

**UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA
COMPUTAÇÃO**

**ABORDAGEM COLABORATIVA PARA
GERENCIAMENTO DE RISCOS DE SEGURANÇA
DA INFORMAÇÃO**

DISSERTAÇÃO DE MESTRADO

Maicon Balke

Santa Maria, RS, Brasil

2015

ABORDAGEM COLABORATIVA PARA GERENCIAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Maicon Balke

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Ciência da Computação, Área de Concentração em Computação Aplicada, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Ciência da Computação.**

Orientadora: Lisandra Manzoni Fontoura
Co-orientador: Luis Álvaro de Lima Silva

Santa Maria, RS, Brasil

2015

Ficha catalográfica elaborada através do Programa de Geração Automática da Biblioteca Central da UFSM, com os dados fornecidos pelo(a) autor(a).

Balke, Maicon
Abordagem colaborativa para gerenciamento de riscos de segurança da informação / Maicon Balke.-2015.
73 p.; 30cm

Orientadora: Lisandra Manzoni Fontoura
Coorientador: Luis Álvaro de Lima Silva
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Informática, RS, 2015

1. segurança da informação 2. Gerenciamento de riscos de segurança da informação 3. Jogos de Diálogos 4. Argumentação I. Fontoura, Lisandra Manzoni II. Silva, Luis Álvaro de Lima III. Título.

© 2015

Todos os direitos autorais reservados a Maicon Balke. A reprodução de partes ou do todo deste trabalho só poderá ser feita mediante a citação da fonte.

. Eletrônico: maiconbalke@gmail.com

**Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Ciência da Computação**

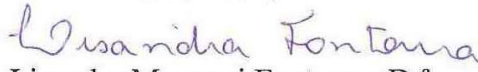
**A Comissão Examinadora, abaixo assinada,
Aprova a Dissertação de Mestrado**

**ABORDAGEM COLABORATIVA PARA
GERENCIAMENTO DE RISCOS DE SEGURANÇA DA
INFORMAÇÃO**


Elaborada por
Maicon Balke

Como requisito parcial para obtenção do grau de
Mestre em Ciência da Computação

COMISSÃO EXAMINADORA:


Lisandra Manzon Fontoura, Dr^a.
(Presidente/Orientadora)


Profa. Giliane Bernardi (UFSM)


Paulo Sérgio Sausen (UNIJUI)

Santa Maria, 18 de dezembro de 2015.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar força e me oportunizar finalizar mais esta etapa da minha vida.

À meus pais Nilton e Maria e à meu irmão Marlon, por me mostrar o caminho, me ensinar a seguir em frente e serem meus grandes exemplos e porto seguro.

Minha namorada Pâmela, pelo carinho, apoio, companhia, paciência e força, que sem isso não teria conseguido chegar até aqui.

À todos os meus familiares e amigos, que estiveram sempre presentes, fornecendo o carinho e o apoio para que tudo pudesse sair como o planejado;

Aos colegas do Laboratório de Computação Aplicada (LaCA), pela convivência, auxílios, discussões e, principalmente, pela amizade;

Aos meus orientadores, Lisandra e Luís Alvaro, que tiveram papel fundamental para que este trabalho fosse concluído. Pela oportunidade fornecida de podermos trabalhar juntos. Pelos ensinamentos, dedicação e amizade

A todas as pessoas que se disponibilizaram e ajudaram na conclusão deste trabalho, fornecendo ideias, discutindo e dispondo do seu tempo para participar das avaliações;

Muito Obrigado!

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Maria

ABORDAGEM COLABORATIVA PARA GERENCIAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

AUTOR: MAICON BALKE
ORIENTADORA: LISANDRA MANZONI FONTOURA
CO-ORIENTADOR: LUIS ÁLVARO DE LIMA SILVA
Local da Defesa e Data: Santa Maria, 18 de dezembro de 2015

Gerenciar riscos é um dos principais processos da gestão de segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Com o objetivo de utilizar diferentes experiências, tarefas colaborativas de gestão de riscos de segurança da informação proporcionam interação argumentativa entre os participantes do projeto envolvidos no desenvolvimento de debates sobre a gestão de riscos de segurança da informação. Neste trabalho, é proposta uma abordagem colaborativa baseada em argumentação para a gestão de riscos de segurança da informação. A abordagem visa garantir, por meio de um conjunto de regras, que determinadas atividades definidas em um processo de gestão de riscos sejam executadas e, dessa forma, a discussão final seja completa e consistente. O protocolo de comunicação é adaptado a um processo de gestão de riscos de segurança definido a partir da ISO/IEC 27005. O protocolo permite estruturar e controlar discussões de riscos realizadas por participantes de um debate usando um sistema de discussão chamado RD System. Um estudo de caso e experimentos foram realizados para validar a proposta deste trabalho. Os resultados apresentaram evidências positivas de aceitação e aplicabilidade da abordagem em discussões de riscos de segurança da informação. Assim como, a definição de um processo e regras de validação melhorou a qualidade das informações da discussão.

Palavras-chave: Segurança da informação, Gerenciamento de riscos de segurança da informação, Jogos de Diálogos, Argumentação.

ABSTRACT

Master's Dissertation
Post-Graduate Program in Informatics
Federal University of Santa Maria

COLLABORATIVE APPROACH TO RISK MANAGEMENT OF INFORMATION SECURITY

AUTHOR: MAICON BALKE
ADVISOR: LISANDRA MANZONI FONTOURA
COADVISOR: LUÍS ALVARO DE LIMA SILVA
Defense Place and Date: Santa Maria, December 18st, 2015

Risk management is one of the main management processes of security information since it aims to identify, analyze, evaluate and control risks that are due to security information. To utilize users' experiences in this process, the utilization of collaborative tasks allows one to exploit argumentative interactions between project participants that are involved in the development of risk management debates regarding security information. The goal of this paper is to propose an argumentation-based collaborative approach to deal with such risk management of security information. The approach aims to guarantee that activities defined in a security risk management process are executed accordingly. In addition, a set of rules is proposed to ensure that the final security risk management debate is complete and consistent with the arguments presented by participants of a security software project. This communication protocol is tailored to a process of security risk management that was particularly defined from the ISO / IEC 27005. The protocol allows users to structure and control risk discussions developed by debate participants using a web-based tool called RD System. A case study and experiments were developed to validate the approach proposed in this this work. The results showed positive evidence of acceptance and applicability of the approach in discussions of information security risks. According to participants, the definition of a process and validation rules improved the quality of the information.

Keywords: Information security, information security risk management Dialogues Games, Argumentation

LISTA DE FIGURAS

Figura 1 - Elementos que a segurança da informação deve atender (STONEBURNER, 2001).....	21
Figura 2- Processo de Gestão de riscos de segurança da informação Fonte: NBR ISO/IEC 27005:2008.	27
Figura 3 - Processo de tratamento do risco - Fonte: NBR ISO/IEC 27005:2008	28
Figura 4 - Fluxo do RD System.....	39
Figura 5 - Processo de discussão de riscos de segurança da informação	48
Figura 6 - Modulo de cadastro de Organização	55
Figura 7 - Modulo de cadastro de contexto onde será feita a discussão	55
Figura 8 - Modulo da discussão com o modulo de validação das regras	56
Figura 9 - Fragmento de uma discussão inconsistente juntamente com as correções.....	59
Figura 10 - Gráficos de dados do questionário do experimento.....	65

LISTA DE TABELA

Tabela 1 - Trabalhos relacionados	17
Tabela 2 - Locuções do protocolo de comunicação que determinam o início e término de uma discussão de riscos	45
Tabela 3 - Atos de locuções específicos para discussão das tarefas de gerenciamento de riscos de segurança da informação	45
Tabela 4 - Atos de locuções de propósito geral que visam permitir uma discussão crítica de riscos e seus planos	46
Tabela 5 - Fragmento de regras de transição de etapa	49

LISTA DE ABREVIATURAS E SIGLAS

RD system	Risk Discussion System
GRSI	Gerenciamento de Riscos de Segurança da Informação
PEnSo	Grupo de Pesquisa em Engenharia de Software
CLEI	Conferência latino-americana de informática
ISO	International Organization for Standardization
PPGI	Programa de Pós-Graduação em Informática
UFSM	Universidade Federal de Santa Maria

SUMÁRIO

LISTA DE FIGURAS	8
LISTA DE TABELA	9
LISTA DE ABREVIATURAS E SIGLAS	10
SUMÁRIO	11
1. INTRODUÇÃO	12
2. TRABALHOS RELACIONADOS	15
3. REFERENCIAL TEÓRICO	19
3.1. Segurança da Informação	19
3.1.1. Os componentes Básicos de Segurança da Informação	22
3.2. Gestão de Riscos de Segurança da Informação	24
3.3. NORMA ISO/IEC 27005:2011	26
3.4. Argumentação	29
3.4.1. Jogos de Diálogos.....	31
3.5. Consistência em Projeto de Software Adaptado para Processo de Colaboração	35
4. PROJETO DE PESQUISA	37
4.1. Contextualização da pesquisa	38
4.2. RD System (Risk Discussion System)	39
5. ABORDAGEM COLABORATIVA EM RISCOS DE SEGURANÇA DA INFORMAÇÃO..	41
5.1. Definições do Protocolo	42
5.1.1. Conjunto de Locuções do Jogo de Diálogo.....	44
5.1.2. Processo para Discussão Colaborativa de Riscos de Segurança da Informação	47
5.1.3. Regras de validação da discussão.....	48
5.1.4. Construção do módulo de validação da discussão	54
6. RESULTADOS E DISCUSSÕES	57
6.1. Estudo de Caso	57
6.2. Experimentos Realizados para Avaliação da Abordagem Proposta	61
7. CONSIDERAÇÕES FINAIS	66
REFERÊNCIAS	68

1. INTRODUÇÃO

Segundo o *Federal Information Security Management Act (FISMA)* (MANAGEMENT, 2015), segurança da informação se refere a proteger os sistemas de informação e as informações contra acesso não autorizado ou uso indevido dessas informações. As atividades relacionadas à segurança da informação têm como objetivo identificar e eliminar as vulnerabilidades de sistemas de computador ou redes de computadores. Porém, os problemas de muitas organizações na implementação de segurança da informação estão relacionados com a dificuldade em definir o que deve ser protegido, qual o nível de proteção necessário e quais ferramentas devem ser utilizadas (DIVISION, 2011).

A priorização das ações em segurança da informação e a falta de exploração das atividades de gestão de risco de segurança de informação (GRSI) podem ser consideradas duas das maiores dificuldades na gestão de segurança (HALEY; LANEY; MOFFETT, 2008a). Normalmente, existe uma ideia de que tudo em segurança é importante, mas comumente não existem recursos financeiros para tratamento de todos os riscos.

Em 2012, foi realizado um estudo pela empresa Kaspersky (QUADRANT; PLATFORMS, 2012), no qual foram entrevistadas 3300 organizações em 22 países, incluindo o Brasil. O resultado do estudo traz a informação de que, para 42% dos entrevistados, a importância dos problemas com crimes virtuais, como roubo de dados, exposição de dados importantes, entre outros, deve aumentar nos próximos anos.

Se a estimativa estiver correta, existirão ainda mais problemas e, como consequência destes, poderão ocorrer eventos que afetarão a integridade, disponibilidade e confiabilidade dos ativos organizacionais. Por esse motivo, torna-se necessário o uso de uma sistemática para identificar os possíveis riscos de segurança de informação em projetos de Tecnologia de Informação e para elaborar um plano de gerenciamento de riscos descrevendo as ações a serem tomadas durante o projeto para manter os fatores de risco sob controle (NOROOZI *et al.*, 2012).

Além disso, é importante a colaboração entre os membros da equipe do projeto visando englobar diferentes visões, compartilhar conhecimento e experiências e fomentar uma discussão sobre riscos de segurança. É importante que pessoas de diferentes níveis organizacionais, tais como gerentes e desenvolvedores participem do processo decisório, pois o conhecimento acerca de um projeto geralmente encontra-se disperso em diferentes fontes.

Atualmente, muitas organizações utilizam o desenvolvimento distribuído de software (PRIKLADNICKI; AUDY, 2007)(HUZITA; SILVA; WIESE, 2008).

Neste tipo de desenvolvimento, diferentes equipes podem trabalhar em diferentes locais, com diferentes fusos horários, dificultando a realização de reuniões presenciais ou videoconferência. Ferramentas de colaboração assíncronas possibilitam a participação de membros que atuam em equipes distribuídas geograficamente (HUZITA; SILVA; WIESE, 2008).

Técnicas de argumentação, assim como sistemas de argumentação típicos, conforme descrito em (REED; WELLS, 2007; TOLCHINSKY *et al.*, 2006), podem ser usadas para facilitar a organização e a compreensão de um diálogo, e dessa forma, auxiliar no desenvolvimento de discussões assíncronas. No cenário de técnicas de argumentação, optou-se por usar jogos de diálogo (BLACK; ATKINSON; KATIE, 2009) no desenvolvimento deste trabalho. Em especial, jogos de diálogo descrevem como organizar a troca de argumentos em uma discussão, por meio da definição de um protocolo de comunicação (BLACK; ATKINSON; KATIE, 2009). Entre outras características, essa estrutura de representação de conhecimento visa identificar e representar passos significativos de interação humana que são típicos de diálogos (NING, 2007).

Um dos problemas relacionados a utilização de jogos de diálogos em tarefas de aquisição e representação de argumentos em discussões colaborativas é a produção de discussões muitas vezes incoerentes, nas quais argumentos apresentados podem estar incompletos. Estas podem levar a equipe do projeto a tomar decisões não acertadas, principalmente por não seguir um processo sistemático de gerenciamento de riscos de segurança da informação. Para garantir que as atividades típicas de gerenciamento de riscos de segurança sejam exploradas nestes cenários de discussão colaborativa usando jogos de diálogo, neste trabalho é estruturado as discussões de riscos de segurança da informação com base nas atividades descritas na norma ISO/IEC 27005. Essa norma foi escolhida porque ela descreve um processo sistemático de segurança da informação. Além disso, visando garantir a obtenção de uma discussão completa e bem estruturada para este problema de aplicação foram propostas regras para validação da consistência de discussões realizadas. As regras têm como objetivo garantir que todas as atividades descritas em um processo de gerenciamento de riscos, elaborado a partir da ISO/IEC 27005, sejam executadas em uma ordem pré-definida. Um sistema *web* para apoiar as discussões de riscos – *Risk Discussion system* (RD system) – é utilizado com o propósito de gerenciar protocolos e interações entre os *stakeholders*, assim disponibilizando um ambiente colaborativo para discussões de riscos de segurança. As discussões de riscos são registradas em uma memória e validadas por meio de um conjunto de regras.

A principal contribuição deste trabalho é a proposta de um protocolo para jogos de diálogos visando atender as necessidades de uma discussão colaborativa de riscos de segurança da informação. Este protocolo utiliza um processo para garantir que a colaboração seja realizada de forma consistente auxiliando os gestores na tomada de decisões sobre riscos de segurança. Para satisfazer este objetivo foram definidos um protocolo de debate, um processo de debate baseado na ISO/IEC 27005 e um conjunto de regras de validação da discussão.

A abordagem proposta nessa pesquisa explora o uso de um protocolo de jogo de diálogo para formalizar e estruturar discussões de riscos em segurança da informação, bem como a utilização do processo descrito na norma ISO 27005 para elaboração de regras de verificação e completude para que a discussão possa ser finalizada de uma forma consistente e completa e, conseqüentemente, registrar estes debates em uma memória de discussões de riscos reutilizável. Além disso, para garantir que experiências de gerenciamento de riscos de segurança sejam exploradas, o trabalho proposto formaliza e estrutura discussões de riscos de segurança da informação e também armazena estes debates em uma memória de discussões. Dessa forma, foi adaptado e utilizado um sistema *web* para apoiar as discussões de riscos – Risk Discussion system (RD system) – com o propósito de gerenciar protocolos e interações entre os *stakeholders*, assim disponibilizando um ambiente colaborativo para discussões de riscos.

Nesta dissertação, também, é apresentado resultados de experimentos realizados para a avaliação da abordagem e do sistema propostos. Os resultados obtidos apresentam evidência positiva da aplicabilidade e usabilidade de ambos, o qual é relevante para incrementar as informações que são usualmente geridas por abordagens tradicionais de gerenciamento de risco de segurança da informação, i.e., aumentar a quantidade e/ou qualidade das informações gerenciadas.

O restante deste trabalho está organizado como segue: no Capítulo 2 é apresentado uma revisão de conceitos importantes para o entendimento deste trabalho; no Capítulo 3 é apresentado o projeto de pesquisa a partir do qual esse trabalho foi definido; no Capítulo 4 é apresentado uma abordagem colaborativa de gerenciamento de risco de segurança da informação baseada em jogos de diálogo proposta neste trabalho; no Capítulo 5 é apresentado uma comparação entre este trabalho e trabalhos relacionados; no Capítulo 6 é apresentado os resultados de experimentos realizados e uma avaliação destes resultados, e por fim; no Capítulo 7 apresentado conclusões e trabalhos futuros.

2. TRABALHOS RELACIONADOS

O presente trabalho envolve a integração de duas áreas de pesquisa distintas: o gerenciamento de riscos de segurança da informação no contexto da Engenharia de Software e a argumentação no contexto da Inteligência Artificial. Logo, o trabalho pode ser analisado segundo pontos de vista distintos, mas complementares. Dentro do contexto da engenharia de software e do gerenciamento de riscos de segurança da informação, este trabalho pode ser comparado com reuniões “tradicionais” de gerenciamento de riscos, bem como com propostas que explorem a colaboração no desenvolvimento destas tarefas. Segundo o ponto de vista da argumentação, este trabalho pode ser comparado com sistemas de argumentação propostos em outros domínios de aplicação. Neste caso, alguns sistemas foram previamente propostos para a solução de problemas na área de gerenciamento de riscos de segurança da informação. A comparação entre estes trabalhos é descrita nas próximas seções.

Yuan (2011) explora a ideia que a avaliação de riscos de segurança usando técnicas de argumentação pode ser formalizada como uma troca de argumentos entre assessores, os quais são especialistas em segurança e agentes de ameaças hipotéticas. Na prática, os avaliadores discutem como o sistema pode ser atacado por um agente de ameaça e os assessores defendem o sistema para verificar se a especificação satisfaz um determinado requisito de segurança. O sistema não conta com técnicas de consistência e completude da discussão, podendo assim terminar a avaliação sem passar por todas as etapas. Este trabalho não é utilizado em locais geograficamente distribuídos.

Franqueira (FRANQUEIRA *et al.*, 2011) explora o uso de catálogos compartilhados de experiência em segurança para apoiar a avaliação de risco e para orientar a argumentação de segurança na busca de respostas e nas fraquezas para a satisfação dos requisitos de segurança. Baseia-se em dois principais conceitos propostos por Haley *et al.* (HALEY; LANEY; MOFFETT, 2008b): a noção da satisfação de requisitos de segurança, bem como a utilização de argumentos divididos entre argumentos externos e internos para demonstrar a segurança do sistema. Os argumentos externos e internos estão relacionados da seguinte forma: o argumento externo formal oferece a estrutura principal que conduz a argumentação interna. Cada uma das premissas dos argumentos exteriores é o começo para uma lista de discussão de argumentos internos onde os participantes podem argumentar de forma informal. Ele fornece uma visão

intuitiva sobre a evolução de um argumento no formato de um debate entre dois oponentes. É representado como uma estrutura de árvore de argumentos e contra-argumentos.

Prakken (PRAKKEN; IONITA; WIERINGA, 2013), cria uma abordagem de argumentação sob medida para avaliação de risco. Ele substitui argumentos informais propostos por Toulmin com argumentos aspíc em uma tentativa de formalizar o processo como um jogo de argumentação em que a equipe troca argumentos sobre como o sistema pode ser atacado e contra ataques que são viáveis para o sistema. O jogo é dinâmico, os defensores podem adicionar ou remover elementos da arquitetura alvo conforme o jogo progride. Essa abordagem tem alcançado uma boa visibilidade, mas devido ao seu alto nível de formalismo, é muito difícil de usar: todos os argumentos têm de ser definidos com relação a uma base de conhecimentos utilizando uma sintaxe rigorosa. Embora o conceito de um jogo de argumentação parece promissora, a alta sobrecarga adicionada pela estrutura lógica formal representa uma ameaça significativa para a escalabilidade e facilidade de utilização da abordagem

Tabela 1 - Trabalhos relacionados

	Yuan (2011)	Franqueira <i>et al.</i> (FRANQUEIRA <i>et al.</i>, 2011)	Prakken <i>et al.</i> (PRAKKEN; IONITA; WIERINGA, 2013)	Gerenciamento colaborativo de riscos de segurança da informação
Qual a área de aplicação destes trabalhos?	Riscos de segurança.	Requisitos de Segurança em projeto de software.	Segurança da informação.	Gerenciamento de riscos de segurança da informação
Qual a técnica Utilizada	Não está claro o padrão de representação utilizado.	Utiliza argumentos informais baseado em premissas feitas por argumentos exteriores que mostram se as propriedades implicam os requisitos de segurança. Expressa em uma linguagem formal, como a lógica proposicional e com argumentos internos para tentar rebater um argumento externo, questionando seus argumentos.	A arquitetura do sistema além de suposições sobre o meio ambiente é especificado como uma teoria da argumentação ASPIC+, e um jogo de argumento definido para a troca de argumentos entre avaliadores e agentes de ameaça.	Utiliza uma linguagem semiformal deliberativo para a representação de jogos de diálogo, bem como técnicas de consistência utilizadas em processos de software adaptado para um protocolo colaborativo, tendo assim a garantia de uma discussão completa.
Como os modelos de argumentação foram desenvolvidos?	Foram desenvolvidos em um processo de gerenciamento de riscos, com base em ataques e defesas usando argumentação (baseado em um estudo da literatura de engenharia da segurança de sistemas).	com base em requisitos de segurança e com catálogos compartilhados representados como uma estrutura de árvore de argumentos e contra-argumentos.	É jogo de argumentação formal sob medida para avaliação de risco em que os avaliadores se alternam entre a desempenhar o papel de defensores e atacantes do sistema, argumentando como o sistema pode ser defendido e atacado.	É organizado por um jogo de diálogo, este trabalho formaliza e estrutura discussões de riscos de segurança da informação com base nas atividades descritas na norma ISO/IEC 27005.
Qual forma de Validação da discussão.	Valida com base em argumentos de atacantes e defensores se o sistema de segurança é ou não confiável de acordo com o jogo de diálogo obtido.	Tem como foco a argumentação que avalia o risco, mas não explora todo um processo de gerenciamento de riscos de segurança da informação.	Após um jogo de argumento lógico é testado o status de aceitação de um argumento em um determinado estado de informação, onde verifica todos os movimentos possíveis logicamente legais sobre a base da teoria da argumentação atual	Jogos de diálogo e processos tem como objetivo garantir que todas as atividades descritas em um processo de gerenciamento de riscos, elaborado a partir da ISO/IEC 27005, sejam executadas em uma ordem pré-definida.

			foram feitas. Mas não tem um teste para concluir se de fato este jogo foi finalizado de forma completa.	
Quem pode usar/Supporte a equipes distribuídas	Este método pode ser feito com especialistas na área tendo em vista que precisa ter conhecimento em ataques e defesa de segurança da informação. Não menciona se gerencia equipes geograficamente distribuídas.	Especialistas na área. Não menciona o gerenciamento de equipes distribuídas.	Como é um jogo baseado em atacantes e defensores através de argumentação formal, os autores alegam que para participar do jogo, precisa ser um especialista na área de segurança da informação.	Dialogo colaborativo tem o papel de troca de conhecimento entre agentes através do protocolo que serve como guia para uma discussão. Sendo assim qualquer pessoa em uma organização pode utilizar, possuindo ou não conhecimento avançado em gerenciamento de riscos de segurança da informação.
Existem sistemas desenvolvidos?	Não existe informação disponível sobre um sistema que esteja disponível.	Há um sistema chamado RISA o gerencia a discussão externa e interna gerando um ataque e defesa de argumentos.	O sistema gerenciar um conjunto de regras para a representação e computação de argumentos formais.	Risk Discussion System versão 4.0 (contendo um módulo para a utilização de verificação da discussão, que é utilizado para a verificar se a discussão foi finalizada passando por todos os professos pré-definidos garantindo assim uma discussão completa e consistente).

3. REFERENCIAL TEÓRICO

Este capítulo apresenta conceitos de gerenciamento de riscos de segurança da informação, processos e argumentação (neste caso, jogos de diálogo), os quais são fundamentais para o entendimento deste trabalho. O intuito desta revisão de conceitos é fornecer uma base de conhecimento nos diferentes tópicos abordados neste trabalho.

3.1. Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização. Ela pode estar presente em muitas formas dentro da organização, pode ser armazenado em uma mídia física, seja na forma de papel, ou pode ser o conhecimento e a experiência de um funcionário e, conseqüentemente, há necessidade de ser adequadamente protegida. Isto é, especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 27002; Bernard, 2007).

Um ponto essencial a ser discutido é a necessidade de explorar colaboração e reuso de informações em tarefas do gerenciamento de riscos de segurança da informação. Sendo assim, a colaboração é importante para garantir que os riscos de um ativo de uma organização sejam identificados e discutidos mediante a utilização de diferentes perspectivas e experiências. Quando diferentes participantes (com diferentes papéis na organização) se envolvem em uma discussão de riscos de segurança da informação, mais riscos tendem a ser identificados e a discussão tende a ser mais completa. Além da colaboração, o reuso de informações pode auxiliar na seleção de riscos e de planos relevantes para contornar tais riscos. Através da análise de informações de projetos passados, gravadas em uma memória de gerenciamento de riscos, participantes podem, por exemplo, realizar consultas sobre planos usados para tratar riscos selecionados. Em geral, o objetivo é buscar planos passados que obtiveram sucesso, os quais possam ser mais prováveis de obter sucesso em um projeto corrente.

Neste contexto, segurança da informação está relacionada com a identificação dos ativos de uma organização e do desenvolvimento e implementação de ferramentas, técnicas, políticas, normas, procedimentos e diretrizes para garantir a confidencialidade, integridade e disponibilidade a esses ativos e promover a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

O Instituto Nacional de Padrões e Tecnologia (DIVISION, 2011; MANAGEMENT, 2015) define que: "Segurança da Informação é a proteção de informação e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de assegurar a integridade, confidencialidade e disponibilidade". Dessa forma, a segurança da informação é necessária, porque a confidencialidade, a integridade e disponibilidade da informação podem ser expostas ou modificadas de forma inadequada, causando assim, riscos à informação (KHIDZIR *et al.*, 2010).

Todos os objetivos de segurança da informação devem permitir que uma organização atenda a todos os seus objetivos de negócios de missão através da implementação de sistemas, políticas e procedimentos para reduzir os riscos relacionados a TI para a organização, e também de seus parceiros e clientes (DIVISION, 2011).

Sendo um dos objetivos de segurança da informação, a análise de riscos deve ser feita para que identifique todos os riscos que ameacem as informações, tendo assim, soluções que previna, evite, reduza ou transfira os riscos.

A exigência de ter a segurança da informação na organização é devido aos fatos que as empresas possuem dados confidenciais e informações, como dados de seus clientes, relatórios financeiros, planos de negócios e projetos, informações de estratégias comerciais de negócios, pesquisas e outras informações que lhes dá uma vantagem competitiva (ZAINI, 2013).

Dessa forma, a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT NBR ISO/IEC 27002).

A segurança da informação deve sempre atender a três elementos (MURPHY; FELLOW, 2009) que podem ser visualizados na Figura 1

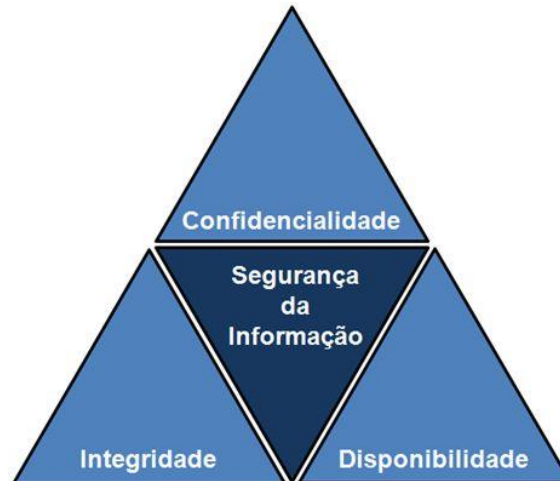


Figura 1- Elementos que a segurança da informação deve atender (STONEBURNER, 2001)

Segundo Barker (2003), confidencialidade é preservar restrições autorizadas no acesso à informação e divulgação, incluindo meios para proteger a privacidade pessoal e informações de propriedade. A confidencialidade é a garantia de que as informações não sejam divulgadas a pessoas não autorizadas, processos ou dispositivos (BARKER, 2003). Assim, aplica-se aos dados armazenados, durante o processamento e quando em trânsito. Dessa forma, a confidencialidade é uma consideração muito importante para qualquer organização lidar com a informação e geralmente é discutido em termos de privacidade.

De acordo com (NIST, 2008), a integridade é definida como a proteção contra modificações imprópria ou destruição das informações, e inclui a garantia de informações não-repúdio e autenticidade. Portanto, a integridade é interpretada para significar a proteção contra a modificação ou destruição de informações não autorizadas, podendo ser vista de uma perspectiva de dados ou de sistema. Dessa forma, a integridade de dados implica que esses não foram alterados de forma não autorizada durante o armazenamento, processamento ou quando em trânsito. Já a integridade do sistema requer quando um sistema estiver em funcionamento como pretendido não seja prejudicada e esteja livre de manipulação não autorizada (BARKER, 2003; WANGEN, 2014).

Disponibilidade é o acesso confiável aos dados e serviços de informação para usuários autorizados (BARKER, 2003). A disponibilidade visa garantir o acesso em tempo útil e confiável do uso de informações. É frequentemente vista como o principal objetivo da segurança da informação de uma organização. Assim, a disponibilidade de informações é uma exigência para garantir que todos os sistemas funcionam prontamente e o serviço não seja negado aos

usuários autorizados. Dessa forma, essa ação deve proteger contra as tentativas intencionais ou acidentais de efetuar o acesso não autorizado e alteração de informações organizacionais ou causar uma negação de serviço ou tentativas de sistema ou de dados utilizados para fins não autorizados.

3.1.1. Os componentes Básicos de Segurança da Informação

Para um gerenciamento colaborativo é necessário à utilização de componentes essenciais de segurança de informação com o intuito de oferecer segurança adequada para organização. Dessa forma, é analisado a interação de alguns agentes considerando certos fatores importantes para a implementação da segurança da informação (Ramos *et al.*, 2008), que são: ativo, ameaça, risco e impacto.

Um ativo de informação é um conjunto de informações, definidos e gerenciados como uma única unidade para que possa ser compreendido, compartilhado, protegido e explorado de forma eficaz. Um ativo também pode ser qualquer elemento da infraestrutura da organização, tais como: software, hardware, ambientes físicos (CAMPOS, 2007).

Leitner *et al.* (2009) e Koronios *et al.* (2006) referem-se à necessidade de distinguir a ampla gama de ativos de uma empresa e classificá-los. Os ativos intangíveis são considerados projetos, conhecimento, software, propriedade intelectual e processos. Já os ativos tangíveis são ativos líquidos (em dinheiro ou existências) e ativos fixos (construção e infraestrutura, equipamentos de informática, máquinas, hardware e de produtos e equipamentos de serviço). Aqui são descritos alguns exemplos de ativos de informação (THE NATIONAL ARCHIVES, 2011).

- Um banco de dados de contatos é um exemplo claro de um único ativo de informação. Cada entrada na base de dados não precisa de ser tratada individualmente; o conjunto de dados pode, ser considerado um ativo de informação. Todas as partes de informação dentro do ativo terão os mesmos riscos associados à privacidade e armazenamento de informações pessoais.
- Todos os arquivos associados a um projeto específico pode ser considerado como um único ativo de informação. Isso pode incluir planilhas, documentos, imagens, e-mails de e para a equipe do projeto e qualquer outra forma de registros. Todos os itens

individuais podem ser reunidos e tratados da mesma forma que eles têm conteúdo semelhante definível, e o mesmo valor, o risco do negócio e ciclo de vida.

- Dependendo do tamanho da organização, pode ser capaz de tratar todo o conteúdo do documento e registros de sistema de gerenciamento eletrônico como um único ativo - mas isso poderia ser um risco como um bem tão grande contendo diversos tipos de conteúdo é susceptível de ser difícil de gerenciar
- Todos os dados financeiros de uma organização podem ser considerado um único ativo. Há riscos muito específicos para o negócio se essa informação for mal administrada, e você também pode ter a obrigação de assegurar a transparência das informações, o que pode ser problemático.

Ameaça é qualquer circunstância ou evento com o potencial para explorar intencionalmente ou não uma vulnerabilidade específica em um sistema de informação, resultando em uma perda de confidencialidade, integridade ou disponibilidade, que pode resultar em dano para um sistema ou organização (SECURITY, 2009).

As ameaças que atuam sobre os ativos são classificadas como: ameaças físicas (normalmente decorrentes de fenômenos naturais), tecnológicas (normalmente são ataques propositados causados por agentes humanos como hackers, invasores, criadores e disseminadores de vírus, mas também por defeitos técnicos, falhas de hardware e software) e humanas (são consideradas as mais perigosas, podendo ser casos de roubos e fraudes causados por ladrões e espiões) (LEITNER *et al.*, 2009).

Já vulnerabilidade se refere a ausência de um mecanismo de proteção, uma falha ou fraqueza com a concepção ou implementação de um sistema de informação (incluindo os procedimentos de segurança e controles de segurança associados com o sistema). Essa falha pode ser causada intencionalmente ou não, através de uma perda de confidencialidade, integridade ou disponibilidade para prejudicar o funcionamento de uma organização (incluindo missões, funções e confiança do público na organização) ou os ativos de uma organização ou indivíduos (incluindo a privacidade) (NIST, 2003, 9), (Ramos *et al.*, 2008).

Discute-se risco como a combinação da probabilidade de um evento e de suas consequências (ABNT ISO/IEC Guia 73:2005). Além disso, o Instituto Nacional de Padrões e Tecnologia (NIST, 2003, p 7) define risco como "... uma combinação de: (i) a probabilidade de que uma vulnerabilidade especial em um sistema de informação agência será intencionalmente ou não explorado por uma ameaça específica resultando em uma perda de confidencialidade, integridade ou disponibilidade, e (ii) o impacto potencial ou magnitude do dano que a perda de

confidencialidade, integridade, disponibilidade”. Os riscos são frequentemente caracterizados qualitativamente por meio de valores como: alto, médio ou baixo (NIST, 2003, p 8).

Impacto se refere ao tamanho do prejuízo, medido através de propriedade mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará. Diferentes ameaças possuem impactos diferentes (Ramos *et al.*, 2008).

3.2. Gestão de Riscos de Segurança da Informação

Vários autores discutem definições de gestão de risco, sendo uma delas definida pela Norma ISO / IEC 31000: 2009 sendo o conjunto de atividades e métodos aplicados em uma organização para gerenciar os vários riscos que podem afetar a realização de objetivos de negócio (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2009). Já Thompson *et al.* (THOMPSON *et al.*, 2005) classificam risco como sendo uma estimativa de incerteza e consequências relacionadas à ocorrência de um evento desejável ou indesejável. Assim, o principal objetivo do Gerenciamento de Riscos de Segurança da Informação (GRSI) é maximizar o lucro a longo prazo e gerir de forma otimizada riscos apresentados por falhas potenciais, incentivos conflitantes e adversários ativos.

O gerenciamento de riscos é uma atividade que conduz a avaliação, mitigação e monitoramento dos riscos, buscando a aplicação coordenada de meios financeiros para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos (ABNT NBR ISO/IEC 27005, 2008; DIVISION, 2011). Do mesmo modo, auxilia a responder as perguntas, por exemplo, como a compra de novas tecnologias irá reduzir a probabilidade de chances de riscos para um determinado ativo; além de priorizar riscos. Além disso, visa identificar e priorizar questões para que a organização saiba quais questões são mais críticas para resolver e alocar os recursos disponíveis para a área mais crítica em primeiro lugar. Dessa forma, acredita-se que o gerenciamento de riscos seja de extrema utilidade, pois não há necessidade da organização realizar todo o processo de gestão de riscos de segurança instantaneamente e simultaneamente, podendo apenas aplicar partes desse processo (KHIDZIR *et al.*, 2010).

Avaliação de risco é o processo geral de análise de risco e avaliação de risco (KOTULIC; CLARK, 2004). A análise de riscos é o uso sistemático de informações para identificar as fontes para estimar o risco. Avaliação de riscos é o processo de comparar o risco estimado com base

em critérios de risco previstos para determinar a importância do risco (KOTULIC; CLARK, 2004).

É preciso também compreender que cada novo controle introduzido para tratar um risco específico produz um risco residual e pode introduzir surgimento ou desaparecimento de novos riscos. Diante desse cenário complexo para a segurança, mais especificamente, a gestão da segurança organizacional, pelo menos três atividades podem ser identificadas e executadas nesta ordem (INÁCIO *et al.*, 2011):

- Levantamento do perfil de riscos de segurança da organização;
- Adoção de controles de segurança compatíveis com o perfil de riscos da organização;
- Reavaliação.

Quando o foco do processo de gerenciamento de riscos é a segurança da informação, chama-se GRSI. Neste caso, um elemento indispensável é o ativo de informação de uma empresa. Um estudo feito pela empresa Kaspersky, em 2012, entrevistou 3300 organizações em 22 países, incluindo o Brasil. O resultado do estudo traz a informação de que, para 42% dos entrevistados, a importância dos problemas com crimes virtuais, como roubo de dados, exposição de dados importantes, entre outros, deve aumentar nos próximos anos. Se a estimativa estiver correta, existirão ainda mais problemas e, como consequência disto, poderão ocorrer eventos que afetarão a integridade, disponibilidade e confiabilidade dos ativos organizacionais (QUADRANT; PLATFORMS, 2012).

Para o gerenciamento de risco de segurança da informação foram criadas várias normas para gerenciar os problemas relacionados à segurança de ativos, por exemplo: STONEBUMER *et al.* (2002), CHEN (2009), Standards Australia and Standards New Zealand (2004), MEULBROEK (2002), INTERNATIONAL (2003), BS (2006).

Já outros métodos, como a NIST 800-39, estabelecem metodologias que centralizam o gerenciamento em torno do patrimônio (WANGEN, 2014). A norma AS / NZS 4360 (STANDARD, 2004) fornece às organizações um processo básico de gestão de risco de segurança da informação, o qual facilita sua aplicabilidade, porém esse gerenciamento não se aplica a ambientes mais complexos, nos quais pode ser necessários o apoio de outras normas (SHEDDEN; RUIGHAVER, 2006). Dentre tais normas, podemos destacar a ISO/IEC 27005 (2008) pertencente a série de normas da ISO/IEC 27000.

ISO / IEC 27005 (2008) é um padrão especializado para GRSI e define o processo formal de gerenciamento de riscos como um processo iterativo de análise e monitoramento de riscos, tais como: definição de contexto, avaliação de riscos, comunicação e tratamento para obter a

aceitação do risco (ABNT NBR ISO/IEC 27005, 2008). Os riscos para os sistemas de informação são geralmente analisados por meio de uma análise probabilística (ABNT NBR ISO/IEC 27005, 2008; STONEBUMER *et al.*, 2002), na qual o impacto para a organização (por exemplo, perda se um risco ocorreu) e a probabilidade de ocorrência do risco são calculados. Assim, avaliação de risco utiliza os resultados da análise, e se o risco for considerado inaceitável, os tratamentos de risco são implementadas, as quais consistem na escolha de uma estratégia e medidas para controlar eventos indesejáveis.

2.2.1 Contexto de implantação para GRSI

O contexto de implantação, segundo a ISO / IEC 27005 (ABNT NBR ISO/IEC 27005, 2008), define os parâmetros internos e externos que devem ser considerados na gestão de riscos. O contexto interno para GRSI geralmente será um produto de diversos fatores, tais como: sistemas de TI, *stakeholders*, governança, relações contratuais, cultura, capacidades, objetivos de negócios. Exemplos de fatores externos relevantes para o estabelecimento contexto são: partes interessadas, ambiente externo, leis e regulamentos, e outros fatores que podem afetar os objetivos das organizações.

A especificação NIST para a identificação de ativos (WUNDER; WALTERMIRE, 2011) define três principais classes de ativos para o sistema de informações relacionadas; (i) pessoas, (ii) a organização e (iii) tecnologia da informação. Além disso, fornece nove subclasses de ativos de tecnologia da informação. Em contraste, ISO / IEC 27005: 2011 usa duas classes de ativos primários, que são: (i) processos de empresas e atividades e (ii) informações, com o apoio de ativos: (i) de hardware, (ii) de software, (iii) de rede, (iv) de pessoas, (v) do site e (vi) estrutura da organização.

3.3. NORMA ISO/IEC 27005:2011

As recomendações descritas na norma ISO/IEC 27005 podem ser aplicadas em organizações como um todo, ou em partes, como os processos de um departamento, uma aplicação ou infraestrutura de TI (BECKERS *et al.*, 2011). Em geral, a ISO/IEC 27005 (2008) define o processo de gestão de risco em termos de atividades coordenadas para dirigir e controlar

o risco de uma organização. Não é necessário seguir todas as etapas do método: quem vai implementá-la irá aplicar o que é mais adequado para o seu estudo de caso. Este é um padrão que, quando aplicada, permite-nos seguir um processo em conformidade com a ISO / IEC 27001:2005.

Esta norma tem por objetivo fornecer “diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001. Entretanto, esta norma não inclui uma metodologia específica para a gestão de riscos de segurança da informação.” (ABNT, 2008, p.vi).

Na Figura 2 podem ser visualizadas as etapas do processo de gestão de risco de segurança da informação. A primeira etapa deste processo é a definição do contexto, contendo a política de segurança da informação registrando e explicitando as informações que devem ser consideradas para a definição do contexto da gestão de risco.

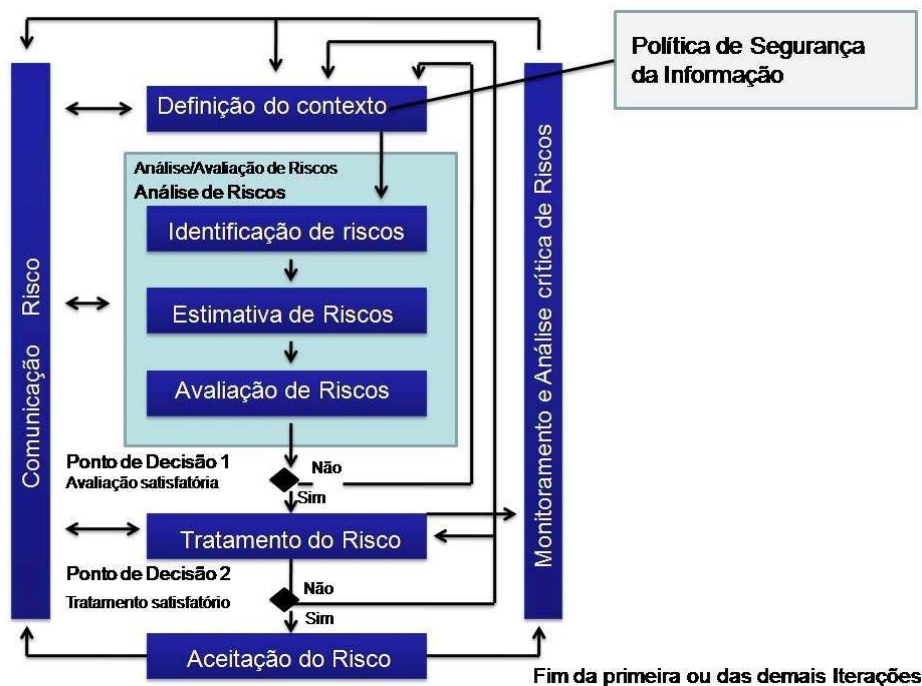


Figura 2- Processo de Gestão de riscos de segurança da informação Fonte: NBR ISO/IEC 27005:2008.

O capítulo 7 da norma contém a definição de contexto, que é essencial, porque nos permitirá definir o ponto de vista da avaliação do risco através da consideração dos riscos associados. O contexto também estabelece uma série de critérios básicos, escopo e limites e as responsabilidades para o processo de gestão de riscos, as quais serão utilizadas como base para a avaliação de risco.

Em seguida, aborda-se o capítulo 8 da norma, o qual refere-se a análise/avaliação de risco, descrevendo e detalhando todo o processo. Dessa forma, ressalta-se que na análise/avaliação de risco existem três etapas que são: identificação de risco, estimativa de risco e avaliação de riscos.

A identificação de riscos constitui na primeira atividade do processo da análise/avaliação de risco, com o objetivo de identificar os eventos que podem impactar negativamente na organização. Já a segunda etapa denominada estimativa de riscos é constituída por metodologias qualitativas ou quantitativas que visam atribuir o valor ao impacto que um risco pode ter e a probabilidade de sua ocorrência. Dessa forma, a estimativa de um risco é realizada através da combinação entre a probabilidade de incidência do risco e suas consequências, assim como descrito na ISO/27005 (ABNT NBR ISO/IEC 27005, 2008).

Por último, a terceira etapa denominada de avaliação de risco é responsável por ordenar os riscos por prioridade comparando o nível estimado do risco e o nível aceitável estabelecido pela organização. A avaliação pode ser considerada satisfatória se estiver de acordo com os critérios propostos pela organização ou revisada de forma mais profunda e detalhada para que os riscos possam ser avaliados de forma satisfatória.

Após a análise/avaliação de risco, no capítulo 9 é apresentado o tratamento do risco de segurança da informação, o qual consiste em implementar controles para reduzir, reter, evitar ou transferir os riscos. Se o tratamento do risco não for satisfatório, ou seja, não resultar em um

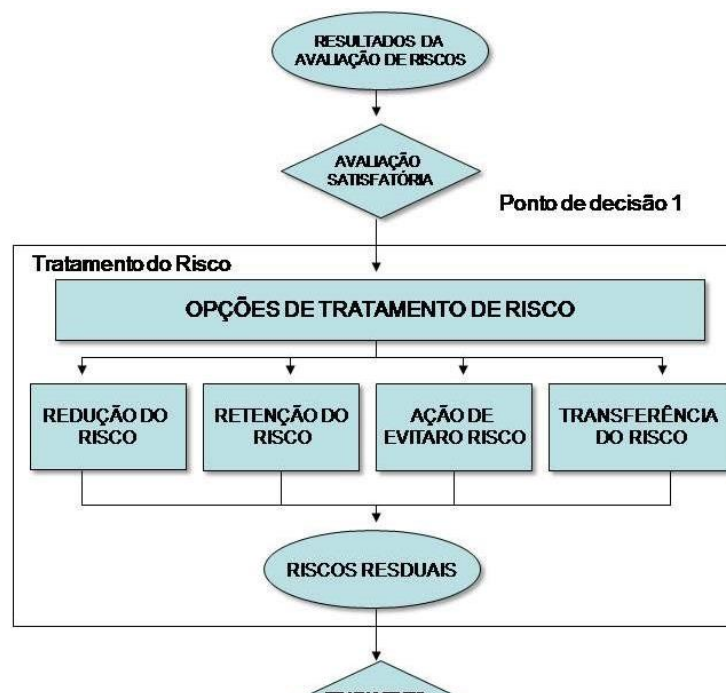


Figura 3- Processo de tratamento do risco - Fonte: NBR ISO/IEC 27005:2008

nível de risco residual que seja aceitável, deve-se iniciar novamente a atividade ou o processo até que

os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esse processo é dividido em: redução do risco, retenção do risco, ação de evitar o risco e a transferência do risco.

Para melhor compreensão do tratamento do risco de segurança da informação, na Figura 3 é apresentado o processo de tratamento do risco. O tratamento de risco pode ser feito tomando quatro decisões: buscar reduzir o risco, evitar o risco, transferir o risco para outro elemento ou organização ou aceitar e reter o risco. Para qualquer uma destas quatro decisões sempre haverá o risco residual.

Após o processo de tratamento do risco, o capítulo 10 refere-se sobre a aceitação do risco de segurança da informação, a qual tem como responsabilidade registrar formalmente a aprovação de planos de tratamento do risco. Para isso, os riscos que serão aceitos e os riscos residuais resultantes devem ser definidos, pois os critérios de aceitação podem ser complexos e envolver estratégias de negócios da organização.

Já no capítulo 11 é apresentado a Comunicação do risco de segurança da informação, a qual refere-se a transmissão de informações referentes aos riscos a todas as partes interessadas, com o objetivo de assegurar que os membros da equipe de um projeto tenham conhecimento sobre os riscos e controles a serem adotados. É necessário determinar as responsabilidades para a comunicação do risco de segurança da informação entre as partes interessadas e envolvidas no SGSI.

Por fim, o capítulo 12 aborda o monitoramento e análise crítica de riscos de segurança da informação, o qual consiste em descrever as responsabilidades e principais atividades de monitoramento de riscos de segurança da informação, para que assim, possa identificar o mais rapidamente possível eventuais mudanças no contexto da organização e garantir uma visão geral e verdadeira dos riscos.

3.4. Argumentação

Neste trabalho, tarefas colaborativas do gerenciamento de riscos são modeladas como um processo de “argumentação” (MOULIN *et al.*, 2002). Argumentação envolve o estudo da concordância e discordância de diálogos e da escrita por meio da qual se apresenta pontos de

vistas aos participantes do diálogo e tem como princípio o ato de usar argumentos para explicar ou justificar um ponto de vista (GROARKE, 2012). Assim, os argumentos são declarações que podem ou não ser verdadeiras em um ponto da discussão, visto que essas declarações devem considerar o auxílio (ou apoio) ou o questionamento (ou contra-argumento) de outros argumentos (MOULIN *et al.*, 2002).

Toulmin (2003) afirma que argumentação é o processo pelo qual afirmações são realizadas e conclusões são inferidas. Podendo assim, estruturar formas de justificar estas conclusões com base em dados, fatos e evidências. Portanto, a argumentação envolve o estudo de acordos e diferenças em um diálogo, no qual os participantes apresentam o seu ponto de vista (AMGOUD; CAYROL, 2002; ANDONE, 2005; DUNG, 1995; MCBURNEY; PARSONS, 2009a)

Neste contexto, é importante ressaltar que técnicas de argumentação buscam capturar e modelar o processo de proposição e análise de argumentos, os quais podem justificar (ou refutar/derrubar) pontos de vista apresentados por participantes de debates. Entre outros objetivos, técnicas de argumentação em ciência da computação buscam permitir a construção de programas capazes de capturar e computar dados e conhecimento oriundos de processos de diálogo, tal como se tais discussões fossem realizadas por agentes computacionais ou seres humanos.

Um dos primeiros estudos da teoria da argumentação foi discutido na teoria de Aristóteles (NOROOZI *et al.*, 2012). Esta teoria de argumentação assume que todo conhecimento, percepções e opiniões que são levantados em um pensamento racional são baseados em conhecimentos, percepções e opiniões já existentes. Visando à análise de argumentações “reais” e em linguagem natural, Toulmin (1958) propôs um modelo de argumentação tomado como uma alternativa à interpretação tradicional da lógica formal. Entretanto, o modelo de Toulmin ocorre entre um argumentador e uma audiência real ou imaginária, em que o argumentador tenta persuadir ou convencer outros de uma afirmação ou proposição em que ele acredita.

A partir do desenvolvimento do estudo sobre argumentação, a Inteligência Artificial faz uso da argumentação principalmente para projetar mecanismos de raciocínio para sistemas multiagente sob incerteza, utilizando as seguintes características: definição de componentes de argumento e de sua interação, a identificação de regras que descrevem processos de argumentação e uso de semântica para identificar sistemas legítimos, fazer argumentação particularmente adequado para projetar mecanismos de raciocínio para sistemas multiagentes (BENCHCAPON; DUNNE, 2007). Além disso, pode representar diálogos entre diversos agentes modelando a troca de argumentos em, por exemplo, a negociação entre os agentes (AMGOUD *et al.*, 2000).

Durante um debate, os argumentos trocados e suas interações podem construir o diálogo. Um agente pode debater e ter como meta a inclusão ou remoção de argumentos e até mesmo fazer críticas. Em um debate, a inclusão de um argumento simplesmente equivale a uma expressão. A remoção de um argumento (SAINT-CYR, 2012) (BISQUERT *et al.*, 2013), pode ser devido a uma objeção ou pode vir da rejeição de uma determinada afirmação não reconhecido como um argumento adequado. A inclusão de ataque pode vir a partir da descoberta de que dois argumentos já enunciados que estão em conflitos.

Em processos colaborativos de tomada de decisões, os participantes contribuem apresentando considerações e evidências de diferentes pontos de vista. Geralmente, o objetivo é desenvolver um conhecimento comum relacionado aos problemas ao invés de simplesmente tentar convencer ou mudar as opiniões de outros participantes. Noroozi *et al.* (2012) ressalta que quando há discussões colaborativas o modelo dialético passa a ser mais utilizado pelos participantes.

O modelo dialético de argumentação representa uma estrutura guiada por regras para assegurar que uma conversa possa ser mediada e organizada. Neste modelo, dois ou mais argumentos podem produzir uma discussão racional a qual pode levar a conclusões melhor fundamentadas ou sólidas (WALTON *et al.*, 2001). Um dos principais benefícios do modelo dialético é a sua capacidade de fornecer um cenário padronizado para as interações que ocorrem entre participantes envolvidos em discussões colaborativas. No contexto dialético de argumentação, um jogo de diálogo é um formalismo que visa representar conhecimento com o objetivo de identificar e representar passos da interação humana. Estes passos são típicos de debates envolvendo múltiplos agentes, sejam estes humanos ou computacionais.

3.4.1. Jogos de Diálogos

O estudo moderno de sistemas formais de diálogo para a argumentação usando jogos de diálogo começou com Charles Leonard Hamblin na área de lógica filosófica. Dialética é o campo de pesquisa voltada ao estudo dos contextos dialéticos nos quais os argumentos são apresentados (HAMBLIN, 1970). Sistemas dialéticos são modelos normativos de diálogo que consistem em (HAMBLIN, 1970):

1. Um conjunto de movimentos, por exemplo, desafio, afirmação, pergunta;

2. um repositório de compromisso para cada familiarizado;
3. um conjunto de regras que regulam os movimentos de diálogo;
4. um conjunto de regras de autorização que definem o efeito dos movimentos sobre os diálogos autorizados.

Jogos de diálogo focalizam a construção de modelos representando práticas típicas de diálogo, movimentos de discussão válidos, aberturas e fechamento de sentenças e regras de interação entre estes diferentes elementos de representação de conhecimento (SCHEUER *et al.*, 2010). Mcburney e Parsons (2009) referem-se a jogos de diálogo como uma forma de representar os passos típicos da interação humana em um diálogo ou debate que envolve múltiplos agentes.

Segundo Yuan *et al.* (2011), um jogo de diálogo pode ser visto como um conjunto de regras que regulamenta os passos ou movimentos dos participantes em um diálogo. São estas regras que organizam e controlam as discussões através da regulação dos participantes à medida que estes contribuem para o desenvolvimento de diálogos. Além disso, essas regras definem a sequência de movimentos admissíveis pelos agentes durante o diálogo, sendo usadas para validar as interações e guiar o processo de diálogo.

Walton e Krabbe (1995) definem uma tipologia de diálogo abrangente com o intuito de identificar seis modelos formais de diálogo, que são:

- Diálogo de busca de informações;
- Diálogo de inquéritos;
- Diálogo de Persuasão;
- Diálogo de negociação;
- Diálogo de deliberação; e
- Diálogo de erística.

Walton e Krabbe analisam o conceito de compromisso no diálogo (WALTON; KRABBE, 1995) para fornecer ferramentas conceituais para a teoria da argumentação e definir um conjunto de tipos de diálogos. A tipologia Walton e Krabbe tem sido útil para dar uma classificação aos diálogos multiagente de acordo com a finalidade que os agentes buscam alcançar individualmente e coletivamente.

Esta classificação é baseada em três fatores: (1) a informação disponível para os participantes, (2) o objetivo do diálogo em si e (3) as metas individuais dos participantes. A lista fornece uma base sólida para cenários de comunicação em grupo entre agentes. Os sete tipos de diálogo primários são os seguintes (WALTON, 2010):

1. **Diálogo de busca de informação:** um participante procura a resposta para alguma pergunta (s) a partir de outro participante, que esse considera que sabe a resposta. Este é o tipo mais simples de diálogo. Uma busca simples no banco de dados é um exemplo.
2. **Diálogo de Inquérito:** participantes colaboram para responder a alguma pergunta (s) cujas respostas não são conhecidos por qualquer um dos participantes (BLACK; HUNTER, 2009).
3. **Diálogo de Persuasão:** uma das partes tenta convencer outra pessoa a adotar uma crença ou ponto-de-vista para endossar uma declaração que o participante não detêm atualmente. Esses diálogos começam com um participante que defende um partido que apoia uma declaração em especial, e procura convencer o segundo a adotar essa mesma declaração. Exemplos no contexto de sistemas multi-agente pode ser encontrado em Atkinson *et al.* (2004), Bentahar *et al.* (2004), Prakken(2005) e Tolchinsky *et al.*(2011).
4. **Diálogo de Negociação:** os *stakeholders* negociam sobre a divisão de algum recurso escasso, com cada uma das partes individuais com o objetivo de maximizar a sua parte. Exemplos no contexto de sistemas multi-agente pode ser encontrado em MCBURNEY *et al.*, (2003) TOLCHINSKY *et al.*, (2011).
5. **Diálogo de Deliberação:** os participantes colaboram a fim de decidir qual ação ou curso de ação a tomar em alguma situação. Os participantes compartilham a responsabilidade de decidir o curso de ação e conjunto comum de intenções ou uma vontade de discutir racionalmente se eles compartilham intenções. Exemplos no contexto de sistemas multiagente pode ser encontrado em Mcburney *et al.*(2007; tolchinsky *et al.*, (2011).
6. **Diálogo de Descoberta:** os participantes precisam encontrar uma explicação dos fatos, o objetivo é escolher a melhor hipótese. Neste diálogo, os participantes encontram e defendem hipóteses adequadas.
7. **Diálogo de Erística:** os participantes discutem verbalmente com cada um com o objetivo de ganhar a troca, como um substituto para o combate físico.

Na abordagem apresentada nesta dissertação optou-se pelo diálogo de deliberação, pois como a intenção deste estudo é a criação de um protocolo de gerenciamento de risco de segurança de informação com a colaboração entre os agentes, o diálogo de deliberação tem como

princípio a troca de conhecimento e de informações até que os participantes cheguem a um determinado acordo.

Mcburney *et al.*,(2007) refere-se que o Diálogo de Deliberação ocorre quando dois ou mais participantes procuram chegar a um acordo conjuntamente sobre um curso de ação. Assim, em um diálogo típico de deliberação, os agentes apresentam propostas de ação. Se a proposta é aceitável para o público aceita-se o diálogo e move para a próxima proposta. O campo de ação aceitável para um agente pode ser selecionado com base em preferências considerando metas.

Mcburney *et al.*,(2007) ressaltam que esses tipos de diálogo são caracterizadas pela ausência de uma autorização inicial fixada por qualquer participante e a ação escolhida pode ser aceitável para todos os interessados. No entanto, os participantes se propõem a expressar posições individuais sobre o que está sendo discutido, com o objetivo de chegar a uma decisão conjunta sobre uma ação. A principal diferença entre deliberação e persuasão é a perspectiva dos agentes no diálogo, sendo que os agentes envolvidos em deliberações são caracterizados por terem um objetivo comum.

Mcburney (MCBURNEY *et al.*, 2002) apresenta uma lista de características desejáveis para protocolos de comunicação com base em argumentação. Com base nesta lista, os autores avaliam vários protocolos de jogo diálogo usando os seguintes critérios (AMGOUD; PARSONS; MAUDET; DIGNUM; DUNIN-KEPLICZ; VERBRUGGE, 2001; MCBURNEY; PARSONS, 2001b):

1. **Declaração de Diálogo Objetivo:** deve ter um propósito (s) declarado publicamente e aceito por todos os participantes.
2. **A diversidade de propósitos individuais:** deve levar em conta a diversidade de propósitos individuais e permitir aos participantes alcançar seus objetivos individuais.
3. **Inclusão:** deve ser inclusivo e não excluir qualquer agente qualificado potencial.
4. **Transparência:** deve ser transparente expondo regras e estrutura para todos os participantes antes do início do diálogo.
5. **Imparcialidade:** deve ser justo para todos os participantes e tratá-los de forma igual.
6. **Regra-Consistência:** As regras de um sistema de dialética deve ser internamente consistente.
7. **Incentivo de resolução:** O sistema dialético deve facilitar término normal do diálogo e não exclui a ajuda de regras ou locuções para terminar.

- 8. Capacitação de auto-transformação:** O sistema dialético deve capacitar os participantes a mudar as suas preferências e largar compromissos anteriores.
- 9. Sistema Simplicidade:** As locuções e regras de um sistema dialético deve ser tão simples quanto possível.
- 10. Computação Simplicidade:** As locuções e regras de um sistema dialético deve ser tão simples quanto possível para minimizar as demandas computacionais.

3.5. Consistência em Projeto de Software Adaptado para Processo de Colaboração

Esse processo de diálogo organizado por um jogo de diálogo tem um claro contraste com uma discussão colaborativa realizada de forma *ad hoc*, em que os participantes de determinado debate poderão chegar a discussões incoerentes, inconsistentes e muitas vezes incompletas. Desse modo, a adoção de processos sistemáticos torna-se adequada por garantir que determinados passos de debate sejam devidamente seguidos em uma sequência pré-definida garantindo a completude e a consistência dos diálogos.

Uma área que trata de aspectos de consistência é a de processos de negócios e *workflows*. Nesta área vários autores, tais como: (MARJANOVIC, 2000), (LI; FAN; ZHOU, 2003), (JINGFU; BINHENG, 2005); apresentam estudos que propõem garantir a consistência de modelos de processo, pois de acordo com Jingfu and Binheng (2005) e (STANDARD, 2004) um modelo de *workflow* que contém inconsistências pode levar à falha na execução de um processo de negócio.

Em uma adaptação de processo é importante compreender a complexidade associada e suas atividades, porque normalmente um processo possui vários elementos interconectados por relacionamento e qualquer inconsistência desse processo poderá ter impacto negativo sobre a execução do projeto. Sendo assim, a exigência de consistência entre suas atividades, tarefas, papéis e relações não contenham nem um tipo de contradição e com isso sejam coerentes entre si (TWENTE, 1997).

Lucas et al(2009) referem que os problemas de inconsistência geram problemas e acabam prejudicando o desenvolvimento de sistemas desde o início. Além disso, segundo DaLi [2007] e Bao (2008) existem diversos tipos de inconsistência, as quais podem acontecer também durante o processo, diretamente relacionadas com a ordem das atividades ou tarefas. Com isso,

pode-se mostrar o motivo que estudos de verificação de inconsistência envolvendo vários tipos de informação tem sido estudado em várias áreas da engenharia de software.

Codd (1970) ressalta um dos primeiros problemas relacionados com o gerenciamento e manutenção de inconsistência foi na área de banco de dados. Esses problemas de inconsistência encontrados foram causados por redundância de informações, resultante de erros nos projetos desenvolvidos.

A partir dessa discussão sobre os problemas de inconsistência, autores começaram a pesquisar e criar formas para que pudessem prevenir essas falhas e assim manter a execução correta de um processo. De acordo com Bao (2008), para atingir esse objetivo foi necessário estabelecer um conjunto de regras, as quais definem requisitos para que exista um ponto de partida e de finalização das atividades e também identifique uma ordem de atividades a serem executadas, ou seja, uma atividade espera que a outra tenha atingido seu objetivo para que a partir disso possa ser iniciada.

Atkinson *et al.* (2007), Bajec *et al.* (2007) e Hsueh *et al.* (2008) referem que essas regras que previnem os problemas de inconsistência são, normalmente, utilizadas entre os autores da área de pesquisa de processos, os quais na prática determinam um momento específico na definição dos processos de software para realizarem a conferência da consistências desses processos, podendo assim constatar se existem falhas de consistência.

A partir disso, Bajec *et al.* (2007) afirmam que a inconsistência nos processos estão relacionados com a incompletude das suas informações. Nesse sentido, os autores referenciam a importância do uso de um metamodelo para a definição de processos que estabeleça regras mínimas de consistência, por meio de seus atributos e suas associações entre classes.

Existem vários tipos de regras de consistência, por exemplo, existem regras que definem a quantidade mínima e máxima de papéis que devem estar associados a tarefa de um processo. Outras regras que, por sua vez, não podem ser expressas através de um metamodelo, mas sim através de uma linguagem como, por exemplo, a natural, (HSUEH *et al.*, 2008) a qual também referêcia o uso de um metamodelo de processo que permita a definição de regras de validação para cada um de seus elementos.

Nota-se que para a atividade de definição de processos é importante a utilização de regras para evitar os problemas de inconsistência e garantir assim, a consistência de um processo de software, englobando todas as etapas do processo, do início ao fim.

4. PROJETO DE PESQUISA

Visando promover discussões de riscos de segurança da informação de forma organizada e a conseqüente construção de uma memória de gerenciamento de riscos, neste trabalho é proposto uma nova abordagem para o gerenciamento colaborativo de riscos de segurança da informação. Como fundamento, esta abordagem tem sua essência a construção e exploração de um protocolo de comunicação bem definido baseado em jogos de diálogo, o qual é particularmente adaptado para responder necessidades típicas de tarefas de gerenciamento de riscos de segurança da informação. Além desse novo jogo de diálogo, este trabalho discute uma adaptação no sistema de discussões de riscos (RD system), o qual visa controlar as discussões baseadas no protocolo de comunicação garantindo discussões completas que por sua vez registrar estas discussões em uma memória de discussões de riscos.

O foco principal da discussão é a análise, avaliação e o tratamento dos riscos. Essas atividades são executadas no início de cada projeto, na etapa de planejamento. Regras adicionais em discussões colaborativas é uma forma de garantir a organização e coerência dos diálogos (MCBURNEY; PARSONS, 2009b). Isso tende a evitar problemas e perda do controle da ordem em que os argumentos são inseridos na discussão, o que poderia vir a dificultar a compreensão do significado dos argumentos utilizados pelos participantes (SCHEUER et al., 2010), ou seja, um conjunto de regras de combinações é descrito por combinações que expressam a forma como estas locuções podem ser executadas (por exemplo, que locução pode ser usada como resposta a determinadas locuções). Desse modo, a adoção de processos sistemáticos torna-se adequada por garantir que determinados passos de debate sejam devidamente seguidos em uma seqüência pré-definida.

É sabido que decisões tomadas a partir de discussões que não seguem corretamente um protocolo podem chegar a conclusões equivocadas e gerar inconsistências no processo como um todo (MCBURNEY; PARSONS, 2009b). Desta forma, a abordagem proposta visa estabelecer um processo para discussão de riscos de segurança de informação baseado na norma ISO/IEC 27005. O protocolo descreve um conjunto de locuções e regras de interação entre as locuções. Para garantir a consistência e completude do processo são estabelecidas regras de consistência da discussão, visando garantir que todas as etapas da discussão sejam executadas de forma consistente.

4.1. Contextualização da pesquisa

A ideia de pesquisar jogos de diálogo no tratamento de atividades de colaboração que ocorrem entre *stakeholders* de um projeto de segurança de informação é parte de um projeto de pesquisa do Programa de Pós-Graduação em Informática (PPGI) da Universidade Federal de Santa Maria (UFSM). Entre outros objetivos, este projeto visa expandir o estado-da-arte de técnicas de gerenciamento de riscos em Engenharia de Software com a proposição de novas abordagens voltadas a uma melhor comunicação, padronização e reutilização de informações, as quais podem ser capturadas em tarefas de gerenciamento de riscos de segurança da informação.

Nesta pesquisa, a técnica de jogos de diálogo está sendo amplamente explorada visando estruturar e guiar uma discussão de riscos de segurança da informação, de forma que seja criado e armazenado dados e conhecimento obtidos nestes processos colaborativos de gerenciamento de riscos. Para expandir e aprimorar o emprego de técnicas de argumentação na área de gerenciamento de riscos, esta dissertação associa o uso de jogos de diálogo com as atividades descritas na ISO/IEC 27005. Além disso, propõe um conjunto de regras que permite validar se a discussão está completa e consistente. Desta forma, os participantes de uma discussão podem visualizar quais pontos da discussão estão faltando e o que precisa para completá-las.

Em geral, a pesquisa no projeto visa permitir o desenvolvimento sistemático de discussões de gerenciamento de riscos. Além disso, ela permite que tais discussões possam ser registradas de modo organizado em uma memória. Atualmente, o projeto de pesquisa em que esta dissertação está inserida também aborda, o emprego de técnicas de raciocínio baseado em casos como forma de consultar e reusar argumentos apresentados em discussões de riscos passadas.

Além disso, um conjunto de esquemas de argumentação para riscos em projeto de software foi estudado, na qual buscam capturar argumentos do cotidiano encontrados em trocas de diálogos (REED; MACAGNO, 2008; WALTON, 2005).

Por fim, a integração de técnicas de raciocínio baseado em casos no contexto de discussões de gerenciamento de riscos é outro trabalho de pesquisa em desenvolvimento no projeto. Na prática, esta técnica considera as características do projeto atual e compara essas propriedades entre discussões de riscos em projetos novos e discussões realizadas em projetos passados, as quais são armazenadas na memória de gerenciamento de riscos.

4.2. RD System (Risk Discussion System)

O Risk Discussion System (RD System) é um sistema para discussão de riscos que possibilita que os diferentes participantes de um projeto discutam riscos de forma colaborativa. Esse sistema está sendo desenvolvido no contexto do projeto de pesquisa e tem o intuito de expandir as técnicas de gerenciamento de riscos, para que haja uma melhor discussão dos riscos e sua reutilização com base em casos passados.

Esse sistema em sua primeira versão v1.0 teve como objetivo controlar as interações dos participantes em uma discussão de riscos em projetos de software com base nas regras de combinação estipuladas para cada ato de locução existente no protocolo de comunicação (Severo *et al.*, 2013).

Já em sua segunda versão, o sistema foi ampliado permitindo utilizar esquema de argumentação para a adição de recursos voltados para o uso sistemático de tais esquemas em meio a discussões colaborativas de riscos (Pozzebon *et al.*, 2014).

Em seguida, foi gerada a versão 3.0 com a implementação de um módulo CBR permitindo que os usuários recuperassem discussões passadas semelhantes, a partir de características dos projetos, palavras-chave ou sentenças. Essa versão teve como objetivo possibilitar aos usuários buscar discussões e soluções em casos passados que possam ser utilizados nos debates atuais.

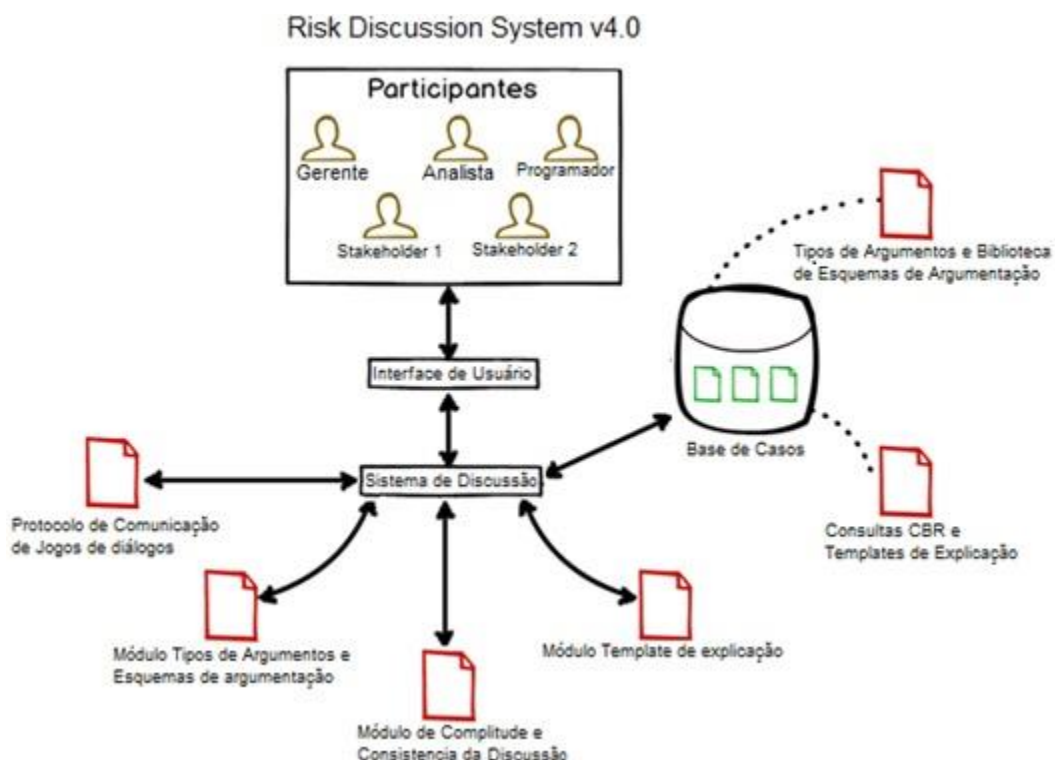


Figura 4 - Fluxo do RD System

Na Figura 4 são exibidos os componentes do RD System v 4.0. Nesta dissertação, foi inserido um módulo no RD System v 4.0 para suprir as necessidades de uma discussão de riscos de segurança da informação. Para isso, foram verificados os passos e processos de gestão de riscos de segurança da informação baseado na norma ISO/IEC 27005.

Para que as regras de consistência possam ser validadas, foi implementado um módulo de verificação, no qual os participantes podem identificar as inconsistências na discussão. Para isso, foi usada a linguagem de programação Java Script, a qual percorre todos os nós da discussão verificando inconsistências baseado nas regras apresentadas na seção 4.1.3.

5. ABORDAGEM COLABORATIVA EM RISCOS DE SEGURANÇA DA INFORMAÇÃO

A exploração de um jogo de diálogo para o desenvolvimento de tarefas de gerenciamento de riscos de segurança da informação permite que participantes discutam de forma colaborativa os riscos inerentes à segurança da informação em projetos de software. Nesse debate, os participantes podem expressar a sua opinião sobre vulnerabilidade, ameaças e riscos envolvendo os ativos. Além disso, podem ser elaborados planos para tratamento de riscos identificados na discussão para que estes possam ser prevenidos, minimizados ou eliminados.

Esse processo de diálogo organizado por um jogo de diálogo tem um claro contraste com uma discussão colaborativa realizada de forma *ad hoc*, na qual os participantes de determinado debate poderão chegar a discussões incoerentes, inconsistentes e muitas vezes incompletas. Desse modo, a adoção de processos sistemáticos torna-se adequada por garantir que determinados passos de debate sejam devidamente seguidos em uma sequência pré-definida. É sabido que decisões tomadas a partir de discussões que não seguem corretamente um protocolo podem chegar a conclusões equivocadas e gerar inconsistências no processo como um todo (MCBURNEY; PARSONS, 2009b). Desta forma, a abordagem proposta visa estabelecer um processo para discussão de riscos de segurança de informação baseado na norma ISO/IEC 27005. O protocolo descreve um conjunto de locuções e regras de interação entre as locuções. Para garantir a consistência e completude do processo são estabelecidas regras de consistência da discussão, visando garantir que todas as etapas da discussão sejam executadas de forma consistente.

Para desenvolver o protocolo de discussão, diversas normas de segurança da informação propostas foram analisadas, tais como: como NIST 800-39 (DIVISION, 2011), AS / NZS 4360(STANDARD, 2004), ISO/IEC 27005. Atualmente, a norma ISO / IEC 27005 é bastante utilizada para implementar sistemas de gestão de segurança da informação pelo fato de fornecer orientações detalhadas sobre a implementação de suas atividades e de como adaptá-las a diferentes tipos de organização (de pequeno a grande porte) (LEITNER *et al.*, 2009).

Para desenvolver um conjunto de atos de locução que pudesse satisfazer os requisitos de tarefas colaborativas em gerenciamento de riscos de segurança da informação, a norma ISO/IEC 27005 foi escolhida por ser um padrão bastante usado e conhecido no mundo todo e também por ser uma versão amadurecida, que passou por diversas atualizações.

Um conjunto muito extenso de locuções pode dificultar o uso do protocolo pelos usuários envolvidos na discussão de riscos de segurança da informação. Em contrapartida, um conjunto muito pequeno de locuções poderá dificultar o entendimento da discussão e o não cumprimento do processo de gerenciamento de riscos de segurança da informação, bem como limitar as possibilidades de expressões das opiniões dos usuários do protocolo.

Em um primeiro momento, foram realizadas análises com base na literatura sobre as etapas comuns nas normas de segurança da informação das organizações, para assim obter um gerenciamento de riscos de segurança da informação. Devido à natureza de discussões colaborativas de riscos, este estudo teve um enfoque em jogos de diálogo voltados para a captura e representação de discussões de deliberações, fazendo com que houvesse um estudo de diferentes jogos de diálogo propostos na literatura. Na prática, a comparação destes diferentes jogos de diálogo permitiu obter um maior entendimento do processo de deliberação, facilitando encontrar e definir um conjunto mínimo de atos de locução capaz de modelar discussões de riscos de segurança da informação desenvolvidas entre participantes de um projeto.

Após finalizar a etapa de conhecimento de jogos de diálogos colaborativos, um protocolo de riscos de segurança da informação baseadas na ISO/IEC 27005 e com ações comuns de deliberação foi elaborado. Este protocolo proposto tem como objetivo organizar um processo de gerenciamento de riscos de segurança da informação de forma colaborativa. Os elementos que compõem o jogo de diálogo proposto neste trabalho são apresentados nas próximas seções desta dissertação.

5.1. Definições do Protocolo

A partir da análise da norma ISO/IEC 27005, atos de locução foram definidos para cada atividade proposta pela ISO. Para cada atividade foi definido um conjunto de locuções que possibilitam aos participantes da discussão executar as atividades previstas pela norma.

Essas atividades são executadas no início de cada projeto, na etapa de planejamento. Para cada atividade descrita na norma ISO/IEC 27005 foi analisada quais locuções seriam necessárias para que a atividade fosse realizada com maior êxito em uma discussão de riscos. Também foram consideradas as entradas e saídas, ações e guias de implementação descritos na ISO/IEC 27005 . Os elementos foram formalizados da seguinte forma:

Definição 1. No protocolo definido neste trabalho e no sistema que o implementa, uma memória de discussões de riscos M consiste de um conjunto de Organizações $Or = \{or_1, or_2, \dots, or_i, \dots, or_n\}$.

Definição 2. Cada Organização or_i consiste de um Contexto onde Ct é um conjunto de contexto da organização $\{ct_1, ct_2, \dots, ct_i, \dots, ct_n\}$.

Definição 3. Cada Contexto consiste de um conjunto de projetos $PR = \{pr_1, pr_2, \dots, pr_i, \dots, pr_n\}$.

Definição 4. Cada projeto pr_i consiste de uma tupla (C, D) no qual C é um conjunto de características do projeto $\{c_1, c_2, \dots, c_i, \dots, c_n\}$ e D é um conjunto de discussões de gerenciamento de riscos $\{d_1, d_2, \dots, d_i, \dots, d_n\}$, realizadas no projeto.

Definição 5. Cada característica c_i do projeto é uma tupla (atributo, valor), onde o conjunto C das características define o contexto no qual o projeto está inserido (por exemplo, características descrevendo o contexto do projeto, o qual descreve se o projeto é realizado através de metodologias planejadas ou ágeis).

Definição 6. Uma discussão d_i é composta por um conjunto de atos de locução no qual será representado por $A = \{a_1, a_2, \dots, a_i, \dots, a_n\}$, os quais auxiliam nas trocas de mensagens durante o fluxo de uma discussão.

Definição 7. Um ato de discussão é composto por uma sentença $s_i \in S$ em conjunto com um operador tal como, por exemplo: informar, perguntar, propor, etc. Estes atos a_i representam diferentes argumentos apresentados em uma discussão por um participante $p_i \in P$.

Definição 8. P é um conjunto de participantes $\{p_1, p_2, \dots, p_i, \dots, p_n\}$ envolvidos na discussão.

Definição 9. Para representar diálogos dos participantes, um conjunto de sentenças representado por $S = \{S_1, S_2, \dots, S_i, \dots, S_n\}$, é o conteúdo apresentado de maneira textual pelos participantes.

Definição 10. O protocolo de gerenciamento de riscos de segurança da informação representado por G_{SM} que por sua vez é composta por uma tupla (L, R, RC) , onde um conjunto de locuções é representado por $L = \{l_1, l_2, \dots, l_i, \dots, l_n\}$, um conjunto de regras de combinação

entre L na qual é representado por $R = \{r_1, r_2, \dots, r_i, \dots, r_n\}$, e um conjunto de regras de consistência entre as locuções que é representado por $RC = \{rc_1, rc_2, \dots, rc_i, \dots, rc_n\}$.

Definição 11. l_i representa uma ação (perguntar, informar, propor, etc) onde os participantes P podem utilizar durante uma discussão d_i . A ordem e em que cada locução pode ser utilizada é definido pelo conjunto R do protocolo.

Definição 12. r_i é definida por uma tupla (l_i, l_j) . Esta tupla é caracterizada por uma locução l_j onde pode ser usada como resposta a um ato de fala apresentado juntamente com uma locução l_i . Através da definição das regras em que as locuções podem ser utilizadas, existe uma garantia de que as locuções obedecerão a um fluxo de diálogo durante a discussão.

Definição 13. RC é definida por L . Uma locução l_j onde deve ser usada como resposta a um ato de fala apresentado juntamente com uma locução l_i para que a discussão possa ter continuidade. Através da definição das regras de consistência em uma discussão, existe uma garantia de que a mesma não tenha fim sem a obrigatoriedade de alguns atos de locução sem resposta.

5.1.1. Conjunto de Locuções do Jogo de Diálogo

Para a construção de um protocolo de gerenciamento colaborativo de riscos de segurança, é necessário descrever as locuções, que podem ser: iniciação, finalização, gerais ou específicas e regras de interação entre locuções. As locuções que determinam o início e o término da discussão são mostradas na Tabela 2. Locuções gerais são aquelas que os participantes usam de forma geral para fomentar a discussão, tais como: perguntar, pedir opinião, argumentar contra, argumentar a favor; assim como apresentado em (SEVERO et al., 2007)(PRAKKEN, 2006). Locuções específicas são relacionadas ao domínio do problema a ser tratado na locução. No caso deste trabalho, o domínio é GRSI e as locuções foram definidas a partir da norma ISO/IEC 27005.

Como o jogo de diálogo foi desenvolvido para representar ações de comunicação entre agentes humanos, as locuções propostas neste protocolo devem ser utilizadas por um participante pi . Portanto, a presença de um participante está implícita nesta descrição de todas as locuções. O conjunto de locuções L está descrito na Tabela 3.

Tabela 2 – Locuções do protocolo de comunicação que determinam o início e término de uma discussão de riscos

Nome: **Iniciar Discussão**

Descrição: Iniciar a discussão com uma afirmação a respeito do assunto a ser abordado no processo de gerenciamento de riscos de segurança da informação.

Exemplo: *Iniciar Discussão*: Discussão do módulo de consulta.

Nome: **Terminar Discussão**

Descrição: Terminar a discussão, não permitindo mais a inserção de novos argumentos no processo de gerenciamento de riscos.

Exemplo: *Terminar Discussão*: Discussão finalizada.

Tabela 3 – Atos de locuções específicos para discussão das tarefas de gerenciamento de riscos de segurança da informação

Nome: **Propor Ativo**

Descrição: possibilita ao participante propor um novo ativo para ser discutido.

Exemplo: *Propor Ativo*: Dados Sigilosos

Nome: **Propor Valor**

Descrição: possibilita ao participante propor um valor para um ativo proposto previamente.

Exemplo: *Propor Valor*: de uma escala de 0 a 10 considero 7.

Nome: **Propor Impacto**

Descrição: possibilita ao participante propor um impacto para um ativo proposto previamente.

Exemplo: *Propor Impacto*: De uma escala de 0 a 10 considero que o impacto deste risco é 8.

Nome: **Propor Probabilidade**

Descrição: possibilita ao participante propor a probabilidade de uma vulnerabilidade proposta previamente.

Exemplo: *Propor Probabilidade*: A probabilidade de ser explorada é baixo.

Nome: **Propor Ameaça**

Descrição: possibilita ao participante propor uma ameaça para uma vulnerabilidade proposta previamente.

Exemplo: *Propor Ameaça*: Saturação do sistema de informação.

Nome: **Propor Vulnerabilidade**

Descrição: possibilita ao participante propor uma vulnerabilidade para um ativo proposto previamente.

Exemplo: *Propor Vulnerabilidade*: Criptografia usada para proteger dados está ultrapassada.

Nome: **Propor Risco**

Descrição: possibilita ao participante propor um risco para um ativo proposto previamente.

Exemplo: *Propor Risco*: Informações confidenciais de clientes.

Nome: **Propor Tratamento**

Descrição: possibilita ao participante propor um tratamento para um risco proposto previamente.

Exemplo: *Propor Tratamento*: Criar criptografias mais avançadas.

Nome: **Propor Consequência**

Descrição: possibilita ao participante propor uma consequência para um ativo proposto previamente.

Exemplo: *Propor Consequência*: Afeta integridade e com isso os dados podem ser divulgados ou modificados causando transtorno e prejuízo.

Nome: **Propor Controle**

Descrição: possibilita ao participante propor controles existentes para um ativo proposto previamente.

Exemplo: *Propor Controle*: é usado padrão de senhas padronizados no ano de 2000.

Em geral, argumentos em uma discussão podem ser contestados de alguma forma, sendo eles uma afirmação ou uma interrogação. Neste contexto, locuções voltadas para a captura e representação de movimentos críticos (investigatórios) de debate foram definidas e são mostradas na Tabela 4.

Tabela 4 – Atos de locuções de propósito geral que visam permitir uma discussão crítica de riscos e seus planos

Nome: **Argumentar a Favor**

Descrição: possibilita ao participante expressar argumento favorável a uma locução proposta previamente.

Exemplo:

Propor Plano: Implementar novas técnicas de criptografia

Argumentar a favor: Concordo, isso irá minimizar as chances de invasão.

Nome: Argumentar Contra

Descrição: possibilita ao participante expressar argumento desfavorável a uma locução proposta previamente.

Exemplo:

Propor Impacto: De uma escala de 0 a 10 considero 8.

Argumentar Contra: O impacto é 5, levando em consideração o contexto onde é discutido.

Nome: Informar

Descrição: possibilita ao participante expressar uma informação a uma locução proposta previamente.

Exemplo: *Informar:* Este tratamento será implementado.

Nome: Perguntar

Descrição: possibilita ao participante questionar sobre uma locução proposta previamente.

Exemplo: *Perguntar:* Este ativo é realmente importante?

Nome: Retirar

Descrição: possibilita ao participante a retirada de uma locução proposta previamente.

Exemplo:

Argumento contra: Esse ativo tem valor baixo.

Argumento contra: Este ativo é importante para a empresa, por isso tem um valor alto

Retirar: Ok.

Nome: Pedir Opinião

Descrição: possibilita ao participante pedir opinião de outros participantes referente a locução proposta previamente.

Exemplo: *Pedir Opinião:* Todos concordam que o impacto do risco é alto?

Nome: Opinar

Descrição: possibilita ao participante expressar opinião em relação a uma locução proposta previamente.

Exemplo: *Pedir Opinião:* Todos concordam que o impacto do risco é alto?

Opinar: Sim.

5.1.2. Processo para Discussão Colaborativa de Riscos de Segurança da Informação

O processo proposto visa estruturar as atividades envolvidas em uma discussão colaborativa de riscos, garantindo que os participantes executem tais atividades em uma sequência pré-definida pelo fluxo do processo. Este processo foi baseado no fluxo de atividades da norma ISO/IEC 27005 e tem como foco as atividades envolvidas no planejamento de riscos inicial, que são: a análise e avaliação de riscos e o tratamento dos riscos identificados. Além do fluxo de execução, foram elaboradas regras que visam garantir a execução de todas as atividades (completude) e restrições e condições sobre as locuções (consistência).

A sequência do processo foi definida a partir dos objetivos da atividade e das entradas e saídas de cada atividade proposta pela ISO/IEC 27005.

Para que o processo seja finalizado, atendendo todos os requisitos da discussão, definiu-se um conjunto de regras que é aplicado para validar a discussão. O processo proposto pode ser visualizado na Figura 5.

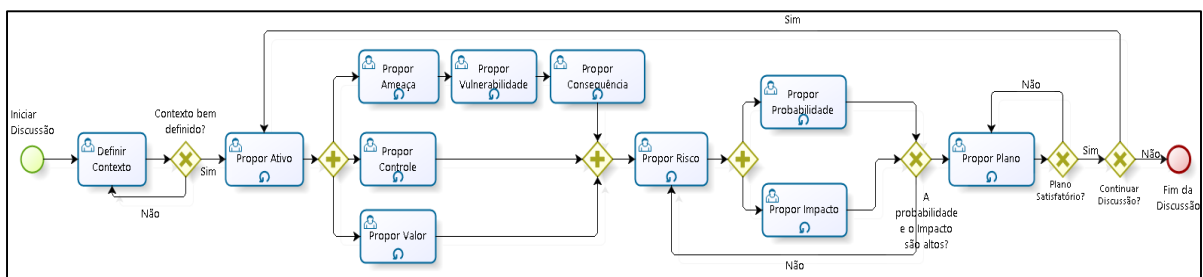


Figura 5 - Processo de discussão de riscos de segurança da informação

5.1.3. Regras de validação da discussão

As regras de combinação descrevem o contexto de cada ato de locução, de forma a organizar o progresso do diálogo. As regras foram classificadas nas seguintes categorias: regras de início, regras de transição, regras internas a etapa e regras de finalização, que são descritas a seguir:

Regra de Início: é a regra que dará início a discussão.

Regra de Transição: valida os requisitos mínimos para passar para a próxima etapa da discussão. Por exemplo, para se propor um risco é necessário ter proposto uma vulnerabilidade, um controle e um valor para o ativo.

Regra Interna a Etapa: verifica se a etapa foi finalizada com todos os requisitos ou somente atingiu o requisito mínimo para continuar a discussão.

Regra de Finalização: valida se a discussão pode ser finalizada, isto é se todas as etapas do processo da discussão foram realizadas com sucesso.

Como exemplo de uma regra interna a etapa, pode-se especificar que é obrigatório utilizar o ato “*informar*” em resposta à locução “*perguntar*”.

Como resultado da aplicação das práticas, é possível identificar atividades não executadas ou inconsistências na execução do processo. Neste caso, os participantes da discussão precisam resolver as inconsistências tornando as discussões completas, evitando transtorno em recuperações de fragmentos de discussões incompletas no futuro. Caso inconsistências identificadas não forem resolvidas, a discussão ficará com status de inconsistente. Para que o processo seja completo, um conjunto de regras estabelecido para serem aplicada em uma discussão foi definido. Para descrever os elementos das regras da discussão, foi utilizado um modelo adaptado do proposto pelo autor (MCBURNEY; PARSONS, 2009) assim criando uma representação na qual possa descrever as regras de transição de etapas. Explicar cada um dos elementos propostos no modelo. Na Tabela 5 podem ser visualizadas as locuções propostas.

Tabela 5 – Fragmento de regras de transição de etapa.

Regra 1. Locução **Iniciar_Discussão(.)**:

Locução: **Iniciar_Discussão**(t, Pi), onde t é a descrição do início da discussão, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter sido realizado um cadastro de Organização (Pi), juntamente com seu contexto.

Significado: Permite ao participante (Pi) dar início a discussão de gestão colaborativa de riscos. Por exemplo: um participante propõe a discussão "Essa discussão tem como objetivo mitigar riscos do Projeto X".

Regra 2. Locução **Finalizar_Discussão(.)**:

Locução: **Finalizar_Discussão**(t, Pi), onde t é a descrição do fim da discussão, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve existir no mínimo a locução *Iniciar_Discussão*(t, Pi) na discussão.

Significado: Permite ao participante(Pi) finalizar a discussão de gestão colaborativa de riscos. Por exemplo: um participante propõe a locução "esta discussão foi finalizada com êxito".

Regra 3. Locução **Propor_Ativo(.)**:

Locução: **Propor_Ativo**(t, Pi), onde t é a descrição do Ativo, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Iniciar_Discussão*(t, Pi) por qualquer participante no âmbito do diálogo.

Resposta: Deve haver a Locução *Pedir_Opinião*(t, Pi) como nó filho de *Propor_Ativo*(t, Pi) por qualquer participante no âmbito do diálogo. Bem como a Locução *Opinar*(t, Pi) como nó filho de *Pedir_Opinião*(t, Pi) pela maioria dos participante no âmbito do diálogo

Validação: A locução *Propor_Ativo*(t, Pi) deverá ter a maioria das opiniões obtidas por meio da locução *Opinar*(t, Pi), tanto positivas quanto negativas. Sendo elas positivas, a proposta de ativo é considerada válida e a discussão pode continuar; caso contrário, a proposta é descartada e o usuário tem que propor um novo Ativo.

Significado: permite a proposição de ativos em um debate de gestão colaborativa de riscos. Por exemplo: um participante da discussão pode propor "Servidor" como um ativo.

Regra 4. Locução **Propor_Valor(.)**:

Locução: **Propor_Valor**(t, Pi), onde t é a descrição do valor do Ativo, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Ativo* (t, Pi), inserida por qualquer participante no âmbito do diálogo.

Resposta: Deve haver a Locução *Pedir_Opinião*(t, Pi) como nó filho de *Propor_Ativo*(t, Pi) por qualquer participante no âmbito do diálogo. Bem como a Locução *Opinar*(t, Pi) como nó filho de *Pedir_Opinião*(t, Pi) pela maioria dos participante no âmbito do diálogo

Validação: A locução *Propor_Valor*(t, Pi) deverá ter no máximo uma proposta válida. Caso houver mais de uma locução *Propor_Valor*(t, Pi) no nó filho da locução *Propor_Ativo*(t, Pi) uma proposta terá que ser descartada.

Significado: permite a proposição de um Valor de importância para o Ativo em um debate gestão colaborativa de riscos. Por exemplo: "de uma escala de 0 a 10 acredito que é 8", que foi proposto por um "Especialista" do projeto.

Regra 5. Locução **Propor Controle(.)**

Locução: **Propor_Control** (t, Pi) , onde t é a descrição dos controles existentes do Ativo, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução $Propor_ativo(t, Pi)$ por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução $Propor_Controle(t, Pi)$ deverá ter no mínimo uma proposta válida. Caso não houver uma locução $Propor_controle(t, Pi)$ no nó filho da locução $Propor_Ativo(t, Pi)$ uma proposta terá que ser apresentada.

Significado: permite a proposição de controles existentes de que é usado para evitar riscos em um debate de gestão colaborativa de riscos. Por exemplo: "é usado *backup* em mais de um servidor", que foi proposto por um "Especialista" do projeto.

Regra 6. Locução **Propor Ameaça(.)**

Locução: **Propor_Ameaça** (t, Pi) , onde t é a descrição do ameaça do Ativo, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução $Propor_Ativo(t, Pi)$ por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução $Propor_Ameaça(t, Pi)$ deverá ter no mínimo uma proposta válida. Caso não houver uma locução $Propor_Ameaça(t, Pi)$ no nó filho da locução $Propor_Ativo(t, Pi)$ uma proposta terá que ser apresentada.

Significado: permite a proposição de Ameaças em um debate gestão colaborativa de riscos. Por exemplo: "Acesso indevido por pessoas não autorizadas", que foi proposto por um "Especialista" do projeto.

Regra 7. Locução **Propor Vulnerabilidade(.)**

Locução: **Propor_Vulnerabilidade**(t, Pi), onde t é a descrição da vulnerabilidade sobre a ameaça, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Ameaça*(t, Pi) proposto por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_Vulnerabilidade*(t, Pi) deverá ter no mínimo uma proposta válida. Caso não houver uma locução *Propor_vulnerabilidade*(t, Pi) no nó filho da locução *Propor_Ameaça*(t, Pi) uma proposta terá que ser apresentada.

Significado: permite a proposição de vulnerabilidade em um debate gestão colaborativa de riscos. Por exemplo: "Criptografia ultrapassada", que foi proposto por um "Especialista" do projeto.

Regra 8. Locução **Propor Consequência**(.)

Locução: **Propor_Consequencia**(t, Pi), onde t é a descrição consequência da vulnerabilidade, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Vulnerabilidade*(t, Pi) por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_consequencia*(t, Pi) deverá ter no mínimo uma proposta válida. Caso não houver uma locução *Propor_consequencia*(t, Pi) no nó filho da locução *Propor_vulnerabilidade*(t, Pi) uma proposta terá que ser apresentada.

Significado: permite a proposição de consequência em um debate gestão colaborativa de riscos. Por exemplo: "Caso for o ataque seja bem sucedido pode haver exposição de dados não autorizados", que foi proposto por um "Especialista" do projeto.

Regra 9. Locução **Propor Risco**(.)

Locução: **Propor_Risco**(t, Pi), onde t é a descrição do risco do Ativo, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Ativo*(t, Pi) com nós filhos contendo as locuções *Propor_Ameaça*(t, Pi), *Propor_Control*(t, Pi), *Propor_valor*(t, Pi) já proposto por Pi .

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_Risco(t,Pi)* deverá ter no mínimo uma proposta válida. Caso não houver uma locução *Propor_Risco(t,Pi)* no nó filho da locução *Propor_Risco(t,Pi)* uma proposta terá que ser apresentada.

Significado: permite a proposição de Riscos em um debate gestão colaborativa de riscos. Por exemplo: "Exposição de dados não autorizados", que foi proposto por um "Especialista" do projeto.

Regra10. Locução **Propor Probabilidade(.)**

Locução: **Propor_Probabilidade(t,Pi)**, onde *t* é a descrição da probabilidade do Risco acontecer sobre o ativo, e *Pi* é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Risco (t,Pi)* por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_Valor(t,Pi)* deverá ter no máximo uma proposta válida. Caso houver mais de uma locução *Propor_Valor(t,Pi)* no nó filho da locução *Propor_Ativo(t,Pi)* uma proposta terá que ser descartada.

Significado: permite a proposição de Probabilidade em um debate gestão colaborativa de riscos. Por exemplo: "de uma escala de 0 a 10 eu acho que a probabilidade de acontecer é 7", que foi proposto por um "Especialista" do projeto.

Regra 11. Locução **Propor Impacto(.)**

Locução: **Propor_Impacto(t,Pi)**, onde *t* é a descrição do impacto do Risco, e *Pi* é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Risco (t,Pi)* finalizada, inserida por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_Impacto (t,Pi)* deverá ter no máximo uma proposta válida. Caso houver mais de uma locução *Propor_Impacto (t,Pi)* como nó filho da locução *Propor_Risco (t,Pi)* uma das propostas terá que ser descartada.

Significado: permite a proposição do impacto causado pelo Risco discutido em um debate de gestão colaborativa de riscos. Por exemplo: um participante propõe que o Risco Acesso não autorizado, e o Impacto em uma escala de 0 a 10, tem um valor 8

Regra 12. Locução **Propor Tratamento(.)**

Locução: **Propor_Tratamento**(t, Pi), onde t é a descrição do Plano para minimização do Risco, e Pi é qualquer participante no âmbito do diálogo.

Precondição: Deve ter a locução *Propor_Risco*(t, Pi) com nós filhos contendo as locuções *Propor_Probabilidade*(t, Pi) e *Propor_Impacto*(t, Pi) por qualquer participante no âmbito do diálogo.

Resposta: Não necessita de locuções como nó filho para que seja válida.

Validação: A locução *Propor_Valor*(t, Pi) deverá ter no máximo uma proposta válida. Caso houver mais de uma locução *Propor_Valor*(t, Pi) no nó filho da locução *Propor_Ativo*(t, Pi) uma proposta terá que ser descartada.

Significado: permite a proposição do impacto causado pelo Risco discutido em um debate de gestão colaborativa de riscos. Por exemplo: um participante propõe que o Risco Acesso não autorizado, e o Impacto em uma escala de 0 a 10, tem um valor 8.

5.1.4. Construção do módulo de validação da discussão

Visando fornecer um sistema para auxiliar no gerenciamento de riscos de segurança da informação, o sistema proposto por SEVERO (2012) foi adaptado. Na versão anterior, a discussão era vinculada a um projeto, na versão atual a discussão é associado a uma organização visando atender os requisitos da ISO/IEC 27005. Para o gerenciamento das regras no processo de discussão, algumas modificações foram realizadas no Risk Discussion system (RD system). Como parte deste trabalho, o módulo desenvolvido tem como objetivo possibilitar que os participantes de um diálogo discutam sobre riscos de segurança da informação e validar a discussão com base no conjunto de regras mostrado anteriormente. Para isso foram desenvolvidas regras na Linguagem JavaScript que realizam a validação conforme as regras descritas na seção 4.1.4 deste trabalho.

A seguir são descritas algumas funcionalidades implementadas em RD System.

Segundo a ISO/IEC 27005, toda organização deve ter um contexto definido, sendo com base nesse contexto que será definido o escopo de limites da discussão. Tendo isso como uma parte importante de informação aos participantes antes da discussão, foi inserido um cadastro de organização (Figura 6), e um cadastro de contexto para organização (Figura 7).

Risk Discussion System Protocols Argument Types Argument Schemes **Organizations** Maicon Balke Logout

Organizartion

Listing organizations

Fantasy Name	Actions
Organization 1	Edit Show Destroy
Organization 2	Edit Show Destroy
Organization 3	Edit Show Destroy
Organization 4	Edit Show Destroy

[+ New Organization](#)

Figura 6 - Modulo de cadastro de Organização

Risk Discussion System Protocols Argument Types Argument Schemes **Organizations** Maicon Balke Logout

Organizartion

Listing Context

Context	Actions
Context 1	Edit Show Destroy
Context 2	Edit Show Destroy
Context 3	Edit Show Destroy
Context 4	Edit Show Destroy

[+ New Context](#)

Figura 7 - Modulo de cadastro de contexto onde será feita a discussão

Na Figura 9 pode ser visualizado o módulo de verificação de inconsistências. Este possibilita aos participantes verificar se a discussão seguiu todos os passos com base nas regras criadas descrita na seção anterior.

The screenshot displays the 'Risk Discussion System' interface. At the top, there is a navigation bar with tabs for 'Protocols', 'Argument Types', 'Argument Schemes', and 'Organizations'. The user 'Macon Balke' is logged in. Below the navigation, there are tabs for 'Discussion', 'CBR', 'Project Important Characteristics', and 'Project Attributes'. The main content area shows a discussion thread with several posts, each with a status icon (plus, exclamation mark, or X) and a title. The posts include:

- [1259] Iniciar Discussão: Start the discussion of information security risks in order to prevent information theft - Maicon Balke
- [1260] Propor Ativo: Confidential customer information
- [1261] Propor Valor: on a scale from 0 to 10 believe it is 8
- [1262] Informar: in view of the customers' integrity being affected by exposure data
- [1263] Propor Controle: Has neither an applied control to minimize attacks yet
- [1264] Propor Impacto: on a scale from 0 to 10 believe it is 3
- [1265] Argumentar Contra: I believe that for an asset that can affect the integrity of customers, the impact should be between 6-8
- [1266] Retirar: okay - Maicon Balke
- [1267] Propor Impacto: on scale from 0 to 10 believe it is 7
- [1268] Propor Ameaça: impairment of information
- [1269] Propor Vulnerabilidade: Software widely distributed with outdated encryption technology - Maicon Balke
- [1270] Propor Consequência: This data can leak and affect the integrity of organizations, as well as data that undertake monetary values
- [1271] Propor Risco: Make Public Confidential customer information

 On the right side, there is a 'Feed' section with a list of actions:

- [1285] Finalizar Discussão: discussion finalized
- [1284] Opinar: Yes
- [1283] Opinar: Yes
- [1282] Opinar: Yes
- [1281] Pedir Opinião: All agree with this treatment
- [1280] Opinar: Yes
- [1279] Opinar: Yes
- [1278] Opinar: Yes
- [1277] Pedir Opinião: All agree with this active
- [1276] Retirar: Retirado
- [1275] Propor Tratamento: Using Symmetric Encryption AES algorithm

 Below the feed, there are sections for 'Free Text' and 'Argument Scheme'. At the bottom right, there are two buttons: 'Validacao' and 'Limpar'.

Figura 8 - Modulo da discussão com o modulo de validação das regras

6. RESULTADOS E DISCUSSÕES

Com o intuito de validar a aplicabilidade da abordagem e do sistema propostos neste trabalho, foram realizados experimentos envolvendo profissionais de computação da área de desenvolvimento de software e um estudo de caso. O estudo de caso descreve um cenário fictício de gerenciamento de risco em segurança da informação e uma discussão de riscos realizada considerando esse cenário. Esse estudo de caso tem como objetivo ilustrar o uso da abordagem proposta. Os experimentos foram realizados através da apresentação do tema gerenciamento de riscos de segurança da informação e da aplicação de questionários aos participantes, contendo questões de múltipla escolha, organizadas usando a escala Likert: concordo plenamente; concordo parcialmente; não concordo nem discordo; discordo parcialmente; e discordo plenamente. Tais experimentos tiveram configuração e objetivos específicos, conforme apresentado nas seções seguintes, onde cada experimento é descrito em detalhes, bem como os resultados dos questionários respondidos pelos participantes e as conclusões alcançadas a partir da análise destes resultados.

6.1. Estudo de Caso

Um estudo de caso foi realizado com a intenção de validar o trabalho proposto. Primeiramente, é descrito o cenário de segurança de informação fictício e, posteriormente, os resultados do estudo de caso.

Cenário

Uma organização busca contribuir com a segurança dos dados de clientes por meio de soluções de segurança em um banco de dados. Para garantir a integridade de dados hospedados, a organização tem de ser capaz de oferecer os serviços de segurança esperados. Esta organização possui representantes espalhados por todo o território nacional.

A missão da organização envolve atividades de servidor de dados. Neste contexto, ela visa proteger a informação de diversos tipos de ameaça para garantir a continuidade dos negócios, minimizando os danos causados por acessos indevidos a informações e maximizando o retorno dos investimentos aplicados em segurança de dados e as oportunidades de negócio. Dentre as

competências relacionadas à segurança da informação desta organização, algumas podem ser citadas:

- A garantia de que a informação está acessível somente a pessoas com acesso autorizado;
- A salvaguarda da exatidão e completude da informação e dos métodos de processamento;
- A garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;
- A garantia de que padrões são verificados e validados;
- Cumprimento de diretrizes e procedimentos operacionais necessários para garantir a segurança da informação.

Problema:

As ameaças, cada vez mais especializadas e inovadoras, superam as estratégias de proteção estabelecidas na organização. Neste caso, esta organização ainda não consegue acompanhar a evolução constante de invasores. Assim, ela sofre com os custos monetários oriundos de incidentes. Portanto, é possível perceber que a organização ainda precisa se dedicar mais a definição e implantação de métodos de proteção. Por exemplo, a detecção de invasores não é efetiva e ainda há um grande desconhecimento deste serviço por parte da empresa. Baseado neste cenário, uma discussão de riscos de segurança é realizada com pessoas ligadas à segurança da informação da organização. Portanto, os participantes da discussão são membros da equipe ou partes interessadas do projeto. Sendo assim, diferentes experiências podem ser capturadas e exploradas na discussão, proporcionando uma chance maior de sucesso em aplicar tratamentos para proteger os ativos.

Definição do Contexto

O contexto deste problema é cadastrado no RD System, onde os gestores identificam requisitos funcionais e o contexto do projeto que está sendo discutido. Estes requisitos podem ser derivados dos objetivos de nível mais alto do sistema. Este cadastro é feito pelo gerente de projeto a fim de disponibilizar todas as informações possíveis aos demais participantes da discussão.

Na Figura 9 é mostrado um fragmento de discussão, elaborado no RD System. Na Figura pode-se visualizar algumas inconsistências e partes incompletas na discussão. Neste caso, a validação desta discussão inicia quando qualquer usuário da discussão seleciona o botão

“verificar”. A partir daí, a discussão é validada com base no conjunto de regras de validação pré-estabelecido.

Na Figura 9 é mostrado um fragmento da discussão sobre riscos de segurança da informação para o estudo de caso. Neste fragmento existem algumas inconsistências que são comuns em discussão que são encerradas sem que as mesmas sejam verificadas, gerando problemas de para consultas futuras.

Algumas regras propostas por esse trabalho foram aplicadas e são explicadas a seguir.

The screenshot displays a discussion thread with the following messages and annotations:

- Message 1:** [1260] Propor Ativo: Informações confidenciais de clientes - Usuário 1. Para que o ativo seja válido, é necessário a aprovação da maioria dos participantes. (Annotated with '1')
- Message 2:** [1272] Propor Impacto: Em uma escala de 0 a 10 acredito que é 8 - Gerente. (Annotated with '2')
- Message 3:** [1275] Propor Tratamento: Usar um algoritmo simétrico de criptografia RC6 que atenda aos requisitos da AES com chaves de 128, 192 ou 256 bits é o suficiente para este projeto - Usuário 1. Para que o tratamento seja válido, é necessário a aprovação da maioria dos participantes. (Annotated with '3')
- Message 1a:** [1277] Pedir Opinião: Todos concordam com este Ativo? - Gerente. (Annotated with '1a')
- Message 2a:** [1264] Propor Impacto: Em uma escala de 0 a 10 acredito que é 3 - Usuário 2. (Annotated with '2a')
- Message 2b:** [1273] Propor Impacto: Em uma escala de 0 a 10 acredito que é 6 - Usuário 2. (Annotated with '2b')
- Message 3a:** [1284] Opinar: Sim - Usuário 2. (Annotated with '3a')

Figura 9 - fragmento de uma discussão inconsistente juntamente com as correções

Regra 1: Validação de Ativo

- **Tipo:** completude
- **Objetivo:** determina que para um ativo ser considerado válido na discussão, a maioria dos participantes deve concordar com a proposição do ativo, ou seja, que o ativo é adequado ao contexto do projeto para o qual está sendo feito a discussão.
- **Descrição da regra:** quando a locução *Propor Ativo* é encontrada pelo algoritmo de validação, é executada a regra 3 descrita na sessão 4.1.4/Tabela 5 para validação. Essa regra determina que, após a proposição de um valor para o ativo, a maioria dos participantes deve opinar por meio da locução *Pedir Opinião* para que o valor do ativo seja considerado válido. No caso desta discussão, não foi utilizada a locução *Pedir Opinião*. Porém, o gerente pode usar a locução *Pedir Opinião* como nó filho de *Propor Ativo* como mostra o fragmento 1a da Figura 9. Assim, os participantes poderão opinar se o ativo é ou não válido. A partir disso, o algoritmo detecta quantas locuções *Opinar* existe na discussão e então verifica se a maioria dos participantes

opinou a favor ou contra. Caso a maioria dos participantes opinou contra, o algoritmo invalida o Ativo proposto (como mostrado na Figura 9 – fragmento 1) e então terá que ser proposto um novo Ativo para a discussão.

Regra 2: Duplicidade de Locuções

- **Tipo:** Consistência
- **Objetivo:** tem como objetivo validar se uma locução filho aparece mais de uma vez para uma mesma locução pai, enquanto só deveria ser permitida uma única locução.
- **Descrição da Regra:** algumas locuções como propor impacto, propor probabilidade devem aparecer uma única vez para cada ativo identificado. Quando mais de uma locução deste tipo aparece, a discussão fica inconsistente, pois não é possível identificar quais dos valores propostos é o valor válido para o ativo. Para tratar desta inconsistência, o responsável poderá escolher um das locuções propostas como válida, ou poderá fomentar a discussão para que todos os participantes cheguem a um consenso e retirar manualmente o impacto(s) inválido(s). Quando a locução *Propor Impacto* é encontrada pelo algoritmo de validação, é executada a regra 11 descrita na sessão 4.1.4/Tabela 5 para validação. Essa regra determina que não pode haver mais de um impacto proposto para o mesmo risco. No caso dessa discussão, existe mais de um impacto proposto como mostrado na Figura 9 – fragmento 2. Quando o algoritmo de validação detecta essa inconsistência, o sistema exibe um formulário (como exibido na Figura 10 – fragmento 2a), questionando qual das locuções *Propor Impacto* deve ser considerada. Assim, o gerente escolhe o impacto válido e o outro retirado automaticamente pelo sistema incluindo a locução *Retirar* como mostrado na Figura 9 - fragmento 2b, ou pode cancelar o recurso e fomentar a discussão para que as pessoas envolvidas discutam até chegar a uma conclusão e efetuem a operação de retirar o impacto inválido manualmente.

Regra 3: Validação Propor Tratamento

- **Tipo:** completude
- **Objetivo:** determina que para que um plano de tratamento seja considerado válido é necessário que a maioria dos participantes concorde com o plano proposto, caso contrário o plano de tratamento deve ser retirado e terá que ser proposto outro novamente.

- **Descrição da Regra:** quando a locução *Propor Tratamento* é encontrada pelo algoritmo de validação, é executada a regra 12 descrita na sessão 4.1.4/Tabela 5 para validação. Essa regra determina que, após a proposição de um tratamento para o risco, a maioria dos participantes deve opinar por meio da locução *Pedir Opinião*, para que o tratamento de minimização ou mitigação do risco seja válido. No caso desta discussão, a locução pedir opinião não foi utilizada, porém o gerente pode, usando a locução pedir opinião como nó filho de *Propor Tratamento*, pedir a opinião dos demais participantes da discussão como mostrado na Figura 9 – fragmento 3a. A partir disso, o algoritmo detecta quantas locuções *Opinar* existe na discussão e então verifica se a maioria dos participantes opinou a favor ou contra. Caso a maioria dos participantes opinou contra, o algoritmo invalida o tratamento proposto e então terá que ser proposto um novo tratamento para o risco.

6.2. Experimentos Realizados para Avaliação da Abordagem Proposta

O experimento foi realizado com o intuito de avaliar a relevância da abordagem proposta e a usabilidade do módulo de discussão de riscos de segurança bem como as regras de validação de consistência da discussão incluídas no RD system. Os principais objetivos deste experimento foram: identificar os pontos fortes e fracos da abordagem, se esta é capaz de suprir as necessidades do gerenciamento de riscos de segurança da informação e reafirmar a necessidade de se utilizar tais ferramentas de apoio às discussões de riscos. Este experimento também envolveu oito participantes, entre gestores em informática, profissionais da área de desenvolvimento e especialistas em segurança da informação os quais foram divididos em dois grupos.

Antes de iniciar este experimento, os participantes receberam um treinamento curto a respeito de processos de gerenciamento de riscos de segurança da informação e do emprego de jogos de diálogo em debates. Além disso, a abordagem e o sistema propostos foram apresentados para os participantes. Foram apresentadas as locuções do protocolo de diálogo para gerenciamento de riscos de segurança da informação, incluindo uma descrição do significado de cada locução, uma visão geral de suas regras de combinação, de exemplos de seus possíveis usos no sistema e das regras de consistência da discussão.

Após esta apresentação, cada participante recebeu um documento contendo: i) a norma ISO/IEC 27005; ii) uma descrição de conceitos de gerenciamento de riscos necessários para o experimento, como o fluxo do processo, métodos a serem utilizados na análise de riscos; iii) os ativos discutidos em projetos reais de segurança da informação que são desenvolvidos pela empresa e iv) checklists de ativos para auxiliar na discussão.

O projeto proposto consistiu na evolução de um sistema de gerenciamento de alunos, o qual envolve dados e histórico de aulas e acontecimentos em sala de aula. Este projeto foi classificado como crítico para a empresa.

Com o experimento apresentado, os participantes realizaram o gerenciamento de riscos de segurança da informação do projeto através da utilização do RD system. Após a discussão colaborativa dos riscos de segurança da informação, os participantes responderam a um questionário de avaliação, contendo nove questões de múltipla escolha, descritas a seguir:

Q1. É importante explorar a colaboração no gerenciamento de riscos de segurança da informação.

Q2. As locuções definidas permitem expressar aspectos importantes em uma discussão de riscos de segurança.

Q3. O esforço para entender uma discussão resultante desse experimento é baixo.

Q4. O protocolo está adequado aos processos da ISO/IEC 27005.

Q5. A descrição do processo de riscos de segurança da informação auxiliou no entendimento dos passos que deveriam ser seguidos na discussão.

Q6. As regras de validação possibilitam identificar atividades não executadas na discussão.

Q7. As regras de validação são importantes para melhorar a qualidade da discussão.

Q8. O feedback fornecido ao usuário auxilia a realização de tarefas no RD System.

Q9. Avalie RD System com uma nota de 0 a 10.

Os resultados obtidos neste experimento através dos dados do questionário de avaliação podem ser observados na Figura 10. A questão Q1 visa analisar a relevância da abordagem colaborativa para o gerenciamento das discussões de riscos. Segundo as respostas obtidas, a grande maioria dos participantes (90%) concorda que é importante explorar a colaboração no gerenciamento de riscos. De acordo com a análise feita a partir das justificativas descritas pelos usuários, a maioria concorda que a melhor maneira de encontrar melhores estratégias envolve a colaboração para que possa envolver uma diversidade de experiências e percepções.

A questão Q2 visa analisar se as locuções apresentadas permitem expressar aspectos importantes em uma discussão de riscos de segurança. Segundo as respostas, a maioria dos participantes (75%) concorda que as locuções expressam aspectos importantes de gerenciamento de riscos. De acordo com a análise feita a partir das justificativas descritas pelos usuários, as locuções atendem os principais pontos-chaves de gerenciamento de riscos de segurança ajudando assim a não haver desvios na comunicação entre participantes.

A questão Q3 visa analisar o esforço para entender uma discussão deste experimento. Segundo as respostas, a maioria dos participantes (50%) concorda que é de fácil entendimento uma discussão gerada através do sistema. Já outros (33,30%) concordam parcialmente com a organização no formato de uma árvore de discussão, sendo que observam que a árvore da discussão é de um modo geral simples e funcional, mas pode existir melhorias para o melhor entendimento das pessoas envolvidas evitando que em discussões com muitos usuários essa organização se torne confusa e difícil de localizar as locuções.

A questão Q4 visa analisar se as locuções estão de acordo com a norma ISO/IEC 27005. Segundo respostas obtidas, a maioria dos participantes (84%) concorda que as locuções expressam o processo de uma discussão de riscos de segurança da informação e, por sua vez, estão adequadas ao processo da ISO/IEC 27005. De acordo com a análise feita a partir das justificativas descritas pelos usuários, o protocolo atende o processo da ISO, desde as locuções e as validações feitas sejam consistentes, principalmente no aspecto de só permitir a definição do risco após a definição do ativo e só finalizar quando todas as argumentações estiverem com o consenso estabelecido que permitem avançar ou não a discussão. Destacaram também que antes de realizar o experimento no sistema utilizaram a ISO para criar uma discussão sem auxílio, a qual se tornou tediosa, sendo necessário muitas revisões e anotações de cada membro da equipe o que tomou muito tempo para verificar apenas um risco.

A questão Q5 visa analisar se a descrição do processo de riscos de segurança da informação auxiliou no entendimento dos passos a serem seguidos na discussão. Segundo respostas obtidas, a maioria dos participantes (83%) concorda que o processo auxilia no entendimento de uma discussão. De acordo com a análise feita a partir das justificativas descritas pelos usuários, o processo facilitou a discussão, tornando-o indispensável e de extrema importância. Os participantes destacaram que para um usuário que não tem experiência, este processo norteia e ajuda a integração do participante na discussão.

A questão Q6 visa analisar se as regras de validação possibilitam identificar atividades não executadas na discussão. Segundo respostas obtidas, a maioria dos participantes (92%) concorda que as regras identificam atividades incompletas na discussão. De acordo com a

análise feita a partir das justificativas descritas pelos usuários, a discussão por ser em uma estrutura de árvore, possibilita que a discussão seja finalizada e muitos pontos importantes não sejam discutidos ou esclarecidos. Com isso as regras de validação realçam onde existem problemas na discussão podendo os participantes corrigirem-os.

A questão Q7 visa analisar se as regras de validação são importantes para melhorar a qualidade da discussão. Segundo respostas obtidas a maioria dos participantes (84%) concorda que as regras são importantes para não deixar a discussão incompleta. De acordo com a análise feita a partir das justificativas descritas pelos usuários as regras permitiram que a discussão seguisse todos os passos e terminasse sem nem uma falha, pois ajuda no direcionamento da discussão mantendo uma coerência e encaminhando a discussão para um consenso, auxiliando a verificar o que já foi feito e o que falta a fazer.

A questão Q8 visa analisar se o *feedback* fornecido ao usuário auxilia a realização de tarefas no RD System. Segundo respostas obtidas a maioria dos participantes (84%) concorda que o *feedback* ajuda na realização de tarefas na discussão. De acordo com a análise feita, a partir das justificativas descritas pelos usuários, o *feedback* mostrou-se eficiente e eficaz, pois atente os requisitos funcionais que a norma exige. Os participantes também levantaram que as mensagens de *feedback* são esclarecedoras e diretas, não deixando dúvidas no que deveria ser feito para eliminar as inconsistências.

A questão Q9 visa avaliar o RD System com uma nota de 0 a 10. Segundo respostas obtidas, a maioria dos participantes avalio o RD System com nota 8,0. De acordo com a análise feita a partir das justificativas descritas pelos usuários o sistema de modo geral é de fácil uso, mas a árvore de discussão pode ser melhorada, principalmente em discussões com muitos usuários ou discussões prolongadas, o acompanhamento da discussão se torna difícil. Algumas sugestões como a ferramenta disparar um e-mail para membro de uma discussão informando as novas interações da equipe foram levantadas, deixando assim os participantes avisados de novas interações na discussão.

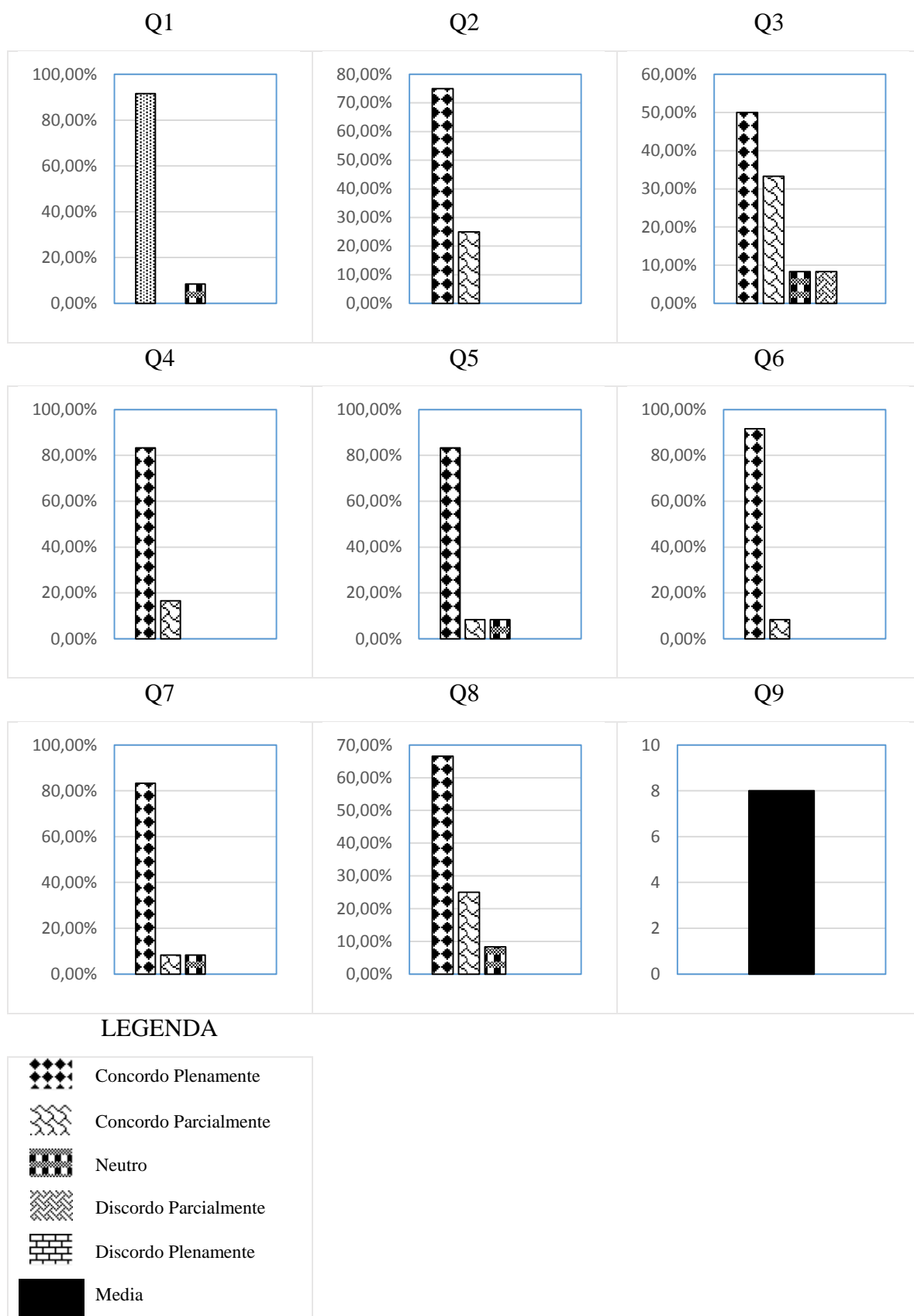


Figura 10 - Gráficos de dados do questionário do experimento

7. CONSIDERAÇÕES FINAIS

O gerenciamento de riscos de segurança da informação é uma etapa importante para o processo de gestão de segurança da informação. Mesmo diante deste fato, poucas empresas executam este gerenciamento, por diversos motivos. A maioria das organizações não possui um processo formal de gerenciamento de riscos ou não possuem processo algum pelos principais motivos que é a sua complexidade e a falta de técnicas que facilitem o processo de gerenciamento de riscos de segurança da informação.

Apesar de alguns trabalhos terem sido propostos na área, ainda existe a necessidade de abordar tópicos como a colaboração (em termos de interação humana que ocorre), captura de dados e conhecimento do processo de discussão de riscos. Visando tratar estes problemas, esta dissertação apresenta uma abordagem colaborativa para o gerenciamento de riscos de segurança da informação. Tal abordagem é construída a partir da definição, aplicação e avaliação de um protocolo de jogo de diálogo para o gerenciamento de riscos de segurança da informação. Este protocolo visa suportar, capturar e estruturar discussões de riscos, bem como registrar estas discussões em uma memória de gerenciamento de riscos de forma completa e consistente.

As contribuições deste trabalho foram testadas usando experimentos, envolvendo uma equipe de gerentes e desenvolvedores de uma empresa. Dentre as contribuições apresentadas neste trabalho, pode-se ressaltar a proposição de um protocolo de discussão de riscos de segurança da informação de forma que obedeça um processo e, assim, atenda aos objetivos de discutir riscos em tarefas colaborativas de gerenciamento de riscos e a adaptação do sistema proposto que suporta esta abordagem para atender as regras de completude e consistência.

Outro benefício dessa pesquisa é a criação de uma memória estruturada de discussões de riscos de forma completa, em que os argumentos utilizados nestas discussões são gravados explicitamente (e indexados por atos de locução correspondentes), visando ampliar os dados e conhecimento geralmente gerenciados por diferentes sistemas de gerenciamento de riscos e de projetos.

Portanto, acredita-se que o experimento apresenta evidência positiva para a relevância do uso de um protocolo de segurança da informação com o auxílio de um processo juntamente com a utilização de regras de completude e consistência de argumentação para proposição de

riscos no ambiente do RD System v4.0. Além disso, este trabalho também foi validado pela apresentação de partes dele em um evento científico das áreas de pesquisa envolvidas nesta dissertação e uma versão preliminar deste trabalho foi apresentada no Conferencia Latino-americana em Informática (CLEI) na forma de um artigo, denominado *Abordagem colaborativa para gestão de riscos de segurança da informação* (BALKE et al., 2015).

Como trabalhos futuros que sugere-se expandir o protocolo proposto com a integração de mais tipos de jogos de diálogos como diálogos de persuasão e ou negociação. Outra área que pode ser explorada em trabalhos futuros é o estudo de formas avançadas de quantificar os riscos e ativos para que com base no contexto definido, se possa eliminar ou aceitar a proposição dos mesmo de forma autônoma com base nos cálculos que são descritos na norma ISO/IEC 27005.

REFERÊNCIAS

- ABNT NBR ISO/IEC 27005. **Gestão de riscos de Segurança da informação**Rio de Janeiro, 2008.
- AMGOUD, L. et al. Modelling dialogues using argumentation a μ . 2000.
- AMGOUD, L.; CAYROL, C. Inferring from Inconsistency in Preference-Based Argumentation Frameworks. p. 125–169, 2002.
- ANDONE, C. A Systematic Theory of Argumentation. The Pragma-Dialectical Approach. **Journal of Pragmatics**, v. 37, n. 4, p. 577–583, 2005.
- ATKINSON, D. C.; WEEKS, D. C.; NOLL, J. Tool support for iterative software process modeling. v. 49, p. 493–514, 2007.
- BAJEC, M.; VAVPOTIČ, D.; KRISPER, M. Practice-driven approach for creating project-specific software development methods. **Information and Software Technology**, v. 49, n. 4, p. 345–365, 2007.
- BALKE, M. et al. Collaborative Approach to Security Risk Management Information. 2015.
- BAO, E. A Study of Rationality Test Rules for Software Process Model. **2008 International Conference on Information Management, Innovation Management and Industrial Engineering**, p. 28–32, dez. 2008.
- BARKER, W. C. Guideline for Identifying an Information System as a National Security System. n. August, 2003.
- BECKERS, K. et al. Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. **2011 Sixth International Conference on Availability, Reliability and Security**, p. 327–333, ago. 2011.
- BENCHCAPON, T.; DUNNE, P. Argumentation in artificial intelligence. **Artificial Intelligence**, v. 171, n. 10-15, p. 619–641, jul. 2007.
- BENTAHAR, J.; MOULIN, B.; CHAIB-DRAA, B. A Persuasion Dialogue Game based on Commitments and Arguments. 2004.
- BLACK, E.; ATKINSON, K.; KATIE, B. Dialogues that Account for Different Perspectives in Collaborative Argumentation. p. 867–874, 2009.

- BLACK, E.; HUNTER, A. An inquiry dialogue system. **Autonomous Agents and Multi-Agent Systems**, v. 19, n. 2, p. 173–209, 2009.
- BS. Information security management systems – security risk management. 2006.
- CAMPOS, A. **Sistema de Segurança da Informação Sumário**. 2. ed. [s.l.] Visual Books, 2007.
- CHEN, T. M. Information Security and Risk Management. 2009.
- DAI, F.; LI, T. Tailoring Software Evolution Process. n. 60463002, p. 782–787, 2007.
- DIVISION, C. S. Managing Information Security Risk. v. 800-39, n. March, p. 88, 2011.
- DUNG, P. M. Artificial Intelligence On the acceptability role in nonmonotonic of arguments and its fundamental reasoning , logic programming and. v. 77, p. 321–357, 1995.
- FRANQUEIRA, V. N. L. et al. Risk and Argument : A Risk-Based Argumentation Method for Practical Security. p. 239–248, 2011.
- GROARKE, L. **Informal logic**. The Stanfo ed.[s.l: s.n.].
- HALEY, C. B.; LANEY, R.; MOFFETT, J. D. Security Requirements Engineering : A Framework for Representation and Analysis Security Requirements Engineering : A Framework for Representation and Analysis. 2008a.
- HALEY, C. B.; LANEY, R.; MOFFETT, J. D. Security Requirements Engineering : A Framework for Representation and Analysis. v. 34, n. 1, p. 133–153, 2008b.
- HAMBLIN, C. L. **Fallacies**. London, UK: [s.n.].
- HSUEH, N. L. et al. Applying UML and software simulation for process definition, verification, and validation. **Information and Software Technology**, v. 50, n. 9-10, p. 897–911, 2008.
- HUZITA, E.; SILVA, C.; WIESE, I. Um conjunto de soluções para apoiar o desenvolvimento distribuído de software. p. 101–110, 2008.
- INÁCIO, L. et al. Introdução à gestão de riscos de segurança da informação. 2011.
- INTERNATIONAL, A. General Security Risk. 2003.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Risk management — Principles and guidelines. 2009.

- JINGFU, Z.; BINHENG, S. Verification of resource constraints for concurrent workflows. **Proceedings - Seventh International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2005**, v. 2005, p. 353–360, 2005.
- JINPING, Y. et al. Multi-party Dialogue Games for Distributed Argumentation System. 2011.
- KHIDZIR, N. Z.; MOHAMED, A.; ARSHAD, N. H. H. Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing. **2010 Second International Conference on Network Applications, Protocols and Services**, p. 234–239, set. 2010.
- KORONIOS, A. et al. INTEGRATION THROUGH STANDARDS – AN OVERVIEW OF INTERNATIONAL STANDARDS FOR ENGINEERING ASSET MANAGEMENT. **2nd World Congress on Engineering Asset Management and the Fourth International Conference on Condition Monitoring (WCEAM 2007), Harrogate, United Kingdom**, p. 1–24, 2006.
- KOTULIC, A. G.; CLARK, J. G. Why there aren't more information security research studies. **Information & Management**, v. 41, n. 5, p. 597–607, maio 2004.
- LEITNER, A. et al. ARiMA - a new approach to implement ISO / IEC 27005. **IEEE intelligent System**, p. 1–6, 2009.
- LI, J.; FAN, Y.; ZHOU, M. Timing constraint workflow nets for workflow analysis. **IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans.**, v. 33, n. 2, p. 179–193, 2003.
- LUCAS, F. J.; MOLINA, F.; TOVAL, A. A systematic review of UML model consistency management. **Information and Software Technology**, v. 51, n. 12, p. 1631–1645, 2009.
- MANAGEMENT, O. O. F. ANNUAL REPORT TO CONGRESS: FEDERAL INFORMATION SECURITY. 2015.
- MARJANOVIC, O. Dynamic verification of temporal constraints in production workflows. **Proceedings 11th Australasian Database Conference. ADC 2000 (Cat. No.PR00528)**, 2000.
- MCBURNEY, P. et al. A Dialogue Game Protocol for Agent Purchase Negotiations. **Autonomous Agents and Multi-Agent Systems**, v. 7, n. 3, p. 235–273, 2003.
- MCBURNEY, P.; HITCHCOCK, D.; PARSONS, S. The eightfold way of deliberation dialogue. **International Journal of Intelligent Systems**, v. 22, n. 1, p. 95–132, jan. 2007.
- MCBURNEY, P.; PARSONS, S. Argumentation in Artificial Intelligence. p. 261–280, 2009a.

- MCBURNEY, P.; PARSONS, S. Dialogue Games for Agent Argumentation. 2009b.
- MCBURNEY, P.; PARSONS, S.; WOOLDRIDGE, M. Desiderata for agent argumentation protocols. **Proceedings of the first international joint conference on Autonomous agents and multiagent systems part 1 - AAMAS '02**, p. 402, 2002.
- MEULBROEK, L. K. Integrated Risk Management for the Firm : A Senior Manager ' s Guide. 2002.
- MOULIN, B.; IRANDOUST, H.; BÉLANGER, M. Explanation and Argumentation Capabilities : Towards the Creation of More Persuasive Agents. p. 169–222, 2002.
- MURPHY, R. H.; FELLOW, N. Cyberspace : Answering. n. June, 2009.
- NING, M. The actuality and countermeasure of net information safety in China. v. 2, 2007.
- NIST. SP 800-60 Volume II : Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. **National Institute of Standards and Technology**, v. II, n. August, 2008.
- NOROOZI, O. et al. Argumentation-Based Computer Supported Collaborative Learning (ABCSCCL): A synthesis of 15 years of research. **Educational Research Review**, v. 7, n. 2, p. 79–106, jun. 2012.
- PRAKKEN, H. Coherence and flexibility in dialogue games for argumentation. **Journal of Logic and Computation**, v. 15, n. 6, p. 1009–1040, 2005.
- PRAKKEN, H. Formal systems for persuasion dialogue. v. 00, p. 1–26, 2006.
- PRAKKEN, H.; IONITA, D.; WIERINGA, R. Risk assessment as an argumentation game. v. 8143, p. 1–17, 2013.
- PRIKLADNICKI, R.; AUDY, J. **Desenvolvimento Distribuído de SORFTARE**. 1. ed. [s.l: s.n.].
- QUADRANT, G. M.; PLATFORMS, E. P. Global IT Security Risks : 2012. p. 21, 2012.
- REED, C.; WELLS, S. Dialogical argument as an interface to complex debates. **Intelligent Systems, IEEE**, p. 6, 2007.
- SCHEUER, O. et al. Computer-supported argumentation: A review of the state of the art. **International Journal of Computer-Supported Collaborative Learning**, v. 5, n. 1, p. 43–102, jan. 2010.

- SECURITY, C. T. ISO/IEC 13335-1 : 2004 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — MANAGEMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY. **Bureau of Indian Standards**, p. 34, 2009.
- SEVERO, F. S. et al. Argumentation-Based Risk Management. 2007.
- SHEDDEN, P.; RUIGHAVER, T. Risk management standards – the perception of ease of use. p. 1–13, 2006.
- STANDARD, A. Z. Standards Australia and Standards New Zealand. AS/NZS 4360:2004. 2004.
- STONEBUMER, G.; GOGUEN, A.; FERINGA, A. Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology. v. 30, n. July, 2002.
- STONEBURNER, G. Information technology security. **NIST Special Publication**, n. December, p. 24, 2001.
- THE NATIONAL ARCHIVES. Identifying Information Assets and Business Requirements. v. 1.2, p. 1–25, 2011.
- THOMPSON, K. M.; DEISLER, P. F.; SCHWING, R. C. Interdisciplinary vision: the first 25 years of the Society for Risk Analysis (SRA), 1980-2005. **Risk analysis : an official publication of the Society for Risk Analysis**, v. 25, n. 6, p. 1333–86, dez. 2005.
- TOLCHINSKY, P. et al. Transplant Availability: Agent Deliberation. **IEEE intelligent System**, p. 8, 2006.
- TOLCHINSKY, P. et al. Deliberation dialogues for reasoning about safety critical actions. **Autonomous Agents and Multi-Agent Systems**, v. 25, n. 2, p. 209–259, 11 maio 2011.
- TOULMIN, S. E. **The Uses of Argument**. [s.l: s.n.].
- TOULMIN, S. E. **The Uses of Argument (Updated edition 2003)**. [s.l: s.n.].
- TWENTE, U. **SITUATIONAL METHOD ENGINEERING**. [s.l: s.n.].
- WALTON, D. et al. Book Review. n. 1995, p. 305–313, 2001.
- WALTON, D. Types of dialogue and burdens of proof. **Frontiers in Artificial Intelligence and Applications**, v. 216, p. 13–24, 2010.
- WALTON, D.; KRABBE, E. C. W. **ommitment in Dialogue: Basic Concepts of Interpersonal Reasoning**. ilustrada ed.[s.l: s.n.].

WANGEN, G. A Comparison between Business Process Management and Information Security Management. v. 2, p. 901–910, 2014.

WUNDER, J.; WALTERMIRE, D. Specification for Asset Identification 1 . 1. 2011.

ZAINI, M. K. Conceptualizing the Relationships between Information Security Management Practices and Organizational Agility. 2013.