C-All-PP e C-CombPP.

Na Tabela 4.8 apresenta-se uma síntese dos critérios de avaliação de segurança propostos.

**Tabela 4.8.** Síntese dos Critérios de Avaliação de Segurança

| *Critério* | *Objetivo Principal* | *Síntese* |
|---|---|---|
| C-All-AD | Reuso | Todos os ADs. |
| C-All-AI-KS | Conformidade | Todos os AIs de uma KS. |
| C-All-DM | Escopo | Todas as DMs são abordadas na KS. |
| C-All-PP | Segurança | Todas as PPs são abordadas na KS. |
| C-All-DM-PP | Escopo + Segurança | Todas as DMs e todas as PPs são abordadas na KS. |
| C-All-KS | Todos | Todas as KS. |
| C-CombDM | Escopo | Todos os AIs, considerando combinações de DMs requeridas. |
| C-CombPP | Segurança | Todos os AIs, considerando combinações de PPs requeridas. |
| C-CombDM-PP | Escopo + Segurança | Todos os AIs, considerando combinações DM-PP requeridas. |

## 4.4 HEURÍSTICAS DE AVALIAÇÃO DE SEGURANÇA

Heurísticas são processos utilizados para obter a solução de um problema sem garantir que esta solução seja a ótima. As heurísticas são métodos para resolução de problemas; o raciocínio heurístico é bom em si, mas não se pode vendê-lo como sendo adequado para provas rigorosas (Polya, 1945). Segundo (Rothermel, Untch, Chu, & Harrold, 1999), as técnicas de priorização de casos de teste (itens de avaliação) são tipicamente heurísticas.

Tinkham & Kaner (2003) discutem o papel das heurísticas no contexto da avaliação exploratória de software. Segundo os autores, toda decisão de um avaliador é tomada sob condições de incerteza e conhecimento insuficiente. Por isso, todas as decisões têm alguma probabilidade de serem incorretas, e essa probabilidade significa que não podemos escolher mecanicamente a próxima coisa a ser feita. Em vez disso, uma vez que cada decisão traz um elemento de risco, passamos às heurísticas. Heurísticas são ferramentas que as pessoas usam para ajudá-los na tomada de decisões.

As heurísticas são diretrizes que nos ajudam a esclarecer ou a resolver um problema. São diretrizes, mas são ***apenas*** diretrizes. Nenhuma heurística é garantida ser aplicável em todas as situações, e uma heurística que funcionou muito bem em uma situação pode não funcionar em outra, ou até piorar em alguns casos. Cabe ao interessado avaliar as heurísticas que considera utilizar para determinar se uma determinada heurística é apropriada para sua situação atual. Mesmo o processo de avaliação de uma heurística para sua aplicabilidade pode ser um processo extremamente útil para ajudar um avaliador a pensar sobre o que ele está tentando

alcançar de diferentes ângulos e talvez ajudá-lo a encontrar uma boa solução para o problema em questão (Tinkham & Kaner, 2003).

No contexto deste trabalho, o termo "Heurística de Avaliação" engloba heurísticas de teste e de verificação. Heurísticas são sempre aproximações, para máximo, para mínimo, para melhor, para pior, etc. e não têm a pretensão de garantir que todas as condições estão satisfeitas. Por exemplo, selecionar os 10 melhores itens de avaliação (AIs) com base em uma medida de cobertura, não garante que não existam conjuntos menores que sejam tão bons quanto esse conjunto, ou ainda que certos conjuntos de 10 itens de avaliação não sejam melhores.

Nesta seção um conjunto de heurísticas de avaliação de segurança é proposto com o objetivo principal de usar medidas de cobertura para selecionar AIs para compor projetos de avaliação.

Cada heurística é uma aproximação para um objetivo. As heurísticas propostas possuem os objetivos de selecionar ou priorizar: (i) *n* melhores AIs, considerando CovDM; (ii) *n* melhores AIs, considerando CovPP; (iii) *n* melhores AIs considerando CovLOC; (iv) *n* melhores KSs considerando CovGLO; (v) *n* melhores ADs (AIs selecionados) considerando CovTOT; (vi) *n* melhores AIs, considerando coberturas (CovDM, CovPP ou CovLOC) acima da média; (vii) n melhores AIs, considerando maior cobertura com menor quantidade de AIs; (viii) n melhores AIs, considerando CovDM e CovPP ao mesmo tempo.

Com estes objetivos em mente, propõem-se as seguintes Heurísticas de Avaliação de Segurança:

**H-CovDM** – Heurística Cobertura de Dimensões de Avaliação (*Coverage of Assessment Dimensions Heuristics*). Visa a selecionar ou priorizar itens de avaliação (AIs) que possuem maior diversidade na cobertura das dimensões de avaliação (CovDM). Esta heurística é uma aproximação ao objetivo de identificar os *n* AIs que cubram a maior quantidade de dimensões da avaliação (DMs), abordando pelo menos um par de DMs com maior distância entre si. Diferentemente dos critérios C-All-DM-PP e C-All-DM, que se apoiam na identificação ou não de DMs nos AIs (*1* ou *0;* aborda ou não-aborda), H-CovDM se apóia na medida de Cobertura de Dimensões (CovDM); esta cobertura baseia-se na diversidade do AI. Ou seja, se o AI aborda somente uma DM, o valor de cobertura será *0,* mas se trata de mais de uma DM, seu valor de cobertura dependerá das distâncias entre DMs (Matrizes de Adjacências). Dessa forma, quanto

maior a distância, maior a diversidade e, consequentemente, maior valor de cobertura. Exemplo de uso da heurística: "Selecionar os 10 melhores AIs, considerando CovDM". Neste caso, haveria uma nota de corte e os 10 AIs com maiores valores de CovDM seriam selecionados. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a diversidade de dimensões de avaliação.

**H-CovPP** – Heurística Cobertura de Propriedades de Segurança (*Coverage of Security Properties Heurístic*). Visa a selecionar ou priorizar itens de avaliação (AIs) que possuem maior diversidade na cobertura de propriedades de segurança (CovPP). Esta heurística é uma aproximação ao objetivo de identificar os *n* AIs que possuem maior abrangência em relação às propriedades de segurança (PPs), abordando pelo menos um par de PPs com maior distância entre si. Diferentemente dos critérios C-All-DM-PP e C-All-PP, que se apoiam na identificação ou não de PPs nos AIs (*1* ou *0;* aborda ou não-aborda), H-CovPP se apoia no cálculo de cobertura de propriedades (CovPP); esta cobertura baseia-se na diversidade do AI. Ou seja, se o AI aborda somente uma PP, o valor de cobertura será *0,* mas se trata de mais de uma PP, seu valor de cobertura dependerá das distâncias entre PPs (Matriz de Adjacências). Dessa forma, quanto maior a distância, maior a diversidade e, consequentemente, maior valor de cobertura. Exemplo de uso da heurística: "Selecionar os 10 melhores AIs, considerando CovPP". Neste caso, haveria uma nota de corte e os 10 AIs com maiores valores de CovPP seriam selecionados. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a diversidade de propriedades de segurança.

**H-CovLOC** – Heurística Cobertura Local (*Local Coverage Heurístic*). Visa a selecionar ou priorizar Itens de Avaliação (AIs) que possuam uma média melhor da soma de CovDM e CovPP (ou seja, CovLOC). Esta heurística é uma aproximação ao objetivo de identificar os *n* AIs que possuem valores mais altos de CovDM e CovPP, considerando a média. Considere 3 AIs (a, b e c) com os seguintes valores: (a) CovDM=*0,450*, CovPP=*0,450*, então CovLOC=*0,450*. (b) CovDM=*0,900*, CovPP=*0,0*, então CovLOC=*0,450*. (c) CovDM=*0,450*, CovPP=*0,800*, então CovLOC=*0,625*. Neste caso, AI (c) será selecionado ou priorizado. Exemplo de uso da heurística: "Selecionar os 10 melhores AIs, considerando CovLOC". Neste caso, haveria uma nota de corte e os 10 AIs com maiores valores de CovLOC seriam selecionados. Neste contexto, não é

garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a diversidade de dimensões de avaliação e de propriedades de segurança na média.

**H-CovGLO** – Heurística Cobertura Global (*Global Coverage Heurístic*). Visa a selecionar ou priorizar uma fonte de conhecimento (KS) que possua uma média melhor da soma das CovLOCs de todos os seus itens de avaliação (AIs). Esta heurística é uma aproximação ao objetivo de identificar as *n* KSs que possuem valores mais altos de CovGLO. Exemplo de uso da heurística: "Selecionar as 2 melhores KSs, considerando CovGLO". Neste caso, as 2 KSs com maiores valores de CovGLO seriam selecionadas. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a média das CovLOC de cada uma das KSs (CovGLO) da base.

**H-CovTOT** – Heurística Cobertura Total (*Total Coverage Heuristics*). Visa a selecionar ou priorizar projetos de avaliação (ADs) que possuam valores mais elevados de CovTOT. Sabendo que um AD é composto por AIs selecionados (SAIs) das KSs, esta heurística é uma aproximação ao objetivo de identificar os *n* ADs que possuam, em seu conjunto de AIs, uma média melhor da soma das CovLOCs (CovTOT). Exemplo de uso da heurística: "Selecionar os 2 melhores ADs, considerando CovTOT". Neste caso, os 2 ADs com maiores valores de CovTOT seriam selecionadas. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a média das CovLOC de cada um dos ADs (CovTOT) da base. Esta heurística pode ser interessante, por exemplo, quando se deseja reusar projetos que se mostraram eficientes em um determinado contexto. Além disso, ADs experimentadas e robustas podem ser candidatas a se tornarem KSs.

**H-AboveAvg** – Heurística Acima da Média (*Above Average Heuristics*). Visa a selecionar ou priorizar itens de avaliação (AIs) que estão acima da média, considerando CovDM, CovPP ou CovLOC de todos os AIs de uma fonte de conhecimento (KS) específica. Esta heurística é uma aproximação ao objetivo de identificar os *n* AIs que possuam valores mais altos de cobertura, considerando como linha de corte a média de uma das coberturas (CovDM, CovPP ou CovLOC). Exemplos de uso da heurística: "Selecionar todos os AIs com valores de CovDM acima da média"; "Selecionar todos os AIs com valores de CovPP acima da média"; "Selecionar os 5 melhores AIs com valores de CovDM, CovPP e CovLOC acima da média". Nestes casos, AIs com maiores valores de

cobertura seriam selecionadas. Neste contexto, não é garantido que os conjuntos resultantes sejam os melhores conjuntos possíveis, mas sim que estes são conjuntos que se apresentam como eficientes com base nas coberturas (CovDM, CovPP ou CovLOC) e considerando a média como nota de corte. Esta heurística pode ser interessante, por exemplo, quando se deseja criar projetos que, considerando a média, se mostraram eficientes em um determinado contexto.

**H-ParetoPercentage** – Heurística Pareto Porcentagem (*Pareto Percentage Heuristics*). Visa a selecionar ou priorizar itens de avaliação (AIs) que possuam melhor cobertura local (CovLOC). Esta heurística é uma aproximação ao objetivo de identificar um conjunto pequeno de *n* AIs para, ao mesmo tempo, atingir uma certa porcentagem de abrangência. Em outras palavras, procura-se melhores resultados de abrangência com menos esforço (número de AIs a serem usados). Exemplos de uso da heurística: "Selecionar os AIs que representam 30% da soma das CovLOC de uma KS"; "Selecionar todos os AIs até o ponto ótimo da soma das CovLOC de uma KS". Nestes casos, os AIs com maiores valores de CovLOC seriam selecionados. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um conjunto que se apresenta como eficiente considerando a soma de todas as CovLOC de uma KS da base.

**H-ParetoFrontier** – Heurística Fronteira de Pareto (*Pareto Frontier Heuristics*). Visa a selecionar ou priorizar melhores AIs, considerando CovDM e CovPP. Segundo Barr (2012), Eficiência Pareto é um estado de alocação de recursos em que é impossível realocá-los tal que a situação de qualquer participante seja melhorada sem piorar a situação individual de outro participante. Quando não há nenhuma solução *z* que domina *x*, ela é dita uma solução não-dominada. O conjunto das soluções não-dominadas para um determinado problema é chamado de conjunto Pareto-ótimo e o conjunto de todos os vetores objetivos não-dominados é chamado de Fronteira de Pareto. Esta heurística é uma aproximação da Fronteira de Pareto, com o objetivo de identificar um conjunto de *n* AIs que apresenta melhores CovDM e CovPP ao mesmo tempo (Bi-objetivo). Exemplos de uso da heurística: "Selecionar os AIs com CovDM e CovPP $>$ *0*"; "Selecionar os AIs com CovDM e CovPP $>$ *0,400*"; "Selecionar os AIs com CovDM $>$ *0,200* e CovPP $>$ *0,350*". Nestes casos, os AIs que apresentam maiores valores de CovDM e CovPP ao mesmo tempo seriam selecionados. Neste contexto, não é garantido que o conjunto resultante seja o melhor conjunto, mas sim que este é um

conjunto que se apresenta como eficiente considerando os valores de pares CovDM e CovPP de uma demandada KS da base.

Na Tabela 4.9 apresenta-se uma síntese da proposta de heurísticas de avaliação de segurança.

**Tabela 4.9.** Síntese das Heurísticas de Avaliação de Segurança

| *Heurística* | *Objetivo* |
|---|---|
| H-CovDM | *n* melhores AIs, considerando CovDM. |
| H-CovPP | *n* melhores AIs, considerando CovPP. |
| H-CovLOC | *n* melhores AIs considerando CovLOC. |
| H-CovGLO | *n* melhores KSs considerando CovGLO. |
| H-CovTOT | *n* melhores ADs (AIs selecionados) considerando CovTOT. |
| H-AboveAvg | *n* melhores AIs, considerando coberturas (CovDM, CovPP ou CovLOC) acima da média. |
| H-ParetoPercentage | *n* melhores AIs, considerando maior cobertura com menor quantidade de AIs. |
| H-ParetoFrontier | *n* melhores AIs, considerando CovDM e CovPP ao mesmo tempo. |

## 4.5 PROTÓTIPO DE SOFTWARE

Um protótipo de software com dois aplicativos foi desenvolvido com o objetivo de validar a abordagem proposta. Os aplicativos calculam a cobertura e possibilitam a seleção de itens de avaliação com base em critérios e heurísticas de avaliação de segurança. Eles estão disponíveis para download no GitHUB (Rosa, Jino, & Teixeira Junior, 2017a).

O primeiro aplicativo (back-end), recebe listas contendo itens de avaliação (AIs) e suas dimensões de avaliação e propriedades de segurança e calcula as coberturas dos AIs. O segundo aplicativo (front-end) fornece a interface gráfica e permite a visualização de informações para seleção dos itens de avaliação durante a geração do projeto de avaliação.

**Aplicativo 1.** O algoritmo de cálculo de cobertura, desenvolvido em ANSI C, considera a diversidade de características de segurança e dimensões de avaliação presentes no itens de avaliação de segurança e visa a fornecer as principais medidas de cobertura usadas na abordagem, a saber: (i) CovDM; (ii) CovPP; e (iii) CovLOC. Então, CovGLO e CovTOT são calculados posteriormente a partir das coberturas básicas.

Apresentamos o algoritmo do cálculo de coberturas por meio de uma descrição em formato "Entrada-Processamento-Saída". Posteriormente, apresentamos partes do código-fonte desenvolvido com comentários (Tabela 4.13).

**Entrada**. Para cada item de avaliação (AI), a função recebe listas de dimensões de avaliação (DM) e propriedades de segurança (PP), no seguinte formato: "*010111*" (palavra de seis caracteres – DM) e "*01011101001*" (palavra de onze caracteres – PP). Cada caractere (*0* ou *1*) significa se o AI aborda (*1*) ou não (*0*) uma DM ou uma PP específica. Por exemplo, "*100110*" significa que as DMs *1*, *4*, e *5* são abordadas pelo AI; "*01101001011*" significa que as PPs *2*, *3*, *5*, *8*, *10*, e *11* são abordados pelo AI.

**Processamento**. Para cada Item de Avaliação (AI), leia as matrizes de adjacências; selecione as distâncias entre pares de AD e PP; calcule a soma das distâncias; calcule a média das distâncias; calcule CovDM e CovPP; calcule a soma de CovDM e CovPP e obtenha sua média; e calcule CovLOC para o AI. Por exemplo, na Tabela 4.10 apresentamos as entradas de dois itens de avaliação (*6.1.5* e *11.5.2*).

**Tabela 4.10.** Exemplos de Entradas e Atribuições (DM e PP)

| *AI* | *Entrada DM / PP* | *Atribuições DM / PP* |
|---|---|---|
| *6.1.5* | *101000 / 00100010100* | *DM: 1,3 / PP: 3,7,9* |
| *11.5.2* | *101101 / 00011100100* | *DM: 1,3,4,6 / PP: 4,5,6,9* |

As distâncias par-a-par das dimensões e propriedades entre si são lidas em duas matrizes de adjacência, a saber: distâncias entre dimensões de avaliação (Matriz 1) e distâncias entre propriedades de segurança (Matriz 2). Posteriormente, as coberturas são calculadas conforme apresentado na Tabela 4.11 (AI *11.5.2*).

**Tabela 4.11.** Exemplo de cálculo de coberturas para o AI 11.5.2

| *Matrizes DM (1) e PP (2)* | *AI* | *Entradas DM / PP* | *Cálculos* |
|---|---|---|---|
| $\begin{bmatrix} 0.0 & 0.5 & 0.2 & 0.6 & 0.7 & 0.9 \\ - & 0.0 & 0.9 & 0.7 & 0.6 & 0.8 \\ - & - & 0.0 & 0.4 & 0.2 & 0.6 \\ - & - & - & 0.0 & 0.5 & 0.2 \\ - & - & - & - & 0.0 & 0.8 \\ - & - & - & - & - & 0.0 \end{bmatrix}$ (1)<br><br>$\begin{bmatrix} 0.0 & 0.9 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & 0.0 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.2 \\ - & - & 0.0 & 0.9 & 0.8 & 0.8 & 0.2 & 0.8 & 0.5 & 0.8 & 0.8 \\ - & - & - & 0.0 & 0.2 & 0.2 & 0.8 & 0.6 & 0.5 & 0.8 & 0.4 \\ - & - & - & - & 0.0 & 0.2 & 0.4 & 0.6 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & - & 0.0 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & - & - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.2 \\ - & - & - & - & - & - & - & - & 0.0 & 0.5 & 0.5 \\ - & - & - & - & - & - & - & - & - & 0.0 & 0.2 \\ - & - & - & - & - & - & - & - & - & - & 0.0 \end{bmatrix}$ (2) | *11.5.2* | *101101 \| 0001110010 0* | *DM: 1,3,4,6 \| PP: 4,5,6,9*<br><br>*CovDM = 0,2 (1-3) + 0,6 (1-4) + 0,9 (1-6) + 0,4 (3-4) + 0,6 (3-6) + 0,2 (4-6) = 2,9 / 6 = 0,483*<br><br>*CovPP = 0,2 (4-5) + 0,2 (4-6) + 0,5 (4-9) + 0,2 (5-6) + 0,5 (5-9) + 0,5 (6-9) = 1,2 / 11 = 0,101*<br><br>*CovLOC = 0,483 + 0,101 = 0,674 / 2 = 0,337* |

**Saída**. Retorna CovDM, CovPP e CovLOC. Como exemplo de saída do algoritmo, a Tabela 4.12 apresenta os valores de saída das coberturas calculados para os AIs *6.1.5* e *11.5.2*.

**Tabela 4.12.** Exemplo de saída: retorno das coberturas para os AIs 6.1.5 e 11.5.2

| *AI* | *Entrada (DM & PP)* | *Saída (CovDM;CovPP;CovLOC)* |
|---|---|---|
| *6.1.5* | *10100000100010100* | *0,033; 0,109; 0,071* |
| *11.5.2* | *10110100011100100* | *0,483; 0,191; 0,337* |

Na Tabela 4.13 o algoritmo para cálculo de coberturas é apresentado.

**Tabela 4.13.** Algoritmo para cálculo de coberturas

| ***CÁLCULO DE COBERTURAS*** | |
|---|---|
| **Require:** $List_{DM}$; $List_{PP}$; $Mat_{DM}$; $Mat_{PP}$ | *Assessment Dimensions (DM) Security Properties (PP);* |
| **ENSURE:** $Coverage \leftarrow Cov_{DM} \cdot Cov_{PP} \cdot Cov_{LOC}$ | *Coverage of Assessment Dimensions ($Cov_{DM}$), Coverage of Security Properties ($Cov_{PP}$), Local Coverage of the Assessment Item ($Cov_{LOC}$)* |
| **Begin** | |
| $SumDist_{DM} \leftarrow$ sumDist($List_{DM}$, $Mat_{DM}$, $Mat_{PP}$) | *Sum the distances of DM and PP* |
| $SumDist_{PP} \leftarrow$ sumDist($List_{PP}$, $Mat_{DM}$, $Mat_{PP}$) | |
| $MAX_{DM} \leftarrow$ Max Value of $List_{DM}$ | |
| $MAX_{PP} \leftarrow$ Max Value of $List_{PP}$ | |
| $Cov_{DM} \leftarrow$ CovCalc($SumDist_{DM}$, $MAX_{DM}$) | *Calculate the coverage* |
| $Cov_{PP} \leftarrow$ CovCalc ($SumDist_{PP}$, $MAX_{PP}$) | |
| $Cov_{LOC} \leftarrow$ CovCalc (($Cov_{DM}$+$Cov_{PP}$), 2) | |
| **return** $Cov_{DM} \cdot Cov_{PP} \cdot Cov_{LOC}$ | *Return the concatenated coverage values* |
| **End** | |
| ***SUMDIST*** | |
| **Require:** $List_x$ ; $Mat_{DM}$; $Mat_{PP}$ | *List for selected items, Adjacency matrixes* |
| **ENSURE:** $Sum_{Dist} \leftarrow \sum Adj_{XX}[i,j]$ for the selected item | *Sum of the adjacency matrix values* |
| **Begin** | |
| $Len_{List} \leftarrow$ length($List_x$) | |
| $Sum_{Dist} \leftarrow 0.0$ | |
| **for each** $L_i \in List_x$ **do** | *Read the adjacency matrices and sum the distances* |
| **if** ($L_i$ = True) **then** | |
| **for** j=0 **to** j< $Len_{list}$ **do** | |
| **if** ($Len_{list}$ = 6 ) **do** | *Actual number of DM* |
| **if** ($Mat_{DM}[i,j]$ > 0.0 **and** $List_x[j]$ = 1 ) **then** | |
| $Sum_{Dist} \leftarrow Sum_{Dist} + Mat_{DM}[i,j]$ | |
| **end if** | |
| **else** | |
| **if** ($Mat_{PP}[i,j]$ > 0.0 **and** $List_x[j]$ = 1 ) **then** | |
| $Sum_{Dist} \leftarrow Sum_{Dist} + Mat_{PP}[i,j]$ | |
| **end if** | |
| **end if** | |
| **end if** | |
| **end for** | |
| **return** $Sum_{Dist}$ | *Returns sum of distances for DM and PP* |
| **End** | |
| ***COVCALC*** | |
| **Require:** $SumDist_{XX}$; $MAX_{XX}$ | *Sum of distances matrixes and list max values* |
| **ENSURE:** $Cov_{XX}$ | *Coverage for DM, PP or LOC* |
| **Begin** | |
| $Cov_{XX} \leftarrow 0.0$ | *The coverage calculation function* |
| **if** ($SumDist_{XX}$ = 0.0) **then return** $Cov_{XX}$ | |
| **end if** | |
| $Cov_{XX} \leftarrow SumDist_{XX}$ / $MAX_{XX}$ | |
| **if (**$Cov_{XX}$ >= 1.0**) then return** 1.0 | |
| **else return** $Cov_{XX}$ | |
| **end if** | |
| **End** | |

**Aplicativo 2.** O segundo aplicativo (front-end), desenvolvido em C#, visa a apoiar o processo de construção dos projetos de avaliação, permitindo a aplicação de conjuntos de critérios de avaliação de segurança de forma estruturada. Primeiro, o engenheiro se autentica no sistema e as fontes de conhecimento são carregadas com os itens de avaliação; depois de escolher uma fonte de conhecimento, selecionamos itens de avaliação, com base em critérios de seleção definidos. Na Figura 4.5, apresentamos uma tela do aplicativo front-end.

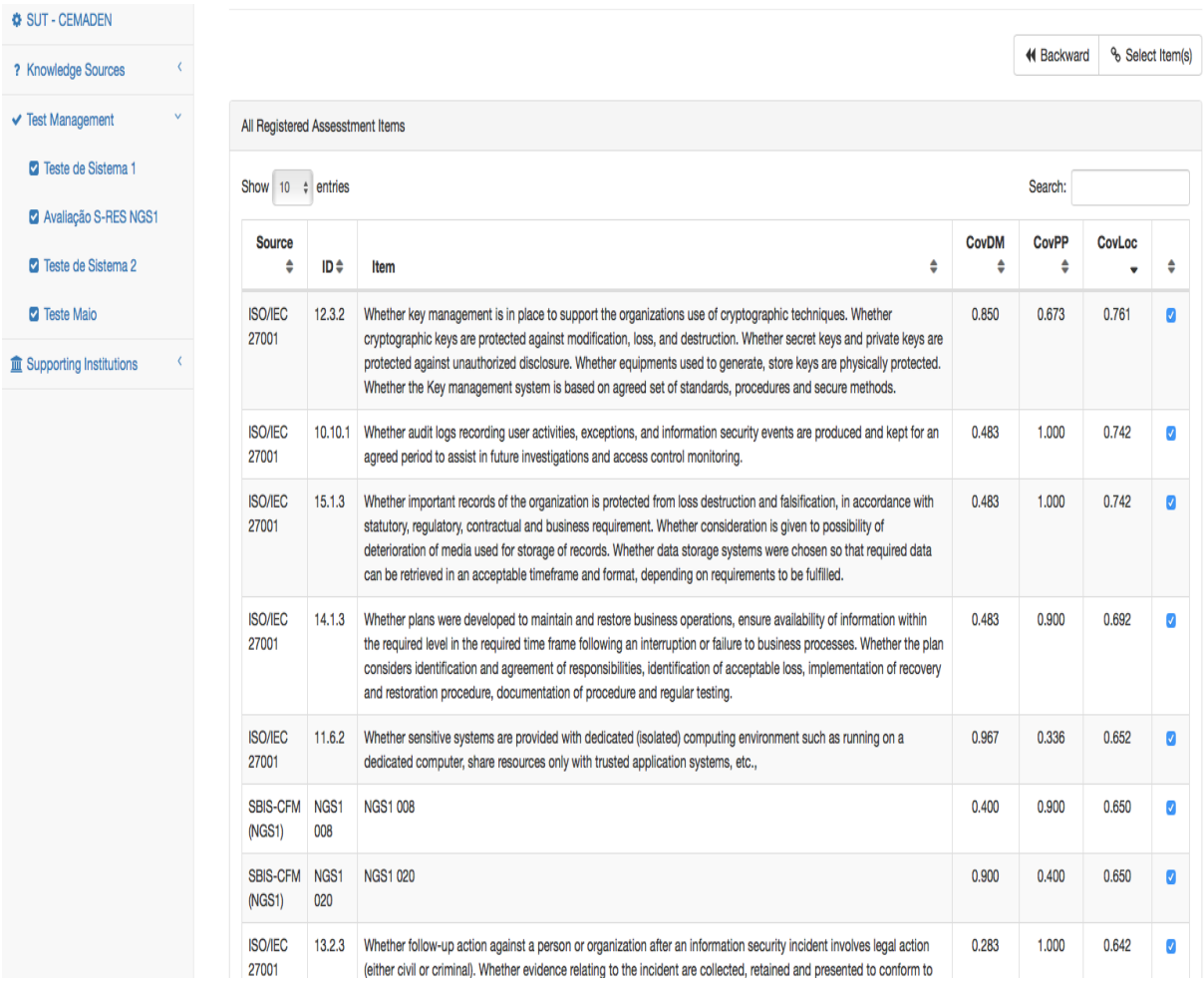


**Figura 4.5.** Protótipo de Software – Parte do *Front-end*

Podemos selecionar itens de avaliação (AIs) disponíveis por cobertura (CovDM, CovPP ou CovLOC). Por exemplo, depois de selecionar AIs de uma fonte de conhecimento (KS), podemos selecionar outros AIs de outras KSs para adicionar ao projeto de avaliação (AD), com base em sua Cobertura Total (CovTOT).

## 4.6 CONSIDERAÇÕES FINAIS

Neste capítulo foi apresentada a abordagem para seleção e análise de itens de avaliação de segurança (HCApp-Sec). HCApp-Sec baseia-se em critérios e heurísticas de avaliação e visa a aumentar a cobertura das dimensões de avaliação e propriedades de segurança nos projetos de avaliação. A abordagem faz uso de formalização conceitual, por meio de uma ontologia (SecAOnto) em avaliação de segurança para: (i) descrever os conceitos principais utilizados; e (ii) apresentar as distâncias entre propriedades e dimensões usadas no cálculo de cobertura. HCApp-Sec pode ser aplicada a qualquer fonte de conhecimento de segurança para selecionar ou priorizar itens de avaliação em relação a, inicialmente, 11 propriedades de segurança e 6 dimensões de avaliação; é possível incorporar novas dimensões e propriedades, bastando apenas formalizar conceitualmente e propor suas distâncias em relação às outras já existentes, atualizando as matrizes de adjacências. Conjuntos de critérios e heurísticas de avaliação são propostos para apoiar a geração de projetos de avaliação com cobertura assegurada de características de segurança.

No próximo capítulo uma prova de conceito é apresentada. O objetivo principal foi aplicar a abordagem proposta (HCApp-Sec) e verificar se é possível selecionar e analisar itens de avaliação para compor projetos de avaliação. Primeiramente, uma fonte de conhecimento (*Knowledge Source* – KS) de segurança foi selecionada; a seleção se deu entre fontes mapeadas bem aceitas na área de segurança da informação, que são consideradas *a priori* mais apropriados para aplicar a abordagem. Então, aplicamos a abordagem à KS selecionada, por meio do uso dos critérios e das heurísticas propostos. Os resultados obtidos são analisados para todos os critérios e heurísticas.

# 5 PROVA DE CONCEITO: SELEÇÃO E ANÁLISE DE ITENS DE AVALIAÇÃO DE SEGURANÇA COM HCAPP-SEC

*"No amount of experimentation can ever prove me right; a single experiment can prove me wrong."*

*Albert Einstein*

Uma prova de conceito foi elaborada para ilustrar a aplicação de HCApp-Sec. As seções seguintes descrevem os passos da prova de conceito:

5.1) Mapeamento de fontes de conhecimento de segurança;

5.2) Seleção da fonte de conhecimento para aplicação;

5.3) Atribuição de dimensões de avaliação e propriedades de segurança para a ISO/IEC 27001 (KS1);

5.4) Cálculo de coberturas para a ISO/IEC 27001 (KS1);

5.5) Seleção e análise de itens de avaliação a partir dos critérios e heurísticas do Capítulo 4.

## 5.1 MAPEAMENTO DE FONTES DE CONHECIMENTO DE SEGURANÇA

Para que projetos de avaliação de qualidade sejam gerados, é crucial encontrar as melhores fontes de itens de avaliação e entender seus objetivos principais e seus formatos de disponibilização.

Para isso, um mapeamento de fontes de conhecimento de segurança foi conduzido. Fontes bem conhecidas foram consideradas candidatas para ser usadas na prova de conceito para compor a base de conhecimento e exercitar a abordagem proposta.

No Apêndice E apresenta-se uma descrição das fontes de conhecimento mapeadas, detalhando conteúdo, objetivo, idioma e formato de seus itens de avaliação. Devido às lógicas de construção serem bastante distintas, alguns requisitos, por exemplo, possibilitar a inclusão de sub-itens, foram identificados para que as fontes sejam incorporadas à base de conhecimento. As fontes (BACEN, 2017; Brasil, 2015; Colombo, 2014), onde o requisito para inclusão na base foi satisfeito, ainda não foram incorporadas à base devido ao idioma ser diferente do da ontologia (inglês); a fonte *Common Criteria* (ISO/IEC, 2008a, 2008b, 2009) será a próxima fonte a ser inserida e avaliada em trabalho futuro.

Na Tabela 5.1 apresenta-se uma síntese do mapeamento de fontes de conhecimento de segurança.

**Tabela 5.1.** Síntese do mapeamento de fontes de conhecimento de segurança

| *Fonte de Conhecimento* | *Objetivo Principal* | *Requisito Satisfeito* | *Incorporado à Base* | *Observações* |
|---|---|---|---|---|
| ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components (ISO/IEC, 2008a, 2008b, 2009) | Avaliação de Produtos Eletrônicos (Hardware e Software) | SIM | NÃO | |
| MITRE *Ten Strategies of a World-Class Cybersecurity Operations Center* (MITRE, 2017) | Estratégias para operação de CSOC (Centro de Operações de Segurança) | NÃO | NÃO | |
| OWASP *Open Web Application Security Project Testing Guide* (OWASP, 2008) | Identificação de Vulnerabilidades em Sistemas Web | NÃO | NÃO | |
| SANS *Critical Security Controls for Effective Cyber Defense* (The SANS Institute, 2015) | Avaliação de Segurança de Software | NÃO | NÃO | |
| ISO/IEC 27001 (ISO/IEC, 2013a) | Avaliação de Segurança | SIM | SIM | |
| SBIS/CFM MOEA Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) (Giulliano et al., 2014) | Avaliação de Software Médico (Registro Eletrônico de dados de pacientes) | SIM | SIM | Parte trata de segurança da informação (2 níveis). Baseado no HIPAA (U.S. Department of Health & Human Services, 2015) |
| *Payment Card Industry Data Security Standard* (PCI/DSS) (PCI Security Standards Council, 2015) | Requisitos e procedimentos da avaliação de segurança de dispositivos de pagamentos com cartão | NÃO | NÃO | |
| FIPS (NIST) *Security Requirements For Cryptographic* | Requisitos para módulos | NÃO | NÃO | |

| *Fonte de Conhecimento* | *Objetivo Principal* | *Requisito Satisfeito* | *Incorporado à Base* | *Observações* |
|---|---|---|---|---|
| *Modules* (140-2) (NIST, 2017a) | criptográficos | | | |
| SOX *Sarbanes-Oxley Act Audit Checklist* (Addison-Hewitt Associates, 2015) | Lista de verificação para auto-avaliação de auditoria da Lei SOX | NÃO | NÃO | |
| *Cybersecurity Capability Maturity Model* (C2M2) (Energy, 2017) | Modelo de Maturidade de Segurança | NÃO | NÃO | |
| BACEN/STN Manual de Segurança da RSFN (BACEN, 2017) | Requisitos de Segurança para redes de dados bancários | SIM | NÃO | |
| SLTI/MPOG ePing-Security (Brasil, 2015) | Segurança para Interoperabilidade em Governo | SIM | NÃO | |
| *Consensus Assessments Initiative Questionnaire* (CSA/CAIQ) (CSA, 2015) | Avaliação de Segurança para ambientes de *Cloud Computing* | NÃO | NÃO | |
| MED-Sec-AWA Checklist (Colombo, 2014) | Medida de Segurança da Informação para Aplicações Web | SIM | NÃO | |

## 5.2 SELEÇÃO DA FONTE DE CONHECIMENTO

ISO/IEC 27001 (ISO/IEC, 2013a) foi escolhida para ser usada na prova de conceito (*Knowledge Source* 1 – KS1), devido aos seguintes fatores:

- **Simplicidade** – Apresenta itens de avaliação no formato de lista de verificação (*Checklist*). Salvaguardas e itens de verificação desta fonte são chamadas de *controles* neste padrão;
- **Adequação** – Foi escrito em língua inglesa e é usado em todo o mundo de forma prática por especialistas em segurança. É possível identificar e atribuir as dimensões de avaliação e as propriedades de segurança propostas na abordagem nos itens de avaliação. Também é possível aplicar todos os critérios de avaliação propostos. Além disso, o formato atual da base de conhecimento aceita a forma de apresentação dos itens de avaliação sem modificações;
- **Maturidade** – Foi construída por especialistas em segurança da informação e pode ser avaliada em relação às características de segurança e escopo de avaliação;
- **Objetividade** – Tem um objetivo claro, ou seja, está focado em avaliar a segurança de sistemas e processos;
- **Diversidade e Complementaridade** – Tem uma base eclética, ou seja, possui um conjunto de itens de avaliação diversificado e complementar.

O principal objetivo de KS1 é apoiar especialistas em segurança e consultores de padrões nos processos de avaliação, certificação ou auditoria.

KS1 possui uma tabela contendo itens de avaliação, conforme exemplo a seguir:

> 11.3.1 – "*Whether there are any security practice in place to guide users in selecting and maintaining secure password*".

O objetivo deste AI é verificar se a organização orienta os usuários na seleção e manutenção de senhas seguras.

## 5.3 ATRIBUIÇÃO DE DIMENSÕES DE AVALIAÇÃO E PROPRIEDADES DE SEGURANÇA PARA ISO/IEC 27001 (KS1)

Aplicamos HCApp-Sec à KS1 e obtivemos as coberturas para seus 133 Itens de Avaliação (AIs). Primeiramente, verificamos quais Dimensões de Avaliação (DM) e Propriedades de Segurança (PP) foram abordadas por todos os AIs de KS1.

Na Tabela 5.2, apresenta-se extrato do conjunto de dados de KS1, incluindo na terceira coluna as dimensões de avaliação (seis caracteres iniciais) e as propriedades de segurança (últimos 11 caracteres) abordadas pelos AIs.

**Tabela 5.2.** Parte do *dataset* de KS1 (DM & PP)

| *KS* | *AI* | *(DM & PP)* |
|---|---|---|
| 1 | 5.1.1 | 00100000000001100 |
| | 5.1.2 | 00100000000001100 |
| | 6.1.1 | 00100000000001100 |
| | 6.1.2 | 00100000000001100 |
| | 6.1.3 | 00100001000001100 |
| | 7.2.2 | 10100010100010000 |
| | 8.1.1 | 10100010010100100 |
| | 8.1.2 | 00100010010010100 |
| | 8.1.3 | 10100010101011100 |

No repositório GitHub (Rosa, Jino, & Teixeira Junior, 2017b) e no Apêndice C apresenta-se o conjunto de dados completo desta prova de conceito contendo todas as atribuições de todos os AIs de KS1.

## 5.4 CÁLCULO DE COBERTURAS PARA ISO/IEC 27001 (KS1)

O próximo passo na aplicação da abordagem consiste no cálculo de coberturas que são usadas nas heurísticas. O Aplicativo 1 (Seção 4.5) foi usado e obtivemos as coberturas para os 133 itens de avaliação.

Na Tabela 5.3 apresenta-se um extrato do conjunto de dados de KS1 (Apêndice C). Conforme mostrado na Tabela 5.3, na terceira coluna apresentam-se as dimensões de avaliação (seis caracteres iniciais) e as propriedades de segurança (últimos 11 caracteres) abordadas pelos AIs; na quarta coluna da tabela as coberturas obtidas (CovDM, CovPP e CovLOC).

**Tabela 5.3.** Parte do *dataset* de KS1

| *KS* | *AI* | *(DM & PP)* | *(CovDM;CovPP;CovLOC;)* |
|---|---|---|---|
| 1 | 5.1.1 | 00100000000001100 | 0.000;0.045;0.023; |
| | 5.1.2 | 00100000000001100 | 0.000;0.045;0.023; |
| | 6.1.1 | 00100000000001100 | 0.000;0.045;0.023; |
| | 6.1.2 | 00100000000001100 | 0.000;0.045;0.023; |
| | 6.1.3 | 00100001000001100 | 0.000;0.164;0.082; |
| | 6.1.4 | 10100000010001100 | 0.033;0.145;0.089; |
| | 6.1.5 | 10100000100010100 | 0.033;0.109;0.071; |
| | 6.1.6 | 00100000000000110 | 0.000;0.045;0.023; |
| | 6.1.7 | 00100000000000000 | 0.000;0.000;0.000; |
| | 6.1.8 | 00100000000001100 | 0.000;0.045;0.023; |
| | 6.2.1 | 10100100010110000 | 0.283;0.136;0.210; |
| | 6.2.2 | 10100100010110000 | 0.283;0.136;0.210; |
| | 6.2.3 | 10100100010111100 | 0.283;0.464;0.373; |
| | 7.1.1 | 00100100000101000 | 0.100;0.018;0.059; |
| | 7.1.2 | 10100110110001000 | 0.283;0.445;0.364; |
| | 7.1.3 | 10100100000101100 | 0.283;0.109;0.196; |
| | 7.2.1 | 10100000110010100 | 0.033;0.309;0.171; |
| | 7.2.2 | 10100010100010000 | 0.033;0.173;0.103; |
| | 8.1.1 | 10100010010100100 | 0.033;0.309;0.171; |
| | 8.1.2 | 00100010010010100 | 0.000;0.364;0.182; |

Para demonstrar os cálculos de cobertura, na Tabela 5.4 apresentamos uma memória de atribuições (DMs e PPs) para 2 AIs (AIs *6.1.5* e *11.5.2*).

**Tabela 5.4.** Entradas e Atribuições (DM e PP) dos AIs 6.1.5 e 11.5.2

| *KS* | *AI* | *Entrada DM / PP* | *Atribuições DM / PP* |
|---|---|---|---|
| 1 | *6.1.5* | *101000 / 00100010100* | *DM: 1,3 / PP: 3,7,9* |
| | *11.5.2* | *101101 / 00011100100* | *DM: 1,3,4,6 / PP: 4,5,6,9* |

As distâncias par-a-par das dimensões e propriedades entre si são lidas em duas matrizes de adjacência, a saber: Distâncias entre Dimensões de Avaliação (Matriz 1) e Distâncias entre Propriedades de Segurança (Matriz 2). Posteriormente, as coberturas são calculadas (CovDM, CovPP e CovLOC) conforme apresentado nas Tabelas 5.5 (AI *6.1.5*) e 5.6 (AI *11.5.2*).

**Tabela 5.5.** Memória de Cálculo de Coberturas para AI 6.1.5

| *Matrizes DM (1) e PP (2)* | *AI* | *Entradas DM / PP* | *Cálculos* |
|---|---|---|---|
| $\begin{bmatrix} 0.0 & 0.5 & 0.2 & 0.6 & 0.7 & 0.9 \\ - & 0.0 & 0.9 & 0.7 & 0.6 & 0.8 \\ - & - & 0.0 & 0.4 & 0.2 & 0.6 \\ - & - & - & 0.0 & 0.5 & 0.2 \\ - & - & - & - & 0.0 & 0.8 \\ - & - & - & - & - & 0.0 \end{bmatrix}$ (1)<br><br>$\begin{bmatrix} 0.0 & 0.9 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & 0.0 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.2 \\ - & - & 0.0 & 0.9 & 0.8 & 0.8 & 0.2 & 0.8 & 0.5 & 0.8 & 0.8 \\ - & - & - & 0.0 & 0.2 & 0.2 & 0.8 & 0.6 & 0.5 & 0.8 & 0.4 \\ - & - & - & - & 0.0 & 0.2 & 0.4 & 0.6 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & - & 0.0 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & - & - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.2 \\ - & - & - & - & - & - & - & - & 0.0 & 0.5 & 0.5 \\ - & - & - & - & - & - & - & - & - & 0.0 & 0.2 \\ - & - & - & - & - & - & - & - & - & - & 0.0 \end{bmatrix}$ (2) | *6.1.5* | *101000 / 00100010100* | *DM: 1,3 \| PP: 3,7,9*<br>*CovDM = 0,2 (1-3) / 6 = 0,033*<br>*CovPP = 0,2 (3-7) + 0,5 (3-9) + 0,5 (7-9) = 1,2 / 11 = 0,109*<br>*CovLOC = 0,033 + 0,109 = 0,142 / 2 = 0,71* |

**Tabela 5.6.** Memória de Cálculo de Coberturas para AI 11.5.2

| *Matrizes DM (1) e PP (2)* | *AI* | *Entradas DM / PP* | *Cálculos* |
|---|---|---|---|
| $\begin{bmatrix} 0.0 & 0.5 & 0.2 & 0.6 & 0.7 & 0.9 \\ - & 0.0 & 0.9 & 0.7 & 0.6 & 0.8 \\ - & - & 0.0 & 0.4 & 0.2 & 0.6 \\ - & - & - & 0.0 & 0.5 & 0.2 \\ - & - & - & - & 0.0 & 0.8 \\ - & - & - & - & - & 0.0 \end{bmatrix}$ (1)<br><br>$\begin{bmatrix} 0.0 & 0.9 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & 0.0 & 0.9 & 0.9 & 0.8 & 0.8 & 0.8 & 0.8 & 0.5 & 0.2 & 0.2 \\ - & - & 0.0 & 0.9 & 0.8 & 0.8 & 0.2 & 0.8 & 0.5 & 0.8 & 0.8 \\ - & - & - & 0.0 & 0.2 & 0.2 & 0.8 & 0.6 & 0.5 & 0.8 & 0.4 \\ - & - & - & - & 0.0 & 0.2 & 0.4 & 0.6 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.5 & 0.8 & 0.2 \\ - & - & - & - & - & - & 0.0 & 0.8 & 0.5 & 0.2 & 0.8 \\ - & - & - & - & - & - & - & 0.0 & 0.5 & 0.2 & 0.2 \\ - & - & - & - & - & - & - & - & 0.0 & 0.5 & 0.5 \\ - & - & - & - & - & - & - & - & - & 0.0 & 0.2 \\ - & - & - & - & - & - & - & - & - & - & 0.0 \end{bmatrix}$ (2) | *11.5.2* | *101101 / 00011100100* | *DM: 1,3,4,6 \| PP: 4,5,6,9*<br>*CovDM = 0,2 (1-3) + 0,6 (1-4) + 0,9 (1-6) + 0,4 (3-4) + 0,6 (3-6) + 0,2 (4-6) = 2,9 / 6 = 0,483*<br>*CovPP = 0,2 (4-5) + 0,2 (4-6) + 0,5 (4-9) + 0,2 (5-6) + 0,5 (5-9) + 0,5 (6-9) = 1,2 / 11 = 0,101*<br>*CovLOC = 0,483 + 0,101 = 0,674 / 2 = 0,337* |

A Tabela 5.7 apresenta os valores de coberturas calculados para os AIs *6.1.5* e *11.5.2*. No repositório GitHub (Rosa, Jino, & Teixeira Junior, 2017b) e no Apêndice C apresenta-se o conjunto de dados completo desta prova de conceito contendo todos os AIs de KS1 com suas respectivas DMs, PPs e coberturas.

**Tabela 5.7.** Memória de Cálculo AIs 6.1.5 e 11.5.2

| *KS* | *AI* | *(DM & PP)* | *(CovDM;CovPP;CovLOC)* |
|---|---|---|---|
| 1 | *6.1.5* | *10100000100010100* | *0,033; 0,109; 0,071* |
| | *11.5.2* | *10110100011100100* | *0,483; 0,191; 0,337* |

## 5.5 SELEÇÃO E ANÁLISE DE ITENS DE AVALIAÇÃO A PARTIR DOS CRITÉRIOS E HEURÍSTICAS PROPOSTOS

Nesta seção apresenta-se uma visão geral dos dados obtidos a partir da aplicação de HCApp-Sec à fonte de conhecimento selecionada (KS1). O objetivo principal na avaliação dos resultados é verificar a aplicabilidade da abordagem, por meio da análise dos dados obtidos da aplicação dos critérios e heurísticas a uma fonte bem conhecida na área de segurança. Todos os critérios e heurísticas propostos foram aplicados e os resultados analisados. Alguns critérios e heurísticas são apresentados em forma de exemplos ou ilustrações (cenários de uso) devido a não termos dados reais até o momento. A seção foi dividida em aplicação dos critérios (5.5.1) e aplicação das heurísticas (5.5.2).

### 5.5.1 Aplicação dos Critérios de Avaliação de Segurança a KS1

Nesta seção exercitamos a abordagem por meio da aplicação dos critérios para selecionar ou priorizar itens de avaliação (AIs). Aplicamos os critérios propostos à fonte de conhecimento ISO/IEC 27001 (KS1), com o objetivo de demonstrar sua aplicabilidade usando uma fonte de conhecimento de segurança bem conhecida. Com exemplos de uso dos critérios, espera-se: (i) verificar a possibilidade de seleção de itens de avaliação; e (ii) analisar se os critérios são satisfeitos ou não e como a fonte aborda as dimensões de avaliação e as propriedades de segurança propostas.

### C-All-KS

C-All-KS pode ser usado para avaliar exaustivamente um sistema, usando todos as fontes de conhecimento (KS) disponíveis na base. Nesta prova de conceito, uma KS foi avaliada, mas outras fontes podem ser usadas. Na Tabela 5.8 uma seleção de todas as fontes da base é simulada; Nesta situação hipotética apresentamos as fontes com suas respectivas CovGLO[2]. Neste exemplo, o critério foi satisfeito, pois 100% das KSs disponíveis na base foram selecionadas. Se selecionássemos somente 3 KSs das 14 disponíveis, teríamos 21,4% (3/14) de satisfação do critério.

**Tabela 5.8.** Exemplo de aplicação de C-All-KS: seleção de todas as KS da base

| *ID* | *KS* | *CovGLO* |
|---|---|---|
| 1 | ISO/IEC 27001 | *0,252* |
| 2 | ISO/IEC 15408 | *0,277* |
| 3 | MITRE *Ten Strategies of a CSOC* | 0,110 |
| 4 | OWASP *Testing Guide* | 0,295 |
| 5 | SANS *Critical Security Controls* | 0,373 |
| 6 | SBIS/CFM MOEA | 0,276 |
| *7* | PCI/DSS | 0,211 |
| 8 | FIPS (NIST) (140-2) | 0,397 |
| 9 | SOX *Audit Checklist* | 0,194 |
| *10* | *Cybersecurity Capability Maturity Model* (C2M2) | 0,144 |
| 11 | BACEN/STN Manual de Segurança da RSFN | 0,234 |
| 12 | SLTI/MPOG ePing-Segurança | 0,245 |
| *13* | CSA/CAIQ | 0,198 |
| 14 | MED-Sec-AWA *Checklist* | 0,128 |

Como pode-se observar na Tabela 5.8, uma ordem de priorização poderia ser estabelecida, por exemplo com base em H-CovGLO (heurística tratada mais adiante nesta seção) ou na quantidade de AIs.

[2] Valores de CovGLO das KS são simulados para demonstração do uso do critério, com exceção de KS1 que apresenta o valor real.
[3] Valores de quantidades de AIs são simulados para demonstração do uso do critério, com exceção de KS1 que apresenta o valor real.
[4] Valores de CovGLO das KS são simulados para demonstração do uso do critério, com exceção de KS1 que apresenta o valor real.
[5] O Ataque de Regras de Negócios *(Business Logic Attack* – BLA) é um ataque que visa a lógica de uma aplicação. Ao contrário dos ataques "tradicionais", técnicos, os ataques à lógica de negócios não contêm solicitações malformadas e incluem valores de entrada legítimos, tornando difícil detectá-los. BLAs abusam da funcionalidade da aplicação, atacando diretamente o negócio (Imperva, 2018).

### C-All-AI-KS

C-All-AI-KS pode ser usado para avaliar a conformidade de um sistema, usando todos os itens de avaliação de uma fonte de conhecimento (KS) disponível na base. Esse tipo de avaliação é bastante usual e geralmente se escolhe a KS que será usada na avaliação com base nos objetivos das KSs, em regulamentação específica ou em práticas de mercado. Nesta prova de conceito, KS1 apresenta 133 itens de avaliação. Por exemplo, se em uma avaliação todos os 133 AIs de KS1 forem selecionados, o critério foi satisfeito; se 80 AIs forem selecionados, 60,15% (80/133) do critério foi satisfeito. Na Tabela 5.9 as quantidades de AIs de todas as fontes da base é simulada; Nesta situação hipotética apresentamos as fontes e suas quantidades de itens de avaliação[3].

**Tabela 5.9.** Exemplo de aplicação de C-All-AI-KS: quantidades de AIs de cada KS da base

| *ID* | *KS* | *Quant. AIs* |
|---|---|---|
| 1 | ISO/IEC 27001 | *133* |
| 2 | ISO/IEC 15408 | *131* |
| 3 | MITRE *Ten Strategies of a CSOC* | *106* |
| 4 | OWASP *Testing Guide* | *126* |
| 5 | SANS *Critical Security Controls* | *175* |
| 6 | SBIS/CFM MOEA | *103* |
| *7* | PCI/DSS | *160* |
| 8 | FIPS (NIST) (140-2) | *179* |
| 9 | SOX *Audit Checklist* | *84* |
| *10* | *Cybersecurity Capability Maturity Model* (C2M2) | *122* |
| 11 | BACEN/STN Manual de Segurança da RSFN | *95* |
| 12 | SLTI/MPOG ePing-Segurança | *161* |
| *13* | CSA/CAIQ | *172* |
| 14 | MED-Sec-AWA *Checklist* | *138* |

[3] Valores de quantidades de AIs são simulados para demonstração do uso do critério, com exceção de KS1 que apresenta o valor real.

### C-All-AD

C-All-AD destina-se a selecionar todos os projetos de avaliação (ADs) que foram construídos anteriormente. Nesta prova de conceito, o exercitamos por meio da criação de 3 ADs de exemplo (Tabela 5.10, coluna 1) com 5 AIs (Tabela 5.10, coluna 2) selecionados aleatoriamente de KS1. A referida tabela apresenta valores de coberturas (CovDM, CovPP, CovLOC e CovTOT) que serão usados na próxima seção, onde as heurísticas são exercitadas.

**Tabela 5.10.** Aplicação de C-All-AD: seleção de todos os ADs gerados

| *AD* | *AI* | *KS* | *CovDM* | *CovPP* | *CovLOC* | *CovTOT* |
|---|---|---|---|---|---|---|
| 1 | 11.6.2 | 1 | 0,967 | 0,336 | 0,652 | |
| 1 | 12.3.2 | 1 | 0,850 | 0,673 | 0,761 | |
| 1 | 11.7.1 | 1 | 0,650 | 0,318 | 0,484 | 0,528 |
| 1 | 11.5.6 | 1 | 0,650 | 0,173 | 0,411 | |
| 1 | 10.3.1 | 1 | 0,650 | 0,018 | 0,334 | |
| - | - | - | - | - | - | - |
| 2 | 10.10.1 | 1 | 0,483 | 1,000 | 0,742 | |
| 2 | 15.1.3 | 1 | 0,483 | 1,000 | 0,742 | |
| 2 | 13.2.3 | 1 | 0,283 | 1,000 | 0,642 | 0,680 |
| 2 | 15.1.5 | 1 | 0,283 | 1,000 | 0,642 | |
| 2 | 9.2.4 | 1 | 0,283 | 0,982 | 0,633 | |
| - | - | - | - | - | - | - |
| 3 | 12.3.2 | 1 | 0,850 | 0,673 | 0,761 | |
| 3 | 10.10.1 | 1 | 0,483 | 1,000 | 0,742 | |
| 3 | 15.1.3 | 1 | 0,483 | 1,000 | 0,742 | 0,718 |
| 3 | 14.1.3 | 1 | 0,483 | 0,900 | 0,692 | |
| 3 | 11.6.2 | 1 | 0,967 | 0,336 | 0,652 | |

Conforme mostrado na Tabela 5.10, com base no critério C-All-AD, selecionamos todos os 3 ADs disponíveis na base, ou seja, o critério foi satisfeito. Como exemplo, se selecionarmos apenas 2 ADs dentre os 3 disponíveis, podemos dizer que 66,7% (2/3) do critério C-All-AD foi satisfeito.

### C-All-PP

C-All-PP destina-se a selecionar KSs que abordem todas as propriedades de segurança (PP). KS1 abordou todos as PPs propostas, ou seja, ao considerar todas os AIs de KS1, todas as PPs estão representadas. KS1 satisfaz o critério porque todos as PPs propostas foram abordadas pelo conjunto de AIs de KS1. Na Figura 5.1 e na Tabela 5.11 (completa no Apêndice C), apresenta-se a quantidade de cada propriedade abordada por todos os AIs de KS1.

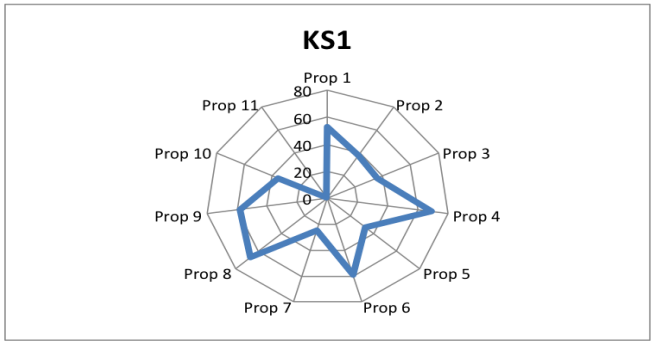


**Figura 5.1.** Quantidade de Propriedades de Segurança abordadas por KS1

Conforme mostrado na Figura 5.1 e na Tabela 5.11, certas propriedades de segurança foram mais abordadas pelos AIs de KS1, tais como, 4, 8, 6, 9 e 1. A propriedade 11 tinha apenas uma atribuição. A propriedade 7 teve 25 atribuições, porque consideramos que a "Privacidade" está relacionada a informações específicas ou pessoais.

**Tabela 5.11.** Quantidade de Propriedades de Segurança (PP) abordadas por KS1

| *KS* | *PP1* | *PP2* | *PP3* | *PP4* | *PP5* | *PP6* | *PP7* | *PP8* | *PP9* | *PP10* | *PP11* | *CovGLO* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 53 | 38 | 36 | 69 | 33 | 59 | 25 | 67 | 58 | 36 | 1 | 0,252 |

Em relação às PPs, KS1 tem uma melhor cobertura das propriedades 4, 8, 6, 9 e 1, enquanto que tem uma cobertura pior das propriedades 11, 10, 7, 5, 3 e 2. Pode-se inferir que KS1 possui melhor desempenho quando está avaliando aspectos relacionados à Disponibilidade, Autenticidade, Legalidade e Auditabilidade; e, ao contrário, KS1 tem um desempenho pior quando avalia a Confidencialidade e a Integridade dos dados.

### C-All-DM

C-All-DM destina-se a selecionar KSs que abordem todas as dimensões de avaliação (DMs). KS1 abordou todos as DMs propostas, ou seja, ao considerar todas os AIs de KS1, todas as DMs estão representadas. KS1 satisfaz o critério porque todos as DMs propostas foram abordadas pelo conjunto de AIs de KS1. Na Figura 5.2 e na Tabela 5.12 (completa no Apêndice C) apresenta-se a quantidade de cada DM abordada por todos os AIs de KS1.

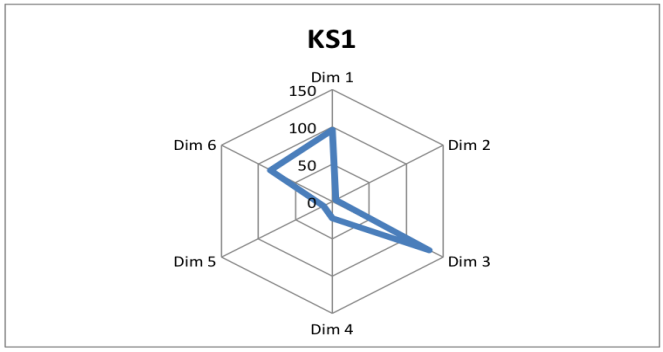


**Figura 5.2.** Quantidade de Dimensões de Avaliação abordadas por KS1

Conforme mostrado na Figura 5.2 a DM 3 (*Process*) se destaca, sendo seguida por 1 e 6. As Dimensões 2 e 5 são muito pouco abordadas por KS1.

**Tabela 5.12.** Quantidade de Dimensões de Avaliação (DM) abordadas por KS1

| *KS* | *DM1* | *DM2* | *DM3* | *DM4* | *DM5* | *DM6* |
|---|---|---|---|---|---|---|
| 1 | 96 | 5 | 131 | 22 | 12 | 84 |

Conforme mostrado na Tabela 5.12, certas dimensões de avaliação (DM) foram mais abordadas pelos AIs de KS1, tais como, 3, 1 e 6. A Dimensão 2 teve apenas cinco atribuições; as dimensões 4 e 5 tiveram respectivamente 22 e 12 atribuições. Em relação às DMs, KS1 aborda predominantemente as dimensões 1, 3 e 6, enquanto que aborda superficialmente as dimensões 2, 4 e 5. KS1 está focada na avaliação de processos e regras de negócios. Percebe-se uma ausência de itens de avaliação que lidam, por exemplo, com Arquitetura do Sistema (DM 2). Além disso, KS1 está focada na atividade de Verificação (por exemplo, verificando a presença de determinado controle), em vez da atividade de Teste (por exemplo, executando o teste do Sistema em Tempo de Execução ou analisando a Estrutura de Código-Fonte – DMs 4 e 5).

### C-CombDM

C-CombDM destina-se a selecionar itens de avaliação (AIs) que combinam certas dimensões de avaliação (DMs), ou seja, os AIs com alguma combinação de DMs. Aplicação do critério: "Selecionar os AIs que apresentam a combinação DM4 e DM6 (k=*2*)". Nesta aplicação, como é uma combinação de 2 DMs (k=*2*), 6,7% (1/15) do critério foi satisfeito; para uma combinação de 3 DMs (k=*3*), 5% (1/20) do critério seria satisfeito. Na Tabela 5.19 apresenta-se um exemplo em que selecionamos os AIs que combinam as DMs 4 e 6 do dataset de KS1.

**Tabela 5.13.** AIs selecionados considerando C-CombDM (DM4-DM6)

| *ID* | *DM1* | *DM2* | *DM3* | *DM4* | *DM5* | *DM6* |
|---|---|---|---|---|---|---|
| 10.10.1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.3.2 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.4.7 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.5.1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.5.2 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.5.3 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.5.5 | 1 | 0 | 1 | 1 | 0 | 1 |
| 11.6.2 | 1 | 1 | 1 | 1 | 0 | 1 |
| 12.3.2 | 1 | 0 | 1 | 1 | 1 | 1 |
| 12.5.5 | 0 | 0 | 1 | 1 | 1 | 1 |
| 14.1.3 | 1 | 0 | 1 | 1 | 0 | 1 |
| 14.1.4 | 1 | 0 | 1 | 1 | 0 | 1 |
| 14.1.5 | 1 | 0 | 1 | 1 | 0 | 1 |
| 15.1.3 | 1 | 0 | 1 | 1 | 0 | 1 |

### C-CombPP

C-CombPP destina-se a selecionar itens de avaliação (AIs) que combinam certas propriedades de segurança (PPs), ou seja, os AIs com alguma combinação de PPs. Aplicação do critério: "Selecionar os AIs que apresentam a combinação PP2 e PP3 (k=*2*)". Nesta aplicação, como é uma combinação de 2 PPs (k=*2*), 1,8% (1/55) do critério foi satisfeito; para uma combinação de 3 DMs (k=*3*), 0,6% (1/165) do critério seria satisfeito. Na Tabela 5.20 apresenta-se um exemplo em que selecionamos os AIs que combinam as PPs 2 e 3 do dataset de KS1.

**Tabela 5.14.** AIs selecionados considerando C-CombPP (PP2-PP3)

| *ID* | *PP1* | *PP2* | *PP3* | *PP4* | *PP5* | *PP6* | *PP7* | *PP8* | *PP9* | *PP10* | *PP11* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.2.3 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 9.2.4 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 10.1.4 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10.8.3 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 10.9.1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 11.3.3 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12.3.2 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 12.4.2 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 12.4.3 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 12.5.5 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 12.6.1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 14.1.3 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 15.1.3 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 15.1.4 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 15.1.6 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 15.3.2 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

### C-CombDM-PP

C-CombDM-PP destina-se a selecionar itens de avaliação (AIs) que combinam certas DMs e certas PPs ao mesmo tempo, ou seja, AIs com alguma combinação de DM-PP. Aplicação do critério: "Selecionar os AIs que apresentam a combinação DM4 e PP3 (k=*2*)". Nesta aplicação, como é uma combinação de 2 PPs (k=*2*), 0,73% (1/136) do critério foi satisfeito. Na Tabela 5.21 apresenta-se um exemplo em que selecionamos os AIs que combinam a DM4 e a PP3 do dataset de KS1.

**Tabela 5.15.** AIs selecionados considerando C-CombDM-PP (DM4-PP3)

| *ID* | *DM1* | *DM2* | *DM3* | *DM4* | *DM5* | *DM6* | *PP1* | *PP2* | *PP3* | *PP4* | *PP5* | *PP6* | *PP7* | *PP8* | *PP9* | *PP 10* | *PP 11* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11.5.3 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 12.3.1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 12.3.2 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 12.4.2 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 12.5.5 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 14.1.3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 15.1.3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 15.1.6 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |

### 5.5.2 Aplicação das Heurísticas de Avaliação de Segurança a KS1

Nesta seção exercitamos a abordagem por meio da aplicação das heurísticas para selecionar ou priorizar itens de avaliação (AIs). Aplicamos as heurísticas propostas à fonte de conhecimento ISO/IEC 27001 (KS1), com o objetivo de propor formas de usar medidas de cobertura para selecionar melhores AIs para comporem projetos de avaliação mais efetivos. Com exemplos de uso das heurísticas, espera-se: (i) verificar a possibilidade de seleção de melhores itens de avaliação; e (ii) analisar como as heurísticas podem ser usadas na seleção ou priorização com base em medidas de cobertura de dimensões de avaliação e de propriedades de segurança.

No contexto deste trabalho, o termo “Heurística de Avaliação” engloba heurísticas de teste e de verificação. Heurísticas são sempre aproximações, para máximo, para mínimo, para melhor, para pior, etc. e não têm a pretensão de garantir que todas as condições estão satisfeitas.

### H-CovDM

H-CovDM destina-se a selecionar ou priorizar AIs que atendam a maior diversidade de dimensões de avaliação, com base em CovDM. Aplicação da heurística: "Selecionar os 5 melhores AIs considerando CovDM". Na Tabela 5.13, apresentamos os 5 melhores e os 5 piores (informativo) AIs do dataset de KS1, segundo a heurística proposta.

**Tabela 5.16.** Aplicação de H-CovDM na seleção e priorização de AIs de KS1

| *KS* | *AI* | *CovDM* | *Obs.* |
|---|---|---|---|
| 1 | 11.6.2 | *0,967* | |
| 1 | 12.3.2 | *0,850* | |
| 1 | 11.7.1 | *0,650* | Melhor |
| 1 | 11.5.6 | *0,650* | |
| 1 | 10.3.1 | *0,650* | |
| - | - | - | - |
| 1 | 6.1.8 | *0,000* | |
| 1 | 8.2.1 | *0,000* | |
| 1 | 8.2.2 | *0,000* | Pior |
| 1 | 8.3.1 | *0,000* | |
| 1 | 6.1.7 | *0,000* | |

### H-CovPP

H-CovPP destina-se a selecionar ou priorizar AIs que atendam a maior diversidade de propriedades de segurança, com base em CovPP. Aplicação da heurística: "Selecionar os 5 melhores AIs considerando CovPP". Na Tabela 5.14, apresentamos os 5 melhores e os 5 piores (informativo) AIs do dataset de KS1, segundo a heurística proposta.

**Tabela 5.17.** Aplicação de H-CovPP na seleção e priorização de AIs de KS1

| *KS* | *AI* | *CovPP* | *Obs.* |
|---|---|---|---|
| 1 | 10.10.1 | *1,000* | |
| 1 | 15.1.3 | *1,000* | |
| 1 | 13.2.3 | *1,000* | Melhor |
| 1 | 15.1.5 | *1,000* | |
| 1 | 9.2.4 | *0,982* | |
| - | - | - | - |
| 1 | 10.10.2 | *0,018* | |
| 1 | 13.1.2 | *0,018* | |
| 1 | 10.8.4 | *0,018* | Pior |
| 1 | 10.8.5 | *0,018* | |
| 1 | 6.1.7 | *0,000* | |

### H-CovLOC

H-CovLOC destina-se a selecionar AIs com melhor CovLOC, ou seja, os AIs com melhor cobertura considerando a média de CovDM e CovPP. Aplicação da heurística: "Selecionar os 5 melhores AIs considerando CovLOC". Na Tabela 5.15 apresentam-se os 5 melhores e os 5 piores (informativo) AIs do dataset de KS1, considerando CovLOC; usamos como sub-heurísticas H-CovPP e H-CovDM para priorização.

**Tabela 5.18.** Aplicação de H-CovLOC na seleção e priorização de AIs de KS1

| *KS* | *AI* | *CovDM* | *CovPP* | *CovLOC* | *Obs.* |
|---|---|---|---|---|---|
| 1 | 12.3.2 | 0,850 | 0,673 | *0,761* | |
| 1 | 10.10.1 | 0,483 | 1,000 | *0,742* | |
| 1 | 15.1.3 | 0,483 | 1,000 | *0,742* | Melhor |
| 1 | 14.1.3 | 0,483 | 0,900 | *0,692* | |
| 1 | 11.6.2 | 0,967 | 0,336 | *0,652* | |
| - | - | | | - | - |
| 1 | 6.1.8 | 0,000 | 0,045 | *0,023* | |
| 1 | 8.2.1 | 0,000 | 0,045 | *0,023* | |
| 1 | 8.2.2 | 0,000 | 0,045 | *0,023* | Pior |
| 1 | 8.3.1 | 0,000 | 0,045 | *0,023* | |
| 1 | 6.1.7 | 0,000 | 0,000 | *0,000* | |

### H-CovGLO

H-CovGLO destina-se a selecionar ou priorizar fontes de conhecimento (KSs) com melhor CovGLO, ou seja, selecionar KSs com melhor abrangência considerando a média de CovLOC de todos os seus AIs. Nesta prova de conceito, a CovGLO de KS1 é *0,252*. Pretende-se comparar esse valor com outras KSs em trabalhos futuros; essa comparação pode ser útil para escolher, por exemplo, quais KSs devem ser usadas em determinadas avaliações de conformidade. Exemplo de aplicação da heurística: "Selecionar as 3 melhores KSs considerando H-CovGLO". Na Tabela 5.16 uma seleção de todas as fontes da base é simulada; Nesta situação hipotética apresentamos as 3 fontes selecionadas em destaque segundo H-CovGLO[4].

**Tabela 5.19.** Exemplo de aplicação de H-CovGLO: seleção de 3 KSs da base

| *ID* | *KS* | *CovGLO* |
|---|---|---|
| ***<8>*** | ***<FIPS (NIST) (140-2)>*** | ***<0,397>*** |
| ***<5>*** | ***<SANS Critical Security Controls>*** | ***<0,373>*** |
| ***<4>*** | ***<OWASP Testing Guide>*** | ***<0,295>*** |
| 2 | ISO/IEC 15408 | *0,277* |
| 6 | SBIS/CFM MOEA | *0,276* |
| *1* | *ISO/IEC 27001* | *0,252* |
| 12 | SLTI/MPOG ePing-Security | *0,245* |
| 11 | BACEN/STN Manual de Segurança da RSFN | *0,234* |
| *7* | PCI/DSS | *0,211* |
| *13* | CSA/CAIQ | *0,198* |
| 9 | SOX *Audit Checklist* | *0,194* |
| *10* | *Cybersecurity Capability Maturity Model* (C2M2) | *0,144* |
| 14 | MED-Sec-AWA Checklist | *0,128* |
| 3 | MITRE *Ten Strategies of a CSOC* | *0,110* |

[4] Valores de CovGLO das KS são simulados para demonstração do uso do critério, com exceção de KS1 que apresenta o valor real.

### H-CovTOT

H-CovTOT destina-se a selecionar projetos de avaliação (ADs) com melhor abrangência, considerando CovTOT (média das CovLOC dos AIs selecionados). Aplicação da heurística: "Selecionar os 3 melhores ADs considerando CovTOT". Na Tabela 5.17, apresentam-se todos os 3 ADs priorizados por CovTOT; usamos como sub-heurísticas H-CovLOC.

**Tabela 5.20.** ADs selecionados ou priorizados considerando H-CovTOT

| *AD* | *AI* | *KS* | *CovDM* | *CovPP* | *CovLOC* | *CovTOT* |
|---|---|---|---|---|---|---|
| 3 | 12.3.2 | 1 | 0,850 | 0,673 | 0,761 | |
| 3 | 10.10.1 | 1 | 0,483 | 1,000 | 0,742 | |
| 3 | 15.1.3 | 1 | 0,483 | 1,000 | 0,742 | *0,718* |
| 3 | 14.1.3 | 1 | 0,483 | 0,900 | 0,692 | |
| 3 | 11.6.2 | 1 | 0,967 | 0,336 | 0,652 | |
| - | - | - | - | - | - | - |
| 2 | 10.10.1 | 1 | 0,483 | 1,000 | 0,742 | |
| 2 | 15.1.3 | 1 | 0,483 | 1,000 | 0,742 | |
| 2 | 13.2.3 | 1 | 0,283 | 1,000 | 0,642 | *0,680* |
| 2 | 15.1.5 | 1 | 0,283 | 1,000 | 0,642 | |
| 2 | 9.2.4 | 1 | 0,283 | 0,982 | 0,633 | |
| - | - | - | - | - | - | - |
| 1 | 12.3.2 | 1 | 0,850 | 0,673 | 0,761 | |
| 1 | 11.6.2 | 1 | 0,967 | 0,336 | 0,652 | |
| 1 | 11.7.1 | 1 | 0,650 | 0,318 | 0,484 | *0,528* |
| 1 | 11.5.6 | 1 | 0,650 | 0,173 | 0,411 | |
| 1 | 10.3.1 | 1 | 0,650 | 0,018 | 0,334 | |

### H-AboveAvg

H-AboveAvg destina-se a selecionar ou priorizar Itens de Avaliação (AIs) com melhor abrangência, considerando os AIs com valores acima da média de CovLOC, CovDM ou CovPP. Aplicação da heurística: "Selecionar os AIs com valores acima da média, considerando CovPP". Na Tabela 5.18, apresentam-se todos os AIs selecionados segundo a heurística H-AboveAvg usando CovPP; adicionalmente, pode-se usar a heurística para selecionar usando CovDM e CovLOC. Para KS1, as médias são as seguintes: CovDM = *0,220*; CovPP = *0,284*; e CovLOC = *0,252*.

**Tabela 5.21.** AIs selecionados considerando H-AboveAvg (CovPP)

| *ID* | *CovPP* |
|---|---|
| 10.10.1 | 1,000 |
| 15.1.3 | 1,000 |
| 13.2.3 | 1,000 |
| 15.1.5 | 1,000 |
| 9.2.4 | 0,982 |
| 14.1.3 | 0,900 |
| 15.3.2 | 0,900 |
| 8.1.3 | 0,855 |
| 12.2.2 | 0,845 |
| 11.4.5 | 0,818 |
| 10.4.2 | 0,745 |
| 12.3.2 | 0,673 |
| 10.9.2 | 0,673 |
| 10.7.3 | 0,645 |
| 15.2.1 | 0,636 |
| 10.8.3 | 0,591 |
| 10.9.1 | 0,591 |
| 12.5.5 | 0,573 |
| 15.1.6 | 0,573 |
| 10.2.2 | 0,573 |
| 10.4.1 | 0,518 |
| 10.6.1 | 0,518 |
| 10.9.3 | 0,518 |
| 12.2.1 | 0,518 |
| 14.1.5 | 0,491 |
| 9.1.4 | 0,473 |
| 9.2.1 | 0,473 |
| 6.2.3 | 0,464 |
| 7.1.2 | 0,445 |
| 12.4.3 | 0,409 |
| 11.4.4 | 0,409 |
| 10.1.3 | 0,409 |
| 12.4.2 | 0,364 |
| 15.1.1 | 0,364 |
| 8.1.2 | 0,364 |
| 9.2.3 | 0,355 |
| 9.2.6 | 0,355 |
| 11.6.2 | 0,336 |
| 11.5.4 | 0,336 |
| 11.7.1 | 0,318 |
| 11.4.1 | 0,318 |
| 7.2.1 | 0,309 |
| 8.1.1 | 0,309 |
| 15.1.4 | 0,309 |
| 12.5.4 | 0,300 |
| 10.2.1 | 0,300 |

### H-ParetoPercentage

H-ParetoPercentage destina-se a selecionar um conjunto pequeno de itens de avaliação (AIs) e, ao mesmo tempo, atingir uma certa porcentagem de abrangência. Em outras palavras, procura-se melhores resultados de abrangência com menos esforço (número de AIs a serem usados). Aplicação da heurística: "Selecionar os AIs tal que a soma das CovLOC apresentam 40% do total da KS". A Tabela 5.22 apresenta a seleção baseada em H-ParetoPercentage.

**Tabela 5.22.** AIs selecionados considerando H-ParetoPercentage

| *ID* | *CovLoc* | *%* |
|---|---|---|
| 12.3.2 | 0,761 | 2,27% |
| 10.10.1 | 0,742 | 4,49% |
| 15.1.3 | 0,742 | 6,71% |
| 14.1.3 | 0,692 | 8,77% |
| 11.6.2 | 0,652 | 10,72% |
| 13.2.3 | 0,642 | 12,64% |
| 15.1.5 | 0,642 | 14,55% |
| 9.2.4 | 0,633 | 16,44% |
| 15.3.2 | 0,592 | 18,21% |
| 10.4.2 | 0,589 | 19,97% |
| 11.4.5 | 0,551 | 21,62% |
| 10.4.1 | 0,542 | 23,24% |
| 12.2.2 | 0,514 | 24,77% |
| 12.5.5 | 0,511 | 26,30% |
| 15.1.6 | 0,503 | 27,80% |
| 12.4.3 | 0,488 | 29,26% |
| 14.1.5 | 0,487 | 30,71% |
| 11.7.1 | 0,484 | 32,16% |
| 10.9.2 | 0,478 | 33,59% |
| 10.7.3 | 0,464 | 34,97% |
| 15.2.1 | 0,460 | 36,34% |
| 10.6.1 | 0,451 | 37,69% |
| 8.1.3 | 0,444 | 39,02% |
| 10.8.3 | 0,437 | 40,32% |

Na Figura 5.3, apresenta-se uma aplicação de H-ParetoPercentage no dataset de KS1 (CovLOC).

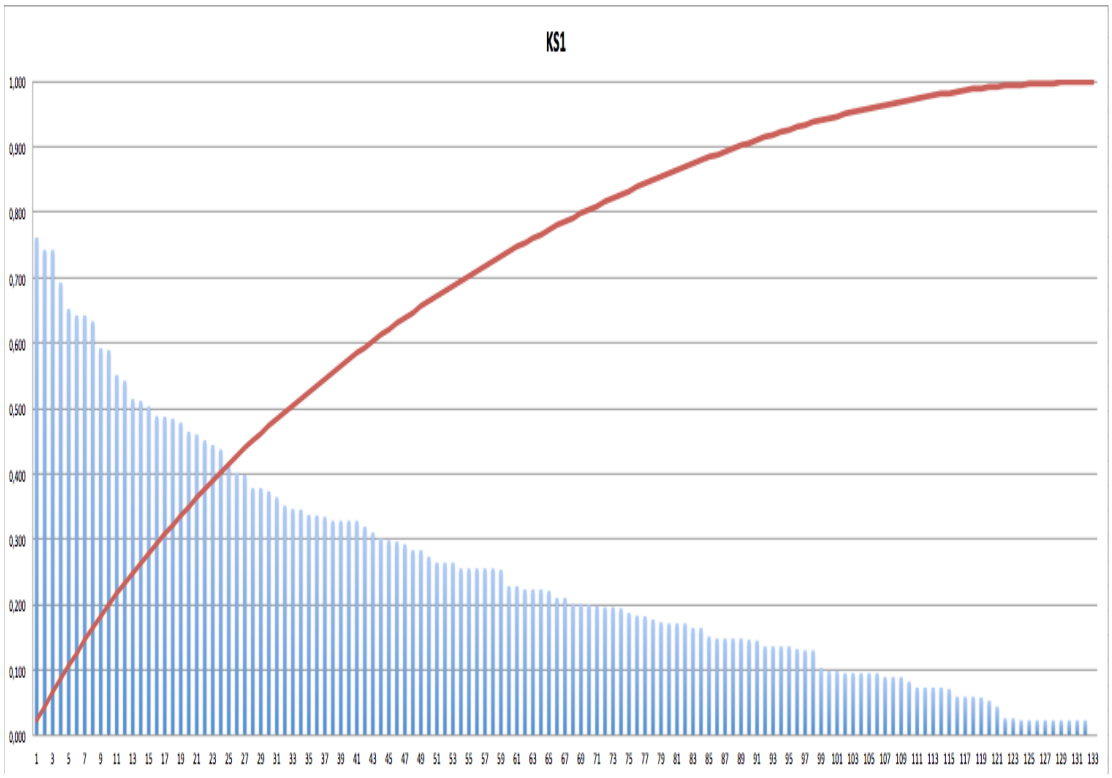


**Figura 5.3.** Aplicação de H-ParetoPercentage ao dataset de KS1

Conforme mostrado na Figura 5.3, depois de ordenar os AIs considerando os valores individuais de CovLOC de todos os AIs, pode-se identificar um ponto de corte, ou seja, onde uma quantidade menor de AIs apresenta uma certa porcentagem de CovLOC, dentre todos os AIs de KS1.

### H-ParetoFrontier

H-ParetoFrontier destina-se a selecionar ou priorizar AIs, considerando CovDM e CovPP ao mesmo tempo (bi-objetivo). Depois de somar as distâncias entre as DMs e as PPs, obtivemos os valores de CovDM e CovPP. Aplicação da heurística: "Selecionar os AIs que apresentam CovDM e CovPP maiores que *0,430*". A Tabela 5.23 apresenta a seleção baseada em H-ParetoFrontier.

**Tabela 5.23.** AIs selecionados considerando H-ParetoFrontier

| *ID* | *CovDM* | *CovPP* |
|---|---|---|
| 10.10.1 | 0,483 | 1,000 |
| 15.1.3 | 0,483 | 1,000 |
| 14.1.3 | 0,483 | 0,900 |
| 10.4.2 | 0,433 | 0,745 |
| 12.3.2 | 0,850 | 0,673 |
| 12.5.5 | 0,450 | 0,573 |
| 15.1.6 | 0,433 | 0,573 |
| 10.4.1 | 0,567 | 0,518 |
| 14.1.5 | 0,483 | 0,491 |

A Figura 5.4 apresenta uma visualização dos AIs de KS1, com os valores de CovDM e CovPP.

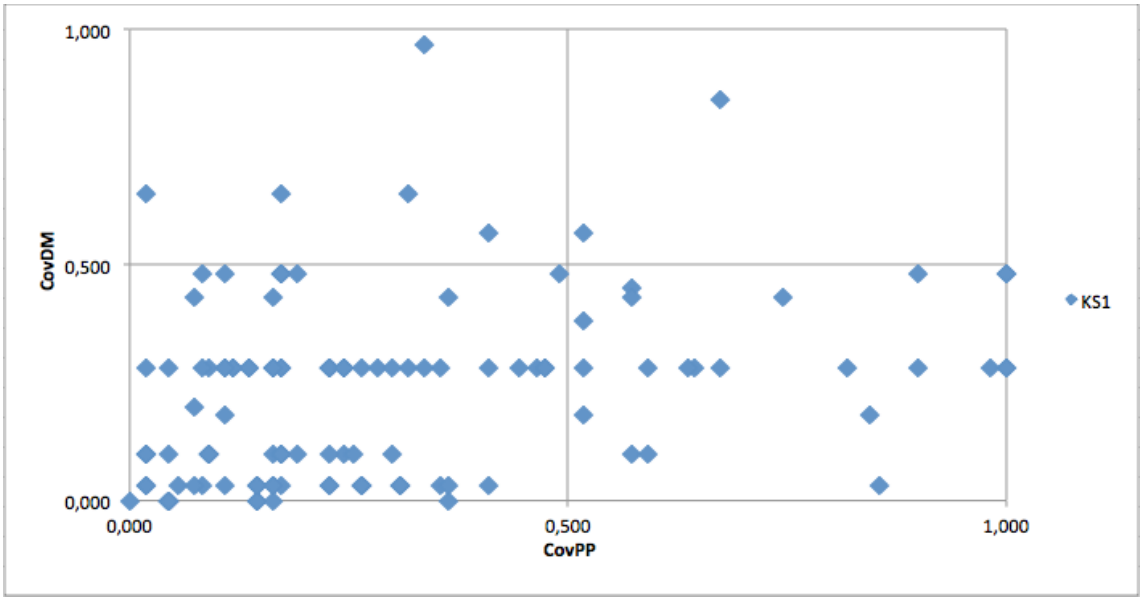


**Figura 5.4.** Visualização dos AIs de KS1 (CovDM e CovPP)

Na Figura 5.4, podem ser vistos todos os itens de avaliação (AIs) de KS1 plotados; O eixo X do gráfico (valores de *0* a *1*) representa CovPP. O eixo Y do gráfico (valores de 0 a 1) representa CovDM. Neste modo de exibição, podem ser identificados pontos que podem ser selecionados ou priorizados, devido a estes alcançarem simultaneamente melhor resultado considerando dois objetivos de cobertura (CovDM e CovPP). Por exemplo, na Figura 5.4, os AIs situados no quadrante superior direito são mais adequados quando considerados os valores de CovDM e CovPP ao mesmo tempo.

## 5.6 CONSIDERAÇÕES FINAIS

HCApp-Sec foi aplicada a uma fonte de conhecimento de segurança bem conhecida (ISO/IEC 27001 – KS1). Foi possível caracterizar KS1 identificando quais dimensões de avaliação e quais propriedades de segurança foram abordadas pelos seus 133 itens de avaliação; são mostradas as quantidades de dimensões e propriedades abordadas por todos os itens de KS1. Todos os critérios e heurísticas propostos foram exercitados na seleção ou priorização dos itens de avaliação de projetos de avaliação de segurança, demonstrando a viabilidade de aplicação da proposta. Identifica-se que a abordagem proposta pode contribuir com pesquisadores de segurança na geração de projetos de avaliação com cobertura assegurada das principais características de segurança e na avaliação *a priori* de fontes de conhecimento de segurança com relação a escopo e segurança. Especificamente, a proposta poderia apoiar: (i) seleção ou priorização de itens com relação à cobertura e abrangência de propriedades de segurança e dimensões de avaliação; (ii) seleção de itens que combinam propriedades ou dimensões específicas; (iii) análise de cobertura de itens de um projeto de avaliação com relação a mais de um objetivo (escopo ou segurança); (iv) análise de uma fonte de conhecimento de segurança com respeito à cobertura de características de escopo e de segurança mais importantes.

# 6 CONCLUSÕES

*"At the end of the day, the goals are simple: safety and security."*

*Jodi Rell*

Este trabalho apresenta uma abordagem baseada em critérios e heurísticas (HCApp-Sec) para selecionar e analisar itens de avaliação de segurança pela identificação de itens de avaliação adequados de fontes de conhecimento de segurança com o objetivo de criar projetos efetivos de avaliação de segurança.

As bases conceituais para a área de avaliação de segurança são propostas considerando o contexto de um processo de avaliação de segurança. Os conceitos-chave da abordagem proposta são descritos na forma de classes de SecAOnto (Ontologia de Avaliação de Segurança).

HCApp-Sec baseia-se em critérios e heurísticas de avaliação e visa a aumentar a cobertura das dimensões de avaliação e propriedades de segurança nos projetos de avaliação. Nossa proposta centra-se em usar critérios e heurísticas de avaliação para selecionar melhores itens de avaliação de forma sistemática assegurando, assim, uma cobertura dos principais aspectos de segurança em projetos de avaliação. HCApp-Sec pode ser aplicada a qualquer fonte de conhecimento de segurança para selecionar ou analisar itens de avaliação em relação a, inicialmente, 11 propriedades de segurança e 6 dimensões de avaliação. É possível incorporar novas dimensões e propriedades, bastando apenas formalizá-las conceitualmente e determinar suas distâncias em relação às outras.

HCApp-Sec foi aplicada a uma fonte de conhecimento de segurança bem conhecida (ISO/IEC 27001 – KS1), as coberturas de seus itens de avaliação foram calculadas, e os resultados foram analisados. KS1 foi caracterizada para saber quais dimensões de avaliação e quais propriedades de segurança foram abordadas pelos seus 133 itens de avaliação; são mostradas as quantidades de dimensões e propriedades abordadas por todos os itens de KS1. Identificou-se que é possível selecionar ou priorizar conjuntos de itens de avaliação com melhores características de escopo e segurança com o apoio de critérios e heurísticas de avaliação definidos *a priori*. É

possível selecionar outros conjuntos de itens de avaliação que cubram mais de um objetivo. Todos os critérios e heurísticas propostos foram aplicados na seleção ou priorização dos itens de avaliação de segurança, mostrando a aplicabilidade de HCApp-Sec.

Depreende-se da revisão de literatura que a avaliação de segurança é uma questão complexa e transversal. Os trabalhos têm buscado resolver a questão por meio de combinações de técnicas, formalização conceitual e uso de padrões e guias de melhores práticas. Os objetivos variam desde a definição conceitual até seleção de casos de teste para avaliações de conformidade. As obras analisadas lidam com um amplo espectro de questões e aplicações relacionadas com segurança da informação. Este fato destaca a necessidade de uma exploração aprofundada do assunto.

O ideal seria que a segurança fosse pensada desde o início do ciclo de desenvolvimento dos sistemas, ou que análises de riscos fossem constantes para garantir sistemas mais seguros, mas geralmente questões relacionadas à segurança da informação somente são priorizadas quando algum incidente grave acontece. HCApp-Sec pode contribuir com abordagens tradicionais de segurança: (i) sistematizando e fornecendo garantias aos avaliadores; (ii) indicando conjuntos de ataques abrangentes e efetivos que poderiam ser usados de maneira dual, ou seja, tanto na geração de armas para defesa ativa, quanto na geração de fontes de conhecimento robustas e na proposição de defesas para sistemas críticos.

Com relação à formalização, as ontologias disponíveis, bem como os resultados relatados, são um ponto de partida; no entanto, nenhum dos trabalhos analisados centra-se em relacionar conceitos das áreas de segurança da informação e de avaliação de software, conforme proposto em HCApp-Sec. Critérios formalizados existem na área de teste, mas não no domínio de segurança da informação, que está muito direcionado à análise de vulnerabilidades conhecidas e técnicas ou ferramentas de ataque/defesa.

Nossa proposta centra-se na aplicação de critérios e heurísticas para a seleção de itens de avaliação, visando a aumentar a cobertura de propriedades de segurança em projetos de avaliação. Medidas de cobertura são propostas para apoiar o processo de seleção dos itens e aplicação de critérios e heurísticas propostos. As medidas de cobertura propostas são úteis para: (i) definir e aplicar critérios e heurísticas para seleção de itens de avaliação; (ii) propor itens de avaliação com alta

cobertura de características de segurança; e (iii) avaliar e propor projetos de avaliação, normas, padrões ou modelos de segurança mais apropriados, usando critérios e heurísticas mensuráveis.

Situações onde HCApp-Sec poderia ser aplicada: (i) seleção dos melhores itens com relação à cobertura de propriedades de segurança ou à cobertura de uma propriedade de segurança específica; (ii) seleção de itens que combinam propriedades ou dimensões específicas; (iii) análise de cobertura de itens de avaliação de um projeto com relação a mais de um objetivo (escopo ou segurança); (iv) definição de uma estratégia de avaliação, ou seja, priorização dos itens de avaliação em uma avaliação de segurança; (v) ou análise de uma fonte de conhecimento de segurança com respeito à cobertura de características de escopo e de segurança mais importantes.

## 6.1 LIMITAÇÕES E TRABALHOS FUTUROS

Nesta seção são discutidos limitações e pontos de evolução para trabalhos futuros.

**Aplicação da Abordagem.** Não analisamos a efetividade dos itens selecionados na fase de execução da avaliação. *Proposta*: Conduzir experimentos usando os itens de avaliação selecionados na fase de execução de uma avaliação de segurança. Por exemplo: (i) gerar um projeto de avaliação (AD) usando a abordagem e outro AD usando outros critérios (ex.: vulnerabilidades conhecidas ou seleção aleatória); (ii) usar os ADs gerados para avaliar um sistema ou dispositivo; (iii) analisar os defeitos encontrados com relação a quantidade, tipos de defeitos, criticidade, propriedades abordadas, etc.

**Dimensões de Avaliação.** Novas dimensões de avaliação devem ser incluídas. Na prova de conceito notou-se que a fonte de conhecimento usada considera superficialmente aspectos puramente humanos, que são muito importantes no contexto da segurança da informação e não são geralmente tratados nas fontes de conhecimento. Pessoas mal intencionadas podem atacar sistemas por diversos motivos, tais como, aprendizado, protesto, vingança, diversão, para ganhar visibilidade, para obter ganhos financeiros etc. A maioria desses ataques não necessitam de tecnologia complexa com custo e complexidade elevados, facilitando o seu uso. Por exemplo, Ataques de Regras de

Negócios[5] (acesso legítimo) e Engenharia Social[6] causam impacto e quase nunca são lembrados em projetos e padrões de avaliação de segurança. Itens de avaliação que considerem aspectos humanos devem ser caracterizados ou mapeados em padrões para poderem compor projetos de avaliação de segurança. Não obstante a questão ser tratada em parte pela dimensão de avaliação "Processo", percebe-se a necessidade de propor uma dimensão específica para abordar essas questões, que muitas vezes vão além dos aspectos técnicos ou processuais. *Proposta*: Incluir a Dimensão "*Human*".

**Propriedades de Segurança.** As propriedades de segurança tratadas são apenas parte do universo de características de segurança; propriedades relevantes em outros domínios de interesse devem ser incluídas. *Proposta*: poderiam ser incluídas as seguintes propriedades: Anonimato (*Anonymity*), Divulgação ou Exposição (*Disclosability*), Unicidade ou Singularidade (*Uniqueness*), Precisão (*Accuracy*), Transparência (*Transparency*), Não-coerção (*Non-coercibility*) (Salini & Kanmani, 2012). Estas estão relacionadas ao domínio e-Voting e poderiam ser aplicadas na seleção de itens para avaliação de sistemas de votação eletrônica. Outras propriedades a serem consideradas seriam: Irrevogabilidade ou Impossibilidade de Reversão (*Irrevocability* ou *Irreversibility*), Capacidade de Sobrevivência e Manutenção (*Survivability* e *Maintainability*) (Avizienis et al., 2004).

**Ontologia.** SecAOnto é uma proposta inicial de ontologia de avaliação de segurança da informação. Ela deve ser exercitada para melhorar sua expressividade e conceitos, relações, propriedades e instâncias de classes devem ser incorporados. Trabalhos não publicados na forma de artigos, tais como trabalhos de conceituação em andamento e ontologias não acadêmicas, devem ser objeto de busca em bases de dados de ontologia (por exemplo, Swoogle (Maryland, 2017)). Os conceitos e a ontologia carecem de melhor validação, pois unem duas áreas de atuação quase sempre consideradas conceitualmente isoladas (Avaliação de Sistemas e Segurança da Informação); por esse motivo o OWL já está disponível (Rosa, Jino, & Teixeira Junior,

[5] O Ataque de Regras de Negócios *(Business Logic Attack* – BLA) é um ataque que visa a lógica de uma aplicação. Ao contrário dos ataques "tradicionais", técnicos, os ataques à lógica de negócios não contêm solicitações malformadas e incluem valores de entrada legítimos, tornando difícil detectá-los. BLAs abusam da funcionalidade da aplicação, atacando diretamente o negócio (Imperva, 2018).

[6] O termo "Engenharia Social" (*Social Engineering* – SE) é um ato de manipulação psicológica de um ser humano que está associado às ciências sociais, mas seu uso foi incorporado por profissionais de segurança da informação (Anderson, 2018; Social-engineer.org, 2018). No contexto de segurança da informação o termo é usado para representar formas de enganar pessoas para conseguir acesso indevido a sistemas ou outros ganhos sem usar a tecnologia e usando habilidades emocionais ou de relacionamento interpessoal.

2017c) para possibilitar essa validação pela comunidade científica. Segundo Souag et al. (2015) ontologias são avaliadas com respeito aos seguintes critérios: (i) Completude: uso ou referência (mapeamento) de outras ontologias descritas na literatura; (ii) Validade: capacidade de fornecer respostas confiáveis a um conjunto de perguntas usando sua terminologia; (iii) Usabilidade: demonstração de que a ontologia pode ser usada para reunir requisitos de segurança e reutilizada em diferentes projetos. *Proposta 1*: Incorporação conceitual de novas áreas de aplicação. Por exemplo, SecAOnto-IoE poderia incorporar novas áreas de conhecimento em expansão, tais como, *Internet of Things/Everything* (IoT/IoE) e paradigmas relacionados (*Cloud/Fog/Edge Computing*). *Proposta 2*: Avaliação de SecAOnto com base nos critérios propostos por Souag et al. (2015).

**Cálculos de Cobertura.** Faz-se necessário aprimorar o cálculo de cobertura, por meio da automatização do preenchimento das matrizes de adjacências; o preenchimento ainda não está implementado, ou seja, os valores das distâncias conceituais entre dimensões e entre propriedades são definidos *a priori* (de forma estática) nas matrizes para possibilitar a prova de conceito. Existem diversas maneiras que poderiam ser usadas para calcular automaticamente as distâncias. Espera-se que as matrizes sejam geradas automaticamente em tempo de cálculo por meio de, por exemplo, uma contagem de termos que identificam os conceitos na ontologia (anotação *IsIdentifiedBy* das Classes). *Proposta*: Criar algoritmo que percorre a ontologia lendo os termos contidos nas anotações dos conceitos para prover uma medida de similaridade sintática entre as classes e preencher dinamicamente as matrizes de adjacências; essa medida posteriormente é usada no cálculo das coberturas. A medida de distância a ser gerada dinamicamente poderia, por exemplo, seguir os princípios de cálculos de similaridade/dissimilaridade propostos por Santini & Jain (1999) e por Boriah, Chandola, & Kumar (2008). Neste caso, uma representação *fuzzy* (escala) poderia ser proposta em substituição à proposta atual (*0* ou *1* – aborda/não-aborda).

**Prova de Conceito.** A amostra de fontes de conhecimento de segurança usada na prova de conceito é pouco representativa (uma fonte); a comparação poderia ser mais rica se fossem usadas mais fontes de conhecimento. *Proposta*: Conduzir um novos experimentos, aplicando HCApp-Sec a outras fontes de conhecimento de segurança e fazer comparação entre os dados das fontes. Os dados obtidos possibilitariam a criação e execução de algoritmos de otimização multi-objetivo para selecionar AIs com melhor

desempenho quando é imposto um conjunto de objetivos conflitantes. A partir de novos experimentos, é possível propor padrões de avaliação de segurança com AIs de várias fontes, possivelmente categorizados por domínios de aplicação, tais como *e-Health*, *e-Voting,* etc. Quando outras fontes de conhecimento de segurança forem incorporadas à base, novos conceitos e termos serão identificados.

**Aplicação de Critérios e Heurísticas.** Uma contribuição interessante seria propor estratégias de avaliação de segurança, estabelecendo ordens de execução de critérios e heurísticas de avaliação de segurança. É possível propor escolhas entre critérios e heurísticas com base no custo, cobertura ou outro parâmetro. Ex.: iniciar a seleção de itens de avaliação com base em critérios mais fracos; usar heurísticas de cobertura bi-objetivo. *Proposta*: aprimorar o software *back-end* que calcula as coberturas para propor projetos de avaliação com base em requisitos (ou restrições de busca), tais como: (i) KSs com CovGLO maior que um dado valor; (ii) AIs que abordem ao mesmo tempo as DMs "*1*" e "*4*" e as PPs "*3*" e "*7*"; (iii) AIs que em projetos anteriores tenham encontrado uma determinada classe de defeito; entre outras várias possibilidades.

**Protótipo de Software.** Apesar de ter servido ao seu propósito de prova conceitual e sua primeira versão ter sido registrada no INPI, o protótipo de sistema desenvolvido precisa ser aprimorado, tanto na arquitetura, quanto na infraestrutura de apoio; para novas versões, é necessário que o sistema execute algumas funções automaticamente para facilitar o trabalho do engenheiro que planeja a avaliação. *Proposta*: uma nova versão do Protótipo de Software poderia ser desenvolvida, com o objetivo de evoluir a arquitetura da solução, automatizar certas funções, integrar componentes e melhorar a infraestrutura de apoio da aplicação.

**Hierarquias de Inclusão e Transitividade.** Pode-se verificar se é possível definir hierarquias de inclusão entre as propriedades de segurança fundamentadas em objetivo, por exemplo, proteção, monitoração, legalização, etc. Uma relação conceitual pode ser pensada entre as propriedades confidencialidade e privacidade, mas isso precisa ser verificado. Outra questão a ser analisada é se a transitividade está presente nas relações conceituais entre propriedades de segurança. *Proposta*: Verificar se é possível definir relações de inclusão ou transitividade entre as propriedades de segurança propostas. Verificar, por exemplo: (i) Se satisfizer Privacidade, satisfaz Confidencialidade; (ii) Se satisfizer todas as propriedades, satisfaz qualquer

propriedade de segurança específica; (iii) Se Privacidade é distante 0,4 de Confidencialidade, e esta é distante 0,3 de Integridade, então Privacidade é distante 0,7 de Integridade? Para verificar essas e outras questões conceituais interessantes, um estudo aprofundado do significado dos termos que identificam as propriedades de segurança precisa ser conduzido.

**Substituição de Heurísticas.** Como as heurísticas são aproximações para objetivos, pode-se pensar em substituí-las por soluções exatas que, por exemplo, selecione o melhor conjunto de *10* AIs; ou um dos menores conjuntos de AIs que cubra 80% das propriedades de segurança. *Proposta*: Desenvolver algoritmos para selecionar melhores conjuntos de itens de avaliação. Por exemplo, métodos meta-heurísticos podem ser aplicados para indicar melhores conjuntos de soluções viáveis.

# REFERÊNCIAS


Addison-Hewitt Associates. (2015). A Guide To The Sarbanes-Oxley Act (SOX). Retrieved November 2, 2015, from http://www.soxtoolkit.com/sox-check.htm

Anderson, R. J. (2018). *Security engineering: a guide to building dependable distributed systems*. Indianapolis: Wiley.

Aschmann, M., Jansen van Vuuren, J., & Leenen, L. (2015). Towards the Establishment of an African Cyber-Army. *Defense Peace Safety and Security, CSIR*.

Avizienis, A., Laprie, J. C., & Randell, B. (2004). Dependability and its Threats: A Taxonomy. *Building the Information Society: Proc. IFIP 18th World Computer Congress, 22-27 August 2004, Toulouse, France*, (July 1834), 91–120. http://doi.org/10.1.1.1.5946

Azevedo, R. R., Freitas, F., Almeida, S. C., Almeida, M. J. S., C., B. F. E., & Veras, W. C. (2008). CoreSec : An Ontology of Security Aplied to the Business Process of Management. *Proceedings of the 2008 ACM Euro American Conference on Telematics and Information Systems*, 13.

BACEN. (2017). BACEN/STN Manual de Segurança da RSFN. Retrieved August 23, 2017, from http://www.bcb.gov.br/sfn/ced/ManualdeSeguran%C7adaRSFN-v32.pdf

Bach, J. (1997). Good Enough Quality: Beyond the Buzzword. *Computer*, 8–97.

Bach, J. M. (2003). Exploratory Testing Explained. Retrieved October 16, 2016, from http://www.satisfice.com/articles/et-article.pdf

Bachlechner, D., Maier, R., Innerhofer-Oberperfler, F., & Demetz, L. (2011). Understanding the management of information security controls in practice. In *9th Australian Information Security Management Conference* (pp. 40–48).

Bai, X., Dong, W., Tsai, W. T., & Chen, Y. (2005). WSDL-Based Automatic Test Case Generation for Web Services Testing. *Proceedings of the IEEE International Workshop*, 220.

Barbosa, E. F., Nakagawa, E. Y., & Maldonado, J. C. (2006). Towards the Establishment of an Ontology of Software Testing. *Seke*. Retrieved from http://www.labes.icmc.usp.br/moduloeducacional/publicacoes/SK06Ellen.pdf

Barr, N. (2012). *The relevance of efficiency to different theories of society*. *Economics of the Welfare State* (5th ed.). Oxford University Press.

Barreto, A. de B. (2013). *Cyber-ARGUS Framework - Measuring Cyber-impact on the Mission*. Technological Institute of Aeronautics (ITA).

Barros, C. P. de, Rosa, F. de F., & Balcão Filho, A. F. (2013). Software Testing With

Emphasis on Finding Security Defects. In *IADIS - The 12th International Conference on WWW/Internet* (pp. 226–228).

Basso, T., Moraes, R. L. O., & Jino, M. (2010). A Methodology for Effectiveness Analysis of Vulnerability Scanning Tools. Retrieved from http://www.dca.fee.unicamp.br/portugues/pesquisa/seminarios/2010/artigos/basso_moraes_jino.pdf

BBC News. (2016a, July 30). Russia cyber attack: Large hack "hits government." Retrieved from http://www.bbc.com/news/world-europe-36933239

BBC News. (2016b, October 22). "Smart" home devices used as weapons in website attack. Retrieved from http://www.bbc.com/news/technology-37738823

Beauvoir, P. (2015). Archi - ArchiMate Modelling Tool. Retrieved November 6, 2015, from http://www.archimatetool.com/

Bechhofer, S., Horrocks, I., van Harmelen, F., Hendler, J., McGuinness, D. L., Patel-Schneider, P. F. ., & Stein, L. A. (2004). OWL Web Ontology Language Reference. Retrieved from http://www.w3.org/TR/owl-ref/

Bermejo, J. (2007). A Simplified Guide to Create an Ontology, 1–12.

Bialas, A. (2017). Computer Support for Risk Management in Critical Infrastructures. *Advances in Network Systems*. Springer.

Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 833–844). ACM.

Biolchini, J., Mian, P. G., Candida, A., & Natali, C. (2005). Systematic Review in Software Engineering. *Engineering*, *679*(May), 165–176. http://doi.org/10.1007/978-3-540-70621-2

Boriah, S., Chandola, V., & Kumar, V. (2008). Similarity Measures for Categorical Data: A Comparative Evaluation. *Proceedings of the 2008 SIAM International Conference on Data Mining*. Society for Industrial and Applied Mathematics.

Bostwick, G. L. (1976). A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision. *California Law Review*, *64*(6), 1447–1483.

Botella, J., Capuron, J.-F., Dadeau, F., Fourneret, E., Legeard, B., & Schadle, F. (2018). Complementary test selection criteria for model-based testing of security components. *International Journal on Software Tools for Technology*. Springer Berlin Heidelberg. http://doi.org/https://doi.org/10.1007/s10009-018-0489-2

Botella, J., Legeard, B., Peureux, F., & Vernotte, A. (2014). Risk-based vulnerability testing using security test patterns. In *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation* (pp. 337–352). Springer Berlin Heidelberg.

Bowen, P., Hash, J., & Wilson, M. (2006). NIST - Information Security Handbook: A Guide for Managers. *NIST Special Publication 800-100*. National Institute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Brasil. (2015). Padrões de Interoperabilidade de Governo Eletrônico - ePING: 2. Segurança. Retrieved October 8, 2015, from http://eping.governoeletronico.gov.br/#p2s2

BSI. (2008). BSI Standard 100-2 IT-Grundschutz Methodology Version 2.0. *British Standards Institution*.

Bueno, P. M. S. (2012). *Geração de Dados de Teste Orientada à Diversidade com o uso de Meta-Heurísticas*. Universidade Estadual de Campinas - UNICAMP.

Bueno, P. M. S., Jino, M., & Wong, W. E. (2011). Diversity oriented test data generation using metaheuristic search techniques. *Information Sciences*, *259*, 490–509. http://doi.org/10.1016/j.ins.2011.01.025

Burnstein, I. (2002). *Practical Software Testing: A Process-Oriented Approach* (New York). Springer.

Carniello, A. (2003). *Teste Baseado na Estrutura de Casos de Uso*. University of Campinas.

Chikh, A., Abulaish, M., Nabi, S., & Alghathbar, K. (2011). An ontology based information security requirements engineering framework. *Secure and Trust Computing, Data Management and Applications*, *186*, 139–146. http://doi.org/10.1007/978-3-642-22339-6_17

CIRT.NET. (2017). Nikto - An Open Source Web Server Scanner. Retrieved August 8, 2017, from https://cirt.net/Nikto2

Colombo, R. M. T. (2014). *Proposta de uma Metodologia de Medição e Priorização de Segurança de Acesso para Aplicações Web*. Universidade de São Paulo - USP.

Copeland, L. (2003). *A Practitionar's Guide to Software Test Design*.

CSA. (2015). *CAIQ/CSA - Consensus Assessments Initiative Questionnaire v3.0.1 / Cloud Security Alliance*. Retrieved from https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/

Daramola, O., Sindre, G., & Stalhane, T. (2012). Pattern-based security requirements specification using ontologies and boilerplates. *2012 2nd IEEE International Workshop on Requirements Patterns, RePa 2012 - Proceedings*, 54–59. http://doi.org/10.1109/RePa.2012.6359973

Darmaillacq, V., Fernandez, J.-C., Groz, R., Mounier, L., & Richier, J.-L. (2006). Test Generation for Network Security Rules. *TestCom*, *3964*, 341–356.

DCSSI. (2016). EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m%7B_%7Debios.html

Delamaro, M. E., Maldonado, J. C., Barbosa, E. F., Vicenzi, A., & Jino, M. (2007). *Introdução ao Teste de Software*.

Diéguez, M., Cares, C., & Cachero, C. (2017). Methodology for the Information Security Controls Selection. In *12th Iberian Conference on Information Systems and Technologies (CISTI)*. Lisbon, Portugal: IEEE. http://doi.org/10.23919/CISTI.2017.7975811

Duarte, L. O., Montes Filho, A., Guerra, A. C., & Rosa, F. de F. (2010). Característica Segurança em Qualidade de Produto de Software (pp. 221–228).

Dürbeck, S., Fritsch, C., Pernul, G., & Schillinger, R. (2010). A semantic security architecture for web services - The access-eGov solution. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 222–227. http://doi.org/10.1109/ARES.2010.117

Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. (2006). Security Ontology: Simulating Threats to Corporate Assets. In *ICISS - Lecture Notes in Computer Science, vol. 4332/2006* (pp. 249–259). Kolkata, India: Springer Berlin / Heidelberg. http://doi.org/10.1007/11961635_17

Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. (2007). Security ontologies: Improving quantitative risk analysis. In *40th Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156–162). Los Alamitos, CA, USA: IEEE Computer Society. http://doi.org/http://doi.ieeecomputersociety.org/10.1109/HICSS.2007.478

Elahi, G. (2009). Security Requirements Engineering: State of the Art and Practice and Challenges. Retrieved from http://www.cs.utoronto.ca/~gelahi/DepthPaper.pdf

Energy, U. D. of. (2017). Cybersecurity Capability Maturity Model (C2M2). Retrieved August 23, 2017, from https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

ENISA. (2011). *Ontology and taxonomies of Resilience*. Retrieved from https://www.enisa.europa.eu/publications/ontology_taxonomies

Evesti, A., Savola, R., Ovaska, E., & Kuusijarvi, J. (2011). The design, instantiation, and usage of information security measuring ontology. *Proceedings of the 4th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, (c), 204–212.

Fantinato, M. (2002). *Critérios de Teste Funcional Baseados em Máquinas de Estado Finitos Estendidas*. UNICAMP.

Felderer, M., Büchler, M., Johns, M., Brucker, A. D., Breu, R., & Pretschner, A. (2016).

Security Testing: A Survey. *Advances in Computers*, *101*, 1–51. http://doi.org/10.1016/bs.adcom.2015.11.003

Feledi, D., & Fenz, S. (2012). Challenges of web-based information security knowledge sharing. *2012 Seventh International Conference on Availability, Reliability and Security*, 514–521. http://doi.org/10.1109/ARES.2012.59

Fenz, S. (2010). Ontology-based generation of IT-security metrics. *ACM Symposium on Applied Computing*, 1833–1839. http://doi.org/10.1145/1774088.1774478

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *… 4th International Symposium on Information …*, 183. http://doi.org/10.1145/1533057.1533084

Fenz, S., Pruckner, T., & Manutscheri, A. (2009). Ontological mapping of information security best-practice guidelines. *Lecture Notes in Business Information Processing*, *21 LNBIP*, 49–60. http://doi.org/10.1007/978-3-642-01190-0_5

Ficco, M., & Romano, L. (2010). A Correlation Approach to Intrusion Detection. http://doi.org/10.1007/978-3-642-16644-0_19

Gartner, S., Ruhroth, T., Burger, J., Schneider, K., & Jurjens, J. (2014). Maintaining requirements for long-living software systems by incorporating security knowledge. *2014 IEEE 22nd International Requirements Engineering Conference (RE)*, 103–112. http://doi.org/10.1109/RE.2014.6912252

Giulliano, C., Lúcio, M., & Galvão, C. (2014). Manual Operacional de Ensaios e Análises para Certificação de S-RES.

Goodrich, M. T., & Tamassia, R. (2010). *Introduction to Computer Security* (1st ed.). Addison-Wesley.

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations. *Milbank Quarterly*, *82*, 581–629. http://doi.org/10.1111/j.0887-378X.2004.00325.x

Grobler, M., van Vuuren, J. J., & Leenen, L. (2012). Implementation of a Cyber Security Policy in South Africa : Reflection on Progress and the Way Forward. *ICT Critical Infrastructures and Society*, *386*(2012), 215–225. http://doi.org/10.1007/978-3-642-33332-3_20

Guarino, N. (1998). Formal ontology and information systems. In *ACM International Conference in Formal Ontology and Information Systems*. Trento, Italy.

Guizzardi, G., Falbo, R., & Guizzardi, R. S. S. (2008). Grounding Software Domain Ontologies in the Unified Foundational Ontology ( UFO ): The case of the ODE Software Process Ontology. In *IBEROAMERICAN WORKSHOP ON REQUIREMENTS ENGINEERING AND SOFTWARE ENVIRONMENTS* (pp. 127–140). Recife, Brazil.

Gyrard, A., Bonnet, C., & Boudaoud, K. (2013). A machine-to-machine architecture to

merge semantic sensor measurements. *Proceedings of the 22nd International Conference on …*, 371–375. Retrieved from http://dl.acm.org/citation.cfm?id=2487945

Gyrard, A., Bonnet, C., Boudaoud, K., Gyrard, A., Bonnet, C., Boudaoud, K., … Bonnet, C. (2014). The STAC ( Security Toolbox : Attacks & Countermeasures ) ontology.

Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy*, *1*(4), 1–23.

Hu, J., Bertok, P., & Tari, Z. (2008). Taxonomy and framework for integrating dependability and security. In *Information Assurance: Dependability and Security in Networked Systems* (pp. 149–170).

Huang, Y. C., Peng, K. L., & Huang, C. Y. (2012). A history-based cost-cognizant test case prioritization technique in regression testing. *Journal of Systems and Software*, *85*(3), 626–637.

Hustadt, U., Motik, B., & Sattler, U. (2005). Data complexity of reasoning in very expressive description logics. *IJCAI*, *5*, 466–471.

Hwang, J., Xie, T., El Kateb, D., Mouelhi, T., & Le Traon, Y. (2012). Selection of regression system tests for security policy evolution. In *Proceedings of the 27th IEEE/ACM international conference on automated software engineering* (pp. 266–269).

Imperva. (2018). Security Glossary. Retrieved from https://www.imperva.com/Resources/Glossary/

ISACA. (2015). ISACA Information Systems Glossary. Retrieved October 16, 2015, from http://www.isaca.org/Pages/Glossary.aspx

ISECON. (2010). OSSTMM 3 – The Open Source Security Testing Methodology Manual.

ISO/IEC. (2008a). ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.

ISO/IEC. (2008b). ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.

ISO/IEC. (2008c). ISO/IEC 21827:2008 Systems Security Engineering - Capability Maturity Model (SSE-CMM).

ISO/IEC. (2009). ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

ISO/IEC. (2011). ISO/IEC 25040:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation process. Retrieved August 31, 2017, from https://www.iso.org/obp/ui/#iso:std:iso-iec:25040:ed-1:v1:en

ISO/IEC. (2013a). ISO/IEC 27001:2013 Information technology -- Security techniques --

Information security management systems -- Requirements.

ISO/IEC. (2013b). ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls.

ISSA-UK. (2015). ISSA 5173 – The Security Standard for SMES. Retrieved November 2, 2015, from https://www.2-sec.com/2011/03/22/issa-5173-the-security-standard-for-smes/

Jouini, M., Rabai, L. B. A., & Khedri, R. (2015). A Multidimensional Approach towards a Quantitative Assessment of Security Threats. *Procedia Computer Science*, *52*(Ant), 507–514. http://doi.org/10.1016/j.procs.2015.05.024

Jutla, D., & Xu, L. (2004). Privacy Agents and Ontology for the Semantic Web. *Americas Conference on Information Systems*, 1760–1767.

Kang, W., & Liang, Y. (2013). A security ontology with MDA for software development. *Proceedings - 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2013*, 67–74. http://doi.org/10.1109/CyberC.2013.20

Kassab, M., Ormandjieva, O., & Daneva, M. (2011). Relational-model based change management for non-functional requirements: Approach and experiment. In *IEEE Fifth International Conference on Research Challenges in Information Science (RCIS)* (pp. 1–9).

Khairkar, A. D., Kshirsagar, D. D., & Kumar, S. (2013). Ontology for detection of web attacks. *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013*, 612–615. http://doi.org/10.1109/CSNT.2013.131

Kiesling, E., Strausß, C., & Stummer, C. (2012). A multi-objective decision support framework for simulation-based security control selection. In *IEEE Seventh International Conference on Availability, Reliability and Security (ARES)*. IEEE.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(TR/SE-0401), 28. http://doi.org/10.1.1.122.3308

Koinig, U., Tjoa, S., & Ryoo, J. (2015). Contrology - An Ontology-Based Cloud Assurance Approach. *2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 105–107. http://doi.org/10.1109/WETICE.2015.43

Kotenko, I., Polubelova, O., Saenko, I., & Doynikova, E. (2013). The ontology of metrics for security evaluation and decision support in SIEM systems. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 638–645. http://doi.org/10.1109/ARES.2013.84

Krötzsch, M., Simančík, F., & Horrocks, I. (2012). A Description Logic Primer. *CoRR*, *abs/1201.4*. Retrieved from http://arxiv.org/abs/1201.4089

Leão, B. D. F., Giulliano, C., Lúcio, M., & Galvão, C. (2013). Manual de Certificação para Sistemas de Registro Eletrônico em Saúde ( S-RES ). *Sociedade Brasileira de Informática Em Saúde*, 92. Retrieved from http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2009_v3-3.pdf

Lewis, W. E. (2000). *Software Testing and Continuous Quality Improvement*. New York: CRC Press LLC.

Li, Z., Sanghi, M., Chen, Y., Kao, M. Y., & Chavez, B. (2006). Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience. In *IEEE Symposium on Security and Privacy* (pp. 15–47). IEEE.

Liu, F.-H., & Lee, W.-T. (2010). Constructing Enterprise Information Network Security Risk Management Mechanism by Ontology. *Journal of Applied Science and Engineering*, *13*(1), 79–87.

Lozano-Tello, A., & Gomez-Perez, A. (2004). ONTOMETRIC: A method to choose the appropriate ontology. *Journal of Database Management*, *15*(2), 1–18.

Maheswari, R. U., & Mala, D. J. (2018). Heuristic-based time-aware multi-criteria test case prioritisation technique. *International Journal of Information Systems and Change Management*. Inderscience. http://doi.org/https://doi.org/10.1504/IJISCM.2017.091275

Maryland, U. of. (2017). Swoogle - Semantic Web Search. Retrieved September 21, 2017, from http://swoogle.umbc.edu/2006/

Massacci, F., Mylopoulos, J., Paci, F., Yu, Y., & Tun, T. T. (2011). An Extended Ontology for Security Requirements. http://doi.org/10.1007/978-3-642-22056-2_64

Medeiros, N., Ivaki, N., Costa, P., & Vieira, M. (2017). Software Metrics as Indicators of Security Vulnerabilities. In *The 28th IEEE International Symposium on Software Reliability Engineering (ISSRE 2017)*. Toulouse, France.

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., & Murukan, A. (2003). Improving Web Application Security Threats and Countermeasures. Microsoft.

Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. *Computer Standards & Interfaces*, *32*(4), 153–165. http://doi.org/10.1016/j.csi.2010.01.006

Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces*, *29*(2), 244–253. http://doi.org/10.1016/j.csi.2006.04.002

Mertl, S. (2016, March 5). How cars have become rolling computers. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/

MITRE. (2015). *Common Vulnerabilities and Exposures (CVE)*. Retrieved from

http://cve.mitre.org/

MITRE. (2017). Ten Strategies of a World-Class Cybersecurity Operations Center. Retrieved August 23, 2017, from https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

Moradian, E., Håkansson, A., & Andersson, J. (2012). *Ontology Based Patterns for Software Security Engineering*. Retrieved from https://books.google.com.br/books?hl=pt-BR&lr=&id=POW2ijBMJNwC&oi=fnd&pg=PA406&ots=H7-vNyRlCo&sig=YrlKG7tUgH7cjjUPp3kZLJBbWHE#v=onepage&q&f=false

Mundie, D. a., & Mcintire, D. M. (2013). The MAL: A Malware Analysis Lexicon. *2013 International Conference on Availability, Reliability and Security*, (February), 556–558. http://doi.org/10.1109/ARES.2013.73

Nabil, S., & Mohamed, B. (2012). Security ontology for semantic SCADA. *CEUR Workshop Proceedings*, *867*, 179–192.

NeOn. (2015). NEON Toolkit. Retrieved October 16, 2015, from http://neon-toolkit.org/

Nespoli, P., Papamartzivanos, D., Marmol, F. G., & Kambourakis, G. (2017). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *IEEE Communications Surveys & Tutorials*, (c), 1–1. http://doi.org/10.1109/COMST.2017.2781126

Neto, A. C. de A. (2012). *Security Beanchmarking of Transactional Systems*. University of Coimbra.

Neubauer, T., Ekelhart, A., & Fenz, S. (2008). Interactive selection of ISO 27001 controls under multiple objectives. In *IFIP International Information Security Conference* (pp. 477–492). Boston, MA: Springer.

NIST. (2008). Technical Guide to Information Security Testing and Assessment - SP 800-115.

NIST. (2015a). NISTIR 7621 - Small Business Information Security: The Fundamentals. Retrieved November 2, 2015, from http://www.nist.gov

NIST. (2015b). *NVD CVSS - Common Vulnerability Scoring System Support v2*. Retrieved from https://nvd.nist.gov/cvss.cfm

NIST. (2017a). FIPS 140-2 Security Requirements for Cryptographic Modules. Retrieved August 23, 2017, from http://csrc.nist.gov/groups/STM/cmvp/

NIST. (2017b). Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication 800-53*. http://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4

Obrst, L. (2010). Ontological architectures. *Theory and Applications of Ontology: Computer Applications. Springer Netherlands.*, 27–66.

Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. *Seventh International Conference on Semantic Technologies for. Intelligence, Defense, and Security – STIDS 2012.*, 49–56. Retrieved from http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf

OSVDB. (2015). Open Sourced Vulnerability Database. Retrieved October 9, 2015, from osvdb.org

Otero, A. R., Otero, C. E., & Qureshi, A. (2010). A multi-criteria evaluation of information security controls using Boolean features. *International Journal of Network Security & Its Applications (IJNSA)*, *2*(4).

OWASP. (2008). OWASP Testing Guide v3.0. *OWASP Foundation*, 349.

OWASP. (2015). OWASP Top 10 Privacy Risks Project. Retrieved October 9, 2015, from https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

Paydar, S., & Kahani, M. (2010). Ontology-based web application testing. *Novel Algorithms and Techniques in Telecommunications and Networking*, 23–27. http://doi.org/10.1007/978-90-481-3662-9-4

PCI Security Standards Council. (2015). Payment Card Industry Data Security Standard (PCI DSS). Retrieved November 2, 2015, from https://www.pcisecuritystandards.org/

Pereira, T. S. M., & Santos, H. (2010). A security framework for audit and manage information system security. *Proceedings - 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology - Workshops, WI-IAT 2010*, 29–32. http://doi.org/10.1109/WI-IAT.2010.244

Pereira, T. S. M., & Santos, H. (2012). An Ontological Approach to Information Security Management. In *7th International Conference on Information Warfare and Security*.

Polya, G. (1945). *How to solve it: A new aspect of mathematical method*. Princeton University Press.

Portokalidis, G., Slowinska, A., & Bos, H. (2006). Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation. *ACM SIGOPS Operating Systems Review.*, 15–27.

Pumvarapruek, N., & Senivongse, T. (2014). Classifying Cloud Provider Security Conformance to Cloud Controls Matrix, *66*.

Ramanauskaite, S., Olifer, D., Goranin, N., & Čenys, A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications and Control*, *8*(6), 878–890.

Rapps, S., & Weyuker, E. J. (1985). Selecting Software Test Data Using Data Flow Information, (4).

Raskjn, V., Hempelmann, C. F., Nirenburg, S., & Lafayette, W. (2002). Ontology in Information Security : A Useful Theoretical Foundation and Methodological Tool. *Workshop on New Security Paradigm*, 53–59. http://doi.org/10.1.1.84.3572

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 1–6. http://doi.org/10.1109/ISADS.2013.6513420

Razzaq, A., Latif, K., Farooq Ahmad, H., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks. *Information Sciences*, *254*, 19–38. http://doi.org/10.1016/j.ins.2013.08.007

Rieke, R., Schütte, J., & Hutchison, A. (2012). Architecting a security strategy measurement and management system. *Proceedings of the Workshop on Model-Driven Security - MDsec '12*, (2), 1–6. http://doi.org/10.1145/2422498.2422500

Rosa, F. de F., Bonacin, R., Bueno, P. M. S., & Jino, M. (2018). Coverage-based Heuristics for Selecting Assessment Items of Security Standards: a core set proposal. In *IEEE International Workshop on Metrology for Industry 4.0 and IoT*. Brescia, Italy: IEEE.

Rosa, F. de F., & Jino, M. (2016). Arquitetura Conceitual para Avaliação de Segurança de Sistemas Web. In L. Rodrigues (Ed.), *Proceedings of 14ª Conferência Ibero Americana WWW/Internet* (pp. 393–397). Lisboa, Portugal: IADIS Press.

Rosa, F. de F., & Jino, M. (2017). A Survey of Security Assessment Ontologies. In J. Kacprzyk (Ed.), *Advances in Intelligent Systems and Computing (AISC)* (569th ed., pp. 166–173). Springer International Publishing. http://doi.org/10.1007/978-3-319-56535-4_17

Rosa, F. de F., Jino, M., & Bonacin, R. (2017). *The Security Assessment Domain: A Survey of Taxonomies and Ontologies*. Campinas/SP, Brazil: Renato Archer Information Technology Center (CTI). Retrieved from https://www.researchgate.net/publication/318015008_The_Security_Assessment_Domain_A_Survey_of_Taxonomies_and_Ontologies

Rosa, F. de F., Jino, M., & Bonacin, R. (2018a). HCApp-Sec: Heuristics and Criteria based Approach for Selecting and Analyzing Security Assessment Items. *Journal of Software: Practice and Experience (Submited)*, 40.

Rosa, F. de F., Jino, M., & Bonacin, R. (2018b). Towards an Ontology of Security Assessment: A Core Model Proposal. (S. (eds) Latifi, Ed.) *Latifi S. (Eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing*. Las Vegas: Springer, Cham. http://doi.org/https://doi.org/10.1007/978-3-319-77028-4_12

Rosa, F. de F., Jino, M., Bonacin, R., & Teixeira-Junior, L. A. L. (2018). An Ontology of Security Assessment. *Journal of Web Semantics (Submited)*, 19.

Rosa, F. de F., Jino, M., & Teixeira Junior, L. A. L. (2017a). Conceptual Architecture for Information Systems Security Assessment. Retrieved March 17, 2017, from

https://github.com/ferruciof/Caissa

Rosa, F. de F., Jino, M., & Teixeira Junior, L. A. L. (2017b). Dataset of KS1 (ISO/IEC 27001) – Assessment Items. Retrieved January 12, 2017, from https://github.com/ferruciof/Files/tree/master/Dataset-KS1

Rosa, F. de F., Jino, M., & Teixeira Junior, L. A. L. (2017c). Security Assessment Ontology - SecAOnto. Retrieved from https://github.com/ferruciof/Files/blob/master/SecAOnto/SecAOnto_V4.owl

Rosa, F. de F., Jino, M., Teixeira Junior, L. A. L., & Balcão Filho, A. F. (2016a). CAISSA - Conceptual Architecture for Information Systems Security Assessment. Retrieved November 28, 2016, from http://caissabeta.myftp.org/

Rosa, F. de F., Jino, M., Teixeira Junior, L. A. L., & Balcão Filho, A. F. (2016b). Framework para Geração de Conjunto de Critérios de Teste de Segurança de Software. INPI. Retrieved from https://github.com/ferruciof/Caissa

Rothermel, G., Untch, R. H., Chu, C. C., & Harrold, M. J. (1999). Test case prioritization: an empirical study. *Software Maintenance, 1999. (ICSM '99) Proceedings. IEEE International Conference On*, 179–188. http://doi.org/10.1109/ICSM.1999.792604

Ryber, T. (2007). *Essential Software Test Design*. Fearless Consulting KB.

Saeki, M., Hayashi, S., & Kaiya, H. (2013). Enhancing Goal-Oriented Security Requirements Analysis Using Common Criteria-Based Knowledge. *International Journal of Software Engineering and Knowledge Engineering*, *23*(05), 695–720. http://doi.org/10.1142/S0218194013500174

Salini, P., & Kanmani, S. (2012). A Knowledge-Oriented Approach to Security Requirements Engineering for E-Voting System, *49*(11), 21–25.

Salini, P., & Kanmani, S. (2013). Ontology-based representation of reusable security requirements for developing secure web applications.

Santini, S., & Jain, R. (1999). Similarity Measures. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *21*(9), 871–883. http://doi.org/10.1109/34.790428

Savola, R. (2007). Towards a taxonomy for information security metrics. *ACM Workshop on Quality of Protection*, 28–30. http://doi.org/10.1145/1314257.1314266

Savola, R., Pentikäinen, H., & Ouedraogo, M. (2010). Towards security effectiveness measurement utilizing risk-based security assurance. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. http://doi.org/10.1109/ISSA.2010.5588322

SEI/CMU. (2015). The OCTAVE Method. Retrieved November 5, 2015, from http://www.cert.org/resilience/products-services/octave/

Semy, S. K., Pulvermacher, M. K., & Obrst, L. J. (2004). *Toward the use of an upper ontology for US government and US military domains: An evaluation.* BEDFORD MA

- USA.

Shahriar, H., & Zulkernine, M. (2011). Taxonomy and classification of automatic monitoring of program security vulnerability exploitations. *Journal of Systems and Software*, *84*(2), 250–269. http://doi.org/10.1016/j.jss.2010.09.020

Social-engineer.org. (2018). What is Social Engineering? Retrieved from https://www.social-engineer.org/about/

Sommerville, I. (2007). *Software Engineering - 8th Edition*. Pearson Education Limited. Retrieved from www.pearsoned.co.uk

Souag, A. (2012). Towards a New Generation of Security Requirements Definition Methodology Using Ontologies. *24th International Conference on Advanced Information Systems Engineering (CAiSE'12)*.

Souag, A., Salinesi, C., Mazo, R., & Comyn-Wattiau, I. (2015). A Security Ontology for Security Requirements Elicitation. http://doi.org/10.1007/978-3-319-15618-7_13

Souag, A., Salinesi, C., Wattiau, I., & Mouratidis, H. (2013). Using security and domain ontologies for security requirements analysis. *Proceedings - International Computer Software and Applications Conference*, 101–107. http://doi.org/10.1109/COMPSACW.2013.124

Souza, E. F. de, & de Souza, E. F. (2014). *Knowledge Management Applied to Software Testing: An Ontology Based*. Instituto Nacional de Pesquisas Espaciais - INPE.

Souza, É. F. de, Falbo, R. de A., & Vijaykumar, N. L. (2017). ROoST: Reference Ontology on Software Testing. *Applied Ontology*, *12*(1), 59–90. http://doi.org/10.3233/AO-170177

Stambul, M. A. M., & Razali, R. (2011). An assessment model of information security implementation levels. In *International Conference on Electrical Engineering and Informatics (ICEEI)*. Bandung, Indonesia: IEEE. http://doi.org/10.1109/ICEEI.2011.6021561

Stanford, C., Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010). State of The Art: Automated Black Box Web Application Vulnerability Testing. *Security and Privacy (SP), 2010 IEEE Symposium On*. Retrieved from http://www.owasp.org/images/2/28/Black_Box_Scanner_Presentation.pdf

Stanford University. (2015). Protégé. Retrieved October 16, 2015, from http://protege.stanford.edu/

Su, Z., & Biennier, F. (2010). End-to-end security policy description and management for collaborative system. *2010 6th International Conference on Information Assurance and Security, IAS 2010*, 137–142. http://doi.org/10.1109/ISIAS.2010.5604183

The Apache Software Foundation. (2017). JENA Ontology API - Apache JENA Framework. Retrieved April 11, 2017, from https://jena.apache.org/documentation/ontology/

The New York Times. (2012, June 21). Obama Order Sped Up Wave of Cyberattacks Against Iran. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

The Open Group. (2018). Archimate Notation. Retrieved May 29, 2018, from http://www.opengroup.org/subjectareas/enterprise/archimate-overview

The SANS Institute. (2015). Critical Security Controls for Effective Cyber Defense. Retrieved from http://www.sans.org/critical-security-controls

The Tesla Team. (2016, June 30). A Tragic Loss.

Tinkham, A., & Kaner, C. (2003). Exploring Exploratory Testing 1, (May 2001), 1–9.

Tsoumas, B., & Gritzalis, D. (2006). Towards an ontology-based security management. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *1*, 985–990. http://doi.org/10.1109/AINA.2006.329

U.S. Department of Health & Human Services. (2015). Health Insurance Portability and Accountability Act (HIPAA). Retrieved November 2, 2015, from http://www.hhs.gov/ocr/privacy/

Vasilevskaya, M. (2013). *Designing Security-enhanced Embedded Systems: Bridging Two Islands of Expertise*. Linköping University, Sweden.

Vecchiato, D. A. (2017). *Beanchmarking User-Defined Security Configurations of Mobile Devices*. University od Campinas.

Vibhandik, R., & Bose, A. K. (2015). Vulnerability assessment of web applications - a testing approach. In *Forth International Conference on Date of e-Technologies and Networks for Development (ICeND)*. Lodz, Poland: IEEE. http://doi.org/10.1109/ICeND.2015.7328531

Vieira, M., Antunes, N., & Madeira, H. (2009). Using web security scanners to detect vulnerabilities in web services. In *International Conference on Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP* (pp. 566–571). IEEE.

Viljanen, L. (2005). Towards an Ontology of Trust. *Computer*, *3592*, 175–184. http://doi.org/10.1007/11537878_18

W3AF.ORG. (2017). W3AF - Open Source Web Application Security Scanner. Retrieved August 8, 2017, from http://w3af.org

W3C. (2015). OWL - Web Ontology Language. Retrieved from http://www.w3.org/2001/sw/wiki/OWL

Wali, A., Chun, S. A., & Geller, J. (2013). A bootstrapping approach for developing a cyber-security ontology using textbook index terms. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 569–576. http://doi.org/10.1109/ARES.2013.75

Weyuker, E. J. (1984). The complexity of data flow for test data selection. *Information Proces - Sing Letters*, *19*(2), 103–109.

Wita, R., Jiamnapanon, N., & Teng-amnuay, Y. (2010). An ontology for vulnerability lifecycle. *3rd International Symposium on Intelligent Information Technology and Security Informatics, IITSI 2010*, 553–557. http://doi.org/10.1109/IITSI.2010.141

Yu, Y. T., & Lau, M. F. (2012). Fault-based test suite prioritization for specification-based testing. *Information and Software Technology*, *54*(2), 179–202.

Zech, P., Felderer, M., Katt, B., & Breu, R. (2014). Security test generation by answer set programming. In *IEEE Eighth International Conference on Software Security and Reliability* (pp. 88–97).

Zhang, S., Caragea, D., & Ou, X. (2011). An empirical study on using the national vulnerability database to predict software vulnerabilities. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6860 LNCS*(PART 1), 217–231. http://doi.org/10.1007/978-3-642-23088-2_15

Zhu, H., & Huo, Q. (2005). Developing a software testing ontology in UML for a software growth environment of web-based applications. *Software Evolution with UML And*, 1–34. Retrieved from http://cms.brookes.ac.uk/staff/HongZhu/Publications/SEUMLXML.pdf

# APÊNDICES

# **APÊNDICE A.** Diagrama de Classes do Protótipo de Software

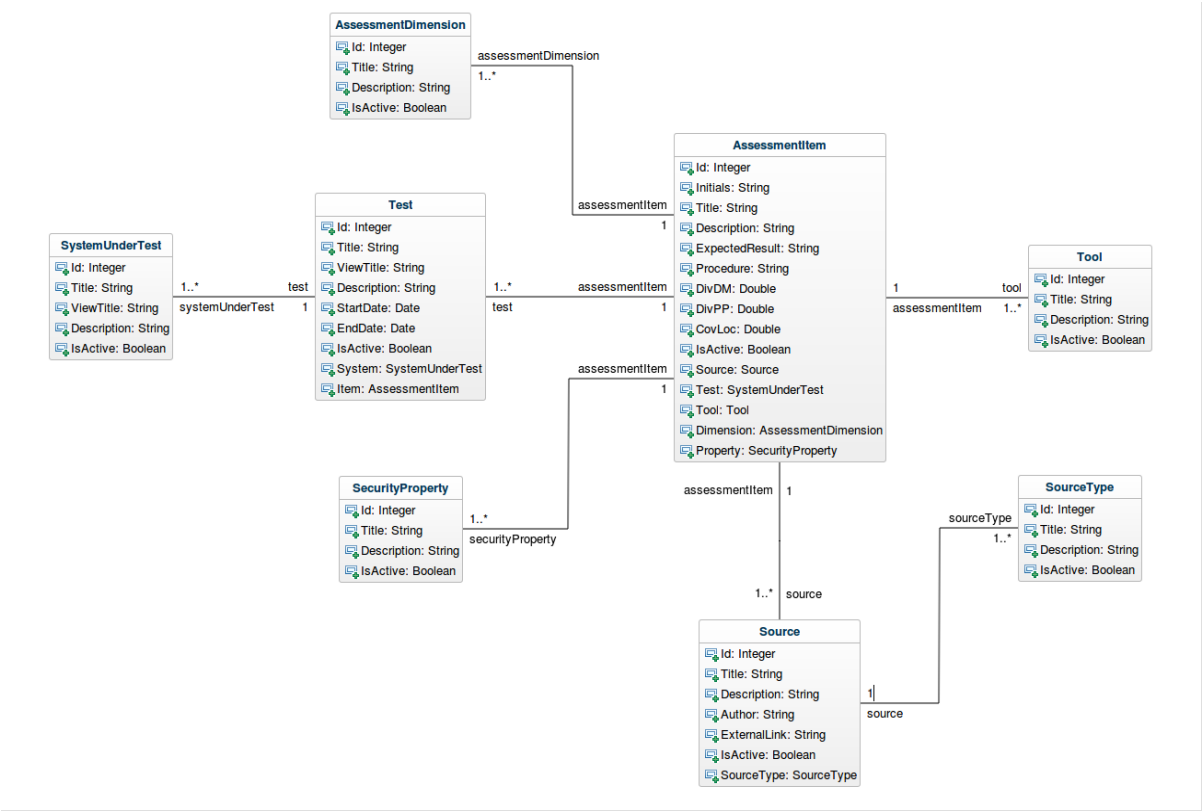


**Figura A.1.** Diagrama de Classes do Protótipo de Software

# **APÊNDICE B.** Modelo Entidade-Relacionamento do Protótipo de Software

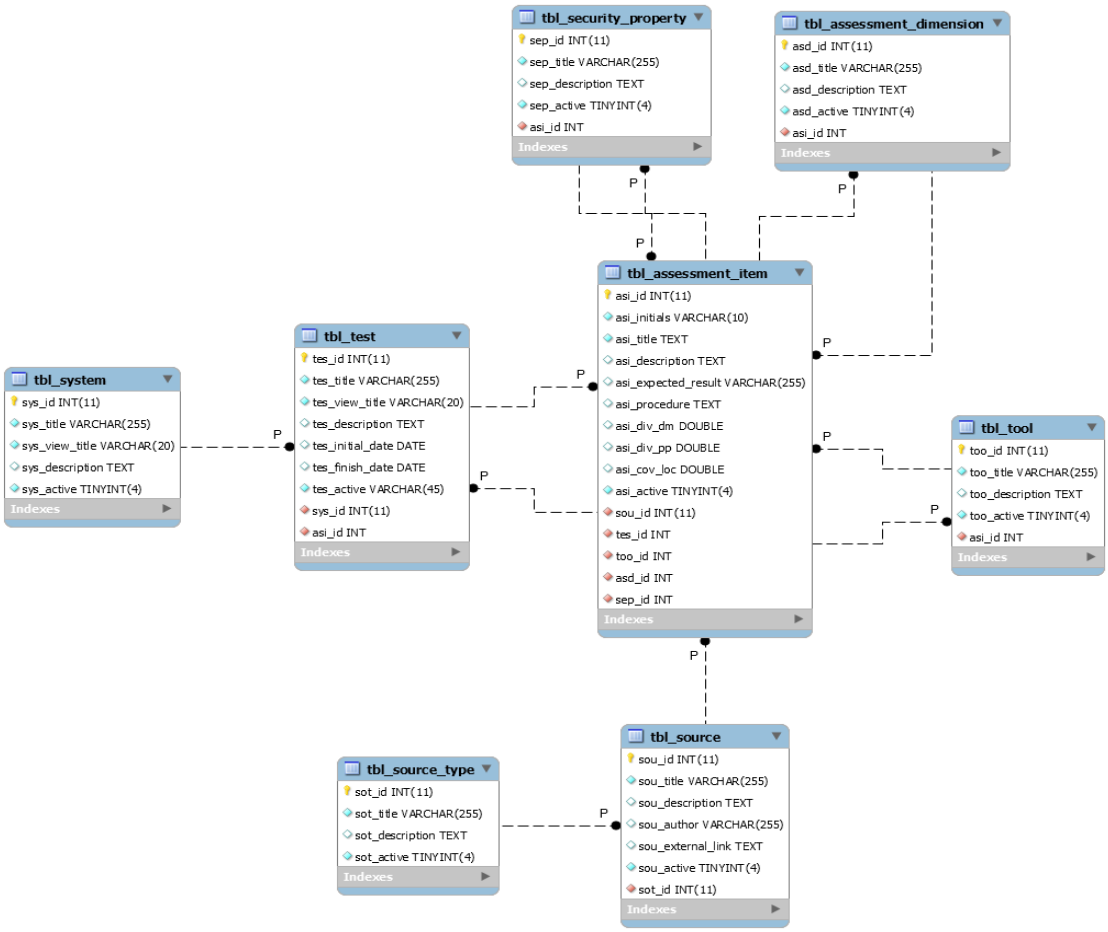


**Figura B.1.** Modelo Entidade-Relacionamento do Protótipo de Software

# APÊNDICE C. *Dataset* completo da Fonte de Conhecimento 1 (KS1)

**Observação**: Itens de avaliação ordenador por CovLOC, CovPP e CovDM.

**Tabela C.1.** *Dataset* completo da Fonte de Conhecimento 1 (KS1)

| *KS* | *ID* | *D1* | *D2* | *D3* | *D4* | *D5* | *D6* | *P1* | *P2* | *P3* | *P4* | *P5* | *P6* | *P7* | *P8* | *P9* | *P10* | *P11* | *CovDM* | *CovPP* | *CovLOC* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 10.10.1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | *0,483* | *1,000* | *0,742* |
| 1 | 15.1.3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | *0,483* | *1,000* | *0,742* |
| 1 | 13.2.3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | *0,283* | *1,000* | *0,642* |
| 1 | 15.1.5 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | *0,283* | *1,000* | *0,642* |
| 1 | 9.2.4 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,982* | *0,633* |
| 1 | 14.1.3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | *0,483* | *0,900* | *0,692* |
| 1 | 15.3.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | *0,283* | *0,900* | *0,592* |
| 1 | 8.1.3 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | *0,033* | *0,855* | *0,444* |
| 1 | 12.2.2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | *0,183* | *0,845* | *0,514* |
| 1 | 11.4.5 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | *0,283* | *0,818* | *0,551* |
| 1 | 10.4.2 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | *0,433* | *0,745* | *0,589* |
| 1 | 12.3.2 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,850* | *0,673* | *0,761* |
| 1 | 10.9.2 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,673* | *0,478* |
| 1 | 10.7.3 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,645* | *0,464* |
| 1 | 15.2.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | *0,283* | *0,636* | *0,460* |
| 1 | 10.8.3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | *0,283* | *0,591* | *0,437* |
| 1 | 10.9.1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | *0,100* | *0,591* | *0,345* |
| 1 | 12.5.5 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | *0,450* | *0,573* | *0,511* |
| 1 | 15.1.6 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | *0,433* | *0,573* | *0,503* |
| 1 | 10.2.2 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,100* | *0,573* | *0,336* |
| 1 | 10.4.1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | *0,567* | *0,518* | *0,542* |
| 1 | 10.6.1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | *0,383* | *0,518* | *0,451* |
| 1 | 10.9.3 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,518* | *0,401* |
| 1 | 12.2.1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | *0,183* | *0,518* | *0,351* |
| 1 | 14.1.5 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | *0,483* | *0,491* | *0,487* |
| 1 | 9.1.4 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | *0,283* | *0,473* | *0,378* |
| 1 | 9.2.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | *0,283* | *0,473* | *0,378* |
| 1 | 6.2.3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | *0,283* | *0,464* | *0,373* |
| 1 | 7.1.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,445* | *0,364* |
| 1 | 12.4.3 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,567* | *0,409* | *0,488* |
| 1 | 11.4.4 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,409* | *0,346* |
| 1 | 10.1.3 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | *0,033* | *0,409* | *0,221* |
| 1 | 12.4.2 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | *0,433* | *0,364* | *0,398* |
| 1 | 15.1.1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,364* | *0,198* |
| 1 | 8.1.2 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | *0,000* | *0,364* | *0,182* |
| 1 | 9.2.3 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,355* | *0,319* |
| 1 | 9.2.6 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | *0,033* | *0,355* | *0,194* |

| *KS* | *ID* | *D1* | *D2* | *D3* | *D4* | *D5* | *D6* | *P1* | *P2* | *P3* | *P4* | *P5* | *P6* | *P7* | *P8* | *P9* | *P10* | *P11* | *CovDM* | *CovPP* | *CovLOC* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 11.6.2 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | *0,967* | *0,336* | *0,652* |
| 1 | 11.5.4 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | *0,283* | *0,336* | *0,310* |
| 1 | 11.7.1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,650* | *0,318* | *0,484* |
| 1 | 11.4.1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,318* | *0,301* |
| 1 | 7.2.1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | *0,033* | *0,309* | *0,171* |
| 1 | 8.1.1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | *0,033* | *0,309* | *0,171* |
| 1 | 15.1.4 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | *0,033* | *0,309* | *0,171* |
| 1 | 12.5.4 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | *0,283* | *0,300* | *0,292* |
| 1 | 10.2.1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,100* | *0,300* | *0,200* |
| 1 | 10.8.2 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | *0,283* | *0,282* | *0,283* |
| 1 | 9.1.6 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,283* | *0,264* | *0,273* |
| 1 | 8.3.3 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,264* | *0,148* |
| 1 | 9.1.1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,264* | *0,148* |
| 1 | 9.1.2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,264* | *0,148* |
| 1 | 9.1.3 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,264* | *0,148* |
| 1 | 13.2.2 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | *0,100* | *0,255* | *0,177* |
| 1 | 9.2.5 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,283* | *0,245* | *0,264* |
| 1 | 11.3.3 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,283* | *0,245* | *0,264* |
| 1 | 15.3.1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | *0,283* | *0,245* | *0,264* |
| 1 | 10.1.4 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,100* | *0,245* | *0,173* |
| 1 | 11.2.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,283* | *0,227* | *0,255* |
| 1 | 11.2.2 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,283* | *0,227* | *0,255* |
| 1 | 11.2.3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,283* | *0,227* | *0,255* |
| 1 | 12.6.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,227* | *0,255* |
| 1 | 14.1.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,227* | *0,255* |
| 1 | 11.4.6 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,100* | *0,227* | *0,164* |
| 1 | 11.3.1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,033* | *0,227* | *0,130* |
| 1 | 15.2.2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,227* | *0,130* |
| 1 | 11.5.2 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | *0,483* | *0,191* | *0,337* |
| 1 | 10.3.2 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | *0,100* | *0,191* | *0,145* |
| 1 | 11.5.6 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,650* | *0,173* | *0,411* |
| 1 | 11.4.7 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | *0,483* | *0,173* | *0,328* |
| 1 | 11.5.1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | *0,483* | *0,173* | *0,328* |
| 1 | 11.5.3 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,483* | *0,173* | *0,328* |
| 1 | 11.5.5 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,483* | *0,173* | *0,328* |
| 1 | 11.4.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,173* | *0,228* |
| 1 | 11.6.1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | *0,283* | *0,173* | *0,228* |
| 1 | 10.7.1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,100* | *0,173* | *0,136* |
| 1 | 10.7.2 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,100* | *0,173* | *0,136* |
| 1 | 10.7.4 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,100* | *0,173* | *0,136* |
| 1 | 7.2.2 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,033* | *0,173* | *0,103* |
| 1 | 12.3.1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,433* | *0,164* | *0,298* |
| 1 | 10.6.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,164* | *0,223* |
| 1 | 11.2.4 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,164* | *0,223* |

| *KS* | *ID* | *D1* | *D2* | *D3* | *D4* | *D5* | *D6* | *P1* | *P2* | *P3* | *P4* | *P5* | *P6* | *P7* | *P8* | *P9* | *P10* | *P11* | *CovDM* | *CovPP* | *CovLOC* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 12.5.2 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,164* | *0,223* |
| 1 | 10.5.1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | *0,100* | *0,164* | *0,132* |
| 1 | 10.2.3 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,164* | *0,098* |
| 1 | 12.5.3 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | *0,033* | *0,164* | *0,098* |
| 1 | 6.1.3 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,164* | *0,082* |
| 1 | 6.1.4 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,145* | *0,089* |
| 1 | 10.1.2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,145* | *0,089* |
| 1 | 15.1.2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,033* | *0,145* | *0,089* |
| 1 | 8.2.3 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,145* | *0,073* |
| 1 | 8.3.2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,145* | *0,073* |
| 1 | 10.1.1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,145* | *0,073* |
| 1 | 6.2.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | *0,283* | *0,136* | *0,210* |
| 1 | 6.2.2 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | *0,283* | *0,136* | *0,210* |
| 1 | 9.2.2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,118* | *0,201* |
| 1 | 12.4.1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,283* | *0,118* | *0,201* |
| 1 | 14.1.4 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | *0,483* | *0,109* | *0,296* |
| 1 | 7.1.3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | *0,283* | *0,109* | *0,196* |
| 1 | 14.1.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | *0,283* | *0,109* | *0,196* |
| 1 | 12.2.3 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | *0,183* | *0,109* | *0,146* |
| 1 | 6.1.5 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | *0,033* | *0,109* | *0,071* |
| 1 | 11.1.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,091* | *0,187* |
| 1 | 10.10.3 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,091* | *0,095* |
| 1 | 10.10.4 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,091* | *0,095* |
| 1 | 10.10.5 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,091* | *0,095* |
| 1 | 10.10.6 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,091* | *0,095* |
| 1 | 13.2.1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,091* | *0,095* |
| 1 | 11.3.2 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,483* | *0,082* | *0,283* |
| 1 | 11.4.3 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,283* | *0,082* | *0,183* |
| 1 | 9.2.7 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,033* | *0,082* | *0,058* |
| 1 | 12.2.4 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | *0,433* | *0,073* | *0,253* |
| 1 | 12.1.1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,200* | *0,073* | *0,136* |
| 1 | 12.5.1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | *0,033* | *0,073* | *0,053* |
| 1 | 11.7.2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | *0,033* | *0,055* | *0,044* |
| 1 | 9.1.5 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | *0,283* | *0,045* | *0,164* |
| 1 | 10.8.1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | *0,100* | *0,045* | *0,073* |
| 1 | 5.1.1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 5.1.2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 6.1.1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 6.1.2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 6.1.6 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 6.1.8 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 8.2.1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 8.2.2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |
| 1 | 8.3.1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | *0,000* | *0,045* | *0,023* |

| *KS* | *ID* | *D1* | *D2* | *D3* | *D4* | *D5* | *D6* | *P1* | *P2* | *P3* | *P4* | *P5* | *P6* | *P7* | *P8* | *P9* | *P10* | *P11* | *CovDM* | *CovPP* | *CovLOC* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 10.3.1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,650* | *0,018* | *0,334* |
| 1 | 13.1.1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,283* | *0,018* | *0,151* |
| 1 | 7.1.1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,018* | *0,059* |
| 1 | 10.10.2 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,018* | *0,059* |
| 1 | 13.1.2 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | *0,100* | *0,018* | *0,059* |
| 1 | 10.8.4 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,033* | *0,018* | *0,026* |
| 1 | 10.8.5 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | *0,033* | *0,018* | *0,026* |
| 1 | 6.1.7 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | *0,000* | *0,000* | *0,000* |
| | | *96* | *5* | *131* | *22* | *12* | *84* | *53* | *38* | *36* | *69* | *33* | *59* | *25* | *67* | *58* | *36* | *1* | ***CovGlo*** | | ***0,252*** |

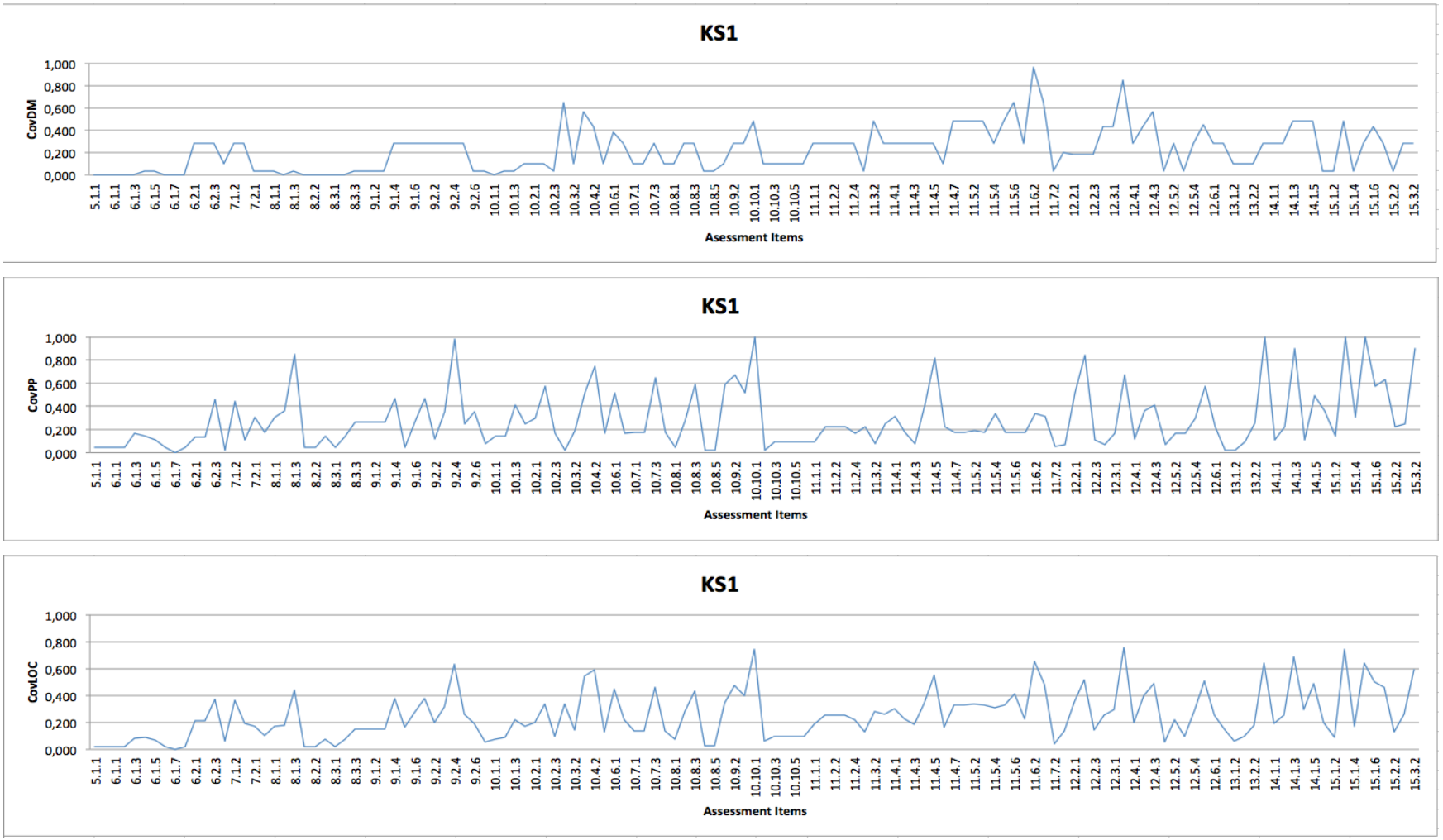


**Figura C.1.** Gráficos do *Dataset* completo de KS1 (CovDM, CovPP e CovLOC)

# APÊNDICE D. Publicações Resultantes da Pesquisa

## 1) Resumos dos artigos produzidos

### *Software Testing with emphasis on Finding Security Defects (2013)*

*The Software Engineering discipline "Software Testing" has not provided a resource for systematically testing a software product with focus on the various aspects related to information security. This was one of the conclusions produced by a literature review conducted in the second half of 2012; a systematic literature review is now under way aiming to provide a more solid perspective on this subject. An approach based on adequately structuring the current knowledge on information security may provide support for effective security testing.*

### *Arquitetura Conceitual para Avaliação de Segurança de Sistemas Web (2016)*

Este trabalho apresenta uma reflexão sobre a necessidade de uma arquitetura conceitual voltada a fazer avaliações de segurança de sistemas web de forma sistemática. A arquitetura possibilita a avaliação de padrões de segurança com relação a sua cobertura de propriedades de segurança e também a geração de casos de teste e a seleção de itens de avaliação mais efetivos. A Arquitetura se apoia conceitualmente em uma ontologia de avaliação de segurança, construída especificamente para esse fim. Além da reflexão sobre o problema, apresenta-se, de forma resumida, a metodologia de revisão bibliográfica utilizada, uma proposta de Arquitetura Conceitual para Avaliação de Segurança de Sistemas Web e uma breve descrição de seus componentes. Este trabalho destina-se a ser útil para pesquisadores e desenvolvedores que buscam criar sistemas web menos vulneráveis.

### *A Survey of Security Assessment Ontologies (2017)*

*A literature survey on ontologies concerning the Security Assessment domain has been carried out to uncover initiatives that aim at formalizing concepts from the "Security Assessment" field of research. A preliminary analysis and a discussion on the selected works are presented. Our main contribution is an updated literature review, describing key characteristics, results, research issues, and application domains of the papers. We have also detected gaps in the Security*

*Assessment literature that could be the subject of further studies in the field. This work is meant to be useful for security researchers who wish to adopt a formal approach in their methods.*

***The Security Assessment Domain: A Survey of Taxonomies and Ontologies (2017)***

*The use of ontologies and taxonomies contributes by providing means to define concepts, minimize the ambiguity, improve the interoperability and manage knowledge of the security domain. Thus, this paper presents a literature survey on ontologies and taxonomies concerning the Security Assessment domain. We carried out it to uncover initiatives that aim at formalizing concepts from the "Information Security" and "Test and Assessment" fields of research. We applied a systematic review approach in seven scientific databases. 138 papers were identified and divided into categories according to their main contributions, namely: Ontology, Taxonomy and Survey. Based on their contents, we selected 47 papers on ontologies, 22 papers on taxonomies, and 11 papers on surveys. A taxonomy has been devised to be used in the evaluation of the papers. Summaries, tables, and a preliminary analysis of the selected works are presented. Our main contributions are: 1) an updated literature review, describing key characteristics, results, research issues, and application domains of the papers; and 2) the taxonomy for the evaluation process. We have also detected gaps in the Security Assessment literature that could be the subject of further studies in the field. This work is meant to be useful for security researchers who wish to adopt a formal approach in their methods and techniques.*

***Towards an Ontology of Security Assessment: a core model proposal (2018)***

*SecAOnto (Security Assessment Ontology) aims at formalizing the knowledge on "Security Assessment". A conceptual formalization of this area is needed, given that there is an overlap of the "Information Security" and "Systems Assessment" areas, concepts are ambiguous, terminology is confounding, and important concepts are not defined. 19 papers on ontology, out of 80 papers of interest, have been selected to be discussed. Most of them are proposals of ontologies on information security; here we propose an ontology to deal specifically with*

*security assessment aspects and particularities. SecAOnto is OWL-based, is publicly available and is devised to be used as a common and extensible model for security assessment. Its foundation comes from glossaries, vocabularies, taxonomies, ontologies, and market's guidelines. The initial version of the ontology, its core model, as well as an application are presented. Our proposal is meant to be useful for security researchers who wish to formalize knowledge in their systems, methods and techniques.*

***Coverage-based Heuristics for Selecting Assessment Items from Security Standards: a core set proposal (2018)***

*In the realm of Internet of Things (IoT), information security is a critical issue. Security standards, including their assessment items, are essential instruments in the evaluation of systems security. However, a key question remains open: "Which test cases are most effective for security assessment?" To create security assessment designs with suitable assessment items, we need to know the security properties and assessment dimensions covered by a standard. We propose an approach for selecting and analyzing security assessment items; its foundations come from a set of assessment heuristics and it aims to increase the coverage of assessment dimensions and security characteristics in assessment designs. We systematize the security assessment process by means of a conceptual formalization of the security assessment area; we also propose security assessment heuristics. Our approach can be applied to security standards to select or to prioritize assessment items with respect to 11 security properties and 6 assessment dimensions. The approach is flexible allowing the inclusion of dimensions and properties. Our proposal was applied to a well know security standard (ISO/IEC 27001) and its assessment items were analyzed. The proposal is meant to support: (i) the generation of high-coverage assessment designs, which include security assessment items with assured coverage of the main security characteristics, and (ii) evaluation of security standards with respect to the coverage of the most important security aspects.*

***A Security Test Process supported by an Ontology Environment (2018)***

*Information security is a critical issue in the context of information sharing and web collaboration. Innovative testing approaches are demanded to verify whether the main security characteristics are provided in the systems. The conceptual formalization level required by security test processes can be supplied by semantic technologies. STEP-ONE is the Security TEst Process supported by ONtology Environment; its foundations come from largely accepted testing process and security testing standards. The STPO (Security Testing Process Ontology) formalizes and makes explicit the main concepts of the domain. We present a conceptual characterization of STEP-ONE and describe a usage scenario to illustrate how the proposal can be applied. The main contributions are the conceptual process and the ontology. Our proposal is meant to be applied for the evaluation of Web-based collaborative systems with respect to security characteristics as well as to make systematic the security testing activities.*

***An Ontology of Security Assessment (2018)***

*Security Assessment is crucial to the development and maintenance of secure systems. In spite of the existence of proposals of knowledge representation models for both Information Security and Systems Assessment, a conceptual formalization of Security Assessment field is needed – usually concepts are ambiguous, terminology is confounding, and definition of important concepts is lacking. We propose SecAOnto (Security Assessment Ontology) with the main objective of formalizing knowledge on Security Assessment. Its foundation comes from existing glossaries, vocabularies, taxonomies, ontologies, and market's guidelines. We also present an application of SecAOnto to identify concepts in descriptions of assessment items; the coverage of security characteristics is determined by using a coverage calculus algorithm. This is an important step for the generation of security assessment criteria. Results highlight the expressiveness of SecAOnto concerning Security Assessment concepts and the feasibility of applying it in real world conditions.*

***HCApp-Sec – Heuristics and Criteria based Approach for Selecting and Analyzing Security Assessment Items (2018)***

*Knowledge sources and their assessment items are essential instruments to evaluate systems security. To create security assessment designs with suitable assessment items we need to know which security properties and assessment dimensions are covered by the knowledge source. We present an approach for selecting and analyzing security assessment items (HCApp-Sec); the foundations come from assessment criteria and heuristics and aims to increase the coverage of assessment dimensions and security characteristics in assessment designs. We systematize the security assessment process by using an ontology of the security assessment area. HCApp-Sec can be applied to any security knowledge source to select or prioritize assessment items with respect to 11 security properties and 6 assessment dimensions. We have applied our proposal to a well know security knowledge source (ISO/IEC 27001) and their assessment items were analyzed. We expect to contribute to security researchers by: (i) generating high-coverage assessment designs by selecting security assessment items with assured coverage of the main security characteristics and (ii) evaluating security knowledge sources with respect to coverage of the most important security aspects.*

## 2) Resultados da Pesquisa

**Tabela D.1.** Resultados da Pesquisa

| *Entregáveis* | *Tipo* | *Autores* | *Local* | *Qualis* | *Status* |
|---|---|---|---|---|---|
| Software Testing with emphasis on Finding Security Defects (2013) | Artigo | Celso Pereira de Barros; Ferrucio de Franco Rosa; Amandio Ferreira Balcão Filho | 12th IADIS International Conference Applied Computing 2013 | - | Publicado |
| Arquitetura Conceitual para Avaliação de Segurança de Sistemas de Informação (2015) | Monografia de Qualificação | Ferrucio de Franco Rosa; Mario Jino | Unicamp | - | Aprovado |
| Arquitetura Conceitual para Avaliação de Segurança de Sistemas Web (2016) | Artigo | Ferrucio de Franco Rosa; Mario Jino | 14th IADIS Conferência Ibero-Americana WWW/Internet e Computação Aplicada | - | Publicado |
| Framework para geração de conjunto de critérios de teste de segurança de software (2016) | Programa de Computador | Ferrucio de Franco Rosa; Amandio Ferreira Balcão Filho; Luiz Antonio Lima Teixeira Junior; Mario Jino | INPI | - | Registrado |
| A Survey of Security Assessment Ontologies (2017) | Artigo | Ferrucio de Franco Rosa; Mario Jino | 5th World Conference on Information Systems and Technologies (*pub. em Springer Recent Advances in Information Systems and Technologies*) | - | Publicado |
| The Security Assessment Domain: A Survey of Taxonomies and Ontologies (2017) | Relatório Técnico | Ferrucio de Franco Rosa; Rodrigo Bonacin; Mario Jino | Researchgate | - | Publicado |
| Towards an Ontology of Security Assessment: a core model proposal (2018) | Artigo | Ferrucio de Franco Rosa; Rodrigo Bonacin; Mario Jino | 15th International Conference on Information Technology – New Generations (ITNG) (*pub. em Springer Recent Advances in Information Systems and Technologies*) | B1 | Publicado |
| Coverage-based Heuristics for | Artigo | Ferrucio de Franco Rosa; | IEEE International Workshop on | - | Publicado |

| *Entregáveis* | *Tipo* | *Autores* | *Local* | *Qualis* | *Status* |
|---|---|---|---|---|---|
| Selecting Assessment Items of Security Standards: a core set proposal (2018) | | Rodrigo Bonacin; Paulo Marcos Siqueira Bueno; Mario Jino | Metrology for Industry 4.0 and IoT | | |
| A Security Test Process supported by an Ontology Environment (2018) | Artigo | Paulo Marcos Siqueira Bueno; Ferrucio de Franco Rosa; Mario Jino; Rodrigo Bonacin | IEEE 29th International Symposium on Software Reliability Engineering (ISSRE) | A2 | Submetido |
| An Ontology of Security Assessment (2018) | Artigo | Ferrucio de Franco Rosa; Rodrigo Bonacin; Luiz Antonio Lima Teixeira Junior; Mario Jino | Journal of Web Semantics | A2 | Submetido |
| HCApp-Sec – Heuristics and Criteria based Approach for Selecting and Analyzing Security Assessment Items (2018) | Artigo | Ferrucio de Franco Rosa; Rodrigo Bonacin; Mario Jino | Journal of Software: Practice and Experience | A2 | Submetido |
| Tese (2018) | Tese | Ferrucio de Franco Rosa; Mario Jino | Unicamp | - | Aprovado |

**APÊNDICE E.** Mapeamento das Fontes de Conhecimento de Segurança

***(i) ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components –*** (ISO/IEC, 2008a, 2008b, 2009)

- **Conteúdo**: Conjunto de requisitos para avaliar a funcionalidade de segurança de produtos de TI, além de medidas que visam a garantir a aplicação destes requisitos a estes produtos durante uma avaliação de segurança.
- **Objetivo**: Avaliação de Produtos Eletrônicos (Hardware e Software)
- **Idioma**: Inglês.
- **Formato**: O documento é dividido em 3 partes, sendo que a primeira traz uma introdução e uma visão geral acerca do modelo, a segunda os componentes funcionais de segurança e a terceira os componentes de garantia de segurança. Cada parte é dividida em seções, subseções e, até mesmo, subseções de subseções, trazendo à tona a necessidade de categorização a fim de correlacionar as seções à sua árvore de subseções.
- **Requisitos**: A fim de manter uma ordem lógica entre as seções e subseções na base de dados, faz-se necessário desenvolver um formato para inclusão de sub-itens na tabela. Requisito satisfeito.

***(ii) MITRE Ten Strategies of a World-Class Cybersecurity Operations Center*** (MITRE, 2017)

- **Conteúdo**: Conjunto de estratégias a serem seguidas por um centro de operações de segurança cibernética (*Cybersecurity Operations Center* – CSOC).
- **Objetivo**: Prover um manual de boas práticas fundamentadas a partir de necessidades específicas do cotidiano de um CSOC.
- **Idioma**: Inglês
- **Formato**: Cada uma das estratégias é redigida em texto corrido e contém fragmentos que, quando separados, poderiam ser transformados em itens de

avaliação, principalmente os relacionados a procedimentos operacionais (processos).

- **Requisitos**: Por ser dividido em estratégias e subdividido em itens, faz-se necessário categorizar cada um dos itens com suas respectivas estratégias, a fim de correlacioná-los e manter uma ordem lógica e padrão entre eles. Apesar de conter itens interessantes do ponto de vista de processos, é necessário analisar com mais detalhe se esta fonte deve fazer parte da base.

***(iii) OWASP Open Web Application Security Project Testing Guide*** (OWASP, 2008)

- **Conteúdo**: Conjunto de requisitos de segurança para sistemas Web.
- **Objetivo**: Identificação de vulnerabilidades em sistemas Web.
- **Idioma**: Inglês.
- **Formato**: O documento possui dois capítulos que podem ser considerados como relevantes: 3) *The OWASP Testing Framework* e 4) *Web Application Security Testing*. O capítulo 3 é subdivido em fases e cada uma dessas fases pode ser considerada como um item de avaliação, o que acabou facilitando a adequação da informação à modelagem atual da tabela. Já o capítulo 4 é mais complexo e requer uma análise mais meticulosa, tendo em vista que é subdividido em 11 subcategorias para um total de 91 itens, sendo que cada um desses itens está subdividido em seções específicas, tais como *Summary, Test Objectives, How to Test, Tools, References* etc.
- **Requisitos**: Adequar a tabela para receber cada um dos itens de avaliação e suas respectivas categorias, bem como cada uma de suas seções, a fim de manter a informação íntegra em relação ao documento original.

***(iv) SANS Critical Security Controls for Effective Cyber Defense*** (The SANS Institute, 2015)

- **Conteúdo**: Documento com ações definidas para os controles, que são um subconjunto do catálogo definido pelo NIST SP 800-53 (NIST, 2017b); este não tem a intenção de substituir o trabalho do NIST, mas de priorizar e focar em um menor número de controles acionáveis com melhor retorno.

- **Objetivo**: O documento concentra-se em apresentar controles de segurança eficazes contras ameaças.
- **Idioma**: Inglês.
- **Formato**: O documento elenca um conjunto de controles e, para cada um desses controles, existe um conjunto de ações que devem ser levadas em consideração para sua implementação.
- **Requisitos**: Para este documento, os controles podem ser entendidos como requisitos de segurança e as ações a serem tomadas seriam seus respectivos itens de avaliação. Seguindo essa lógica, esta fonte não demandaria modificações, mas uma melhor análise precisa ser feita.

*(v) ISO/IEC 27001 Information Security Management* (ISO/IEC, 2013a)

- **Conteúdo**: Este documento é um *checklist* dos parâmetros das normas BS 17799 e ISO/IEC 27001 de 2005.
- **Objetivo**: O objetivo principal deste documento é auxiliar consultores das referidas normas nos processos de certificação ou auditoria de segurança da informação em organizações.
- **Idioma**: Inglês
- **Formato**: O documento possui uma tabela contendo informações sobre os níveis dentro do *checklist*, dentro da norma, o título da seção e os controles (idem *Common Criteria*).
- **Requisitos**: Tal como *Common Criteria*, faz-se necessário incluir um campo para identificar o nível do controle e, caso necessário, correlacioná-lo com seu pai, a fim de manter uma ordem lógica para a visualização da informação. Requisito satisfeito.

*(vi) SBIS/CFM MOEA Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)* (Giulliano et al., 2014)*, baseado no HIPAA* (U.S. Department of Health & Human Services, 2015)

- **Conteúdo**: Este documento é destinado à certificação SBIS-CFM e se baseia em conceitos e padrões nacionais e internacionais da área de Informática em Saúde.

- **Objetivo**: Prover uma lista de verificação e procedimentos operacionais para certificação de sistemas que lidam com informações de saúde de pacientes.
- **Idioma**: Português.
- **Formato**: Os requisitos elencados no documento são classificados em dois níveis de garantia de segurança (NGS). Os S-RES são classificados em Acesso Local (instalado em um único computador) e Acesso Remoto (permite acesso simultâneo ao sistema). Os requisitos, por sua vez, estão divididos em seções e, para cada uma das seções, existe uma tabela de ações (itens de avaliação) a serem seguidas. Cada ação possui um ID, um Título, um Requisito e uma identificação sobre se o requisito é mandatório de acordo com sua classificação (Acesso Local ou Remoto).
- **Requisitos**: Analisando o formato com que a informação é disponibilizada no manual, as especificações que impactariam diretamente na modelagem da tabela seriam: a definição sobre o Nível de Garantia de Segurança que caracteriza cada uma das seções e, consequentemente, cada uma das ações; a classificação do S-RES entre local ou remoto e a caracterização de registro obrigatório ou não. Requisitos satisfeitos.

***(vii) Payment Card Industry Data Security Standard (PCI DSS)*** (PCI Security Standards Council, 2015)

- **Conteúdo**: Apresenta um conjunto de requisitos técnicos e operacionais para avaliar a segurança de dispositivos que manipulam cartões de pagamento.
- **Objetivo**: Aprimorar a segurança dos dados de portadores de cartões e promover uma adoção de medidas de segurança de dados na indústria de cartões de pagamento.
- **Idioma**: Inglês.
- **Formato**: Cada requisito possui N outros “sub-requisitos”, que são considerados controles. Para cada controle pode-se ter N procedimentos de teste e uma orientação sobre como implementar/executar este controle.
- **Requisitos**: Necessidade de criação de uma nova tabela (1-n) para armazenar os procedimentos de teste.

*(viii) FIPS (NIST) Security Requirements For Cryptographic Modules (140-2)* (NIST, 2017a)

- **Conteúdo**: Este documento especifica os requisitos de segurança que devem ser atendidos por um módulo criptográfico utilizado dentro de um sistema de segurança que protege informações sensíveis, porém, não classificadas.
- **Objetivo**: Prover um conjunto de requisitos para avaliação de sistemas criptográficos, tais como, chips criptográficos, leitores biométricos que criptografam o *template*, entre outros.
- **Idioma**: Inglês.
- **Formato**: FIPS 140-2 prevê quatro níveis crescentes e qualitativos de segurança (Nível 1, Nível 2, Nível 3 e Nível 4), sendo eles destinados a cobrir uma gama de aplicações e ambientes em que podem ser empregados módulos criptográficos. Cada um dos requisitos corresponde a uma subseção da seção 4 e, cada um deles é redigido em texto corrido contendo fragmentos que, quando separados, podem ser convertidos em itens de avaliação.
- **Requisitos**: Por ser dividido em subseções, faz-se necessário categorizar cada um dos fragmentos do texto com a sua respectiva seção, a fim de correlacioná-los e de manter uma ordem lógica. Faz-se necessário criar uma categorização à parte ou uma adaptação do conteúdo à estrutura da base.

*(ix) SOX Sarbanes-Oxley Act Audit Checklist* (Addison-Hewitt Associates, 2015)

- **Conteúdo**: O documento apresenta uma lista de verificação de comitê de auditoria que visa a garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para criação de comitês encarregados de supervisionar suas atividades e operações.
- **Objetivo**: Simplificar a verificação da conformidade com requisitos contidos na Lei SOX por parte do comitê de auditoria da própria instituição.
- **Idioma**: Inglês.
- **Formato**: O documento é dividido em títulos, que são subdivididos em seções, e que possuem N itens.

- **Requisitos**: Há necessidade de categorizar cada um dos itens de acordo com suas respectivas seções e títulos. Para tanto, faz-se necessária a criação de uma nova tabela responsável por categorizar cada um desses itens, a fim de manter uma correlação entre itens, seções e títulos e, consequentemente, uma ordem lógica da informação. Pode-se também reinterpretar o documento, extraindo os itens diretamente, numerá-los e verificar se é possível agrupar.

*(x) Cybersecurity Capability Maturity Model (C2M2)* (Energy, 2017)

- **Conteúdo**: Apresenta um guia de boas práticas de segurança cibernética associados a tecnologias da informação e tecnologias de operações, bem como os ativos e ambientes em que atuam.
- **Objetivo**: Auxiliar organizações a avaliar e implementar melhorias em seus programas de segurança cibernética.
- **Idioma**: Inglês.
- **Formato**: O Capítulo 5 do guia está dividido entre objetivos e práticas, sendo que, cada uma das práticas é atribuída ao domínio de acordo com o indicador de nível de maturidade que se deseja atingir.
- **Requisitos**: Criação de um campo que possibilite a categorização do item em relação ao domínio que será avaliado e de outro campo para identificar o nível de maturidade.

*(xi) BACEN/STN Manual de Segurança da RSFN* (BACEN, 2017)

- **Conteúdo**: O documento apresenta um conjunto de requisitos de segurança a serem implementados para garantir Integridade, Confidencialidade, Disponibilidade e Não-repúdio das informações trafegadas na Rede do Sistema Financeiro Nacional (RSFN) do Brasil.
- **Objetivo**: Consolidar os entendimentos contidos nos documentos expedidos pelo GT-Segurança da Rede do Sistema Financeiro Nacional – RSFN. O GT-Segurança da RSFN, institucionalizado pela Circular 3.424, de 12/12/2008 e regulamentado pelo Comunicado 18.655, de 02/07/2009, é constituído por representantes do Banco Central do Brasil (Bacen), da Secretaria do Tesouro Nacional, das associações de bancos de âmbito

nacional, das câmaras e dos prestadores de serviço de compensação e de liquidação participantes da RSFN. Os requisitos de segurança são implementados para garantir a Integridade, a Confidencialidade, a Disponibilidade e o Não-repúdio das informações trafegadas.

- **Idioma**: Português
- **Formato**: Os requisitos são disponibilizados no documento a partir de níveis, sendo dividido em seções, subseções e subseções de subseções, levando à necessidade de categorização a fim de correlacionar as seções à sua árvore de subseções.
- **Requisitos**: A fim de manter uma ordem lógica entre as seções e subseções, faz-se necessário desenvolver um formato para inclusão de sub-itens na tabela. Requisito satisfeito.

*(xii) SLTI/MPOG ePing-Segurança* (Brasil, 2015)

- **Conteúdo**: Este documento define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a segurança na utilização da Tecnologia da Informação e Comunicação (TIC) na interoperabilidade de serviços do Governo Eletrônico.
- **Objetivo**: Estabelecer condições de mínimas de segurança na interação entre Poderes, esferas de governo e com a sociedade em geral.
- **Idioma**: Português.
- **Formato**: Os requisitos são disponibilizados no documento a partir de níveis, sendo dividido em seções, subseções e subseções de subseções, levando à necessidade de categorização a fim de correlacionar as seções à sua árvore de subseções.
- **Requisitos**: A fim de manter uma ordem lógica entre as seções e subseções, faz-se necessário desenvolver um formato para inclusão de sub-itens na tabela. Requisito satisfeito.

*(xiii) Consensus Assessments Initiative Questionnaire (CSA/CAIQ)* (CSA, 2015)

- **Conteúdo**: Este documento apresenta uma lista de verificação para avaliar a segurança de sistemas em ambiente de *Cloud Computing*.

- **Objetivo**: Prover um conjunto de requisitos para avaliar e priorizar segurança em provedores de ambientes de nuvem.
- **Idioma**: Inglês.
- **Formato**: O documento segue um formato bastante complexo, pois tenta listar um grande número de controles, mapeando várias Fontes de Conhecimento de Segurança (incluindo várias listadas neste trabalho), com uma referência cruzada para itens relacionados ao tema *cloud computing*.
- **Requisitos**: Devido à complexidade de sua organização e a conter vários controles de várias fontes citadas, a incorporação desta fonte na base demandaria um estudo mais aprofundado.

*(xiv) MED-Sec-AWA Checklist* (Colombo, 2014)

- **Conteúdo**: Este documento apresenta uma lista de verificação para avaliar o processo de autenticação em sistemas Web.
- **Objetivo**: Prover um método para avaliar e priorizar segurança.
- **Idioma**: Português.
- **Formato**: O documento segue o formato perguntas e respostas, sendo estas abertas (livre descrição) ou fechadas (Sim/Não, Existe/Não-Existe etc.).
- **Requisitos**: A fim de manter uma ordem lógica entre as seções e subseções, faz-se necessário desenvolver um formato para inclusão de sub-itens na tabela. Requisito satisfeito.

# ANEXOS

**ANEXO A.** Fonte de Conhecimento KS1 ISO/IEC 27001

| *AI* | *Descrição* |
|---|---|
| 5.1.1 | *Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.* |
| 5.1.2 | *Whether the policy states management commitment and sets out the organizational approach to managing information security.* |
| 6.1.1 | *Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.* |
| 6.1.2 | *Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities.* |
| 6.1.3 | *Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.* |
| 6.1.4 | *Whether management authorization process is defined and implemented for any new information processing facility within the organization.* |
| 6.1.5 | *Whether the organizations need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed. Does this address the requirement to protect the confidential information using legal enforceable terms?* |
| 6.1.6 | *Whether there exists a procedure that describes when, and by whom: relevant authorities such as Law enforcement, fire department etc., should be contacted, and how the incident should be reported.* |
| 6.1.7 | *Whether appropriate contacts with special interest groups or other specialist security forums, and professional associations are maintained.* |
| 6.1.8 | *Whether the organizations approach to managing information security, and its implementation, is reviewed independently at planned intervals, or when major changes to security implementation occur.* |
| 6.2.1 | *Whether risks to the organizations information and information processing facility, from a process involving external party access, is identified and appropriate control measures implemented before granting access.* |
| 6.2.2 | *Whether all identified security requirements are fulfilled before granting customer access to the organizations information or assets.* |
| 6.2.3 | *Whether the agreement with third parties, involving accessing, processing, communicating or managing the organizations information or information processing facility, or introducing products or services to information processing facility, complies with all appropriate security requirements.* |
| 7.1.1 | *Whether all assets are identified and an inventory or register is maintained with all the important assets.* |
| 7.1.2 | *Whether each asset identified has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.* |
| 7.1.3 | *Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented.* |
| 7.2.1 | *Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.* |
| 7.2.2 | *Whether an appropriate set of procedures are defined for information labelling and handling, in accordance with the classification scheme adopted by the organization.* |
| 8.1.1 | *Whether employee security roles and responsibilities, contractors and third party users were defined and documented in accordance with the organizations information security policy. Were the roles and responsibilities defined and clearly communicated to job candidates during the pre-employment process?* |
| 8.1.2 | *Whether background verification checks for all candidates for employment, contractors, and third party users were carried out in accordance to the relevant regulations.*<br>*Does the check include character reference, confirmation of claimed academic and professional qualifications and independent identity checks?* |
| 8.1.3 | *Whether employee, contractors and third party users are asked to sign confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment contract.*<br>*Whether this agreement covers the information security responsibility of the organization and the employee, third party users and contractors.* |
| 8.2.1 | *Whether the management requires employees, contractors and third party users to apply security in accordance with the established policies and procedures of the organization.* |
| 8.2.2 | *Whether all employees in the organization, and where relevant, contractors and third party users, receive appropriate security awareness training and regular updates in organizational policies and procedures as it pertains to their job function.* |
| 8.2.3 | *Whether there is a formal disciplinary process for the employees who have committed a security breach.* |

| *AI* | *Descrição* |
|---|---|
| 8.3.1 | *Whether responsibilities for performing employment termination, or change of employment, are clearly defined and assigned.* |
| 8.3.2 | *Whether there is a process in place that ensures all employees, contractors and third party users surrender all of the organizations assets in their possession upon termination of their employment, contract or agreement.* |
| 8.3.3 | *Whether access rights of all employees, contractors and third party users, to information and information processing facilities, will be removed upon termination of their employment, contract or agreement, or will be adjusted upon change.* |
| 9.1.1 | *Whether a physical border security facility has been implemented to protect the information processing service.*<br>*Some examples of such security facilities are card control entry gates, walls, manned reception, etc.* |
| 9.1.2 | *Whether entry controls are in place to allow only authorized personnel into various areas within the organization.* |
| 9.1.3 | *Whether the rooms, which have the information processing service, are locked or have lockable cabinets or safes.* |
| 9.1.4 | *Whether the physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster should be designed and applied. Whether there is any potential threat from neighbouring premises.* |
| 9.1.5 | *Whether physical protection and guidelines for working in secure areas is designed and implemented.* |
| 9.1.6 | *Whether the delivery, loading, and other areas where unauthorized persons may enter the premises are controlled, and information processing facilities are isolated, to avoid unauthorized access.* |
| 9.2.1 | *Whether the equipment is protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.* |
| 9.2.2 | *Whether the equipment is protected from power failures and other disruptions caused by failures in supporting utilities.*<br>*Whether permanence of power supplies, such as a multiple feed, an Uninterruptible Power Supply (ups), a backup generator, etc. are being utilized.* |
| 9.2.3 | *Whether the power and telecommunications cable, carrying data or supporting information services, is protected from interception or damage.*<br>*Whether there are any additional security controls in place for sensitive or critical information.* |
| 9.2.4 | *Whether the equipment is correctly maintained to ensure its continued availability and integrity.*<br>*Whether the equipment is maintained, as per the suppliers recommended service intervals and specifications.*<br>*Whether the maintenance is carried out only by authorized personnel.*<br>*Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures.*<br>*Whether appropriate controls are implemented while sending equipment off premises.*<br>*Are the equipment covered by insurance and the insurance requirements satisfied?* |
| 9.2.5 | *Whether risks were assessed with regards to any equipment usage outside an organizations premises, and mitigation controls implemented.*<br>*Whether the usage of an information processing facility outside the organization has been authorized by the management.* |
| 9.2.6 | *Whether all equipment, containing storage media, is checked to ensure that any sensitive information or licensed software is physically destroyed, or securely over-written, prior to disposal or reuse.* |
| 9.2.7 | *Whether any controls are in place so that equipment, information and software is not taken off-site without prior authorization.* |
| 10.1.1 | *Whether the operating procedure is documented, maintained and available to all users who need it.*<br>*Whether such procedures are treated as formal documents, and therefore any changes made need management authorization.* |
| 10.1.2 | *Whether all changes to information processing facilities and systems are controlled.* |
| 10.1.3 | *Whether duties and areas of responsibility are separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services.* |
| 10.1.4 | *Whether the development and testing facilities are isolated from operational facilities. For example, development and production software should be run on different computers. Where necessary, development and production networks should be kept separate from each other.* |
| 10.2.1 | *Whether measures are taken to ensure that the security controls, service definitions and delivery levels, included in the third party service delivery agreement, are implemented, operated and maintained by a third party.* |
| 10.2.2 | *Whether the services, reports and records provided by third party are regularly monitored and* |

| *AI* | *Descrição* |
|---|---|
| | *reviewed.*<br>*Whether audita are conducted on the above third party services, reports and records, on regular interval.* |
| 10.2.3 | *Whether changes to provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed.*<br>*Does this take into account criticality of business systems, processes involved and re-assessment of risks* |
| 10.3.1 | *Whether the capacity demands are monitored and projections of future capacity requirements are made, to ensure that adequate processing power and storage are available.*<br>*Example: Monitoring hard disk space, RAM and CPU on critical servers.* |
| 10.3.2 | *Whether system acceptance criteria are established for new information systems, upgrades and new versions.*<br>*Whether suitable tests were carried out prior to acceptance.* |
| 10.4.1 | *Whether detection, prevention and recovery controls, to protect against malicious code and appropriate user awareness procedures, were developed and implemented.* |
| 10.4.2 | *Whether only authorized mobile code is used.*<br>*Whether the configuration ensures that authorized mobile code operates according to security policy.*<br>*Whether execution of unauthorized mobile code is prevented.*<br>*(Mobile code is software code that transfers from one computer to another computer and then executes automatically. It performs a specific function with little or no user intervention. Mobile code is associated with a number of middleware services.)* |
| 10.5.1 | *Whether back-ups of information and software is taken and tested regularly in accordance with the agreed backup policy.*<br>*Whether all essential information and software can be recovered following a disaster or media failure.* |
| 10.6.1 | *Whether the network is adequately managed and controlled, to protect from threats, and to maintain security for the systems and applications using the network, including the information in transit.*<br>*Whether controls were implemented to ensure the security of the information in networks, and the protection of the connected services from threats, such as unauthorized access.* |
| 10.6.2 | *Whether security features, service levels and management requirements, of all network services, are identified and included in any network services agreement.*<br>*Whether the ability of the network service provider, to manage agreed services in a secure way, is determined and regularly monitored, and the right to audit is agreed upon.* |
| 10.7.1 | *Whether procedures exist for management of removable media, such as tapes, disks, cassettes, memory cards, and reports.*<br>*Whether all procedures and authorization levels are clearly defined and documented.* |
| 10.7.2 | *Whether the media that are no longer required are disposed of securely and safely, as per formal procedures.* |
| 10.7.3 | *Whether a procedure exists for handling information storage.*<br>*Does this procedure address issues, such as information protection, from unauthorized disclosure or misuse?* |
| 10.7.4 | *Whether the system documentation is protected against unauthorized access.* |
| 10.8.1 | *Whether there is a formal exchange policy, procedure and control in place to ensure the protection of information.*<br>*Does the procedure and control cover using electronic communication facilities for information exchange.* |
| 10.8.2 | *Whether agreements are established concerning exchange of information and software between the organization and external parties.*<br>*Whether the security content of the agreement reflects the sensitivity of the business information involved.* |
| 10.8.3 | *Whether media containing information is protected against unauthorized access, misuse or corruption during transportation beyond the organizations physical boundary.* |
| 10.8.4 | *Whether the information involved in electronic messaging is well protected.*<br>*(Electronic messaging includes but is not restricted to Email, Electronic Data Interchange, Instant Messaging)* |
| 10.8.5 | *Whether policies and procedures are developed and enforced to protect information associated with the interconnection of business information systems.* |
| 10.9.1 | *Whether the information involved in electronic commerce passing over the public network is protected from fraudulent activity, contract dispute, and any unauthorized access or modification.*<br>*Whether Security control such as application of cryptographic controls are taken into consideration.*<br>*Whether electronic commerce arrangements between trading partners include a documented* |

| *AI* | *Descrição* |
|---|---|
| | *agreement, which commits both parties to the agreed terms of trading, including details of security issues.* |
| 10.9.2 | *Whether information involved in online transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.* |
| 10.9.3 | *Whether the integrity of the publicly available information is protected against any unauthorized modification.* |
| 10.10.1 | *Whether audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.*<br>*Whether appropriate Privacy protection measures are considered in Audit log maintenance.* |
| 10.10.2 | *Whether procedures are developed and enforced for monitoring system use for information processing facility.*<br>*Whether the results of the monitoring activity reviewed regularly.*<br>*Whether the level of monitoring required for individual information processing facility is determined by a risk assessment.* |
| 10.10.3 | *Whether logging facility and log information are well protected against tampering and unauthorized access.* |
| 10.10.4 | *Whether system administrator and system operator activities are logged.*<br>*Whether the logged activities are reviewed on regular basis.* |
| 10.10.5 | *Whether faults are logged analysed and appropriate action taken.*<br>*Whether level of logging required for individual system are determined by a risk assessment, taking performance degradation into account.* |
| 10.10.6 | *Whether system clocks of all information processing system within the organization or security domain is synchronised with an agreed accurate time source.*<br>*(The correct setting of computer clock is important to ensure the accuracy of audit logs)* |
| 11.1.1 | *Whether an access control policy is developed and reviewed based on the business and security requirements.*<br>*Whether both logical and physical access control are taken into consideration in the policy.*<br>*Whether the users and service providers were given a clear statement of the business requirement to be met by access controls.* |
| 11.2.1 | *Whether there is any formal user registration and de-registration procedure for granting access to all information systems and services.* |
| 11.2.2 | *Whether the allocation and use of any privileges in information system environment is restricted and controlled i.e., Privileges are allocated on need-to-use basis, privileges are allocated only after formal authorization process.* |
| 11.2.3 | *Whether the users are asked to sign a statement to keep the password confidential. The allocation and reallocation of passwords should be controlled through a formal management process.* |
| 11.2.4 | *Whether there exists a process to review user access rights at regular intervals. Example: Special privilege review every 3 months, normal privileges every 6 moths.* |
| 11.3.1 | *Whether there are any security practice in place to guide users in selecting and maintaining secure passwords.* |
| 11.3.2 | *Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment. .*<br>*Example: Logoff when session is finished or set up auto log off, terminate sessions when finished etc.,* |
| 11.3.3 | *Whether the organisation has adopted clear desk policy with regards to papers and removable storage media*<br>*Whether the organisation has adopted clear screen policy with regards to information processing facility* |
| 11.4.1 | *Whether users are provided with access only to the services that they have been specifically authorized to use.*<br>*Whether there exists a policy that does address concerns relating to networks and network services.* |
| 11.4.2 | *Whether appropriate authentication mechanism is used to control access by remote users.* |
| 11.4.3 | *Whether automatic equipment identification is considered as a means to authenticate connections from specific locations and equipment.* |
| 11.4.4 | *Whether physical and logical access to diagnostic ports are securely controlled i.e., protected by a security mechanism.* |
| 11.4.5 | *Whether groups of information services, users and information systems are segregated on networks.*<br>*Whether the network (where business partners and/ or third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls.*<br>*Whether consideration is made to segregation of wireless networks from internal and private* |

| *AI* | *Descrição* |
|---|---|
| | *networks.* |
| 11.4.6 | *Whether there exists an access control policy which states network connection control for shared networks, especially for those extend across organizations boundaries.* |
| 11.4.7 | *Whether the access control policy states routing controls are to be implemented for networks. Whether the routing controls are based on the positive source and destination identification mechanism.* |
| 11.5.1 | *Whether access to operating system is controlled by secure log-on procedure.* |
| 11.5.2 | *Whether unique identifier (user ID) is provided to every user such as operators, system administrators and all other staff including technical. Whether suitable authentication technique is chosen to substantiate the claimed identity of user. Whether generic user accounts are supplied only under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.* |
| 11.5.3 | *Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.,* |
| 11.5.4 | *Whether the utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.* |
| 11.5.5 | *Whether inactive session is shutdown after a defined period of inactivity.*<br>*(A limited form of timeouts can be provided for some systems, which clears the screen and prevents unauthorized access but does not close down the application or network sessions.* |
| 11.5.6 | *Whether there exists restriction on connection time for high-risk applications. This type of set up should be considered for sensitive applications for which the terminals are installed in high-risk locations.* |
| 11.6.1 | *Whether access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.* |
| 11.6.2 | *Whether sensitive systems are provided with dedicated (isolated) computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,* |
| 11.7.1 | *Whether a formal policy is in place, and appropriate security measures are adopted to protect against the risk of using mobile computing and communication facilities.*<br>*Some example of Mobile computing and communications facility include: notebooks, palmtops, laptops, smart cards, mobile phones.*<br>*Whether risks such as working in unprotected environment is taken into account by Mobile computing policy.* |
| 11.7.2 | *Whether policy, operational plan and procedures are developed and implemented for teleworking activities.*<br>*Whether teleworking activity is authorized and controlled by management and does it ensure that suitable arrangements are in place for this way of working.* |
| 12.1.1 | *Whether security requirements for new information systems and enhancement to existing information system specify the requirements for security controls.*<br>*Whether the Security requirements and controls identified reflects the business value of information assets involved and the consequence from failure of Security.*<br>*Whether system requirements for information security and processes for implementing security is integrated in the early stages of information system projects.* |
| 12.2.1 | *Whether data input to application system is validated to ensure that it is correct and appropriate.*<br>*Whether the controls such as: Different types of inputs to check for error messages, Procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process etc., are considered.* |
| 12.2.2 | *Whether validation checks are incorporated into applications to detect any corruption of information through processing errors or deliberate acts.*<br>*Whether the design and implementation of applications ensure that the risks of processing failures leading to a loss of integrity are minimised.* |
| 12.2.3 | *Whether requirements for ensuring and protecting message integrity in applications are identified, and appropriate controls identified and implemented.*<br>*Whether an security risk assessment was carried out to determine if message integrity is required, and to identify the most appropriate method of implementation.* |
| 12.2.4 | *Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.* |
| 12.3.1 | *Whether the organization has Policy on use of cryptographic controls for protection of information. .*<br>*Whether the policy is successfully implemented.*<br>*Whether the cryptographic policy does consider the management approach towards the use of cryptographic controls, risk assessment results to identify required level of protection, key management methods and various standards for effective implementation.* |
| 12.3.2 | *Whether key management is in place to support the organizations use of cryptographic* |

| *AI* | *Descrição* |
|---|---|
| | *techniques.*<br>*Whether cryptographic keys are protected against modification, loss, and destruction.*<br>*Whether secret keys and private keys are protected against unauthorized disclosure.*<br>*Whether equipments used to generate, store keys are physically protected.*<br>*Whether the Key management system is based on agreed set of standards, procedures and secure methods.* |
| 12.4.1 | *Whether there are any procedures in place to control installation of software on operational systems. (This is to minimise the risk of corruption of operational systems.)* |
| 12.4.2 | *Whether system test data is protected and controlled.*<br>*Whether use of personal information or any sensitive information for testing operational database is shunned.* |
| 12.4.3 | *Whether strict controls are in place to restrict access to program source libraries.*<br>*(This is to avoid the potential for unauthorized, unintentional changes.)* |
| 12.5.1 | *Whether there is strict control procedure in place over implementation of changes to the information system. (This is to minimise the corruption of information system.)*<br>*Whether this procedure addresses need for risk assessment, analysis of impacts of changes,* |
| 12.5.2 | *Whether there is process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security after the change to Operating Systems.*<br>*Periodically it is necessary to upgrade operating system i.e., to install service packs, patches, hot fixes etc.,* |
| 12.5.3 | *Whether modifications to software package is discouraged and/ or limited to necessary changes.*<br>*Whether all changes are strictly controlled.* |
| 12.5.4 | *Whether controls are in place to prevent information leakage.*<br>*Whether controls such as scanning of outbound media, regular monitoring of personnel and system activities permitted under local legislation, monitoring resource usage are considered.* |
| 12.5.5 | *Whether the outsourced software development is supervised and monitored by the organization.*<br>*Whether points such as: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc., are considered.* |
| 12.6.1 | *Whether timely information about technical vulnerabilities of information systems being used is obtained.*<br>*Whether the organizations exposure to such vulnerabilities evaluated and appropriate measures taken to mitigate the associated risk.* |
| 13.1.1 | *Whether information security events are reported through appropriate management channels as quickly as possible.*<br>*Whether formal information security event reporting procedure, Incident response and escalation procedure is developed and implemented.* |
| 13.1.2 | *Whether there exists a procedure that ensures all employees of information systems and services are required to note and report any observed or suspected security weakness in the system or services.* |
| 13.2.1 | *Whether management responsibilities and procedures were established to ensure quick, effective and orderly response to information security incidents.*<br>*Whether monitoring of systems, alerts and vulnerabilities are used to detect information security incidents.*<br>*Whether the objective of information security incident management is agreed with the management.* |
| 13.2.2 | *Whether there is a mechanism in place to identify and quantify the type, volume and costs of information security incidents.*<br>*Whether the information gained from the evaluation of the past information security incidents are used to identify recurring or high impact incidents.* |
| 13.2.3 | *Whether follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal).*<br>*Whether evidence relating to the incident are collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).*<br>*Whether internal procedures are developed and followed when collecting and presenting evidence for the purpose of disciplinary action within the organization.* |
| 14.1.1 | *Whether there is a managed process in place that addresses the information security requirements for developing and maintaining business continuity throughout the organization.*<br>*Whether this process understands the risks the organization is facing, identify business critical assets, identify incident impacts, consider the implementation of additional preventative controls and documenting the business continuity plans addressing the security requirements.* |
| 14.1.2 | *Whether events that cause interruption to business process is identified along with the probability and impact of such interruptions and their consequence for information security.* |
| 14.1.3 | *Whether plans were developed to maintain and restore business operations, ensure availability of* |

| *AI* | *Descrição* |
|---|---|
| | *information within the required level in the required time frame following an interruption or failure to business processes.*<br>*Whether the plan considers identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing.* |
| 14.1.4 | *Whether there is a single framework of Business continuity plan.*<br>*Whether this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance.*<br>*Whether business continuity plan addresses the identified information security requirement.* |
| 14.1.5 | *Whether Business continuity plans are tested regularly to ensure that they are up to date and effective.*<br>*Whether business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when plan is evoked.* |
| 15.1.1 | *Whether all relevant statutory, regulatory, contractual requirements and organizational approach to meet the requirements were explicitly defined and documented for each information system and organization.*<br>*Whether specific controls and individual responsibilities to meet these requirements were defined and documented.* |
| 15.1.2 | *Whether there are procedures to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.*<br>*Whether the procedures are well implemented.*<br>*Whether controls such as: publishing intellectual property rights compliance policy, procedures for acquiring software, policy awareness, maintaining proof of ownership, complying with software terms and conditions are considered.* |
| 15.1.3 | *Whether important records of the organization is protected from loss destruction and falsification, in accordance with statutory, regulatory, contractual and business requirement.*<br>*Whether consideration is given to possibility of deterioration of media used for storage of records.*<br>*Whether data storage systems were chosen so that required data can be retrieved in an acceptable timeframe and format, depending on requirements to be fulfilled.* |
| 15.1.4 | *Whether data protection and privacy is ensured as per relevant legislation, regulations and if applicable as per the contractual clauses.* |
| 15.1.5 | *Whether use of information processing facilities for any non-business or unauthorized purpose, without management approval is treated as improper use of the facility.*<br>*Whether a log-on a warning message is presented on the computer screen prior to log-on.*<br>*Whether the user has to acknowledge the warning and react appropriately to the message on the screen to continue with the log-on process.*<br>*Whether legal advice is taken before implementing any monitoring procedures.* |
| 15.1.6 | *Whether the cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.* |
| 15.2.1 | *Whether managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.*<br>*Do managers regularly review the compliance of information processing facility within their area of responsibility for compliance with appropriate security policy and procedure* |
| 15.2.2 | *Whether information systems are regularly checked for compliance with security implementation standards.*<br>*Whether the technical compliance check is carried out by, or under the supervision of, competent, authorized personnel.* |
| 15.3.1 | *Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business process.*<br>*Whether the audit requirements, scope are agreed with appropriate management.* |
| 15.3.2 | *Whether access to information system audit tools such as software or data files are protected to prevent any possible misuse or compromise.*<br>*Whether information system audit tools are separated from development and operational systems, unless given an appropriate level of additional protectizon.* |