UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ANÁLISE/AVALIAÇÃO DE RISCOS DE SEGURANÇA DE INFORMAÇÃO: QUANTIFICAÇÃO DE CONFIANÇA COMO UM PARÂMETRO DE REDUÇÃO DE DESVIOS DE RESULTADOS POR CAUSAS HUMANAS

DISSERTAÇÃO DE MESTRADO

Víctor Leonel Orozco López

Santa Maria, RS, Brasil

2014

ANÁLISE/AVALIAÇÃO DE RISCOS DE SEGURANÇA DE INFORMAÇÃO: QUANTIFICAÇÃO DE CONFIANÇA COMO UM PARÂMETRO DE REDUÇÃO DE DESVIOS DE RESULTADOS POR CAUSAS HUMANAS

Víctor Leonel Orozco López

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

Orientador: Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS, Brasil

2014

López, Víctor Leonel Orozco

Análise/avaliação de riscos de segurança de informação: Quantificação de confiança como um parâmetro de redução de desvios de resultados por causas humanas / por Víctor Leonel Orozco López. – 2014.
100 f.: il.; 30 cm.

Orientador: Raul Ceretta Nunes
Dissertação (Mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Informática, RS, 2014.

1. Segurança. 2. Analise de riscos. 3. Confiança. 4. Fatores humanos. I. Nunes, Raul Ceretta.

E-mail: vlopez@inf.ufsm.br

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Informática

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

ANÁLISE/AVALIAÇÃO DE RISCOS DE SEGURANÇA DE INFORMAÇÃO: QUANTIFICAÇÃO DE CONFIANÇA COMO UM PARÂMETRO DE REDUÇÃO DE DESVIOS DE RESULTADOS POR CAUSAS HUMANAS

elaborada por
Víctor Leonel Orozco López

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

COMISSÃO EXAMINADORA:

Raul Ceretta Nunes, Dr.
(Presidente/Orientador)

Lisandra Manzoni Fontoura, Dr[a]. (UFSM)

Carlos Alberto Maziero, Dr. (UTFPR)

Santa Maria, 28 de Fevereiro de 2014.

AGRADECIMENTOS

Sem medo de errar posso afirmar que estes dois anos de mestrado foram fundamentais na minha formação profissional. Porém nunca imaginei a importância que esta viagem teria para a minha vida. Assim, gostaria de agradecer antes que tudo a Deus. Obrigado senhor por me proporcionar a sabedoria necessária para finalizar este trabalho, eu sei que nunca estive sozinho durante este tempo.

Da mesma forma gostaria de agradecer a todas as instituições e pessoas que fizeram possível a minha estadia no Brasil. A Universidade Federal de Santa Maria (UFSM), a Organização de Estados Americanos (OEA) e o grupo Coimbra de Universidades Brasileiras (GCUB), obrigado pelo financiamento e a oportunidade. Espero não defraudar as suas expectativas para ser um agente de câmbio no meu país.

Agradeço também ao meu orientador Prof. Dr. Raul Ceretta Nunes que durante estes dois anos sempre teve a disposição para me orientar na conclusão deste trabalho. Sua ajuda foi fundamental para construir as bases para a minha vida como pesquisador e espero algum dia orientar com a mesma didática e profissionalismo com que realiza seu trabalho.

Agradeço aos mestrandos do PPGI que durante o mestrado tiveram a paciência para tentar entender meu portunhol, valeu galera foi graças a todos vocês que conseguí falar português!. Especial agradecimento ao pessoal do GTSeg, GPSCOM e GRECA: Giani, Sandro, Tarcisio, Samuel, Juliano, Gleizer, Felipe, Taciano, Fabricio, Andreia, Rafaela, Henrique, obrigado pelas dicas para sobreviver no Brasil. Sem sequer perceber vocês foram meus professores de português, geografia, economia, politica e tudo o que eu precisei para sobreviver no Brasil. Obrigado também pela parceria durante as aulas, viagens e na Universidade mesma. De aqui em diante sempre que eu der uma olhada para alguma escada vou lembrar dos amigos que fiz nestes dois anos, acreditem!.

Agradeço também a aquelas pessoas que sem me conhecer deram a sua ajuda desinteressada para um estrangeiro recém-chegado ao Brasil: Andre, Ana Julia, Katiele, Helen, Andreia, Ana, e principalmente aos meus colegas de aventura e apartamento, Ivan e Cristina. Foi uma experiencia única conhecer todos vocês e desejo tudo de bom para as suas vidas.

Por último agradeço à minha família, pelo suporte emocional nos momentos difíceis. A sua compreensão, exemplo, e as suas palavras de conforto foram fundamentais para conseguir mais um objetivo. Obrigado Leonel, Heidy, Liliam, Evelyne, este logro foi graças a todos vocês.

“Cuando despertó, el dinosaurio todavía estaba allí”
— AUGUSTO MONTERROSO

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Informática
Universidade Federal de Santa Maria

ANÁLISE/AVALIAÇÃO DE RISCOS DE SEGURANÇA DE INFORMAÇÃO: QUANTIFICAÇÃO DE CONFIANÇA COMO UM PARÂMETRO DE REDUÇÃO DE DESVIOS DE RESULTADOS POR CAUSAS HUMANAS

AUTOR: VÍCTOR LEONEL OROZCO LÓPEZ
ORIENTADOR: RAUL CERETTA NUNES
Local da Defesa e Data: Santa Maria, 28 de Fevereiro de 2014.

A gestão de riscos constitui uma base para a tomada de decisão, uma vez que cria uma visão que permite identificar e controlar os riscos que podem comprometer os ativos de uma determinada organização. A norma ISO 27005:2011 afirma que um dos passos fundamentais em um plano de gerenciamento de risco é a definição de políticas de segurança mediante o uso de avaliação de riscos para estimar a gravidade das ameaças que uma determinada organização enfrenta. Apesar da existência de várias metodologias para realizar avaliações de risco exitosas, evidência prévia tem demonstrado que a presença de fontes de dados humanas podem produzir desvios nos resultados, podendo comprometer a continuidade dos negócios com investimentos realizados de forma desnecessária ou equivocada.

Utilizando-se o nível de confiança das fontes humanas para dar ênfase aos indivíduos considerados como mais confiáveis, este trabalho apresenta uma proposta para reduzir desvios mediante o uso de ponderações nas avaliações de risco. O conceito de confiança utilizado é uma função de confiança entre os colegas de trabalho e de avaliações de desempenho, o que permite criar um processo evolutivo que refina as noções de confiança a partir da execução continua dos ciclos de gestão de risco.

A avaliação da evolução do processo de gestão do risco ao longo de diversos períodos de tempo demonstrou que o uso de coeficientes de confiança em análise/avaliação de riscos pode efetivamente aumentar a precisão das estimativas de riscos. Como resultado o modelo de quantificação de confiança desenvolvido possibilitou a criação de uma ferramenta para minimizar desvios de resultados por causas humanas.

Palavras-chave: Segurança. Analise de riscos. Confiança. Fatores humanos.

ABSTRACT

Master Dissertation
Computer Science Graduate Program
Federal University of Santa Maria

RISK ASSESSMENT IN INFORMATION SECURITY: QUANTIFICATION OF TRUST AS A PARAMETER TO REDUCE BIASES IN RESULTS AS A PRODUCT OF HUMAN FACTORS

AUTHOR: VÍCTOR LEONEL OROZCO LÓPEZ
ADVISOR: RAUL CERETTA NUNES
Defense Place and Date: Santa Maria, February 28th, 2014.

Risk management constitutes a basis for decision making since it creates a view that allows to identify and control risks that can compromise the assets of a given organization. The standard ISO 27005:2011 states that one of the fundamental steps on a risk management plan is the definition of security policies with the usage of risk assessment to estimate the severity of the threats that a given organization faces. Despite the existence of several methodologies to achieve successful risk assessments, preview evidence has demonstrated that the presence of human data sources for risk assessments can produce biased results, thus compromising the business continuity as a result of unnecessary or wrong investments.

Using the confidence level of human sources to give emphasis to individuals considered as more reliable, this work presents a proposal to reduce biases by using weights in risk assessments. The concept of trust used is a function of trust among coworkers and performance evaluations, which allowed to create an evolutionary process that refines the notions of trust through the execution of continuum cycles of risk management .

A validation of the evolution of the process of risk management during various periods of time showed that the use of coefficients of trust in risk assessment can effectively improve the accuracy of risk estimates. As a result the developed model for quantification of trust enabled the creation of a tool to minimize deviations of results due human causes.

Keywords: Risk analysis. Security. Trust. Human factors.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARIMA	*Austrian Risk Management Approach*
AURUM	*Automated Risk and Utility Management*
BYOD	*Bring your own device*
CRI	*Composite Risk Index*
DI	*Interações diretas de confiança*
DO	*Direct Observations*
FMEA	*Failure Model and Effect Analysis*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ISRAM	*Information Security Risk Analysis Method*
KPI	*Key Performance Indicators*
KRI	*Key Risk Indicators*
NPR	*Número de Prioridade de Risco*
PDCA	*Plan-Do-Check-Act*
SGSI	*Sistema de Gestão de Riscos de Segurança de Informação*
WI	*Witness Information*

LISTA DE SÍMBOLOS

T_{ij}	Confiança de um nó i para um nó j
$\tilde{T}_{ij}$	Confiança indireta de um nó i para um nó j
$N(i)$	Conjunto de agentes vizinhos de i
β	ator de limite de alcance de TrustWebRank
τ	Parâmetro de controle de alcance da confiança calculada com TrustWebRank
κ	Parâmetro de controle para reduções na atualização de confiança
γ	Parâmetro de controle para aumentos na atualização de confiança
$\breve{T}_{ij}$	Confiança atualizada de um nó i para um nó j

SUMÁRIO

1 INTRODUÇÃO

Os riscos de segurança da informação podem ser definidos como a probabilidade de que uma vulnerabilidade seja explorada por uma ameaça com o objetivo de causar um impacto negativo nos ativos de uma organização. Diante da existência dos riscos os processos de gestão de riscos, no ambiente de tecnologias da informação, possibilitam que os administradores de tecnologias possam balancear os custos econômicos e operacionais para a criação de medidas de segurança efetivas contra os principais riscos (ANDRESS, 2011).

Durante o ano de 2013 a empresa de consultoria PriceWaterhouseCoopers realizou uma pesquisa a nível mundial acerca da importância da segurança de informação dentro do planejamento de investimentos na área de tecnologias da informação nas empresas (PRICEWATERHOUSECOOPERS, 2013). Dos 575 executivos entrevistados no Brasil, menos da metade (45%) dos participantes espera um aumento dos orçamentos na área de segurança nos próximos 12 meses. A conjuntura econômica foi apontada como a principal limitante ao aumento, citada por 46% dos respondentes. No mesmo estudo, ressalta-se o fato que, apesar do aumento de incidentes de segurança, as práticas tradicionais tal como a de gestão de riscos são apontadas com menor tendencia a receber aumentos orçamentários, se comparadas com áreas de segurança emergentes como proteção de dados, dispositivos móveis e redes sociais online.

Por outro lado, a norma ISO/IEC 27005:2011 (ISO/IEC, 2011c) estabelece que as técnicas de gestão de riscos são ferramentas concebidas para guiar os investimentos em segurança de informação baseando-se no panorama de ameaças que uma organização enfrenta. Assim, a gestão de riscos permite apresentar aos gestores de investimentos uma visão do estado e a prioridade dos riscos potenciais a ser enfrentados, para que os investimentos em tratamento de riscos sejam realizados de acordo com os objetivos da organização. De forma geral, os processos de gestão de riscos são criados como um conjunto de diretrizes, já que os mesmos apresentam uma serie de etapas que visam identificar, investir e monitorar o tratamento dos riscos. Ao mesmo tempo proporcionam a liberdade de escolha entre diversas metodologias para estas etapas, considerando que as atividades de uma organização para outra podem apresentar diferenças significativas. Porém, cada metodologia pode apresentar análises baseadas em diferentes origens, técnicas e metodologias de análise de dados, o que consequentemente pode derivar na criação de divergências entre os resultados de metodologias que teoricamente são aplicáveis num mesmo contexto.

A existência destas divergências pode resultar em problemas de segurança se a metodologia escolhida apresentar resultados fora da realidade de riscos da empresa, além de influenciar as ações destinadas ao tratamento de riscos, que também podem ser desviadas. Assim, diversos autores (SEGUDOVIC, 2006; FENG; LI, 2011) tem ressaltado a necessidade de criar e melhorar os métodos para cada uma das etapas da gestão de riscos, onde a exatidão de resultados é um dos objetivos mais almejados para melhorar a efetividade dos investimentos em segurança da informação, na qual a falta de orçamento é uma limitante constante. Sendo esta limitante um dos principais motivos pelos quais este trabalho explora uma técnica de quantificação de confiança para a redução de desvios causados pela influência humana.

1.1 Motivação

Dentro das etapas que compõem as atividades da gestão de riscos, a etapa de análise/avaliação de riscos tem especial importância, já que os dados gerados nesta etapa proporcionam a base de um processo de gestão de riscos exitoso, constituindo um componente fundamental ao conduzir atividades e investimentos (PRICEWATERHOUSECOOPERS, 2008). Assim, entre vários esforços para tratar as divergências entre metodologias de análise/avaliação de riscos (CLEMEN; WINKLER, 1999; WORKMAN, 2012; BANERJEE, 2011; KHAMBHAMMETTU et al., 2013), a solução proposta por Amaral, Amaral e Nunes (2010) minimiza as diferenças entre metodologias mediante a criação de uma composição de resultados de diferentes metodologias de avaliação de riscos, projetadas para o contexto de segurança de informação. As metodologias usadas foram: ISRAM (KARABACAK; SOGUKPINAR, 2005), AURUM (EKELHART; FENZ; NEUBAUER, 2009), FMEA (STAMATIS, 2003) e ARIMA (LEITNER; SCHAUMULLER-BICHL, 2009).

Apesar da normalização alcançada pela composição de métodos, Amaral, Amaral e Nunes (2010) demonstraram que quando os efeitos negativos das divergências entre as metodologias são eliminados, a subjetividade da informação pode também gerar perturbações nos resultados da análise/avaliação de riscos, sendo que esta subjetividade é um reflexo do uso de dados não determinísticos em forma de opiniões humanas capturadas mediante entrevistas. Porém, as causas e consequências da subjetividade humana tem sido estudadas desde diferentes pontos de vista, tais como psicologia (SEARS, 1983), sociologia (WINSHIP; MARE, 1992) e administração (CARTER; KAUFMANN; MICHEL, 2007), onde cada um destes estudos apresenta características particulares que dificultam a criação de uma solução universal para o tratamento

da subjetividade em processos de tomada de decisões.

Embora a eliminação dos dados não determinísticos possa parecer a abordagem mais lógica, estes dados podem fornecer informações que não são perceptíveis com dados determinísticos. Em particular, os dados não determinísticos tem sido elegidos como um paliativo para o fracasso dos métodos determinísticos para representar interações sociais (SENIK, 2005). Nesta linha, tanto trabalhos antigos (CLARKE, 1988) quanto novos (BANERJEE, 2011) demonstram que a área de gestão de riscos de segurança da informação não é alheia à subjetividade. De acordo com Workman (2012), a literatura de tomada de decisões em segurança de informação, procura incrementar a precisão das estimativas de risco mediante os fatores situacionais, porém desconsiderando os desvios subjetivos que podem afetar esses fatores.

Com a utilização de origens de dados não-determinísticos existe a necessidade de criar metodologias de análise/avaliação de riscos que considerem a natureza subjetiva das origens, para que a informação obtida através deles possa ser aproveitada sem prejudicar a precisão dos resultados, ou seja a precisão das estimativas de riscos e consequentemente a precisão das atividades de gestão de riscos.

1.2 Objetivos e Contribuições

Diante deste cenário, o objetivo deste trabalho é propor um processo de quantificação de confiança como um suporte para a redução de desvios de resultados por causa do julgamento humano. Como hipótese para a realização deste trabalho tem-se assumido que é possível estabelecer o nível de confiabilidade de uma opinião humana e que esse nível pode ser aproveitado para dar ênfase àquelas opiniões que podem fornecer uma visão de riscos mais efetiva.

A proposta baseia-se no fato de que a confiança e os riscos são conceitos estreitamente relacionados, uma vez que os seres humanos utilizam a confiança para atuar em presença de riscos e facilitar interações (JOSANG; GRAY; KINATEDER, 2003). Além de que, diante da existência de informação subjetiva, a única forma de afirmar que os dados subjetivos são confiáveis depende da confiabilidade na origem dos dados. Dados provenientes de origens confiáveis são considerados também como confiáveis (KO; KIRSCH; KING, 2005).

Considerando que a confiança pode ser quantificada se as variáveis certas forem selecionadas (MANCHALA, 2000) e dada a existência de indivíduos que exercem um papel chave dentro das redes sociais construídas mediante a interação entre colegas dentro de uma organização (TSVETOVAT; KOUZNETSOV, 2011), este trabalho formaliza a quantificação de

confiança em termos de informação de testemunhas -i.e. as percepções de confiança entre os indivíduos da organização- e observações diretas -i.e. a avaliação dos resultados obtidos com as estimativas de riscos dos indivíduos- sendo esta a principal contribuição do trabalho.

Adicionalmente, foram realizadas as atividades seguintes para apoiar o desenvolvimento da abordagem proposta:

1. Seleção de técnicas comuns compatíveis com a norma ISO 27005:2011 , tais como análise/avaliação baseada em entrevistas, estimativa de riscos utilizando uma composição de metodologias de risco e monitoramento do desempenho usando indicadores chave de risco;

2. A adaptação de um algoritmo tradicional de reputação para as características da gestão de riscos e a criação de um coeficiente de relevância baseado em percepções locais de confiança entre membros de uma organização;

3. O desenvolvimento de um processo evolutivo para à atualização das percepções de confiança baseado na performance dos tratamentos de risco; e

4. Uma validação mediante a criação de um cenário de simulação com redes sociais que permite analisar o impacto e a evolução da confiança frente a diferentes comportamentos.

1.3 Organização do Texto

O texto da dissertação está organizado da seguinte forma. O Capítulo 2 apresenta uma fundamentação teórica que aborda os conceitos importantes para a compreensão do trabalho. O Capítulo 3 apresenta a proposta de quantificação de confiança e trabalhos relacionados. No Capítulo 4 é apresentada a construção do simulador com o qual o desempenho da proposta foi avaliada. O Capítulo 5 realiza a avaliação do processo mediante simulação. Por fim, o Capítulo 6 descreve as conclusões do trabalho e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Com objetivo de clarificar os elementos necessários para a integração da quantificação de confiança dentro das atividades da análise/avaliação de riscos, este capítulo realiza uma revisão literária dos principais conceitos que abrangem a segurança da informação (seção 2.1), a gestão de riscos (seção 2.2), a metodologia de avaliação de riscos onde a problemática de desvios foi detectada(seção 2.3), assim como modelos computacionais para quantificação de confiança (seção 2.4) e a descrição do modelos de quantificação de confiança, que foram utilizados para propor a abordagem de redução de desvios (seção 2.5).

2.1 Segurança de informação

A informação é um conceito que forma parte da dinâmica da sociedade atual, principalmente como resultado da quase ubíqua adoção de tecnologias computacionais, as quais possibilitam que os usuários tenham acesso a informação trivial quanto relevante desde diversos dispositivos, tais como computadores, smartphones e outros (ANDRESS, 2011).

Mesmo que os benefícios do aumento da conectividade dos usuários tenham sido amplamente discutidos e elogiados, o aumento de dispositivos de "consumo de informação" também traz consigo novos problemas. De modo que, quando a informação apresenta uma natureza sensível -e.g dados bancários, documentos confidenciais-, a intercepção de informação por parte de indivíduos externos pode gerar um conjunto de problemas de segurança, desde roubo de ativos, extorsão, perdas monetárias até persecução jurídica por danos a terceiros. Situação que como Kessel e Allan (2013) ressaltam, tem apresentado um aumento quase-exponencial nos últimos anos.

Uma vez que os sistemas de informação são expostos a diversos tipos de ameaças, a segurança de informação tem como objetivo "proteger os sistemas de informação e a informação do uso, discussão, disrupção, modificação ou destruição de dados não autorizada" para o qual normas como a ISO/IEC 27001:2011 (ISO/IEC, 2011a) estabelecem uma série de atividades e requisitos para garantir que o impacto das falhas de segurança seja o mínimo, tais como:

- Propiciar o entendimento dos requisitos de segurança de informação de uma organização e da necessidade de estabelecer uma política e objetivos de segurança de informação;
- Implementar e operar controles para gerenciar os riscos de segurança de informação;

- Monitorar e analisar criticamente a efetividade destes controles; e
- Melhorar continuamente os processos de segurança baseado em medições objetivas.

Portanto, para levar a cabo discussões acerca dos problemas de segurança de informação, se faz necessária a definição de modelos e terminologia comum que possa ser utilizada como base de discussão entre gestores de segurança de informação.

Um destes modelos adotado pela norma ISO 27002:2011 (ISO/IEC, 2011b) é o modelo CID constituído pelas propriedades confidencialidade, disponibilidade e integridade, as quais compõem uma base de discussão para todas aquelas medidas de segurança de informação, para o qual são apresentadas as suas definições de acordo com Andress (2011).

- **Confidencialidade:** Propriedade que se refere à habilidade de proteger os dados de qualquer entidade que não tenha autorização para ler o conteúdo dos dados. Esta propriedade pode ser perdida com a perda de dispositivos, acessos não autorizados, roubo de informação por parte de entes alheios às organizações e ações similares.
- **Disponibilidade:** Propriedade que se refere à habilidade de garantir que os dados podem ser acessados pelas entidades autorizadas no momento que são explicitamente requeridos. Esta propriedade pode ser perdida caso a continuidade dos sistemas de informação não seja garantida, falhas de infraestrutura física ou se os recursos dos sistemas de informação são esgotados voluntaria ou involuntariamente.
- **Integridade:** Propriedade que se refere à habilidade de prevenir que os dados sejam alterados em formas não desejadas. Esta propriedade pode ser perdida no caso de acessos não autorizados que alteram a informação salva, ou mediante o "envenenamento" das origens de dados, situação que gera informação errônea.

Uma vez que a terminologia das questões de segurança tem sido definida, é também preciso definir terminologia relativa aos problemas de segurança que podem comprometer as propriedades de segurança, que por sua vez são apresentados a seguir.

- **Ativo de informação:** Um ativo é tudo aquilo que representa algum valor para uma organização, assim é considerado como ativo de informação todo objeto ou elemento de informação que seja necessário para a execução das atividades de negócio em uma organização determinada.

- **Ameaça:** Ameaça é tudo aquilo que tem o potencial de causar um prejuízo sobre um ativo. As ameaças geralmente são especificas dentro de cada contexto, podendo ser tecnológicas ou naturais.

- **Vulnerabilidade:** Vulnerabilidade é uma fragilidade de um ativo que pode ser explorada por uma ameaça com o objetivo de causar uma perda. Da mesma forma que as ameaças, as vulnerabilidades geralmente são especificas de cada ativo e contexto.

- **Impacto:** Impacto são todos aqueles eventos inesperados e indesejados que acontecem quando uma ameaça explora uma vulnerabilidade satisfatoriamente.

- **Risco:** Risco é a predisposição de que uma ameaça consiga aproveitar as vulnerabilidades de um ativo causando impacto. Geralmente os riscos são expressos e medidos em termos de probabilidade de que os eventos indesejados ocorram.

Para mitigar ou prever o impacto negativo causado por estes riscos, se faz preciso criar controles de segurança, os quais podem pertencer às categorias seguintes:

- **Controles físicos:** São aqueles controles sobre as instalações físicas onde os sistemas de informação estão instalados ou onde a informação está sendo armazenada. Por exemplo fechaduras, guardas de segurança, sistemas de ar condicionado, sistemas de respaldo de energia.

  Apesar de que estes controles possam parecer fora do escopo da segurança de informação, realmente são os fatores mais críticos para garantir a continuidade dos sistemas de informação, já que se não existe habilidade de garantir a segurança física dos sistemas de informação, qualquer outro controle de segurança se torna irrelevante.

- **Controles lógicos:** Frequentemente chamados de controles técnicos, são todos aqueles controles de segurança visados para a proteção de sistemas, redes e entornos que processam, transmitem e armazenam informação. Por exemplo senhas, encriptação, controles de acesso lógicos, sistemas de *firewall* e sistemas de detecção de intrusões.

  Quando estes controles são estabelecidos de forma correta, significa que qualquer elemento interno ou externo não terá a capacidade de acessar informação fora do que tem-se pre-estabelecido para ele.

- **Controles administrativos:** Os controles administrativos são todas aquelas regras, políticas, procedimentos, guias que essencialmente são definidas em papel. Estabelecem o comportamento mínimo esperado dos membros de uma organização em diferentes níveis de autoridade. Por exemplo, políticas de mudança de senhas, rotação de pessoal, políticas de preferencias de fornecedores, controles de acesso baseados em responsabilidades entre outros.

  Por tudo isto, quando se menciona o termo "medidas de segurança de informação", são todos aqueles controles que são criados para evitar ou minimizar ataques sobre as propriedades de segurança dos diferentes ativos de informação.

2.2 Gestão de riscos de segurança de informação

Considerando os problemas de segurança de informação que uma determinada organização pode enfrentar, existe a necessidade de estabelecer uma política abrangente de segurança de informação para garantir a confidencialidade, integridade e disponibilidade dos ativos de informação vitais para o andamento continuo das atividades da organização.

Assim, as metodologias de gestão de riscos de segurança de informação surgem como uma resposta a esta necessidade, onde a gestão de riscos proporciona um guia destinado a coordenação de todas as atividades de implantação de controles de segurança de informação de forma sistemática.

De acordo com Coleman (2011), a gestão de riscos corresponde àquelas atividades, decisões táticas e estratégicas para controlar riscos oriundos de oportunidades que podem ser exploradas. O processo de gestão de riscos corresponde a ações para administrar a medição, quantificação e priorização dos riscos.

Para definir a importância da gestão de riscos Bernstein e Yuhas (2005) denotam que os riscos são transcendentais na vida de qualquer projeto, e que a marca de sucesso para qualquer projeto é estabelecida pela habilidade de identificar riscos e desenvolver planos de contingência para conviver com eles. Na mesma linha, Boehm (1991) ressalta que um conceito fundamental na gestão de riscos é a "exposição aos riscos", onde a exposição aos riscos é a probabilidade de obter uma saída não satisfatória de um processo, o que gera perdas para os afetados.

Atualmente, e especificamente dentro da área de gestão de riscos de segurança de informação, existem várias metodologias de gestão de risco, tais como COSO (MOELLER, 2011), Risk It (ISACA, 2009), NIST 800-30 (STONEBURNER; GOGUEN; FERINGA, 2002), as

quais por sua vez apresentam seus próprios requerimentos ou estão em conformidade total ou parcial com normas e padrões que estabelecem os requisitos básicos que devem ser considerados num processo de gestão de riscos, sendo uma das normas mais adotadas a norma ISO 27005:2011 (ISO/IEC, 2011c).

2.2.1 ISO/IEC 27005:2011

O objetivo da norma ISO 27005:2011 (ISO/IEC, 2011c) é fornecer diretrizes para a implantação de um processo de gestão de riscos, atendendo os requisitos para a implementação de um sistema de gestão de riscos de segurança de informação (SGSI) apresentados na norma ISO 27001:2011 (ISO/IEC, 2011a), a qual propõe a estrategia PDCA "Plan-Do-Check-Act" para estruturar todos os processos de segurança de informação.

A figura 2.1 apresenta as etapas que constituem o processo de gestão de riscos da norma ISO 27005:2011, onde pode-se observar que o processo tem natureza cíclica. Neste ciclo, a saída de uma etapa fornece informação para a continuação do processo, e do mesmo modo todas as informações geradas durante a execução do ciclo de gestão são utilizadas para melhorar a visão e retroalimentar a execução subsequente, melhorando e atualizando periodicamente a visão de riscos da organização.

Uma das características do processo definido na norma ISO 27005:2001 é que mesmo que ele seja constituído por etapas definidas, a norma não obriga a utilização de metodologias especificas para cada uma destas etapas. Assim, a norma é utilizada como um conjunto de requisitos e recomendações que proporcionam a liberdade para que cada organização tenha a possibilidade de escolher as metodologias que sejam adequadas às características da organização, setor de atividade econômica e contexto de segurança e riscos. As etapas que constituem o processo de gestão de riscos são descritas a seguir.

- **Definição do contexto:** Nesta etapa são definidos os critérios necessários para a gestão de riscos de segurança da informação, entre os quais se incluem a definição do escopo, definição dos limites e o estabelecimento de um grupo/organização apropriada para operar a gestão de riscos de segurança da informação.

- **Análise/avaliação de riscos:** Esta etapa determina um valor representativo dos ativos, as ameaças e as vulnerabilidades que podem gerar um impacto nos ativos. Além disso, esta etapa identifica os controles existentes e sua eficácia, estima as possíveis consequências

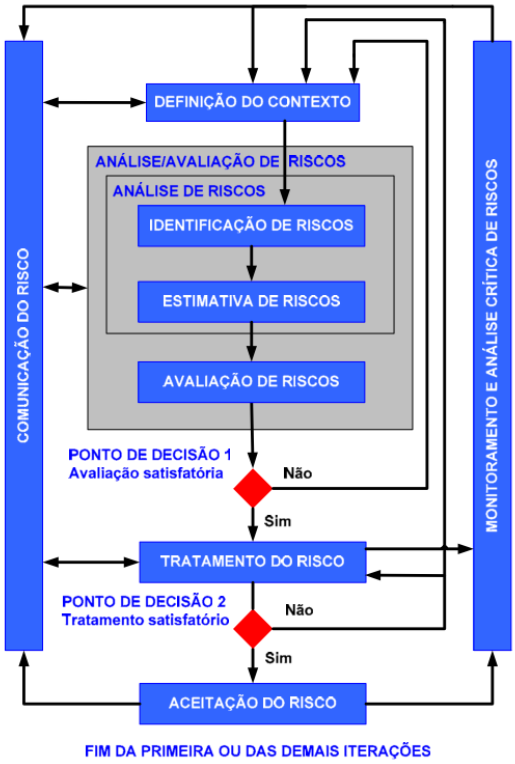

Figura 2.1 – Processo de Gestão de Riscos

de uma falha de segurança e prioriza os riscos de acordo com os critérios estabelecidos na definição do contexto. Do mesmo modo, esta etapa é composta por três subetapas que podem ser executadas isoladamente de forma iterativa, aprofundando a avaliação de riscos com cada uma das execuções.

- **Identificação de riscos:** O objetivo desta etapa é a identificação de riscos, para determinar posteriormente os eventos que tem o potencial de causar uma perda nos ativos de informação. Para isso a etapa determina como, onde e porquê a perda pode acontecer. Como resultado desta etapa é obtida uma lista de ativos, e uma lista de processos do negócio relacionados aos ativos e sua relevância.
- **Estimativa de riscos:** A estimativa de risco tem como objetivo estabelecer a magnitude das consequências potenciais e a probabilidade dessas consequências ocorrerem, geralmente esta etapa é executada mediante metodologias quantitativas ou qualitativas dependendo das características da organização. Como saída desta etapa é obtida uma lista de consequências, e a sua avaliação referente a um cenário de incidentes relativos aos ativos e critérios de impacto.
- **Avaliação de riscos:** A etapa de avaliação de riscos tem como objetivo compa-

rar os riscos estimados com os critérios de avaliação de riscos definidos durante a definição do contexto, obtendo como saída uma lista de riscos ordenados por prioridade de acordo com os critérios de avaliação de riscos e associados aos cenários de incidentes que os provocam.

- **Tratamento do risco:** A etapa de tratamento de riscos tem como objetivo responder a todos aqueles riscos que tem sido selecionados para serem tratados, visando minimizar o seu impacto caso ocorram. Com base na lista de prioridades obtida na avaliação de riscos, os gestores de riscos elegem entre reduzir, reter, evitar ou transferir os riscos, definindo com isso o plano de tratamento de riscos.

- **Aceitação do risco:** A etapa de aceitação de riscos tem como objetivo registrar formalmente a motivação e os responsáveis de todos aqueles riscos que vão ser assumidos. Com base na lista de prioridades obtida na avaliação de riscos, os gestores de riscos descrevem o porquê de cada um dos risco foi ou não foi aceito, obtendo como resultado uma declaração de aplicabilidade.

- **Comunicação do risco:** A fase de comunicação de riscos é de caráter permanente, representa a troca interativa de todas aquelas informações sobre os riscos obtidas através da gestão de riscos. É conveniente que todas as informações sobre riscos sejam compartilhadas entre os membros do comitê gestor de riscos e todas as outras partes interessadas, gerando um entendimento contínuo do processo de gestão de riscos de segurança da informação e dos resultados obtidos.

- **Monitoramento e análise crítica do risco:** Com base em todas as informações sobre os riscos obtida através das atividades da gestão de riscos, a etapa de monitoramento e análise crítica do risco tem como objetivo que os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente para manter uma visão geral dos riscos, gerando um alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização.

2.3 Metodologia para análise e avaliação de riscos por composição de métodos

Considerando a importância da fase de análise/avaliação de riscos e a constante necessidade de resultados cada vez mais precisos, o trabalho apresentado por Amaral, Amaral e Nunes

(2010) procurou incrementar a precisão das atividades da gestão de riscos mediante a redução de erros na priorização de riscos via uma composição de metodologias de avaliação.

O uso ponderado de diferentes métodos reduz a probabilidade de erro, ou seja, os resultados não dependem exclusivamente de um método, de modo que, quando acontece um erro num dos métodos, os outros métodos servem como base para melhorar a exatidão dos resultados, anulando assim os desvios por causa das disparidades entre as técnicas utilizadas pelos métodos para um mesmo contexto.

Para lograr a composição de métodos, são considerados como prioridade os riscos que são indicados pela maioria dos métodos mediante sete fases nas quais são definidas diretrizes para a sua aplicação prática como se apresenta na Figura 2.2.

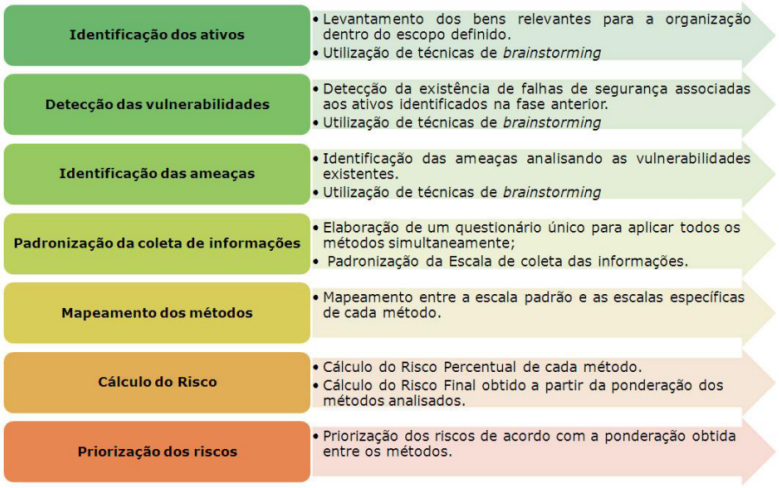

Figura 2.2 – Metodologia para análise e avaliação de riscos por composição de métodos
Fonte: Amaral, Amaral e Nunes (2010)

A composição de métodos, esta alinhada com as atividades descritas na norma ISO 27005:2011, onde a priorização de riscos é obtida baseando-se nos resultados individuais dos métodos ISRAM (KARABACAK; SOGUKPINAR, 2005), AURUM (EKELHART; FENZ; NEUBAUER, 2009), ARIMA (LEITNER; SCHAUMULLER-BICHL, 2009) e FMEA (STAMATIS, 2003). As etapas são descritas com maiores detalhes a seguir.

2.3.1 Identificação dos ativos

O primeiro passo é a identificação dos ativos. Entende-se como ativos primários todos aqueles ativos que tenham relação com "informação", incluindo Hardware, Software, Recursos de Rede, Recursos Humanos, Instalações Físicas, Estrutura da Organização e outros. O padrão adotado pela metodologia de composição de métodos para realizar a avaliação de riscos é o

brainstorming por ser uma técnica que procura representar a diversidade de opiniões e ideias.

A composição de métodos recomenda que os participantes do *brainstorming* sejam pertencentes a diferentes áreas e que os participantes tenham competências diferentes, mas que também tenham conhecimento considerável dos objetivos da organização, pois suas experiências agregam valor na obtenção de informações abrangentes para o processo de análise de riscos.

2.3.2 Detecção das vulnerabilidades

Logo depois de identificar os ativos, a detecção de vulnerabilidades é levada a cabo para verificar a existência de falhas de segurança nos ativos identificados. Assim, para cada ativo são identificadas todas as vulnerabilidades mediante *brainstorming* onde a relação entre ativos e vulnerabilidades é considerada de um-pra-muitos, já que um ativo pode ter inúmeras vulnerabilidades associadas.

2.3.3 Identificação das ameaças

Uma vez que as vulnerabilidades tenham sido identificadas, é preciso analisar as vulnerabilidades em relação com os seus ativos. Assim novamente para cada vulnerabilidade identificada é realizada uma sessão de *brainstorming* para identificar as possíveis ameaças, sendo que a relação entre vulnerabilidades e ameaças também possui uma relação de um-para-muitos já que uma vulnerabilidade pode ter inúmeras ameaças associadas.

É também recomendável que as ameaças identificadas sejam de natureza genérica em lugar de ameaças específicas já que a especificação de ameaças pode ser um processo demorado e muitas ameaças podem ser consideradas como parte de uma ameaça genérica maior -e.g. roubo de pendrives e roubo de computadores são ao mesmo tempo ameaças físicas de perda de informação-.

2.3.4 Padronização da coleta de informações

Uma vez que tem se identificado os ativos, vulnerabilidades e ameaças, é possível elaborar um questionário único com estas informações para padronizar a coleta de dados através de uma interação única que será utilizada posteriormente para calcular a prioridade de riscos.

Assim os participantes devem responder mediante uma escala Likert (muito baixa, baixa,

média, alta, muito alta) a melhor resposta que representa a sua opinião acerca de:

- **Probabilidade** da ameaça se concretizar;
- Dificuldade de **detecção** de ameaças antes de que elas atinjam os ativos;
- Frequência de **ocorrência** da ameaça; e
- **Impacto ou severidade** no caso que a ameaça concretize a exploração da vulnerabilidade.

2.3.5 Mapeamento dos métodos

Uma vez que a coleta de informação tenha sido padronizada, é também preciso estabelecer uma padronização entre os métodos da composição. Para isso, as estimativas coletadas mediante o questionário são mapeadas aos valores de cada metodologia conforme a Tabela 2.1.

Tabela 2.1 – Mapeamento entre os métodos que conformam a composição de resultados

Composição	FMEA and ISRAM	AURUM		ARIMA	
Escala padrão	Probabilidade e impacto	Probabilidade	Impacto	Probabilidade	Impacto
Muito Baixa	1	0.1	10	VL	L
Baixa	2	0.1	10	L	L
Média	3	0.5	50	M	M
Alta	4	1	100	H	H
Muito Alta	5	1	100	VH	H

2.3.6 Cálculo do risco

Logo depois do mapeamento, é o momento de calcular a prioridade dos riscos. Aqui, os valores são calculados com base nas fórmulas definidas em cada método considerando sua escala específica de pesos. Porém, para que os valores obtidos possam ser comparados é necessário que estejam na mesma escala. Para atingir este proposito, as equações são ajustadas mediante diferentes valores percentuais em relação ao seu total, obtendo como resultado as fórmulas apresentadas em (2.1) as quais são utilizadas para obter um valor representativo de cada método na mesma escala.

$$
\begin{aligned}
Arima &= ((i + ((p-1) * 0.5)) * 100)/5 \\
Isram &= ((p * i) * 100)/25 \\
Aurum &= ((p * i) * 100)/100 \\
Fmea &= ((s * o * d) * 100)/125
\end{aligned}
\tag{2.1}
$$

Vale a pena ressaltar que a fórmula para FMEA foi expressa em termos de probabilidade e impacto mediante uma aproximação numérica para encontrar valores equivalentes, já que todas as outras metodologias utilizavam estes valores unicamente.

A partir de aqui, os resultados são então agrupados mediante a equação (2.2) para cada um dos métodos entre todos os participantes, onde MTR_i = risco calculado mediante um método i, M_r = grupo de resultados que correspondem ao método e m = resultados individuais.

$$
MTR = \frac{\sum\limits_{m \in M_r} m}{|M_r|} \tag{2.2}
$$

Finalmente, o índice composto de riscos (CRI) -i.e. o indicador da prioridade do risco- é então calculado como a média aritmética dos riscos calculados por cada método, definido formalmente na equação (2.3).

$$
CRI = \frac{\sum\limits_{i \in [Arima, Isram, Aurum, Fmea]} MTR_i}{4} \tag{2.3}
$$

2.3.7 Priorização dos riscos

Dada a lista de valores CRI, é possível classificar os riscos existentes, pois estarão na mesma escala percentual, onde cada um dos membros do comitê de avaliação de riscos deve decidir se o risco será tratado ou aceito.

Apesar da padronização alcançada pela metodologia criada por Amaral, Amaral e Nunes (2010), a execução de um caso de estudo demonstrou que quando os efeitos negativos das divergências entre as metodologias são eliminados, a subjetividade da informação pode também gerar desvios nos resultados da análise/avaliação de riscos, sendo que esta subjetividade é um reflexo do uso de dados não determinísticos em forma de opiniões humanas capturadas mediante a entrevistas padronizadas.

2.4 Confiança e gestão de riscos

Clemen e Winkler (1999) estabelecem no seu trabalho que o "julgamento de especialistas" pode prover informação para previsões, tomada de decisões e análise/avaliação de riscos que de outra forma não seria possível obter, dado que existem evidências de que a informação subjetiva tem aumentado a efetividade de processos em áreas tão diversas como economia, tecnologia, meteorologia, predição de avalanches, inteligência militar e riscos ambientais, dentre outros.

Na mesma linha Senik (2005) ressalta o fato de que em diversas ocasiões, os dados subjetivos tem sido selecionados como um paliativo das falhas dos métodos econômicos tradicionais para representar interações não exclusivas das condições do mercado, as quais nem sempre são ajustadas baseando-se nos movimentos de preço, tais como preferências, interdependência, aprendizagem social e transações simbólicas.

Consequentemente, dentro da gestão de riscos é muito importante aproveitar as opiniões subjetivas, porém dando maior importância àquelas com maior nível de confiabilidade, já que a única forma de afirmar que as informações subjetivas são confiáveis, depende das origens dos dados, onde aqueles provenientes de origens verossímeis são percebidos como mais confiáveis (KO; KIRSCH; KING, 2005).

Para Mcknight e Chervany (1996) a confiança é a medida em que uma das partes está disposta a depender de algo ou alguém em uma determinada situação, com uma sensação de relativa segurança. Para Josang, Gray e Kinateder (2003), a confiança e os riscos são conceitos intimamente relacionados, já que os seres humanos utilizam a confiança como um parâmetro para avaliar relações que envolvem risco.

Lund, Solhaug e len (2010) expressam explicitamente que confiança e riscos são conceitos estreitamente relacionados, porque uma parte importante de administrar a confiança é o entendimento dos riscos envolvidos em interações onde saídas positivas e negativas são possíveis. Assim, a confiança é apenas uma crença mantida pelo outorgante em relação ao comportamento, de tal forma que a confiança é fundamental para confrontar decisões que precisam ser feitas, mesmo que exista falta de evidência acerca do comportamento futuro do depositário da confiança.

Dada a importância e as possibilidades que a confiança tem em relação aos riscos, se faz necessário utilizar modelos de quantificação que permitam estabelecer o nível de confiabilidade

de uma opinião, transação, participante ou qualquer outro elementos de risco dentro de um processo, por tal motivo alguns desses modelos são descritos a seguir.

2.4.1 Quantificação de confiança

A quantificação de confiança para a melhoria de processos que tem relação com decisões estratégicas e investimentos tem um largo histórico (MANCHALA, 2000; BACHMANN, 2006; MARTIN, 2008; TRUNITS, 2010), e dentro destes trabalhos, Manchala (2000) apresenta uma revisão sistemática de confiança em comércio eletrônico, onde a mesma tem sido utilizada para incrementar a segurança das transações por causa do incremento generalizado de clientes e do aumento que este tipo de comércio tem experimentado desde sua concepção.

Para Manchala (2000) a confiança é o melhor parâmetro para inferir se uma entidade terá o comportamento que se espera dela, ressaltando que a maioria das políticas de segurança em comércio eletrônico são desenvolvidas para neutralizar os possíveis problemas relacionados com falhas de segurança e riscos, tentando proporcionar uma garantia de que as transações serão realizadas unicamente pelos participantes autorizados, representando a confiança computacional mediante senhas, histórico de compras e outros indicadores.

Vale a pena ressaltar também que a definição de risco para o comércio eletrônico, não difere das definições expostas previamente, de modo que os riscos em transações eletrônicas são definidos como a probabilidade de que um processo possa apresentar resultados positivos ou negativos. De modo que se uma transação é considerada como arriscada, ela apresentará um impacto maior no caso do resultado ser uma perda.

Porém, a computação de confiança expressa em diferentes dimensões computacionais apresenta diversos desafios, já que a mesma é difícil de quantificar porque a maioria das ocasiões implica na criação de modelos computacionais complexos (GOLBECK, 2006) os quais geralmente são construídos com base em alguma das variáveis seguintes (MANCHALA, 2000):

- **Custo:** Na maioria de ocasiões, o risco de uma atividade é diretamente proporcional ao custo/valor da mesma, já que quanto maior e o custo, maior será o risco.

- **Histórico de transações:** O histórico de transações é uma medição direta da confiança onde transações com resultados positivos ou negativos podem ser utilizadas como um relatório de experiências não refutáveis no caso em que uma verificação seja precisa.

- **Compensação:** O nível de confiança de uma atividade é aumentado com a existência de

intermediários confiáveis e/ou intermediários que atuem como seguradores.

- **Padrões de desempenho:** É possível detectar atividade anormal baseado em trocas no padrão de comportamento das atividades.
- **Uso dos sistemas:** Quando o número de atividades aumenta em um sistema computacional, o risco aumenta como consequência da sobrecarga e as possível quedas do sistema.
- **Tempo:** O número de atividades num determinado período de tempo pode ser um indicador de atividade suspeita.
- **Inclusão:** Ao contrário da compensação, as atividades que envolvem intermediários que tenham sido comprometidos no passado diminuem a confiança.

2.4.2 Modelos e tipos de confiança computacional

Considerando a existência de diversas variáveis que representam as diferentes dimensões de confiança para a criação de modelos de quantificação, é preciso definir previamente uma tipologia para o entendimento da confiança como um conceito computacional.

Pinyol e Sabater-Mir (2011) indicam que em anos recentes tem sido criadas diferentes classificações e modelos de confiança computacionais, onde a classificação mediante características cognitivas tem ganhado maior destaque, já que a maioria da literatura da área utiliza este tipo de classificação sem que exista um padrão ou norma das características a ser consideradas.

Dentro deste tipo de classificações (SABATER; SIERRA, 2005; PAOLUCCI; BALKE; CONTE, 2006; BALKE; KöNIG; EYMANN, 2009) um dos trabalhos mais difundidos na literatura de ciências da computação é o trabalho de Sabater e Sierra (2005), onde a confiança é classificada de acordo com diferentes dimensões, sendo estas o paradigma adotado pelo modelo de confiança, origens de informação, visibilidade, granularidade, comportamento e tipo de opiniões. Estas dimensões são descritas a seguir.

- **Paradigma:** Os dois paradigmas de confiança mais comuns são os paradigmas numéricos e cognitivos. O primeiro paradigma se refere a modelos onde a confiança é construída em base a crenças e escalas, deixando de lado uma representação explicita de atitudes cognitivas que descrevam confiança e reputação. Por outro lado o paradigma cognitivo geralmente é utilizado para criar modelos de representação social, ou seja, que consideram

atitudes cognitivas entre os relacionamentos estabelecidos entre os entes cuja confiança está sendo quantificada.

- **Origens de informação:** Os modelos de confiança e confiança como conceito podem se classificar de acordo com as origens de informação que os modelos de quantificação utilizam para determinar confiança ou reputação, sendo estes:

  - **Experiências diretas:** São as origens de dados que geram melhores resultados, existindo a possibilidade de quantificar interações diretas (DI) e observações diretas (DO).
  - **Informação de testemunhas (WI):** É qualquer informação de um ente acerca da confiabilidade de outro ente com o qual tem interagido previamente.
  - **Informação sociológica (S):** Análise de relacionamentos entre os entes, geralmente é computada se existe informação de redes sociais.
  - **Prejulgamento (P):** Geralmente são utilizados quando não existe nenhuma outra informação para inicializar processos de quantificação de confiança, sendo os estereótipos uma das formas mais frequentes de prejulgamento.

- **Visibilidade:** Nesta dimensão, a confiança entre entes pode ser considerada como uma propriedade global que todos os entes podem observar, ou podem ser consideradas como propriedades privadas e subjetivas que cada ente constrói baseado nas suas relações com outros entes.

- **Granularidade:** Se refere à magnitude da dependência do contexto que um modelo de quantificação possuí, já que a estimação da confiança de um objeto em particular depende do contexto no qual esta inserido, -e.g. a confiança nas habilidades duma pessoa para dirigir um carro não terá o mesmo nível caso o contexto seja um jogo de futebol-.

- **Hipóteses de comportamento:** A maioria dos modelos de quantificação de confiança consideram três níveis de comportamento esperados por parte dos entes:

  - **Nível 0:** Modelos de quantificação onde os entes maliciosos -i.e. aqueles que proporcionam informação errada- não são considerados.
  - **Nível 1:** Modelos que consideram entes que ocultam informação, mas que desconsideram a possibilidade de que informação errada seja proporcionada.

  - **Nível 2:** Modelos onde entes que fornecem informação errada são considerados.

- **Tipo de opiniões:** De forma geral existem dois grandes tipos de opiniões de confiança, de tal forma que existem dois tipos de modelos, aqueles que consideram a confiança como informação discreta ou binaria, e modelos que representam a confiança mediante valores de intervalos contínuos e permitem análises mais aprofundadas.

2.4.3 Técnicas de quantificação

De acordo com Manchala (2000) e Grandison (2003) existem duas categorias no que se refere a técnicas de quantificação de confiança, sendo estas: i) técnicas baseadas em modelos numéricos e ii) técnicas baseadas em lógica difusa.

Ambos tipos de técnicas têm como objetivo explicar a noção de confiança que existe entre um grupo de agentes, permitindo decidir se um relacionamento baseado em confiança pode ser estabelecido, além do valor inicial apropriado para esta confiança. Os modelos numéricos representam a confiança como um valor real e arbitrário que pode ser utilizado por processos computacionais, enquanto os modelos de lógica difusa representam a confiança como etiquetas linguísticas que representam um intervalos possível de valores, podendo definir também modelos matemáticos para manipular numericamente as etiquetas.

Para conhecer um pouco destas técnicas, a seguir são descritas as características de algumas destas abordagens.

- **Técnicas de quantificação direta:** Neste tipo de modelos duas ou mais variáveis podem ser utilizadas para descrever o nível de confiança de uma transação, com a única limitante que as variáveis tem que ter uma relação logica para fornecer uma significância na definição do modelo de confiança. Como exemplos deste tipo de técnicas pode se mencionar (MARSH, 1994) e (SEN; SAJJA, 2002).

- **Técnicas baseadas em análise de reputação:** Muitos sistemas de comércio eletrônico utilizam este tipo de modelos. Como norma geral tanto os compradores quanto os vendedores mantêm um histórico das transações passadas -i.e. reputação- para ser utilizado posteriormente durante as avaliações de confiança. Alguns exemplos deste tipo são (MANCHALA, 2000) e (XIONG; LIU, 2003).

- **Técnicas baseadas em cadeias de confiança:** Neste tipo de técnicas, as noções de confiança para cada um dos membros da transação são utilizadas em conjunto para estabelecer

o nível total de confiabilidade das transações, fornecendo uma visão geral do nível de confiança dos relacionamentos. Como exemplo deste tipo de técnicas pode-se mencionar (CHANG et al., 2008) e (HE et al., 2010).

- **Técnicas baseadas em análises probabilísticas:** A ideia básica deste tipo de técnicas é que o comportamento das partes que constituem uma transação pode ser modelado como uma distribuição probabilística a partir de um conjunto de saídas de interações prévias, sendo êxito ou fracasso as mais frequentes. Assim a tarefa de computar a confiança é realizada mediante a inferência dos parâmetros da distribuição comportamental de uma das partes. Como exemplos deste tipo de técnicas pode se mencionar (BOREALE; CELESTINI, 2013) e (CHAN; CHO; ADALI, 2012).

- **Técnicas baseadas em análise de redes sociais:** Este tipo de abordagens são ideais diante da necessidade de considerar a estrutura para a construção de confiança e a disseminação de informação acerca de confiança. O uso de confiança em redes sociais nasce das condições próprias das redes sociais onde membros interagem entre eles, motivo pelo qual a confiança tem um papel fundamental no sucesso das comunidades. Pode se mencionar como exemplos (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003) e (ZHOU; HWANG; CAI, 2008).

2.4.4 Seleção de um modelo de quantificação de confiança para gestão de riscos

Apesar das inúmeras possibilidades que se adquirem com o uso dos modelos de quantificação de confiança, como foi demonstrado anteriormente, o processo de quantificação de confiança não é trivial, dado que é preciso selecionar, adaptar ou criar um modelo em particular.

Lukas e Walgenbach (2010) afirmam que o mínimo de características que um modelo de confiança deve ter para ser considerado satisfatório é:

1. A quantificação deve considerar a presença de perdas;

2. A quantificação deve evitar ingenuidade;

3. A confiança precisa evoluir através do tempo e incrementar ou decrementar o seu valor de acordo com os resultados obtidos em atividades prévias.

Alguns dos modelos que cumprem com estas características são quantificação direta, modelos tradicionais de reputação (MANCHALA, 2000) e finalmente modelos de redes sociais

(BURT; KILDUFF; TASSELLI, 2013), onde este últimos foram eleitos tendo em conta seu suporte para características complexas, sendo estas:

- As redes sociais criam modelos de confiança baseados tanto em experiências quanto nas relações entre entes existentes (CROSS; PARKER; BORGATTI, 2002);
- A modelagem com redes sociais incrementa a robustez dos modelos de quantificação de confiança, sendo este um dos motivos para o incremento do seu uso em ambientes tradicionalmente baseados em modelos de reputação simples (PINYOL; SABATER-MIR, 2011);
- A maioria dos modelos de confiança baseada em redes sociais apresentam as características enumeradas por Lukas e Walgenbach (2010).

2.5 Redes sociais

As redes sociais são estruturas de suporte para o estudo das interações sociais, conformadas por nós ou agentes conectados por enlaces que representam interações entre eles (TSVETOVAT; KOUZNETSOV, 2011), onde estes enlaces podem ser relações do tipo valores, ideias, amizade, intercâmbio de produtos, comunicação, entre outros.

Tradicionalmente, o uso de redes sociais como ferramenta de análise requer que as propriedades seguintes sejam consideradas:

- **Homofilia:** Uma tendência inerente de qualquer individuo para se associar e desenvolver laços com seus semelhantes, o que significa que as redes pessoais de cada individuo terão certo nível de homogeneidade conformada em base a aspectos demográficos, pessoais e de comportamento, o que consequentemente limita o tamanho das mesmas. Este limite de redes tem implicações fortes já que influencia a forma em que os indivíduos recebem informações, as atitudes que eles tomam, e as interações e as experiencias que eles desenvolvem (MCPHERSON; SMITH-LOVIN; COOK, 2001).
- **Fenômeno do mundo pequeno:** O fenômeno descreve que no máximo existirá uma separação de seis agentes entre um par aleatório de membros da rede social (WATTS, 1999). Nesta linha, existe evidência que confirma este fenômeno em redes sociais online, redes de e-mail, redes formadas por atores de cinema, diretores de organizações e a comunidade científica (WATTS, 2003). Porém este fenômeno não implica que o mundo moderno seja

em si mesmo um mundo pequeno, já que ele é mais parecido a um conjunto de mundos pequenos fracamente acoplados entre eles.

Cross, Parker e Borgatti (2002) afirmam que a construção de conhecimento organizacional como a confiança entre colegas de uma mesma organização é um processo social, onde a velocidade da construção deste conhecimento é totalmente dependente da facilidade com que os indivíduos e as unidades organizacionais trocam informação, existindo assim uma oportunidade de identificar pessoas com uma função de liderança entre seus vizinhos.

O indicador da liderança é conhecido computacionalmente como centralidade (TSVETOVAT; KOUZNETSOV, 2011), uma medida de poder, influência ou conjunto de características individuais que indica a importância de uma pessoa dentro de uma rede social. Este indicador pode ser calculado baseado em diferentes critérios, tais como:

- **Grau de centralidade:** Métrica que indica o número de conexões entrantes e saintes para cada agente da rede social.
- **Proximidade:** Métrica que indica o alcance das mensagens emitidas por um agente dentro de uma rede social.
- **Gargalo:** Métrica que indica se um agente constitui um gargalo, e por tanto uma ponte fundamental na difusão de conhecimento.
- **Medições compostas:** Métricas complexas dependentes de contexto construídas a partir de variáveis que indicam a importância de um agente dentro do contexto especifico.

2.5.1 Quantificação de confiança com redes sociais

Sherchan, Nepal e Paris (2013) afirmam que a quantificação de confiança com redes sociais tem experimentado um incremento de interesse por parte da academia e indústria, aumento motivado principalmente pelo incremento na adoção de redes sociais online o que significa que a informação para análise é cada vez mais acessível.

Para entender as diferenças entre as propriedades dos métodos de quantificação de confiança em redes sociais deve-se considerar que os métodos são geralmente dependentes de contexto e da informação disponível. Os modelos e propriedades que fazem um método diferente do outro são descritos nas subseções a seguir.

- **Modelo de coleta de informação:** A informação para quantificar confiança pode ser coletada mediante três origens:

  - **Atitudes:** As atitudes são representações cognitivas do grau de afinidade que existe entre agentes, ou seja, a visão positiva e negativa que um agente apresenta em relação a outro membro da rede social (BAGHERIAN et al., 2009). Existe a possibilidade que os agentes sejam ambivalentes, o que significa que um agente pode apresentar uma visão positiva e negativa ao mesmo tempo para as características de outro agente (ZAHED-BABELAN, 2012). Ao contrario da personalidade, as atitudes são desenvolvidas mediante experiências, assim autores como Jones (1996) argumentam que confiança é uma forma de atitude afetiva;
  - **Experiências:** As experiências são as evidencias que suportam a percepção dos membros de uma rede social em relação aos outros. As experiências podem ser de caráter implícito ou explicito, onde as primeiras são produto de fatores externos e as últimas são um produto de interações diretas entre agentes (SHERCHAN; NEPAL; PARIS, 2013). Para refinar as experiências pode-se utilizar mecanismos de *feedback*, já que experiências tanto positivas quanto negativas podem gerar mudanças nas atitudes entre agentes (PUJOL; SANGüESA; DELGADO, 2002);
  - **Comportamentos:** Os comportamentos são formalmente definidos como padrões de interações -i.e. padrões de experiências-, os quais influenciam diretamente no aumento e diminuição do nível de confiança percebido de cada agente. Mudanças significativas nos padrões de comportamento fazem com que os membros da rede social percebam que a atitude de um agente dentro da rede apresenta mudanças, o que representa uma razão válida para alterar a confiança que existe entre agentes (ROMER, 2000).

- **Modelo de avaliação e quantificação de confiança:** As abordagens de avaliação e quantificação de confiança podem ser classificadas em três grandes grupos: avaliações baseadas em análise estrutural, avaliações baseadas em análise das interações dos membros da rede, existindo ainda a possibilidade de combinar ambos abordagens.

  - **Avaliação estrutural:** É uma das formas mais básicas de análise de confiança. Este tipo de abordagem quantifica a confiança em relação a como os agentes estão relacionados dentro da rede, ou seja, o grau de centralidade. O número de conexões

entrantes e saintes de um agente pode ser um indicador da confiabilidade do agente, porém não é um indicador contundente considerando que as experiências que são geradas nestas relações podem ser tanto positivas quanto negativas (BUSKENS, 1998);

  - **Avaliação de interações:** Neste tipo de avaliação os modelos computam a confiança como um produto das interações entre agentes. Contrário às análises estruturais puras, este tipo de análise desconsidera a estrutura da rede social, a qual pode proporcionar informação significativa acerca de como os membros de uma comunidade estão relacionados (LIU et al., 2008);
  - **Avaliação hibrida:** Como seu nome indica, são avaliações que consideram a estrutura da rede social e as interações que nela acontecem. Neste tipo de modelo a avaliação implícita é realizada mediante as interações dos membros da rede, enquanto a avaliação explicita de confiança é realizada analisando a estrutura da rede (TRIFUNOVIC; LEGENDRE; ANASTASIADES, 2010).

- **Modelo de disseminação de confiança:** Considerando que a confiança dentro de uma rede social é dinâmica e evolui no tempo, Sherchan, Nepal e Paris (2013) identificaram dois modelos de disseminação de informação que podem ser utilizados: Disseminação baseada em recomendações e disseminação baseada em visualizações.

  - **Modelos baseados em recomendação:** Em este tipo de disseminação de informação, geralmente acontece uma agregação de opiniões, ou seja, a confiança de um agente para outro é um produto da combinação entre a percepção baseada em experiências entre agentes e a opinião que os vizinhos tem acerca do agente depositário de confiança.
  - **Modelos de visualização:** A visualização de conexões de confiança como um grafo é outro meio de divulgação de informações de confiança. Os grafos mostram a força da conexão entre dois agentes, e permitem eleger as conexões mais adequadas para disseminar informação, seja mediante a força da conexão, distância entre agentes e critérios clássicos de teoria de grafos.

2.6 TrustWebRank

Uma vez que a proposta desta pesquisa é aproveitar a confiança como um indicador da confiabilidade dos agentes dentro de uma organização, e consequentemente a confiabilidade das suas opiniões, foi preciso selecionar um modelo de quantificação compatível com as características da gestão de riscos.

Assim, diversas abordagens tais como EigenTrust (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003), Tidal-Trust (GOLBECK, 2006), PowerTrust (ZHOU; HWANG; CAI, 2008) e TrustWebRank (WALTER; BATTISTON; SCHWEITZER, 2009) foram considerados para modelar e quantificar a confiança existente na estrutura organizacional. Modelos que são descritos a seguir:

- **EigenTrust:** Um algoritmo de gestão de reputação projetado para redes peer-to-peer. O algoritmo cria um coeficiente de confiança para cada um dos membros da rede social baseando-se nos registros de compartilhamento de arquivos.
  Modelo de coleta de informação: Experiencias.
  Modelo de avaliação de confiança: Hibrido.
  Modelo de disseminação de confiança: Recomendações.

- **Tidal-Trust:** Um modelo de quantificação de confiança projetado para web semática. O modelo cria coeficientes de confiança a partir dos relacionamentos entre uma dupla de indivíduos utilizando um vocabulário FOAF. A abordagem é criada a partir da hipótese de vizinhos com maior coeficiente de confiança tem maior probabilidade de concordar acerca do comportamento de um terceiro em comum.
  Modelo de coleta de informação: Experiencias.
  Modelo de avaliação de confiança: Hibrido.
  Modelo de disseminação de confiança: Recomendações.

- **GossipTrust:** GossipTrust é um algoritmo projetado para a agregação de coeficientes globais de confiança para redes peer-to-peer. A sua principal contribuição radica no fato de que GossipTrust é aplicavel tanto para redes P2P estruturadas quanto dinâmicas, utilizando mensagens *Gossip* para a disseminação de informação.

Modelo de coleta de informação: Experiencias.
Modelo de avaliação de confiança: Hibrido.
Modelo de disseminação de confiança: Recomendações *Gossip*.

- **TrustWebRank:** TrustWebRank é um algoritmo projetado para sistemas recomendadores. A sua característica principal é que a confiança é quantificada de forma personalizada e dinâmica utilizando o conceito de *feedback centrality*, o que permite superar algumas das limitantes de outras métricas, particularmente que não é negligente diante da existência de grafos com ciclos.
  Modelo de coleta de informação: Experiencias personalizadas e estimativas.
  Modelo de avaliação de confiança: Hibrido.
  Modelo de disseminação de confiança: Recomendações.

Com base nas carateristicas anteriores, o algoritmo TrustWebRank o modelo selecionado pelas seguintes razões:

1. TrustWebRank constrói a quantificações de confiança mediante uma combinação de experiências (DO) e atitudes presentes na rede social en forma de testemunhas (WI). Esta característica permite que o *bootstrap* da quantificação possa ser realizado unicamente com a quantificação das atitudes, o que consequentemente que elimina a dependência obrigatória em históricos de tratamentos de riscos ou de interações entre agentes para determinar a confiança;

2. O processo de evolução de confiança de TrustWebRank foi originalmente construído para representar evoluções de confiança humanas, baseado em acumulação de resultados e disseminação de informação mediante recomendações.

3. Desde a sua publicação TrustWebRank evoluiu em diferentes contextos, tais como redes sociais distribuídas (CARCHIOLO et al., 2010), formação de coligações (WALTER, 2011), avaliação de confiança distribuída (CARCHIOLO et al., 2012), fator que indica a flexibilidade deste modelo;

4. TrustWebRank foi projetado para fazer predições de confiança sobre agentes que não apresentam relações diretas de confiança, o que para o contexto de gestão de riscos sig-

nifica que não é obrigatória uma relação direta entre todos os membros da organização sempre que eles estejam numa rede social conexa.

Formalmente TrustWebRank é definido como um modelo de quantificação de "confiança personalizada" utilizando recomendações para avaliar a confiança direta e indireta entre uma dupla de agentes i e j. Assim, a confiança direta é a confiança imediata que existe entre a dupla de agentes, enquanto a confiança indireta é inferida a partir da confiança direta e das opiniões dos vizinhos de i acerca da confiabilidade de j. A condição é que TrustWebRank deve ser utilizado dentro de um cenário que possibilite estabelecer relações de confiança entre os agentes, e que os agentes possam expressar a sua opinião acerca de objetos e/ou a confiabilidade de outros agentes que compõem a rede social.

Tabela 2.2 – Elementos do algoritmo de quantificação de confiança

Elemento	Significado
T_{ij}	Confiança direta de i para j
$\tilde{T}_{ij}$	Confiança indireta de i para j
$N(i)$	Conjunto de agentes vizinhos de i
β	Fator de limite de alcance de TrustWebRank
T	Matriz de valores de confiança direta entre agentes
S	Matriz estocástica com confiança direta normalizada
$\tilde{T}$	Matriz estocástica com o conjunto de confianças indiretas inferidas mediante TrustWebRank

Para a compreensão das atividade executadas por TrustWebRank, considere-se os elementos listados na Tabela 2.2. Por definição, a confiança indireta $\tilde{T}_{ij}$ entre um par de agentes i e j corresponde à soma entre a normalização da confiança direta de i para j (S_{ij}) e o somatório da relação de confiança direta normalizada de i para os agentes k que pertencem ao grupo $N(i)$ e a respectiva confiança indireta dos vizinhos de i ($N(i)$) para j, ajustado por um parâmetro de controle de alcance $\beta = 0.8$. A equação (2.4) formaliza este cálculo, onde cada um dos valores da normalização é dado pela equação (2.5).

$$\tilde{T}_{ij} = S_{ij} + \beta \sum_{k \in N_i} S_{ik} \tilde{T}_{kj} = 1 \qquad \forall i, j \tag{2.4}$$

$$S_{ij} = \frac{T_{ij}}{\sum\limits_{k \in N_i} T_{ik}} \tag{2.5}$$

Embora TrustWebRank tenha sido projetado para ser executado por cada agente de forma independente, ou seja, passo-a-passo, as propriedades do modelo permitem que ele possa ser expresso em forma matricial como se apresenta na equação (2.6), onde I representa a matriz identidade.

$$\tilde{T} = (I - \beta S)^{-1} S \tag{2.6}$$

Adicionalmente às formas anteriormente apresentadas, existe uma opção de calcular os valores de confiança indireta de TrustWebRank utilizando uma abordagem iterativa como se expressa na equação (2.7), motivado principalmente pelo fato que a inversão da matriz da equação (2.6) representa um custo computacional alto que pode não ser ideal em redes de grande escala.

$$\tilde{T}_{ij}^{(k+1)} = S_{ij} + \beta \sum_{l \in N_i} S_{il} \tilde{T}_{lj}^{(k)} = 1 \qquad \forall i, j \tag{2.7}$$

TrustWebRank atualiza os coeficientes de confiança utilizando uma equação denominada função de utilidade, onde a atualização da confiança de um agente i para um agente j é definida como a diferença entre a opinião do agente i para o objeto o e a predição de j para o objeto o, denominada $u_{ij}(t)$, a qual posteriormente é utilizada para calcular o novo valor de confiança $\breve{T}_{ij}$ mediante a equação (2.8), onde o valor de $\gamma = 0.6$ é um parâmetro de controle da expansão das recomendações definido pelos criadores do algoritmo.

$$\breve{T}_{ij} = \begin{cases} \gamma T_{ij}(t) + (1-\gamma)|u_{ij}(t)| \\ if\ u_{ij}(t) > u_{thr}\ or\ -u_{thr} \leq u_{ij}(t) \leq 0 \\ \gamma T_{ij}(t) - (1-\gamma)|u_{ij}(t)| \\ if\ u_{ij}(t) < -u_{thr}\ or\ 0 \leq u_{ij}(t) \leq u_{thr} \end{cases} \tag{2.8}$$

2.7 Conclusões parciais

Atualmente, os sistemas de informação assumem um papel estratégico e relevante dentro das organizações, porém esta dependência faz com que estes sistemas se encontrem cada vez mais expostos a diversos tipos de ameaças, motivo pelo qual é preciso identificar as ameaças que colocam em risco os ativos da organização. A identificação e gerenciamento de ameaças geralmente implica no uso de metodologias de gestão de riscos, as quais podem apresentar divergências por causa da subjetividade do julgamento humano, situação que pode comprometer

o resultado final. Como a literatura expõe a confiança e o risco são conceitos estreitamente relacionados. A confiança pode ser utilizada como um parâmetro para avaliar o nível de confiabilidade de um membro de uma organização e por conseguinte a confiabilidade das suas avaliações de risco. Porém, o cálculo de confiança é considerado um problema complexo e altamente dependente de contexto. Em anos recentes modelos robustos de quantificação de confiança tem utilizado redes sociais como suporte para análise organizacional, dado que esta considera os relacionamentos que existem no entorno, os quais podem descrever características das interações que existem entre os membros da organização.

Neste capitulo foram apresentados conceitos fundamentais de confiança computacional e gestão de riscos, com o objetivo de prover uma fundamentação teórica para a criação de um processo de quantificação de confiança como suporte às atividades da gestão de riscos de segurança de informação, apresentado no capitulo 3.

3 QUANTIFICAÇÃO DE CONFIANÇA COMO UM PARÂMETRO DE REDUÇÃO DE DESVIOS DE RESULTADOS POR CAUSAS HUMANAS

Este capítulo apresenta a metodologia de gestão de riscos com quantificação de confiança para redução de desvios nos resultados. Primeiro são descritas as premissas sobre as quais a proposta foi criada (seção 3.1) e depois é realizada uma descrição e detalhamento de cada um dos componentes que constituem a metodologia (seção 3.3). Posteriormente é apresentada a interação entre os componentes da proposta (seção 3.4), os trabalhos relacionados (seção 3.5) e finalmente são apresentadas as conclusões parciais do capítulo (seção 3.6).

3.1 Premissas de funcionamento

Dado que as metodologias de gestão de riscos são dependentes de contexto, a seguir são descritas as condições ambientais sobre as quais é proposta a solução para a redução de desvios:

1. **Estrutura da organização** Assume-se que é possível mapear a estrutura da organização a ser analisada através de uma rede social informal, formada por enlaces que representam a interação entre os membros da organização, os quais atuam como agentes. Esta estrutura tem sido utilizada como ferramenta para mapear a dinâmica real de comunicação entre membros de uma organização, com o objetivo de comparar a dinâmica real frente à dinâmica definida na documentação interna das organizações (ALLEN; JAMES; GAMLEN, 2007).

2. **Confiança inicial** Assume-se que no inicio da gestão de riscos existe um nível de confiança quantificável entre os membros da organização como produto das interações entre eles, ou seja, informação de testemunhas (WI). Adicionalmente, também se assume que esta confiança pode ser utilizada como confiança *bootstrap* para que a confiabilidade das opiniões seja considerada a partir da primeira execução. De acordo com Golbeck (2006) existem diversas técnicas tais como métricas de desempenho, qualificações semânticas e outras.

3. **Cultura organizacional** Assume-se que a organização onde as atividades de gestão de risco serão realizadas apresenta as seguintes características:

(a) a organização tem os recursos para implementar todas as fases do ciclo de gestão de riscos, especialmente a etapa de monitoramento;

(b) a organização tem a disposição de atualizar a percepção de confiança baseada em resultados de tratamentos de riscos anteriores -i.e. observações diretas (DO)-;

(c) a organização não requer um nível especifico em relação ao comportamento malicioso, portanto é possível utilizar um modelo de nível 0 (sem tratamento de comportamento malicioso);

(d) as atividades do processo de análise/avaliação de riscos são executadas por um comitê gestor de riscos em representação de todos os membros da organização.

3.2 Visão geral da metodologia proposta

O objetivo alvo da inclusão da quantificação de confiança dentro das atividades da análise/avaliação de riscos é a redução dos desvios de resultados por causas humanas. Assim, a principal ação para alcançar esta redução é o estabelecimento do nível de confiança das opiniões com relação aos riscos de segurança de informação que a organização confronta, o que posteriormente permite utilizar a confiança quantificada para dar enfase às opiniões que sejam consideradas como mais confiáveis baseado na relação que existe entre a confiabilidade do emissor e as suas opiniões. Para lograr este objetivo, a metodologia estabelece um nível de confiança como parte das atividades de gestão de riscos, e este nível é refinado conforme os resultados do tratamento de riscos sejam disponibilizados, dinâmica exemplificada na Figura 3.1.

Para refinar os coeficientes de confiança, a metodologia aproveita a natureza cíclica da gestão de riscos. Assim, no inicio de cada ciclo de gestão os coeficientes de confiança de cada um dos participantes são criados ou atualizados (quantificação de confiança). Logo, estes coeficientes são utilizados como pesos matemáticos dentro da fase de análise e avaliação de riscos, o que dá como resultado a lista de prioridade de riscos formada por valores de índice composto de riscos (Composite Risk Index - CRI), que agora consideram a confiança do emissor das avaliações dentro do valor de prioridade de cada risco. Depois, esta lista ponderada com os coeficientes de confiança é utilizada para efetuar as atividades de tratamento de risco, ao mesmo tempo que o desempenho deste tratamento é monitorado, registrando a efetividade das opiniões em relação aos resultados obtidos no tratamento de riscos através de indicadores chave de risco

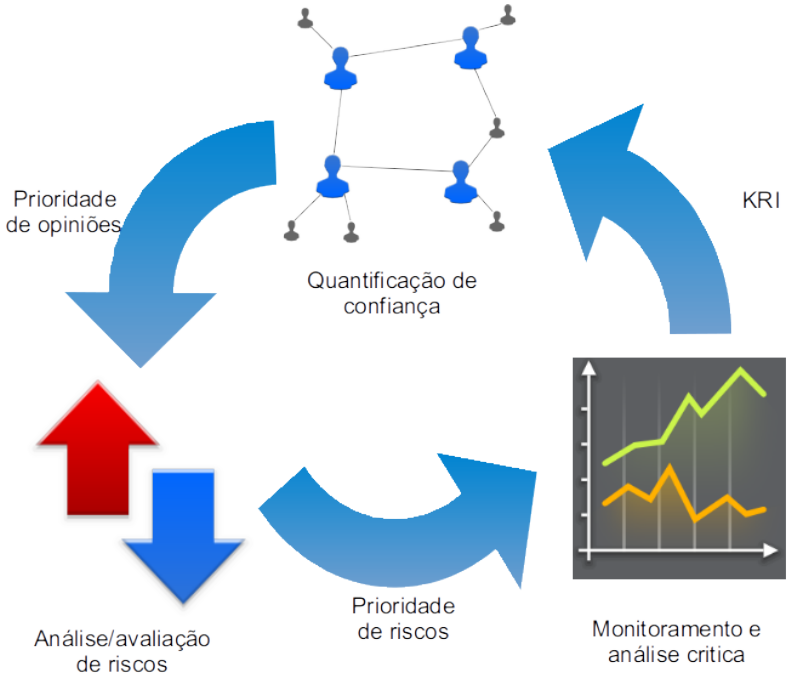

Figura 3.1 – Visão geral do uso da metodologia

(Key Risk Indicators - KRI). Os coeficientes de confiança são então atualizados com base nestes resultados.

3.3 Componentes da metodologia de gestão de riscos baseada em confiança

A metodologia proposta é baseada no ciclo de gestão de riscos definido na norma ISO 27005:2001 (vide seção 2.2.1). De modo que foram modificadas as características de três técnicas existentes para introduzir a confiança dentro das atividades do ciclo de gestão de riscos, obtendo como resultado o ciclo de gestão de riscos apresentado na Figura 3.2.

Como pode-se observar na Figura 3.2, a metodologia propõe o uso de três coeficientes para a introdução de confiança dentro do processo de gestão de riscos, sendo estes:

1. $Relevncia$ Representa a confiança global quantificada para um individuo membro da organização;

2. CRI**:** Representa o nível de criticidade dos riscos, o qual é modificado na proposta para considerar a confiança do fornecedor das estimativas de risco; e

3. P_{risco}**:** Representa a efetividade do tratamento de riscos, sendo também utilizado para atualizar a visão de confiança baseando-se nos resultados do ciclo de gestão de riscos.

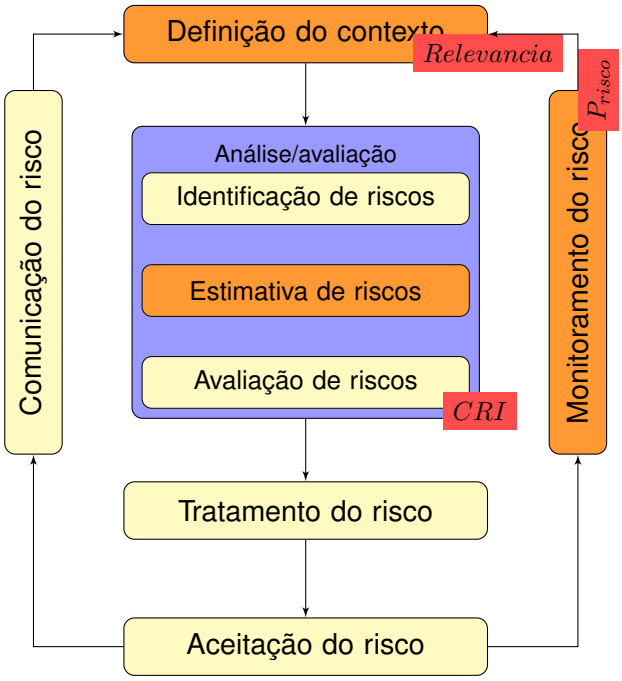

Figura 3.2 – Gestão de riscos com redução de desvios

A quantificação dos valores para estes coeficientes é descrita com maiores detalhes durante o restante do capitulo.

3.3.1 Quantificação de confiança

Considerando que as redes sociais são um método viável para quantificação de confiança em entornos com intervenção humana (vide seção 2.5), esta abordagem aproveita um modelo de quantificação de confiança denominado TrustWebRank (WALTER; BATTISTON; SCHWEITZER, 2009) (vide seção 2.6). Os coeficientes de confiança gerados por TrustWebRank representam as visões personalizadas de confiança que existem entre os participantes da rede social. Portanto, para a utilização do modelo dentro da gestão de riscos foi criado um coeficiente global que quantifica a confiança baseado nas percepções individuais, denominado $R = Relevancia$.

Para calcular o coeficiente de confiança adotou-se o TrustWebRank. A informação é coletada em forma de atitudes de confiança que existem entre os colegas de trabalho -i.e. informação de testemunhas (WI)- durante a primeira execução do ciclo de gestão de riscos, e em forma de experiências diretas mediante métricas de desempenho -i.e observações diretas (DO)- a partir da segunda execução, criando assim um modelo hibrido de quantificação de confiança mediante recomendações.

3.3.2 Análise/avaliação de riscos

Para a realização das etapas de análise/avaliação de riscos, foi adotada a metodologia de composição de métodos apresentada por Amaral, Amaral e Nunes (2010) onde o problema de desvios dos resultados foi percebido originalmente (vide seção 2.3), mas qualquer outra metodologia poderia ser utilizada.

Para introduzir a confiança quantificada dentro da fase de análise, foi selecionada uma abordagem de ponderações matemáticas simples -i.e em forma de multiplicações-, já que evidencia prévia tem demonstrado que este tipo de técnica apresenta melhor desempenho computacional em comparação com abordagens mais complexas e os resultados gerados são equivalentes (CLEMEN; WINKLER, 1999). Como resultado da introdução da confiança obtêm-se um índice composto de riscos ($CRI = CompositeRiskIndex$) que agora inclui a confiabilidade da opinião do avaliador.

Ressalta-se o fato que com a introdução do coeficiente de confiança o intervalo de valores para CRI será reduzido, como consequência da multiplicação entre os valores de confiança e estimativas de risco. Porém, esta situação não foi tratada devido a que o objetivo dos valores CRI não são utilizados em nenhuma outra equação, já que o único objetivo destes é fornecer um valor que possa ser interpretado como prioridade.

3.3.3 Monitoramento e análise crítica de riscos

Para monitorar e avaliar de forma crítica o desempenho das atividades de tratamento de riscos, este trabalho utiliza a quantificação do desempenho mediante indicadores chave de risco (KRI), dado que estes indicadores tem sido utilizadas em metodologias de gestão de riscos amplamente difundidas, tais como Risk IT (ISACA, 2009) ou COSO (MOELLER, 2011).

Os indicadores chave de risco são métricas instantâneas do estado dos eventos que propiciam a aparição dos riscos -i.e os eventos que promovem a exploração de vulnerabilidades-, de modo que os KRI são utilizados como ferramentas de retroalimentação, para que os gestores de riscos possam avaliar a efetividade da sua visão de riscos com cada novo ciclo da gestão de riscos. Além disso, a revisão constante dos KRI permite que atividades corretivas sejam executadas, especialmente quando o nível destes indicadores apresenta valores acima do limite aceitável para os eventos que propiciam os riscos.

Deve ser observado que para cada um dos riscos pode existir mais de um evento que propicie a sua aparição, e da mesma forma um evento pode ser causa da aparição de multiples riscos, criando assim uma relação entre eventos de riscos e riscos do tipo muitos-para-muitos. Consequentemente, para monitorar a efetividade do tratamento de riscos, este trabalho condensa os resultados do tratamento em um indicador de desempenho denominado P_{risco}, criado a partir da avaliação de tratamento de riscos apresentada por (TALBOT, 2012), onde a efetividade do tratamento de riscos é expressada como o estado esperado dos eventos de riscos e o estado alcançado por estes eventos durante o tratamento de riscos.

3.4 Interação entre os componentes

Nesta seção são detalhadas as fases da metodologia suportada pela confiança (ilustrada na Figura 3.2), definindo um roteiro para a aplicação da metodologia com o objetivo de proporcionar uma melhor compreensão da integração entre os elementos.

3.4.1 Definição de contexto e quantificação de confiança

Na etapa inicial do ciclo de gestão de riscos, é preciso estabelecer o escopo e limites do plano de gestão de riscos. Para cobrir esta necessidade a norma ISO 27005:2011 recomenda estabelecer pelo menos os itens seguintes:

1. Critérios básicos de avaliação;
2. Critérios básicos de impacto;
3. Critérios para aceitação de risco;
4. Escopo e limites; e
5. Criação de uma organização a cargo da gestão de riscos.

Seguindo as normas estabelecidas pela composição de métodos adotada, a ferramenta indicada para a definição destes itens é a realização de sessões de *brainstorming* entre as unidades organizacionais participantes da gestão de riscos, já que as técnicas de *brainstorming* procuram obter a maior diversidade de opiniões e ideias, mas permitindo chegar a consensos entre os participantes.

Paralelo à definição destes itens, a introdução de confiança requer que os coeficientes da mesma sejam quantificados antes de realizar qualquer outra atividade -i.e paralelo à definição de contexto-. Assim, para levar a cabo a quantificação de confiança, foi selecionada a forma matricial de TrustWebRank, já que esta permite realizar o cálculo de confiança indireta em uma única execução, sempre que os coeficientes de confiança direta entre participantes estejam disponíveis.

Durante a primeira execução do ciclo de gestão de riscos é preciso estabelecer o nível de confiança direta -i.e confiança *bootstrap*- que existe na forma de informação de testemunhas (WI) entre os individuos membros da organização. Para levar a cabo esta atividade, foi seleccionada como ferramenta a avaliação entre participantes mediante uma escala padronizada de qualificação semântica, na qual os participantes estabelecem um perfil de confiança para os seus vizinhos a partir de um conjunto de etiquetas semânticas que posteriormente são mapeadas para valores numéricos dentro do intervalo $[0 - 1]$. A Tabela 3.1 apresenta as equivalências entre as etiquetas e os valores.

Tabela 3.1 – Equivalência entre de etiquetas semânticas e valores iniciais de confiança

Etiqueta semântica (confiança no vizinho)	Valor atribuído
Confiança total	1
Confiança moderada	0.6
Confiança mínima	0.3

Depois que os valores iniciais de confiança são estabelecidos, as estimativas servem como dados semente para a execução do cálculo de quantificação de confiança indireta mediante TrustWebRank. O cálculo destes valores permite converter as visões de confiança entre pares de agentes, para valores que representam uma composição criada a partir das opiniões diretas, as opiniões dos vizinhos para o agente avaliado -i.e recomendações-, a confiança nas opiniões dos outros e a estrutura da rede social.

Como resultado do cálculo de TrustWebRank, é obtido um conjunto de visões personalizadas de risco, ajustadas pela confiança dos vizinhos. Porém para utilizar esses valores dentro das avaliações de riscos, é preciso converter-las para um valor que represente a confiança de cada agente como um todo, ou seja, um valor de confiança global criado a partir das percepções personalizadas. Consequentemente, foi proposta uma nova métrica denominada $R = Relevancia$, onde a relevância R_i de um agente i dentro da rede é definida como a média aritmética dos valores de confiança indireta de cada agente l, porém que apresentam um valor

de confiança para i acima do limite $\tau = 0.01$. A equação de relevância é formalizada em (3.1).

$$R_i = \frac{\sum\limits_{l \in N > \tau} \tilde{T}_{li}}{|N > \tau|} \tag{3.1}$$

O limite τ é necessário para descartar todos os valores de confiança que foram geradas mediante as recomendações mas que são pouco significativas, condição que também foi relatada numa das variantes de TrustWebRank(CHANDRA et al., 2012), motivo pelo qual conservou-se o valor τ=0.01.

Nota-se que o valor de relevância pode ser utilizado para selecionar os agentes que compõem o comitê gestor de riscos, tendo como critério a confiabilidade das suas opiniões. Porém, uma seleção baseada unicamente na confiança dos indivíduos não é obrigatória desde que a confiança das opiniões seja representada dentro das equações de estimativas de riscos.

3.4.2 Identificação de riscos

Em conformidade com a composição de métodos de Amaral, Amaral e Nunes (2010), o *brainstorming* é de novo a técnica adotada para realizar a identificação dos riscos. Porém, desta vez o *brainstorming* é realizado unicamente entre os participantes do comitê gestor de riscos. Mediante o *brainstorming* o comitê gestor define os ativos, vulnerabilidades e ameaças que se enquadram no escopo do contexto definido para a gestão de riscos, onde a combinação destas três variáveis da como resultado os riscos cuja gravidade será estimada e posteriormente tratada.

Como exemplo destes resultados a Tabela 3.2 apresenta um conjunto de possíveis valores de ativos, vulnerabilidades e ameaças dentro do contexto de infraestrutura de suporte para sistemas de informação.

Mediante a combinação das três colunas apresentadas en la Tabela 3.2 é possível definir os riscos que a organização confronta, por exemplo ao combinar os elementos da fila um se obtêm como resultado "o risco que o uso de senhas com baixa complexidade permita o vazamento de informações confidencias armazenadas no banco de dados".

Tabela 3.2 – Exemplo de identificação de ativos, vulnerabilidades e ameaças

Lista e ativos	Lista das vulnerabilidades	Lista de ameaças
Banco de dados	Baixa complexidade de senhas	Vazamento de informações confidenciais
Banco de dados	políticas de respaldo inadequadas	Perda de informação
Código fonte	Vazamento de código fonte	Vazamento de informações confidenciais
Computadores	políticas de uso inadequadas	Ataque de vírus/hackers
Servidores	Falha nos sistemas de energia	Comprometimento da continuidade do sistema
Funcionários	Doença	Baixa na produtividade
Sala dos servidores	Mecanismos de acesso simples	Acesso indevido à sala dos equipamentos
Usuários	Alta rotatividade de pessoal	Infiltração de espiões

3.4.3 Estimativa de riscos

Posterior à definição dos riscos, torna-se possível estimar a gravidade do impacto caso estes ocorram. Novamente em conformidade com a composição de métodos de (AMARAL; AMARAL; NUNES, 2010), esta etapa se realiza mediante a utilização de uma entrevista padronizada onde o comitê gestor de riscos expressa a sua opinião acerca da probabilidade, impacto/severidade, detecção e ocorrência de cada um dos riscos, mediante uma escala de Likert de 5 passos como foi descrito nas sessões 2.3.4 e 2.3.5, onde foi apresentado a equivalência entre os valores estimados e os valores numéricos para cada um dos métodos que fazem parte da composição.

Uma vez mapeados os valores, é possível estimar um valor numérico para a prioridade de cada risco, considerando agora a confiança. Como resultado uma variante das equações de composição de riscos consideram a relevância (R), conforme as equações (3.2).

$$\begin{aligned} Arima &= ((i + ((p-1) * 0.5)) * 100) * R_i/5 \\ Isram &= ((p * i) * 100) * R_i/25 \\ Aurum &= ((p * i) * 100) * R_i/100 \\ Fmea &= ((s * o * d) * 100) * R_i/125 \end{aligned} \tag{3.2}$$

A introdução do coeficiente de relevância faz com que as estimativas de riscos variem em função do valor da confiança, obtendo como resultado um conjunto de estimativas de riscos de magnitude $n_p * n_r * n_m$ onde n_p corresponde ao número de participantes do comitê de avaliação de riscos, n_r ao número de riscos e n_m ao número de métodos que constituem a composição (4).

Com este conjunto de resultados, é então preciso criar um valor unico e representativo de todas as metodologias que fazem parte da composição. Assim, a equação (3.3) colapsa os valores de todas as metodologias num único valor MTR através de uma média aritmética simples, reduzindo a magnitude do grupo de valores para $n_p * n_r$.

$$MTR = \frac{\sum_{m \in M_r} m}{|M_r|} \tag{3.3}$$

Finalmente, para guiar a tomada de decisões com relação aos riscos, os valores MTR são condensados para obter o valor CRI para cada um dos riscos r. De forma semelhante com a equação para o cálculo de MTR, a equação para o cálculo do CRI não sofreu nenhuma alteração, e o valor do CRI é calculado como a média aritmética do grupo de valores MTR_r que corresponde aos resultados concernentes ao risco r como se mostra na equação (3.4), obtendo como resultado uma lista de valores CRI de magnitude n_r que agora reflete a confiança nas opiniões dos avaliadores de riscos.

$$CRI = \frac{\sum_{i \in [Arima, Isram, Aurum, Fmea]} MTR_i}{4} \tag{3.4}$$

3.4.4 Avaliação de riscos

A partir da lista de valores CRI o comitê gestor de riscos tem a possibilidade de priorizar os riscos de acordo com o seu nível de criticidade, e consequentemente os riscos com maior valor CRI devem ser considerados com maior atenção, e consequentemente devem considera-se maiores recursos para estes riscos.

3.4.5 Tratamento e aceitação de riscos

Uma vez que os riscos tenham sido avaliados e ordenados por prioridade, o comitê gestor de riscos decide se cada um deles será aceito ou tratado. Para aqueles que sejam considerados prioritários no tratamento de riscos existe a possibilidade de tratá-los mediante quatro ações, sendo estas: reduzir, omitir, reter ou terceirizar.

Adicional à decisão entre tratamento ou aceitação, a nova metodologia tem como requerimento adicional a definição dos eventos que propiciam a aparição dos riscos. Esta definição é necessária já que a efetividade do tratamento de riscos constitui a base da atualização do modelo de confiança.

Para lograr a definição dos eventos de risco adotou-se novamente uma abordagem de $brainstorming$, onde se definem os eventos que propiciam a aparição dos riscos, cujo resultado se exemplifica na Tabela 3.3.

Tabela 3.3 – Exemplo de identificação de indicadores chave de risco

Risco	Indicadores chave de risco (KRI)	Sugestão de quantificação
Comprometimento da continuidade do sistema por falhas no fornecimento de energia para os servidores	Falhas no fornecimento da energia	Quantidade de falhas durante o ultimo trimestre
	Integridade da energia de respaldo	Porcentagem da integridade reportado pelos equipamentos no-break
	Suspensão programada do fornecimento de energia	Taxa de falhas programadas vs falhas imprevistas
Ataque de vírus por políticas de uso do computador inadequadas	Falhas dos computadores em produção	Quantidade de equipamentos danificados por causa de vírus
	Chamadas à área de suporte técnico	Quantidade de chamadas por causa de vírus
	Estado de atualização do software	Conformidade de atualizações com os reportes CVE publicados durante o ultimo mês

A Tabela 3.3 exemplifica a definição de indicadores chave de risco (KRI). Durante a definição dos KRI é obrigatório que para cada risco exista um conjunto de métricas que proporcionam uma visão do estado do tratamento do risco, e para cada uma destas métricas também é obrigatório definir a forma como elas serão quantificadas, já que a forma quantificação de cada KRI é dependente da natureza da métrica.

3.4.6 Comunicação de risco

Considerando que a fase de comunicação de riscos representa a troca interativa de todas aquelas informações sobre os riscos obtidas através da gestão de riscos, esta fase não precisa nenhuma alteração significativa em relação a introdução da confiança, e o seu objetivo é cumprido sempre que a informação acerca dos riscos e o seu tratamento seja compartilhada entre os interessados.

3.4.7 Monitoramento de riscos

Na etapa de monitoramento de riscos é definido como o desempenho do tratamento será avaliado em relação com as opiniões de risco. Assim, foi criado um indicador denominado P_{risk} o qual representa comparativamente o estado esperado dos eventos que propiciam o riscos e os indicadores de cada um destes eventos, ou seja, os KRI.

Como norma geral, os KRI são capturas instantâneas do estado atual dos eventos de risco, onde a captura destes valores é dependente da natureza dos mesmos existindo ainda a possibilidade de utilizar *frameworks* para a definição dos mesmos (IMMANENI; MASTRO; HAUBENSTOCK, 2004; DAVIES et al., 2006; The Institute of Operational Risk, 2010).

Consequentemente o indicador P_{risk} para um risco r foi modelado como a diferença entre a media aritmética do grupo de valores V_{MaxKRI} que contém o máximo valor alcançado pelos eventos que propiciam a aparição do risco r, e a média aritmética do grupo de valores $V_{Esperado}$ que contém o valor esperado para cada um dos KRI que têm uma relação com o risco r. Este cálculo é formalizado na equação (3.5).

$$P_{risk} = \frac{\sum\limits_{v \in V_{MaxKRI}} v}{|V_{MaxKRI}|} - \frac{\sum\limits_{v \in V_{Esperado}} v}{|V_{Esperado}|} \tag{3.5}$$

Como pode se observar na equação, se a magnitude da variável V_{MaxKRI} excede ou iguala a magnitude da variável $V_{Esperado}$ significa que o tratamento de risco teve um desempenho aceitável e consequentemente o valor de P_{risco} será positivo. Ao contrário, se o valor de $V_{Esperado}$ é menor do que o valor de V_{MaxKRI} significa que o tratamento de riscos não foi suficientemente bom para que todos os eventos que propiciam a aparição de risco atinjam seu estado esperado, motivo pelo qual é possível afirmar que ainda existe uma necessidade de investir maiores recursos no tratamento do risco r. Portanto P_{risco} constitui também um indicador da qualidade -i.e. confiabilidade por observação- das opiniões de risco dos participantes do comitê gestor de riscos.

Por ultimo, assume-se que o valor valor representativo do estado do evento de risco será mapeado para uma escala de valores com intervalo $[0, 1]$, e que a frequência de captura de valores será escolhida no momento de definir como este evento será monitorado, fato que restringe os possíveis valores de P_{Risk} para o intervalo continuo $(-1, 1)$.

3.4.8 Análise critica e atualização da confiança

Uma vez que o monitoramento dos KRI fornece informação para a análise das ações de tratamento de riscos, o grupo de gestão de riscos pode aproveitar essa informação para atualizar o contexto durante o reinicio do ciclo de gestão. Além disso, uma vez que tem se determinado de forma numérica a efetividade do tratamento de riscos mediante os valores P_{Risk}, é também possível retroalimentar o modelo de confiança com as observações diretas (DO).

Na sua definição original, TrustWebRank atualiza os coeficientes de confiança utilizando uma equação denominada função de utilidade (vide seção 2.6), porém dentro do contexto de gestão de riscos não é viável a utilização da equação original para o cálculo de $\breve{T}_{ij}$, já que o conceito de utilidade -i.e. a percepção de efetividade de uma recomendação- não existe, e além disso o valor de relevância (R) que foi utilizado dentro da composição de métodos é global e a confiança deve ser atualizada de par para par.

Assim, a equação de utilidade é simplificada como $u_{ij}(t) = P_{Risk}$, onde j pode ser qualquer agente que apresenta uma opinião acerca do risco correspondente a P_{Risk} -i.e. um membro da rede social que por sua vez seja membro do comitê gestor de riscos-, o que significa que as opiniões que qualquer agente i apresenta para as opiniões do avaliador j serão atualizadas em função dos resultados obtidos com as opiniões de j alterando a recomendação.

Para lograr esta atualização, foi criada uma nova versão da equação de atualização, desta vez reproduzindo um comportamento de atualização de tipo *"positivo devagar-negativo rápido"*, já que evidência prévia tem demonstrado que o incremento da confiança é um processo lento, mas o decremento da mesma não depende de muitos eventos onde o resultado seja uma perda ou decepção (JONKER; TREUR, 1999).

Enquanto o limite original γ foi mantido para regular o incremento de confiança, foi introduzido um novo limite κ onde a diferença de magnitudes entre os limites faz com que o decremento seja mais rápido do que o incremento, expressando também de forma direta a percepção de confiança original para que a atualização seja mais moderada. Esta nova versão é formalizada na equação (3.6) onde $\breve{T}_{ij}$ corresponde à atualização da confiança de i para o agente j e os valores para os coeficientes γ e κ são determinados mediante simulação na seção 5.2.

$$\breve{T}_{ij} = \begin{cases} T_{ij} + (1-\gamma)|P_{Risk}| \\ if\ P_{Risk} > 0 \\ T_{ij} - (1-\kappa)|P_{Risk}| \\ if\ P_{Risk} \leq 0 \end{cases} \tag{3.6}$$

3.5 Trabalhos relacionados

Um dos primeiros trabalhos que relatam os efeitos da subjetividade no contesto de análise/avaliação de riscos é o trabalho apresentado por Clarke (1988). No seu trabalho apresenta-se evidencia de que as decisões acerca de riscos tecnológicos são essencialmente politicas. Estabelecendo também que, no caso que o processo de análise/avaliação de riscos seja utilizado

para verificar a conformidade da empresa com regulamentações e não para definir estas regulamentações, os gestores de risco podem ser afetados pelo seu próprio julgamento, sugerindo também que os esforços para a redução de desvios devem ser focados em aqueles indivíduos que realizam as decisões relacionadas aos riscos.

No trabalho de Clemen e Winkler (1999), ressalta-se o fato que a informação subjetiva pode fornecer informação importante para as previsões de riscos, estabelecendo também que uma das maiores dificuldades para lidar com informação subjetiva é o método utilizado para determinar um consenso entre os avaliadores de risco, tanto para análises matemáticas quanto para análises de comportamento. As caraterísticas dos modelos matemáticos permitem a introdução de tratamentos corretivos, porém a maioria de estes métodos omitem a especificação de como estas melhorias devém ser introduzidas. Por outro lado, as análises de comportamento procuram o consenso confrontando os participantes mediante um processo de negociação, condição que pode criar polarização onde o domínio de um subgrupo é provável.

Workman (2012) relata que muitos dos autores dentro da literatura de tomada de decisões tentam aumentar a precisão das técnicas mediante fatores situacionais, porém a maioria desta literatura não considera os desvios que podem afetar esses fatores, sugerindo que os desvios de resultados são um problema de pesquisa ainda aberto e que precisa maiores estudos.

Banerjee (2011) tenta reduzir os desvios em análises/avaliações de riscos de segurança modificando a escala de percepção de riscos, baseando-se na hipótese que a percepção de riscos tem natureza logarítmica e não lineal como as soluções atuais (afirmação sustentada também por (FENG; LI, 2011)). Portanto o trabalho propõe uma escala de análise/avaliação de riscos onde as estimativas se ajustam a uma curva logarítmica e a linha de mediocridade de risco percebido é ajustada.

No mesmo contexto pero com uma abordagem gerencial, o trabalho de ao, Nunes e López (2012) foca seus esforços de redução de desvios mediante a utilização de uma seleção controlada dos membros do comitê de análise/avaliação de riscos. Esta seleção é realizada mediante a definição de competências que os participantes devem cumprir para fazer parte do comitê de avaliação de riscos, permitindo realizar a seleção dos participantes de uma forma fundamentada.

Dentro do contexto de *smart grids*, Lopez, Alcaraz e Roman (2013) propõe um mecanismo de alertas que monitora a aparição de padrões comportamentais dentro dos sistemas que conformam o *smart grid*. Este mecanismo cria alertas que devem ser executadas por operado-

res humanos, designando a responsabilidade de execução utilizando reputações. Este trabalho reconhece a existência de indivíduos com competências diferentes, determinando a reputação deles utilizando variaveis como *feedback*, criticidade da alerta, carga de trabalho do operador e tempo de resposta requerido para o incidente.

Finalmente Khambhammettu et al. (2013) apresenta um *framework* para análise/avaliação de riscos em sistemas de controle de acesso, especificamente para realizar as decisões relacionadas com autorizações mediante comparativas utilizando uma abordagem de quatro dimensões: sensibilidade do objeto, confiabilidade do usuário e dois enfoques que que combinam variáveis de sensibilidade e confiança.

Este trabalho difere dos anteriores pelas razões seguintes:

1. Apresenta a criação de uma técnica de redução de desvios para o contexto de análise/avaliação de riscos de segurança;

2. A proposta não requere a seleção dos participantes baseando-se em competências;

3. A escala de risco percebida não é reconfigurada e as modificações são introduzidas nas equações de consenso de opiniões;

4. É apresentado uma abordagem baseada em confiança que pode utilizar diversas origens de confiança inicial, sempre que estas origens possam ser mapeadas para um intervalo numérico.

3.6 Conclusões parciais

Neste capitulo foi proposta uma metodologia para a introdução da confiança computacional dentro das atividades da gestão de riscos de segurança de informação. Com o objetivo de minimizar o desvio nos resultados por causas humanas, ela implementa e modifica diversas técnicas sobre o ciclo genérico de gestão de riscos definido na norma ISO 27005:2011. Desta forma, as estimativas de riscos refletem a confiabilidade do avaliador de riscos, permitindo reduzir os desvios através da valorização de opiniões consideradas como mais fiáveis.

A abordagem apresenta um roteiro das atividades que devem ser realizadas em cada fase, facilitando o entendimento da interação dos componentes. A lista de priorização ao final de cada ciclo de gestão de riscos ajuda no melhoramento do coeficiente de confiança de cada membro do comitê avaliador de riscos.

4 CRIAÇÃO DE UM SIMULADOR DE AVALIAÇÃO DE RISCOS

Este capítulo apresenta criação de um simulador de gestão de riscos para avaliar as implicações da proposta apresentada no capitulo 3. Primeiro são descritas as características gerais do simulador (seção 4.1) e os seus componentes (seção 4.2), depois são descritas as opções de parametrização com as quais o simulador foi criado (seção 4.3) . Posteriormente o funcionamento geral do simulador é formalizado mediante pseudocódigo (seção 4.4), e finalmente são apresentadas as conclusões parciais do capítulo (seção 4.5).

4.1 Arquitetura do simulador de gestão de riscos

Considerando que a realização de vários ciclos de gestão de riscos mediante casos de estudo precisaria de um tempo considerável para gerar dados analisáveis, foi necessária a utilização de um simulador que permitisse avaliar a viabilidade e implicações da metodologia de redução de desvios.

Apesar da existência de diversos simuladores e metodologias consolidadas dentro do contexto de análise/avaliação de riscos -e.g. simulações determinísticas com método Monte Carlo (PAPAGEORGIOU; PASKOV, 1999)-, um dos principais problemas para a utilização destes simuladores é o fato que as análises são dependentes de contexto. Durante os últimos anos tem sido criados simuladores para contextos tão diversos como projetos de infraestrutura física (DAILAMI; LIPKOVICH; DYCK, 1999), proteção de infraestrutura critica (AUBIGNY, 2009), riscos financeiros (LIU, 2010), e mais recentemente riscos de segurança (ZHENG et al., 2013), onde cada um destes simuladores tenta resolver uma necessidade especifica não considerada pelos antecessores. Assim, o analise da literatura da área revelou que ate o momento não existe nenhum simulador de analise/avaliação de riscos que considere elementos próprios de redes sociais, motivo pelo qual foi necessária a criação de um simulador personalizado para os testes.

Um dos objetivos almejados durante a construção do simulador foi que mesmo que ele permitisse a personalização das condições de teste, as simulações teriam que ser executadas sem influenciar diretamente os resultados, evitando qualquer tipo de influência na forma de convergência para resultados ideais mas não realistas. Assim o simulador foi construído utilizando rotinas de geração de valores aleatórios para aqueles valores que normalmente seriam coletados durante o ciclo de gestão de riscos.

Com a criação das rotinas de geração, o usuário estabelece as condições de simulação através de perfis que representam intervalos predeterminados de valores, permitindo assim a introdução de um elemento de aleatoriedade onde o usuário tem a opção de selecionar perfis de comportamento para a geração de valores e a opção de estabelecer valores para os coeficientes de controle (β, τ, κ e γ), mas não tem a possibilidade de influenciar diretamente nos valores finais que serão utilizados dentro das formulas de estimativas de riscos e avaliação de desempenho.

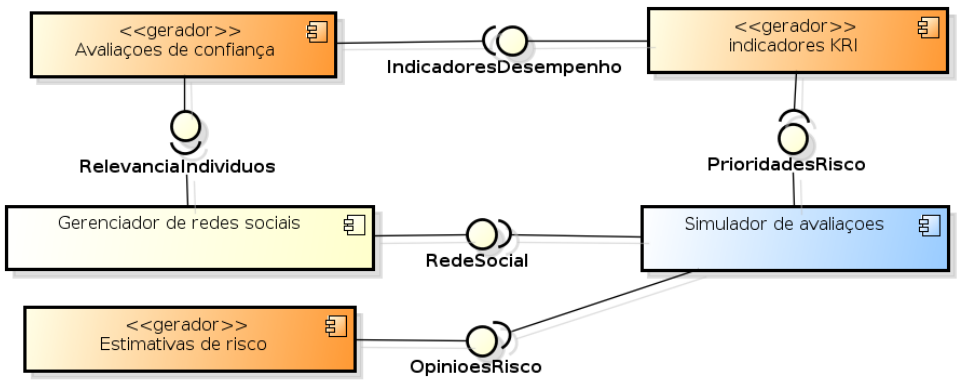

Figura 4.1 – Diagrama de componentes do simulador de riscos

A arquitetura do simulador, é apresentada na Figura 4.1, e como pode se observar, o simulador esta composto por cinco módulos, sendo três módulos geradores de valores (avaliações de confiança, estimativas de riscos e indicadores KRI), um módulo a cargo da modelagem estrutural da organização (gerenciador de redes sociais) e um módulo a cargo da coordenação das simulações, existindo interfaces entre os módulos que representam os valores que são oferecidos por cada um deles e a relação existente entre os módulos. A funcionalidade destes módulos é descrita com maior detalhe na seção seguinte.

4.2 Componentes do simulador

4.2.1 Simulador de avaliações

O módulo simulador de avaliações funciona como o gerenciador das atividades do simulador, sendo as suais principais atribuições :

- Inicializar e manter o controle das estruturas de dados que representam os riscos, avaliações, desempenho, e qualquer outra estrutura que seja utilizada pelos módulos do simu-

lador;

- Coordenar a execução dos submódulos de geração aleatória de valores, gerenciador de redes sociais e as simulações; e
- Combinar os resultados intermédios e processar os dados que representam os resultados das avaliações de riscos, os quais são salvos para análises posteriores.

4.2.2 Administrador da rede social

Dado que a proposta de redução de desvios representa a estrutura entre os membros da organização como uma rede social, onde os agentes apresentam opiniões de confiança entre eles, o simulador cria estas estruturas utilizando o algoritmo de geração de redes sociais apresentado por Kleinberg (2000), implementado mediante a biblioteca de análise de redes sociais JUNG (O'MADADHAIN; FISHER; SMYTH, 2005) a qual é frequentemente usada para implementações de análises de redes sociais na linguagem de programação Java.

Como descrito na seção 2.5, o uso de redes sociais como ferramenta de análise tem demonstrado a existência das propriedades "homofilia"e "mundo pequeno", as quais são inerentes às redes sociais no mundo real. Assim, o algoritmo de Kleinberg (2000) foi selecionado pela sua capacidade de reproduzir estas propriedades mediante o uso de uma distribuição estatística de tipo *power-law*, considerando a evidencia prévia que as redes sociais seguem este tipo de distribuição (CHOROMANSKI; MATUSZAK; MIEKISZ, 2013).

Além da geração da estrutura da rede, o administrador da rede social é o responsável por atribuir um perfil de confiança para cada agente. Este perfil é utilizado posteriormente durante a geração dos coeficientes de confiança direta entre os agentes, onde a seleção do perfil depende dos parâmetros estabelecidos para a simulação -i.e. o número de opiniões confiáveis-.

4.2.3 Gerador de avaliações diretas de confiança

Visando criar uma equivalência entre os coeficientes gerados e as etiquetas semânticas de confiança inicial definidas na seção 3.4.1, o gerador de avaliações diretas de confiança gera os coeficientes a partir dos perfis que foram atribuídos para cada um dos agentes, lembrando que este perfil define as avaliações que um agente determinado receberá por parte dos seus vizinhos. A Tabela 4.1, apresenta os intervalos de valores implementados no simulador e as etiquetas semânticas equivalentes.

Tabela 4.1 – Equivalência entre de etiquetas semânticas e valores iniciais de confiança

Etiqueta semântica	Valor atribuído	Perfil de simulação	Intervalo de valores
Confiança total	1	CONFIÁVEL	(0.6,1]
Confiança moderada	0.6	SEMI-CONFIÁVEL	[0.3,0.6]
Confiança mínima	0.3	CONHECIDO	[0,0.3)

Na tabela pode-se observar que para cada etiqueta semântica de confiança foi criado um intervalo de valores, estes intervalos possibilitam que o usuário configure o simulador de tal forma que não tenha controle total sobre os coeficientes de confiança inicial, permitindo também a possibilidade de expandir o simulador mediante geradores mais complexos sempre que eles trabalhem acima do mesmo intervalo de valores.

4.2.4 Gerador de estimativas de risco

De forma similar ao gerador de avaliações diretas de confiança, o módulo gerador de avaliações de riscos gera os valores de severidade, ocorrência, impacto e probabilidade para cada um dos riscos. Estes valores são gerados em função dos perfis de cada um dos riscos, que por sua vez são atribuídos a partir dos parâmetros estabelecidos para a simulação -i.e. quantidade de riscos errados-. A tabela 4.2 apresenta os intervalos de valores possíveis para cada perfil de risco.

Tabela 4.2 – Intervalos de geração de valores de riscos

Perfil de simulação	Intervalo de valores
ALEATÓRIO	[muito baixo, baixo, médio, alto, muito alto]
SECUNDÁRIO	[muito baixo, baixo, médio]
CRITICO	[alto, muito alto]

Como pode-se observar na tabela, os valores são gerados na forma de valores dentro da escala de Likert que foi descrita na seção 3.4.3. Assim, mesmo que os valores de estimativa de risco sejam gerados de acordo a um perfil, o usuário não tem controle sobre o valor especifico dentro da escala que será simulado, e consequentemente não influencia diretamente no valor de CRI que será gerado, uma vez que este é o resultado do mapeamento das estimativas para valores numéricos mediante a composição de métodos.

4.2.5 Gerador de indicadores KRI

Considerando que é necessário retroalimentar o modelo de confiança mediante resultados de tratamentos de riscos -i.e. observações diretas (DO) - , foi criado um gerador de indicadores KRI com os perfis apresentados na Tabela 4.3

Tabela 4.3 – Intervalos de geração de valores KRI

Perfil de simulação	Intervalo de valores
ALEATÓRIO	[-0.5,0.5]
BOM	[0,0.5]
RUIM	[-0.5,0]

Apesar de que matematicamente o intervalo de valores possíveis para os KRI seja (-1,1), como pode se observar na Tabela o intervalo para os KRI foi reduzido visando obter uma simulação realista, dado que para que um indicador KRI obter os resultados extremos, teria que existir um fracasso total no tratamento de riscos frente a um KRI desejado com desempenho de 100% ou um êxito total no tratamento de riscos frente a um KRI desejado com um valor mínimo perto de 0%.

4.2.6 Interface gráfica

Para parametrizar as condições de simulação, o usuário tem a possibilidade de inserir as condições de teste mediante uma interface gráfica criada na plataforma Java, a qual é apresentada na Figura 4.2

A interface gráfica é divida em três seções, a seção A contém campos para o ingresso dos valores parametrizáveis da simulação (descritos na seção 4.3), a seção B apresenta uma área destinada a apresentar os gráficos que representam a rede que está sendo analisada e os gráficos estatísticos a partir das simulações, e a seção C contém os controles de execução das simulações, sendo estes avaliação de impacto da confiança, avaliação da evolução da confiança e avaliação por tamanho da população, (testes que são descritos com maior detalhe no Capítulo 5) além de um controle auxiliar para exportar a visualização e redesenhar os gráficos.

4.3 Parâmetros de simulação

A Figura 4.3 mostra os controles de simulação como apresentados na interface gráfica do simulador, os quais foram divididos em três categorias : i) controles para a criação de redes

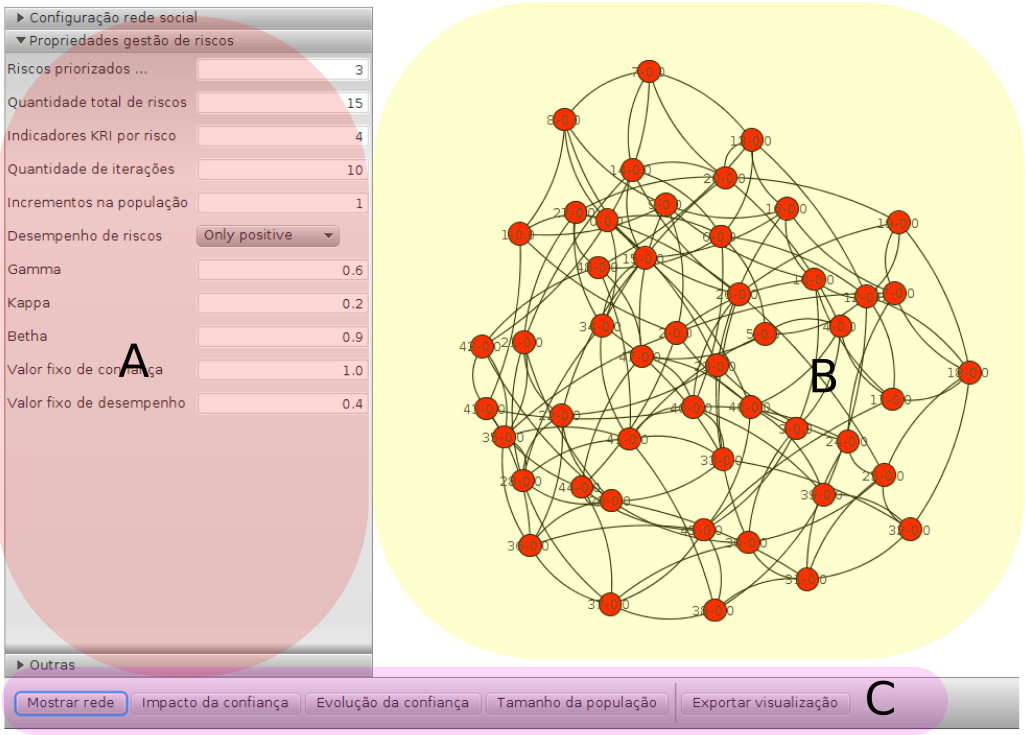

Figura 4.2 – Simulador de gestão de riscos

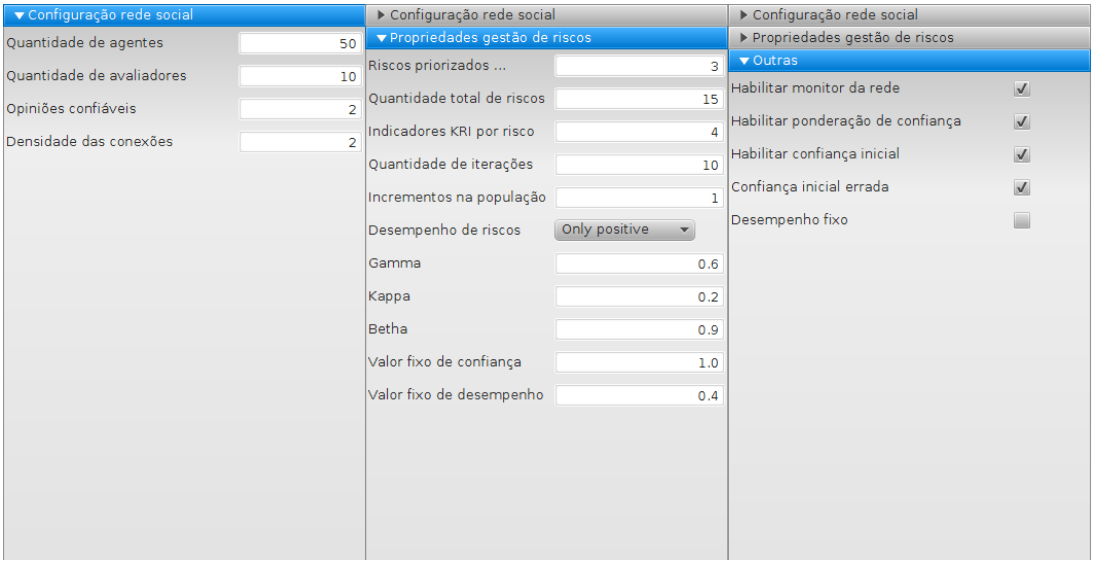

Figura 4.3 – Parâmetros de simulação

sociais, ii) controles para as propriedades de riscos e iii) opções adicionais da simulação. Os controles de cada categoria são descritos a seguir.

4.3.1 Configuração da rede social

Estes parâmetros incluem aqueles que controlam a geração da rede social, estão inclusos nesta categoria:

- **Quantidade de agentes:** Como o nome indica, este parâmetro estabelece a população total que compõe a rede social;
- **Quantidade de avaliadores:** Parâmetro que define a quantidade de avaliadores que compõem o comitê gestor de riscos, dentro do simulador são selecionados aqueles agentes com melhor índice de relevância a partir da confiança individual que é gerada pelo simulador;
- **Opiniões confiáveis:** Parâmetro que define a quantidade de opiniões que serão consideradas como confiáveis -i.e. o número de avaliadores cujo perfil de confiança inicial será alto-; e
- **Densidade das conexões:** Estabelece número o de ligações entre agentes, ou seja, o número de enlaces que cada agente deveria ter dentro da rede. Este parâmetro é um aproximado já que o número final de enlaces é definido mediante o algoritmo de Kleinberg (2000).

4.3.2 Propriedades da gestão de riscos

Estes parâmetros incluem aqueles que controlam as variáveis relacionadas com a gestão de riscos, estão inclusos nesta categoria:

- **Quantidade de riscos priorizados erroneamente:** Este parâmetro define o número de riscos que serão considerados como priorizados de forma errada, tomando como base para a sua geração o perfil definido para cada risco;
- **Quantidade total de riscos:** Parâmetro que define a quantidade total de riscos a ser avaliados;

- **Indicadores KRI por risco:** Parâmetro que define o número de indicadores KRI que serão gerados para cada um dos riscos;
- **Quantidade de iterações:** Define quantas iterações de riscos serão realizadas. Dependendo da simulação que seja executada, estas iterações podem ser realizadas sobre diferentes redes sociais;
- **Incrementos no tamanho da população:** No caso de testes com diversos tamanhos de rede, este parâmetro define quantas vezes será realizado um aumento do número de agentes.
- **Padrão do desempenho de riscos:** Parâmetro que define se será simulado um tratamento de riscos com desempenho positivo, desempenho negativo ou com mudanças aleatórias no desempenho entre execuções do ciclo de gestão de riscos;
- **Valor Beta** Parâmetro que define o valor β que será utilizado durante a execução da atualização de confiança, este parâmetro limita o alcance das recomendações;
- **Valor Gamma:** Parâmetro que define o valor γ que será utilizado durante a execução de TrustWebRank, este parâmetro limita a velocidade de decremento de confiança;
- **Valor Kappa:** Parâmetro que define o valor κ que será utilizado durante a execução de TrustWebRank, este parâmetro limita a velocidade de incremento de confiança;
- **Valor fixo de confiança:** Quando o teste é configurado para representar ausência de confiança inicial, este parâmetro estabelece o valor de confiança direta que será atribuído para cada um dos agentes; e
- **Valor fixo de desempenho:** Quando o teste é configurado para representar desempenho fixo no tratamento de riscos, este parâmetro substitui o calculo de riscos P_{risco}.

4.3.3 Configuração geral da simulação

Estes parâmetros incluem aqueles que controlam as condições gerais da simulação e do simulador, estão inclusos nesta categoria:

- **Habilitar monitor da rede:** Parâmetro que habilita o monitor da estrutura da rede social. Quando ativado, o simulador atualiza o monitor com todas as estruturas de rede

social que são utilizadas durante a simulação. Porém implica maior consumo de recursos computacionais;

- **Habilitar ponderação de confiança:** Parâmetro que habilita o uso de confiança dentro das simulações, quando ativado o simulador utiliza as equações modificadas para suporte à confiança, caso contrario é utilizada a composição de riscos original. Este parâmetro é útil para comparar o desempenho entre a composição original e a modificada;

- **Habilitar confiança inicial:** Diante da existência de entornos onde não é possível a quantificação da confiança inicial, quando ativado este parâmetro libera a geração de confiança inicial baseada em perfis, caso contrario o valor da confiança inicial é fixo e estabelecido mediante outro parâmetro;

- **Confiança inicial errada:** Considerando que a confiança inicial pode ser errada, este parâmetro habilita a geração de confianças inicias erradas, cuja magnitude depende do perfil habilitado para os avaliadores; e

- **Desempenho fixo:** Da mesma forma que a confiança inicial errada, este parâmetro controla a geração de resultados de desempenho variáveis ou fixos, é especialmente útil para análises onde é preciso descartar a variabilidade do desempenho do tratamento de riscos.

4.4 Algoritmo de execução de simulações

Por ultimo para formalizar a interação entre os componentes, o pseudocódigo apresentado na Figura 4.4 descreve a sequência de execução dos módulos durante uma simulação padrão.

Para a execução de uma simulação, são necessários um objeto p que contém todos os valores parametrizáveis descritos na seção 4.3 e um número de iterações *iterations* para a obtenção de um valor representativo a partir da simulação.

Na linha 1 o gerador de redes sociais cria a estrutura que representa a organização a partir das caraterísticas descrita no objeto p, e posteriormente na linha 3 são gerados os coeficientes de confiança em forma de opiniões entre vizinhos -i.e. informação de testemunhas (WI)- para cada um dos agentes que constituem a organização. Na linha 5 os valores de confiança individuais entre os vizinhos são utilizados para computar o coeficiente de Relevância (R) mediante *TrustWebRank*, o que permite formar o comitê gestor de riscos na linha 6 a partir dos agentes

Data: p um conjunto de parâmetros que descrevem a simulação; $iterations$ o número de interações desejadas
Result: Resultados do simulador de gestão de riscos

```
   /* Geração de confiança                                          */
 1 social_network ← createSocialNetwork(p);
 2 foreach agent in the social_network do
 3 |   agent ← generateDirectTrust(agent);
 4 end
 5 social_network ← computeWithTrustWebRank(social_network);
 6 risk_committee ← createRiskCommittee(social_network, p);
   /* Análise/avaliação de riscos                                   */
 7 for i=1 to iterations do
   |   /* Criação de riscos                                        */
 8 |   risks_set ← generateRisks(p);
   |   /* Geração de estimativas e computo de CRI                  */
 9 |   foreach risk in the risks_set do
10 |   |   risk ← assessRisk(risk,risk_committee);
11 |   end
   |   /* Tratamento de riscos e geração de KRI                    */
12 |   foreach risk in the risks_set do
13 |   |   P_risk_set add generateTreatmentPerformance(risk, p);
14 |   end
15 |   saveResults(P_risk_set);
   |   /* Atualização de confiança                                 */
16 |   foreach agent in the social_network do
17 |   |   if agent is inside risk_comitee then
18 |   |   |   social_network ←updateDirectTrust(agent,
   |   |   |   social_network,P_risk_set);
19 |   end
20 |   social_network ← computeWithTrustWebRank(social_network);
21 end
```

Figura 4.4 – Sequencia de geração de valores e rotinas de gestão de riscos

com um melhor coeficiente de relevância.

Uma vez formado o comitê, procede-se à execução dos ciclos de gestão de riscos. Como primeiro passo na linha 8 são geradas as estruturas de dados que representam os riscos como um análogo à fase de identificação de riscos (de novo a partir dos parâmetros armazenados em p) e posteriormente na linha 9 são executadas as rotinas que representam as etapas que formam a fase de análise/avaliação de riscos, obtendo como resultado um valor (CRI) para cada um dos riscos salvando-lo na mesma estrutura de dados dos riscos.

Com os riscos e seus valores de prioridade (CRI) procede-se à etapa de tratamento de riscos. Na linha 13 é gerado um coeficiente P_{risk} o qual é posteriormente armazenado no *array* de dados P_{risk}_set o qual contém os indicadores da qualidade do tratamento de riscos de acordo com os parâmetros p.

Por último e utilizando os resultados do tratamento de riscos, procede-se a atualizar a confiança dos agentes a partir dos resultados obtidos durante o tratamento -i.e. observações diretas (DO)-. No ciclo apresentado na linha 16 se percorre a rede social para identificar aqueles agentes que fazem parte do comitê gestor de riscos. Na linha 18 a confiança dos vizinhos para estes agentes é atualizada conforme os resultados utilizando a equação de atualização de confiança modificada para o contexto de gestão de riscos, com o qual a rodada seguinte de *TrustWebRank* na linha 20 atualizara os coeficientes de relevância a partir da confiança individual atualizada.

4.5 Conclusões parciais

Neste capítulo foram descritas as características do simulador desenvolvido para avaliar a proposta de quantificação de confiança para redução de desvios por causas humanas em análise/avaliação de riscos.

O objetivo da simulador é avaliar as implicações da abordagem proposta durante diversas rodadas do ciclo de gestão de riscos e diversos patrões de resultados, dada a impossibilidade de analisar-las mediante a execução de ciclos de gestão de riscos por causa do tempo e dos recursos que a sua execução exige, contribuindo assim para a validação da proposta.

O simulador foi criado de tal forma que permite a parametrização de experimentos, habilitando ao usuário parametrizar a geração de coeficientes de confiança, estimativas de risco e resultados de desempenho do tratamento de risco mediante módulos de geração de valores dentro de intervalos de valores preestabelecidos em forma de perfis de comportamento.

Para a implementação do simulador foi utilizada a linguagem de programação Java, implementando um projeto com um total de 4 pacotes, 33 classes, 230 métodos, equivalentes á 3.219 linhas de código fonte. O uso do simulador permite variar as condições com as quais o ciclo de gestão de risco é executado, tornando possível a avaliação dos pontos fortes e fracos da proposta de redução de desvios, tal como demonstrado no capitulo 5.

5 ANÁLISE E RESULTADOS

Este capítulo realiza a análise da incorporação da confiança na análise e avaliação de riscos e do impacto na redução de desvios por causas humanas. A seção 5.1 apresenta a justificativa para o tamanho da organização e do comitê gestor de riscos utilizado durante as simulações. A seção 5.2 apresenta as simulações preliminares mediante as quais foram determinados os valores para os coeficientes de incremento e decremento de confiança (γ e κ). A seção 5.3 descreve as perguntas de pesquisa que foram utilizadas para avaliar os resultados das simulações. A seção 5.4 apresenta a avaliação dos efeitos do uso de ponderações de confiança na análise/avaliação de riscos. A seção 5.5 apresenta os resultados das simulações concernentes ao comportamento evolutivo dos coeficientes de confiança. Finalmente a 5.6 apresenta as conclusões parciais do capitulo.

5.1 Tamanho da rede social e do comitê gestor de riscos

Como passo prévio à realização das simulações e procurando gerar simulações representativas da realidade empresarial, foram procurados valores para duas variáveis cruciais:

1. O tamanho adequado para a simulação da estrutura organizacional -i.e. rede social-; e
2. O tamanho adequado para o comitê gestor de riscos.

Dentro do território brasileiro a legislação vigente estabelece que as empresas devem ser classificadas de acordo ao lucro gerado durante um ano fiscal, porém para fins práticos existe uma classificação alternativa de empresas a qual as classifica de acordo com o número de funcionários que fazem parte delas (SEBRAE/SC, 2014), a qual é apresentada na Tabela 5.1.

Tabela 5.1 – Classificação de empresas por quantidade de funcionários

Tipo	Quantidade de funcionários
Micro-empresa	até 9 empregados
Empresa pequena	de 10 a 49 empregados
Empresa média	de 50 a 99 empregados
Empresa grande	mais de 100 empregados

Considerando que as micro-empresas dificilmente terão a capacidade de criar um programa de gestão de riscos e que as empresas pequenas e médias são as que mais crescem no

território brasileiro (PME, 2013), considera-se 50 como um tamanho adequado para a realização das simulações já que representa o ponto intermédio entre as empresas pequenas e médias.

Por outro lado, até o momento não existe uma quantidade estandardizada para as pessoas que devem fazer parte do comitê gestor de riscos, uma vez que o comitê deve estar conformado idealmente por indivíduos de todas as áreas da organização e estas áreas variam de uma empresa a outra(AMARAL; AMARAL; NUNES, 2010). Trabalhos anteriores tem demonstrado que a conformação de um comitê gestor de riscos com uma quantidade grande de membros pode aumentar o poder do comitê ná tomada de decisões (KALBERS; FOGARTY, 1993), porém enquanto maior seja o tamanho do comitê gestor de riscos existira uma maior dificuldade para coordenar os seus esforços (DALTON et al., 1999).

Observações prévias têm demonstrado que os comitês gestores de riscos geralmente são constituídos por 7.78 até 17.80 pessoas (NG; CHONG; ISMAIL, 2013), enquanto outras observações estabelecem unicamente que na média os comitês gestores de riscos são constituídos por 7.44 membros (MCNULTY; FLORACKIS; ORMROD, 2012). Portanto e considerando que não existe um estudo com tamanhos do comitê gestor de risco ideais, para as simulações foi adotado o intervalo de analise [5,20], de modo que as análises permitam visualizar facilmente as implicações de comitês gestores de riscos pequenos e grandes, sem que os valores extremos estejam longe do observado na vida real. Da mesma forma, no caso dos testes onde o tamanho do comitê gestor de riscos não é variável, adotou-se um comitê de tamanho 10 para facilitar a análise das simulações.

5.2 Coeficientes de controle

Para determinar um valor adequando para os coeficientes de incremento e decremento de confiança, foi realizada uma simulação preliminar com as condições descritas na Tabela 5.2.

Tabela 5.2 – Condições de teste para coeficientes de controle

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	Fixo com confiança inicial de magnitude 1 entre todos os agentes
Desempenho do tratamento de riscos	Fixo com magnitude de 0.4 tanto para incrementos e decrementos

A simulação foi configurada para minimizar a influência dos valores iniciais de confiança e os resultados do tratamento de risco, permitindo avaliar o impacto real da magnitude dos coeficientes γ e κ, obtendo os resultados apresentados nas Figuras 5.1 e 5.2 que representam a evolução do coeficiente de relevância de um dos membros do comitê de gestão de riscos.

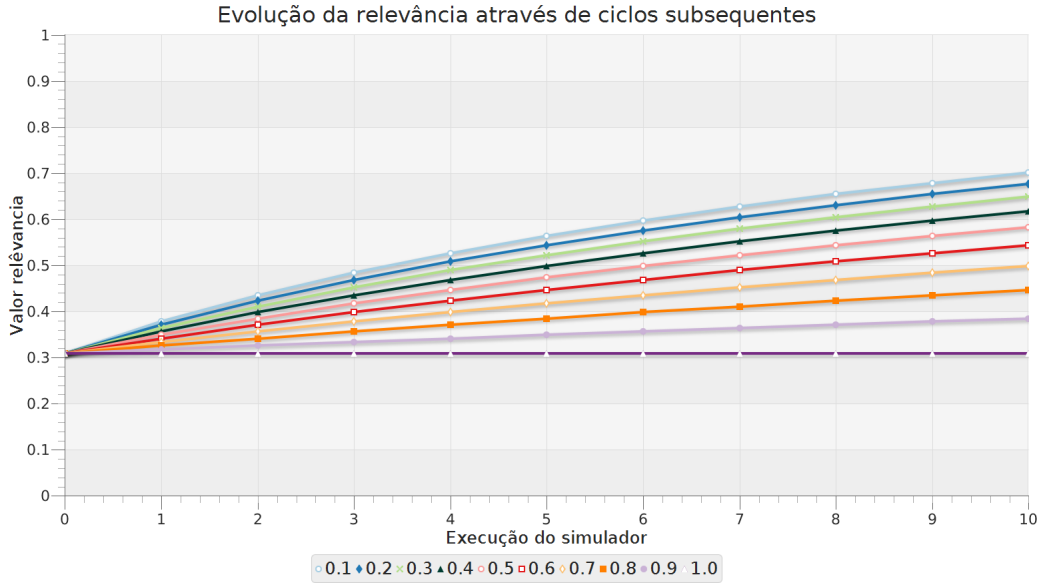

Figura 5.1 – Simulações para γ

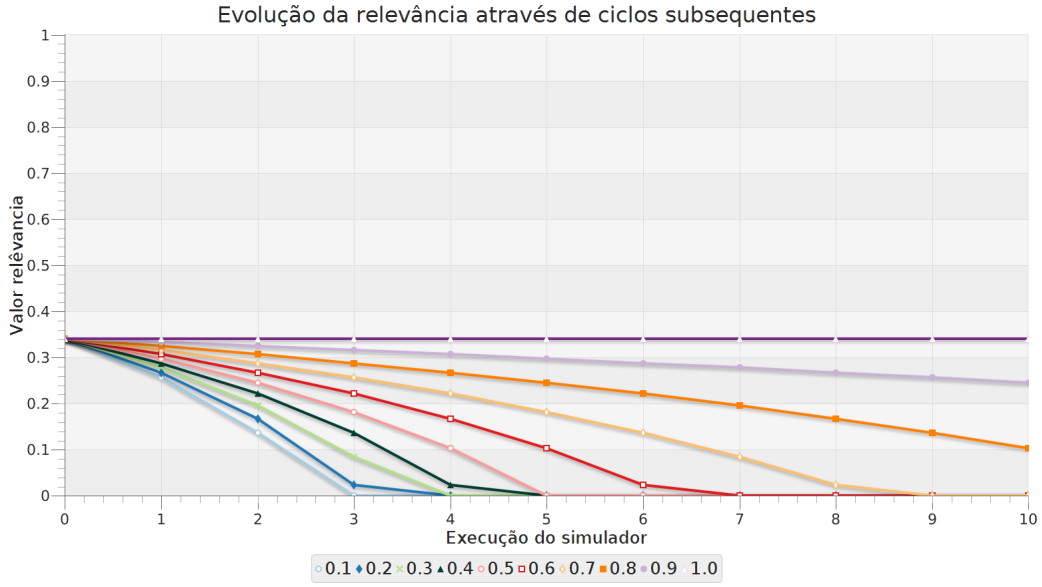

Figura 5.2 – Simulações para κ

A Figura 5.1 apresenta a evolução dos coeficientes de relevância para diferentes valores de γ. Quanto maior for o valor de γ menor será a velocidade com a qual o coeficiente de relevância aumenta o seu valor, atingindo um ponto onde não existe nenhum incremento no caso que $\gamma = 0.1$. Com estes resultados pode se afirmar que o valor original de TrustWebRank

$\gamma = 0.6$ encontra-se num ponto intermédio entre um incremento de confiança acelerado e uma ausência de aumento de confiança, motivo pelo qual é conservado.

A Figura 5.2 apresenta a evolução dos coeficientes de relevância para diferentes valores de κ. Observa-se de novo que quanto maior for o valor de κ, menor será a velocidade de decremento de confiança. Para o contexto de gestão de riscos é necessário que o decremento da confiança seja rápido para penalizar aquelas opiniões erradas. Assim, se considera $\kappa = 0.2$ como um valor adequado, já que com este valor consegue-se descartar as opiniões erradas a partir da quarta execução, observando-se uma relevância mínima a partir da terceira execução. Este valor foi selecionado em detrimento de $\kappa = 0.1$ para deixar uma pequena margem para modificações, além de que o impacto pode acelerar-se quando as simulações não apresentem confiança homogênea.

5.3 Descrição dos testes da proposta

Com o objetivo de estabelecer se a proposta de uso da confiança efetivamente incrementa a precisão dos resultados da análise/avaliação de riscos, os experimentos para a análise comparativa entre a composição de métodos original criada por Amaral, Amaral e Nunes (2010) e a modificação suportada por confiança, foram pautados nos questionamentos seguintes:

1. A proposta logra incrementar a precisão das estimativas de risco?
2. O tamanho do comitê de avaliação de riscos influência na efetividade da proposta?
3. A proposta reproduz a dinâmica de confiança de tipo "positivo devagar-negativo rápido"?
4. A proposta é resistente à presença de coeficientes de confiança errados? e
5. A confiança inicial constitui um fator decisivo no modelo de confiança?.

Para criar uma plataforma de testes para proporcionar respostas a estes questionamentos, foram selecionados alguns critérios de avaliação que podiam ser representados de forma adequada mediante simulação, sendo estes:

- **Quantidade de ocorrências em zona de não tratamento:** Representa o número de priorizações de riscos considerados como altos dentro da zona de não tratamento para um período de tempo determinado. Considera-se que o risco esta fora da zona de tratamento

quando o risco é priorizado fora do primeiro terço de prioridades, sendo propensos a receber poucos investimentos no tratamento de riscos;

- **Tempo para descartar opiniões de risco erradas:** Caracteriza a capacidade de contenção de opiniões que levam a priorizações de risco erradas. Nos testes é representado como o número de ciclos que são requeridos para atingir um valor zero de *Relevância* em presença de resultados negativos, indicando assim a habilidade para descartar opiniões erradas.

5.4 Impacto das ponderações de confiança

Nesta seção serão detalhados os experimentos que avaliaram a redução de riscos altos estimados em zona de não tratamento. Para os fins das simulações, considera-se que a precisão das estimativas aumenta quando existe uma redução na quantidade de riscos altos que são priorizados fora da zona de tratamento.

5.4.1 Impacto na prioridade de risco

Para demonstrar a influência das ponderações matemáticas na priorização dos riscos, ou seja, na precisão das priorizações, o simulador foi configurado com as condições descritas na Tabela 5.3.

Tabela 5.3 – Condições de teste para a avaliação da influência da confiança

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	2 agentes com perfil CONFIÁVEL, demais com perfil SEMI-CONFIÁVEL
Quantidade de riscos	12 riscos
Prioridade real dos riscos	2 riscos com impacto de tipo CRITICO(r_1 e r_2), demais como SECUNDÁRIO

Este cenário de simulação representa uma condição clara de desvio, onde dois avaliadores com o perfil de confiança mais alto expressam as suas opiniões corretamente, ou seja, avaliam os riscos r_1 e r_2 com um perfil CRITICO, enquanto os outros avaliadores estimam a prioridade dos riscos com um perfil SECUNDÁRIO, configurando todas as outras avaliações com um perfil SECUNDÁRIO para gerar resultados que permitissem observar a real influencia

dos coeficientes de relevância.

Foram executados 20 testes independentes sobre estruturas de rede social diferentes, executando 10 análises/avaliações de riscos com a composição de riscos original, e 10 análises/avaliações de riscos com a composição que incluí a quantificação de confiança, para determinar se o coeficiente de relevância efetivamente influencia o valor final da prioridade do risco.

A Figura 5.3 apresenta lado a lado os resultados obtidos nas 20 simulações. Especificamente as prioridades obtidas pelos riscos (r_1 e r_2), tanto para a composição original ($O1, ..., O10$) quanto para a modificada ($M1, ..., M10$).

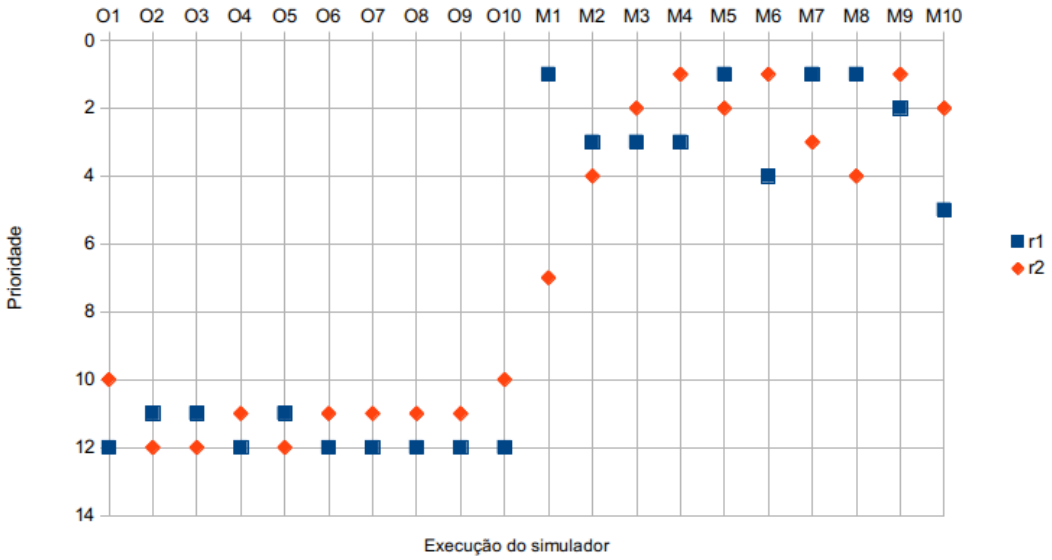

Figura 5.3 – Análise/avaliação de riscos original vs. modificada

Na figura pode se observar que os riscos r_1 e r_2 não atingem posições prioritárias durante a análise/avaliação com a composição de métodos original por causa dos desvios nos resultados. Portanto, no caso do orçamento destinado ao tratamento de riscos não permitir cobrir todos os riscos, estes riscos têm alta probabilidade de ficar fora do tratamento e ser assumidos durante a fase de aceitação de riscos, aumentando assim o risco potencial da organização.

Por outro lado, as 10 execuções com a composição que inclui as ponderações mostraram uma melhoria na precisão das estimativas de riscos, reduzindo assim os efeitos do desvio. Como pode se observar, nestes testes as estimativas de riscos r_1 e r_2 atingem o primeiro terço de prioridades na maioria das execuções, o que significa que os pesos matemáticos calculados em base à confiança efetivamente provocam o aumento da prioridade de risco.

Uma vez que foi demonstrado que as ponderações influenciam corretamente a priorização dos riscos, deve-se também analisar as implicações das ponderações em termos de riscos priorizados fora da zona de tratamento. Para isso, foram executadas 50 simulações tanto para a composição de métodos original quanto para a proposta baseada em confiança. Porém, como se apresenta na Tabela 5.4 as condições ambientais foram ligeiramente alteradas para avaliar se as ponderações são efetivas com outras proporções de desvio nos resultados, evitando analisar sempre o mesmo conjunto de dados para não fornecer conclusões tendenciosas.

Tabela 5.4 – Condições de teste para a avaliação do número de riscos fora da zona de tratamento

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	**3 agentes** com perfil CONFIÁVEL, qualquer outro considerado com perfil SEMI-CONFIÁVEL
Quantidade de riscos	**15 riscos**
Prioridade real dos riscos	**3 riscos** com impacto de tipo CRITICO(r_1, r_2 e r_3), outros considerados como SECUNDÁRIO
Quantidade de execuções	50 execuções sobre grafos independentes
Métricas a ser avaliadas	Quantidade de riscos altos priorizados fora da zona de tratamento

Neste experimento, o simulador foi configurado novamente para representar um desvio claro, definido como as opiniões certas que são negligenciadas por causa da sua proporção em relação com a quantidade total de opiniões. Assim, as simulações reproduzem um cenário onde os riscos r_1, r_2 e r_3 são avaliados como CRITICO unicamente pelos avaliadores com perfil de confiança CONFIÁVEL, e como SECUNDÁRIO pelos outros avaliadores, configurando todas as outras avaliações com um perfil SECUNDÁRIO para gerar resultados que permitissem observar quantos riscos altos são estimados fora da zona de tratamento com ambas abordagens.

A partir da execução das simulações foram obtidos os resultados apresentados na Figura 5.4 e na Figura 5.5, onde os resultados mostram a prioridade para o risco r_2 sobre 50 estruturas de rede social diferentes, tanto para a composição de métodos original quanto para a composição modificada, com uma zona de tratamento de magnitude 5 -i.e. o primeiro terço de prioridades-.

Nos resultados pode-se constatar que enquanto o processo original gerou 16 priorizações fora da zona de tratamento, a composição suportada por confiança conseguiu reduzir este número para 7, demonstrando de novo que o processo é capaz de reduzir os riscos altos priorizados fora da zona de tratamento sempre que seja possível quantificar a confiança. Nota-se também o

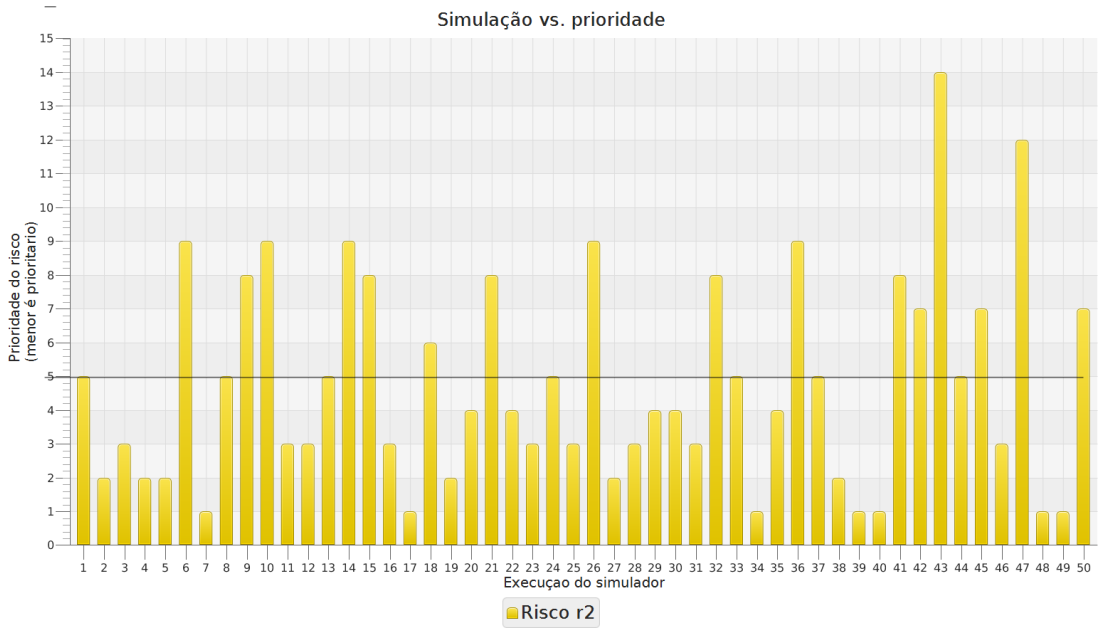

Figura 5.4 – Valores CRI de r_2 para a composição original de riscos

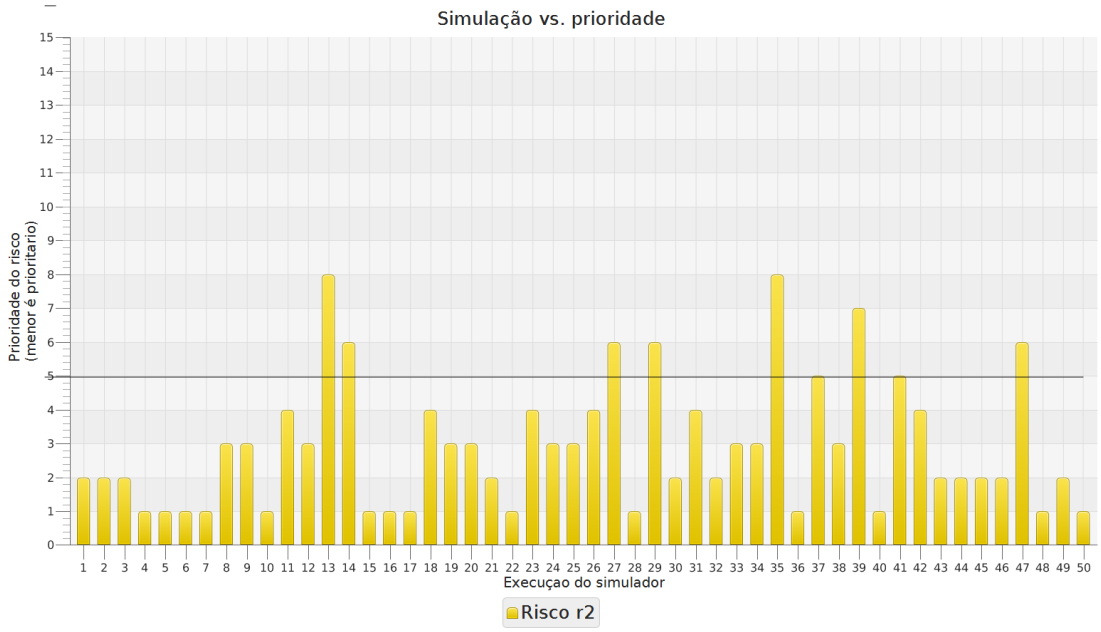

Figura 5.5 – Valores CRI de r_2 para a composição suportada por confiança

que o risco r_2 apresenta melhores posições de prioridade durante as 50 execuções (observando-se também estes resultados para os riscos r_1 e r_3), situação que pode ser interpretada como uma melhoria na precisão das estimativas

5.4.2 Influência do tamanho do comitê de avaliação de riscos

Considerando que o desvio nos resultados é causado pela proporção entre estimativas de risco certas e erradas -i.e. riscos altos priorizados dentro e fora da zona de tratamento-, foi realizado um experimento para determinar se a relação entre opiniões certas -i.e. aquelas acorde com a realidade de risco- e o tamanho total do comitê de avaliação de riscos diminui a efetividade das ponderações de confiança, utilizando as condições descritas na Tabela 5.5.

Tabela 5.5 – Condições de teste para as provas do comitê de avaliação de riscos

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	Variável durante o teste de 5 a 20 agentes
Perfil de confiança dos avaliadores de risco	Quantidade de avaliadores com perfil CONFIÁVEL proporcional ao tamanho do comitê de avaliação, demais com perfil SEMI-CONFIÁVEL
Quantidade de riscos	**15 riscos**
Prioridade real dos riscos	**3 riscos** com impacto de tipo CRITICO(r_1, r_2 e r_3), demais como SECUNDÁRIO
Quantidade de execuções	50 execuções por cada tamanho de comitê de avaliação de riscos
Métricas a ser avaliadas	Quantidade de riscos altos priorizados fora da zona de tratamento

Durante este teste foi simulado um desvio similar ao da seção anterior, onde os três riscos considerados como CRITICO são qualificados de forma certa durante todas as execuções pelos agentes com perfil CONFIÁVEL, enquanto todos os outros agentes os avaliam como SECUNDÁRIO, configurando todas as outras avaliações com um perfil SECUNDÁRIO para gerar resultados que permitissem melhorar a visão da análise.

Seguidamente, foram executadas simulações de comités de avaliação de riscos cujo tamanho foi variado desde 5 até 20 agentes, executando 50 simulações para cada tamanho de rede social, ou seja, um total de 750 simulações. Foi considerado como valor representativo de cada bloco de 50 simulações o número de ocasiões onde os riscos foram priorizados fora da zona de tratamento, obtendo os resultados apresentados nas Tabela 5.6 que apresenta os resultados obtidos com a composição de métodos original, e a composição modificada, para uma proporção

entre *opiniões certas* / *tamanho do comitê* $\cong 0.25$.

Tabela 5.6 – Simulações de impacto de confiança com uma proporção de 25% entre opiniões certas e o total de avaliadores de risco

Proporção (Opiniões certas/Tamanho do comitê)	Riscos altos fora de zona de tratamento (original)	Riscos altos fora de zona de tratamento (modificada)	Modificado/Original
1/5	67	56	0.84
1/6	73	67	0.92
1/7	79	66	0.84
2/8	63	57	0.90
2/9	66	54	0.82
2/10	62	52	0.84
2/11	61	60	0.98
3/12	58	47	0.81
3/13	54	36	0.67
3/14	56	51	0.91
3/15	52	46	0.88
4/16	64	41	0.64
4/17	50	47	0.94
4/18	55	47	0.85
4/19	53	45	0.85
5/20	51	35	0.69
Incidentes totais	959	812	

As simulações com uma proporção de 0.25 apresentadas na Tabela 5.6 demonstraram que a ênfase nas opiniões confiáveis incrementa a precisão das estimativas de riscos, reduzindo a quantidade de riscos com alta prioridade fora da zona de tratamento de 959 com a composição de métodos original para 812 com a composição de métodos baseada em confiança, uma relação 812/959=0.85.

Observa-se que a relação entre a quantidade de riscos altos priorizados fora da zona de tratamento com ambas composições de métodos apresenta um valor menor do que 1 em todas as ocasiões, o que significa que a proposta conserva suas propriedades de redução independentemente do tamanho do comitê de avaliação de riscos. Assim também, com o aumento da quantidade de membros do comitê gestor de riscos, a variabilidade nas estimativas faz com que o número de riscos altos estimados fora da zona de tratamento diminuía à medida que o tamanho do comitê gestor de riscos aumenta.

Para avaliar se a magnitude da proporção entre opiniões de riscos certas e o tamanho total do comitê gestor de riscos impacta na efetividade da metodologia baseada em confiança, foram realizadas duas simulações adicionais para as proporções *opiniões certas* / *tamanho do comitê* $\cong 0.5$ e *opiniões certas* / *tamanho do comitê* $\cong 0.75$, cujos resultados são apresentados nas tabelas 5.7 e 5.8 respectivamente.

O experimento com uma proporção de magnitude 0.5 apresentado na Tabela 5.7 mostrou que a proporção entre opiniões certas e o tamanho total do comitê gestor de riscos, efetivamente influência na precisão das estimativas de riscos, já que o numero de riscos priorizados fora da

Tabela 5.7 – Simulações de impacto de confiança com uma proporção de 50% entre opiniões certas e o total de avaliadores de risco

Proporção (Opiniões certas/Tamanho do comitê)	Riscos altos fora de zona de tratamento (original)	Riscos altos fora de zona de tratamento (modificada)	Modificado/Original
2/5	53	43	0.81
3/6	47	27	0.57
3/7	41	34	0.83
4/8	33	19	0.58
4/9	42	32	0.76
5/10	23	10	0.43
5/11	22	15	0.68
6/12	19	10	0.53
6/13	23	14	0.61
7/14	22	15	0.68
7/15	12	11	0.92
8/16	14	10	0.71
8/17	19	7	0.37
9/18	12	5	0.42
9/19	17	8	0.47
10/20	10	9	0.90
Incidentes totais	409	269	

zona de tratamento foi reduzido tanto para a composição original de métodos, quanto para a composição de métodos baseada em confiança.

Mesmo assim, a proposta baseada em confiança conservou as suas propriedades de redução, observando-se novamente que a relação entre ambas metodologias apresenta em todas as ocasiões uma magnitude menor do que 1, logrando reduzir o numero de riscos altos fora da zona de tratamento desde 409 para 269, uma relação 269/409=0.66.

Tabela 5.8 – Simulações de impacto de confiança com uma proporção de 75% entre opiniões certas e o total de avaliadores de risco

Proporção (Opiniões certas/Tamanho do comitê)	Riscos altos fora de zona de tratamento (original)	Riscos altos fora de zona de tratamento (modificada)	Modificado/Original
3/5	28	21	0.82
4/6	21	12	0.67
5/7	15	9	0.67
6/8	7	5	0.86
6/9	11	5	0.55
7/10	5	3	0.80
8/11	7	3	0.57
9/12	2	0	0.00
9/13	3	1	0.33
10/14	2	1	0.50
11/15	1	1	1.00
12/16	2	1	0.50
12/17	0	1	N/A
13/18	0	1	N/A
14/19	1	0	0.00
15/20	0	1	N/A
Incidentes totais	105	65	

Por ultimo a simulação com uma proporção de magnitude 0.75 apresentada na Tabela 5.8 confirma que o incremento de opiniões confiáveis -i.e. o incremento na magnitude da proporção-, incrementa também a efetividade da abordagem baseada em confiança. Nestes novos experimentos, a composição de métodos original priorizou 105 riscos fora da zona de tratamento enquanto a composição baseada em confiança reduziu este número para 65, uma

relação de 65/105 = 0.62.

Com base nos valores das relações entre riscos priorizados fora da zona de tratamento para os três experimentos (apresentados na Tabela 5.9), pode-se afirmar que com um número maior de opiniões confiáveis, o impacto e benefícios das ponderações matemáticas são incrementados por causa da relação *opiniões certas* / *tamanho do comitê*.

Tabela 5.9 – Resumo de testes de impacto de confiança com diferentes tamanhos de comitê gestor de riscos

opiniões certas/tamanho do comitê	composição original/composição baseada em confiança	Redução alcançada
0.25	0.85	15%
0.50	0.66	34%
0.75	0.62	38%

5.5 Evolução dos coeficientes de confiança

Nesta seção é avaliada a evolução dos coeficientes de confiança, frente a cenários de evolução do ciclo de gerenciamento de riscos. Primeiro se realiza uma simulação para avaliar as implicações de que a confiança inicial seja errônea, depois é simulada uma ausência total de confiança inicial, e por ultimo se avalia la evolução frente a um patrão aleatório de efetividade nas opiniões de riscos.

5.5.1 Resistência a confiança inicial errada

Uma condição que foi evidente durante a realização dos experimentos que avaliaram o impacto da ponderação de confiança, foi o fato que em condições indesejáveis, como coeficientes de $Relevancia$ inicial errados, o processo poderia dar ênfase a aquelas opiniões erradas, gerando resultados indesejados. Assim, para verificar a influência de opiniões iniciais erradas, foi criado um experimento com as condições descritas na Tabela 5.10.

Neste experimento, os dois agentes com perfil CONFIÁVEL avaliam os riscos r_1, r_2, r_3 com perfil SECUNDÁRIO (avaliação errada) enquanto todos os outros agentes com menor coeficiente de $Relevancia$ avaliam estes riscos como CRITICO (avaliação certa). Além disso, qualquer outra opinião foi configurada como SECUNDÁRIO, para exemplificar claramente o desvio.

A Figura 5.6 apresenta a variação dos resultados de *Relevância* durante 10 execuções

Tabela 5.10 – Condições de teste para confiança inicial errada

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	2 agentes com peril CONFIÁVEL, demais com perfil SEMI-CONFIÁVEL
Quantidade de riscos	15 riscos
Prioridade real dos riscos	3 riscos com impacto de tipo CRITICO(r_1, r_2 e r_3), demais como SECUNDÁRIO
Quantidade de execuções	10 testes consecutivos acima da mesma estrutura

consecutivas na mesma estrutura, representando a evolução dos coeficientes de confiança para todos os membros do comitê de avaliação de riscos. A simulação mostrou que os coeficientes de $Relevancia$ para os agentes 14 e 29 (os agentes com melhor perfil de confiança dentro da rede social) sofreram um decremento nos seus coeficientes de confiança por causa das suas opiniões erradas. Isto demonstra que a atualização de confiança efetivamente ajusta os coeficientes como resposta ao baixo desempenho no tratamento dos riscos.

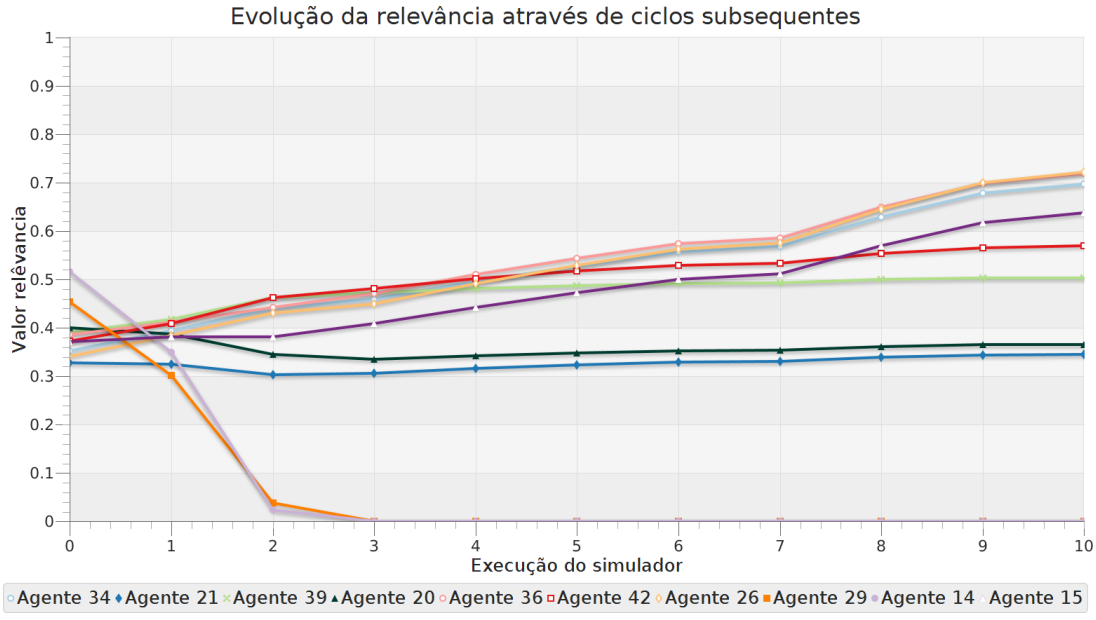

Figura 5.6 – Evolução da relevância com confiança inicial errada

Adicionalmente, foi também observado que os coeficientes de relevância alcançaram resultados similares aos valores das opiniões certas a partir da segunda execução e sendo definitivamente eliminados na quarta execução, enquanto os coeficientes positivos aumentaram com uma velocidade menor, o que significa que a dinâmica de confiança “positivo devagar-negativo rápido” foi reproduzida de forma adequada.

5.5.2 Ausência de confiança inicial

Considerando a existência de cenários onde não e factível medir a confiança inicial que existe entre os membros da organização, foi planejado um experimento com as condições apresentadas na Tabela 5.11.

Tabela 5.11 – Condições de teste para ausência de confiança inicial

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	2 agentes com perfil CONFIÁVEL, demais com perfil SEMI-CONFIÁVEL
Quantidade de riscos	15 riscos
Prioridade real dos riscos	3 riscos com impacto de tipo CRITICO(r_1, r_2 e r_3), demais como SECUNDÁRIO
Quantidade de execuções	10 testes consecutivos acima da mesma estrutura organizacional

Durante a execução do experimento, foi mudada a fase de quantificação inicial de confiança, substituindo-a por valores fixos de confiança entre os agentes com magnitude 1. Assim, a partir desta simulação foram obtidos os resultados apresentados na Figura 5.7.

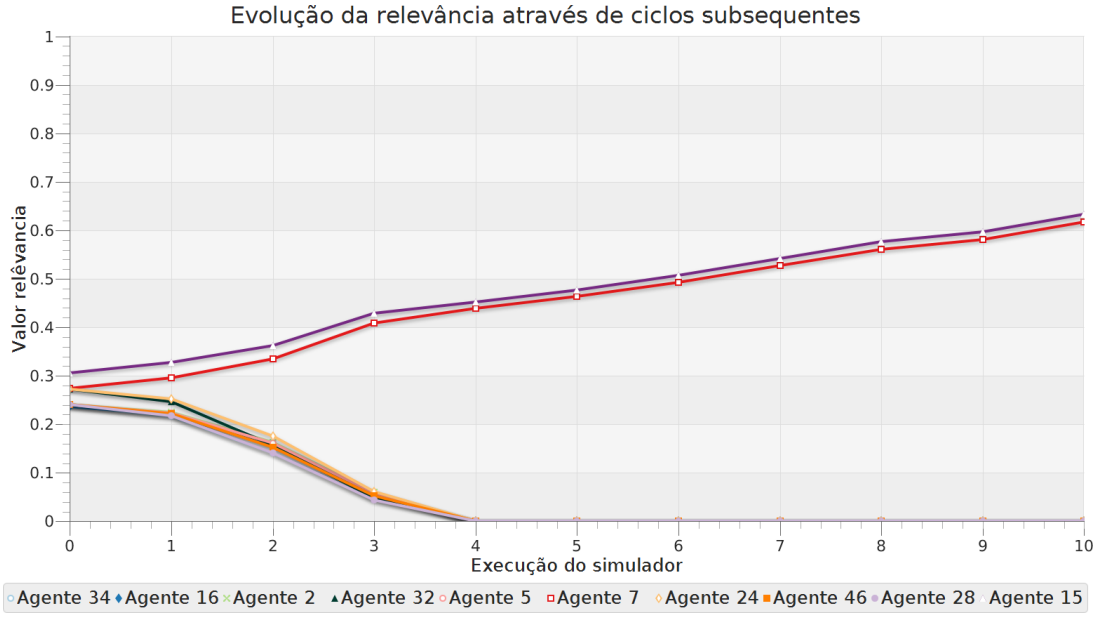

Figura 5.7 – Evolução da relevância sem valores de confiança inicial

A Figura 5.7 mostra que como uma consequência da presença de valores fixos de confiança, todos os agentes recebem valores de relevância quase uniformes no inicio da simula-

ção, existindo algumas diferenças sutis entre os agentes, resultado da estrutura da rede social. Contudo, as simulações mostram novamente que a atualização de confiança ainda reproduz a dinâmica "positivo devagar-negativo rápido" o que significa que a abordagem é capaz de atualizar os coeficientes de relevância, baseando-se unicamente nos resultados de desempenho no tratamento de riscos.

Pode-se observar também que em comparação com o teste da seção 5.5.1, a quantificação de confiança gerou coeficientes de confiança indireta mais baixos e consequentemente coeficientes de relevância mais baixos no inicio da simulação. Porém, esta condição não se considera como relevante porque a dinâmica de confiança "positivo devagar-negativo rápido" ainda é reproduzida, lembrando que os valores de CRI que são obtidos com estes coeficientes de confiança, não são utilizados em nenhum outro cálculo e só servem como índice para guiar as decisões do tratamento de riscos.

5.5.3 Evolução de confiança aleatória

Considerando que os experimentos demonstram que a abordagem consegue reproduzir o comportamento e aumento de efetividade desejado nas estimativas de risco, foi criado um último teste com um padrão de comportamento mais natural com câmbios aleatórios na efetividade das estimativas de riscos, utilizando as condições descritas na Tabela 5.12.

Tabela 5.12 – Condições de teste para evolução de confiança aleatória

Característica	Valor
Tamanho da rede social	50 agentes
Tamanho do comitê de avaliação de riscos	10 agentes
Perfil de confiança dos avaliadores de risco	2 agentes com perfil CONFIÁVEL, demais com perfil SEMI-CONFIÁVEL
Quantidade de riscos	15 riscos
Prioridade real dos riscos	3 riscos com impacto de tipo CRITICO(r_1, r_2 e r_3), demais como SECUNDÁRIO
Quantidade de execuções	10 testes consecutivos acima da mesma estrutura organizacional

O simulador foi configurado para que os agentes mudassem aleatoriamente as suas opiniões com relação à criticidade dos riscos configurando as avaliações com um perfil ALEATÓRIO. Esta condição provocou mudanças aleatórias nos resultados do tratamento de riscos e igualmente nos coeficientes de confiança, obtendo os resultados apresentados na Figura 5.8.

Na Figura 5.8 observa-se que os coeficientes de relevância responderam corretamente às

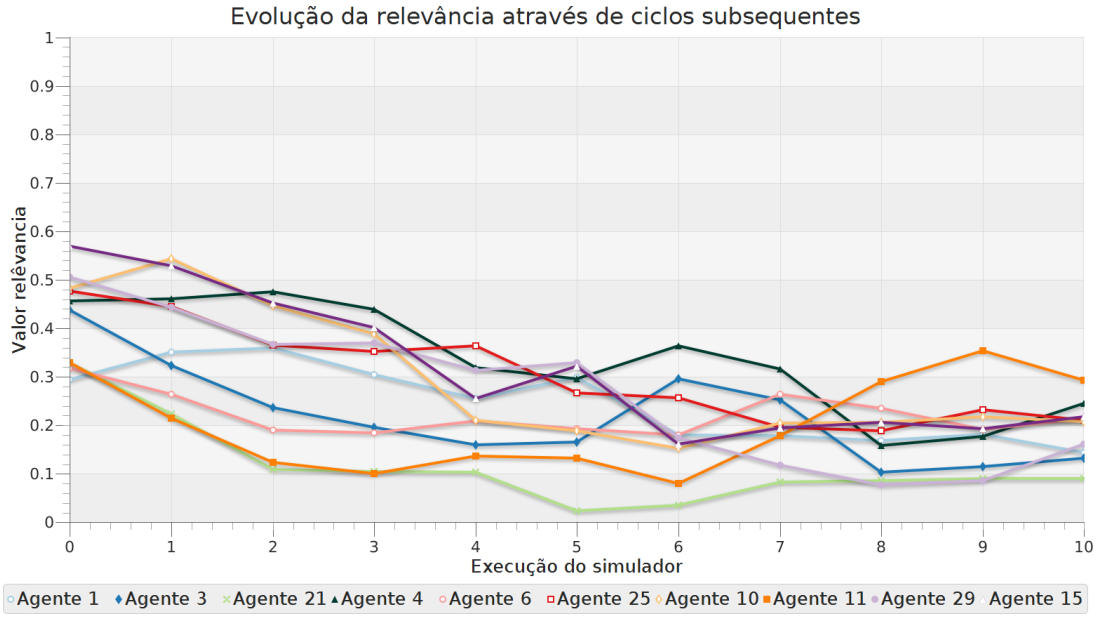

Figura 5.8 – Evolução da confiança com mudanças aleatórias de desempenho no tratamento de riscos

mudanças na efetividade do tratamento de riscos, onde os resultados negativos de novo representam um impacto maior já que ante a presença de perdas os valores de relevância para todos os agentes apresentam uma magnitude menor até o final do ciclo 10. Mesmo assim, com os resultados obtidos é possível concluir que o processo de atualização respondeu de forma certa às mudanças aleatórias no desempenho do tratamento de risco. Aqueles agentes com opiniões erradas constantes como os agentes 23 e 22 alcançaram valores de relevância baixos mesmo tendo a confiança uma confiança alta no inicio da simulação, e agentes como o 35 aumentaram os seu coeficiente de relevância como consequência da melhoria das suas avaliações.

Finalmente, pode ser observado que os pesos de confiança são refinados em cada execução gerando um efeito de "memória de confiança", onde os resultados de todas as execuções passadas são condensados na relevância como produto do processo de atualização que considera confiança atual e os resultados do tratamento de riscos (vide seção 3.4.8).

5.6 Conclusões parciais

Neste capítulo foram apresentados os resultados obtidos com a simulação da metodologia proposta no capítulo 3. O uso da confiança possibilitou dar ênfase naquelas estimativas de risco consideradas como mais confiáveis por causa da relação entre a confiabilidade do emissor de confiança e as suas opiniões.

Os resultados demonstraram que este enfase pode reduzir de forma significativa o desvio nas estimativas de risco, sempre que seja possível quantificar a confiança. O processo de atualização de confiança foi capaz de refinar os coeficientes de relevância baseado nos desempenho dos tratamentos de riscos respondendo tanto a resultados positivos quanto negativos com uma dinâmica de confiança "positivo devagar-negativo rápido", porém a efetividade da proposta resultou dependente da proporção entre estimativas de risco certas e o tamanho total do comitê de avaliação de riscos.

6 CONCLUSÕES

Trabalhos prévios evidenciaram a existência de desvios nos resultados de análises e avaliações de riscos como consequência do uso de dados subjetivos -i.e. opiniões humanas- para a criação de estimativas de risco. Tais desvios têm como consequência tratamentos de riscos guiados de forma errônea, os quais podem gerar prejuízos por causa de riscos não tratados e que são explorados por ameaças de segurança de informação.

Embora a eliminação da informação subjetiva seja plausível, a visão de análise que este tipo de informação proporciona faz com que seja necessário criar modelos de gestão de riscos que considerem e tratem com a subjetividade. Porém a grande maioria dos esforços para melhorar a exatidão das atividades da análise/avaliação de riscos estão focados no tratamento de fatores situacionais, mas muitos destes esforços negligenciam a existência da subjetividade que pode afetar estes factores, motivo pelo qual o problema de pesquisa é considerado ainda aberto (WORKMAN, 2012).

Este trabalho propôs a criação de uma abordagem de quantificação de confiança como um suporte para a redução de desvios causados pelas opiniões humanas dentro do contexto de gestão de riscos de segurança de informação. Para o desenvolvimento do trabalho as principais atividades desenvolvidas foram: i) a avaliação das possibilidades do uso da confiança dentro do contexto de gestão de riscos; ii) a identificação e descrição de modelos de reputação computacional; iii) a adaptação e integração de um modelo de quantificação de confiança visando dar suporte à atualização de confiança baseada no desempenho dos tratamentos de riscos; e iv) a avaliação das vantagens e limitantes da abordagem mediante a criação de um cenário de simulação por computador.

A motivação principal para o uso de confiança como um fator de apoio foi o fato que a confiança e os riscos são conceitos estreitamente relacionados (LUND; SOLHAUG; LEN, 2010). No entanto o uso da confiança requer a criação de modelos complexos de quantificação, onde a criação é altamente dependente do contexto e das dimensões que precisam ser analisadas (GOLBECK, 2006). O maior desafio é a construção da noção de confiança baseada em historia ou recomendações.

Análise da literatura prévia evidenciou a existência de duas tendências para a criação de modelos de confiança, sendo a primeira a criação de modelos baseados exclusivamente em avaliações de interações previas e a segunda a criação de modelos complexos multidimensionais.

Dentro desta última tendência, a quantificação de confiança com redes sociais tem atraído especial atenção, principalmente como consequência do aumento da disponibilidade de informação por causa do uso de redes sociais online. Outro motivo é a robustez obtida com estes modelos porque consideram as interações entre os membros da rede e a estrutura de interação.

A proposta foi criada sobre a base do ciclo de gestão de riscos genérico definido na norma ISO 27005:2011, integrando um modelo de quantificação de confiança baseado em redes sociais, um método de análises/avaliação de riscos por composição de métodos e uma técnica de retroalimentação de confiança baseada na avaliação do desempenho de tratamento de risco usando indicadores KRI.

A integração das três ferramentas foi realizada mediante a criação de um coeficiente de relevância que representa um coeficiente global de confiança baseado em percepções locais. Este coeficiente foi introduzido posteriormente como uma ponderação matemática dentro das fórmulas de estimativas de riscos, dando como resultado um índice composto de riscos(CRI) que considera a confiabilidade do fornecedor da estimativa de risco. Este índice é utilizado no tratamento de riscos, e no monitoramento do seu desempenho para retroalimentar o modelo de confiança, aproveitando as características cíclicas da gestão de riscos.

Para conhecer as vantagens e limitantes desta abordagem, foi criado um simulador personalizado onde os experimentos demonstraram que o uso de ponderações matemáticas é uma abordagem factível, e que com algumas modificações as percepções de confiança criadas com redes sociais podem ser utilizadas dentro das atividades da análise/avaliação de riscos de segurança para reduzir os desvios nos resultados.

A solução proposta consegue reproduzir uma dinâmica de confiança onde a penalização por causa de opiniões errôneas é mais rápida do que o ganho causado pelas opiniões certas, dinâmica formalmente conhecida como "positivo devagar-negativo rápido"a qual é considerada como a ideal para seres humanos (JONKER; TREUR, 1999). Além disso as etapas da metodologia proposta são dependentes unicamente da saída da etapa anterior, o que permite considerar a criação de extensões da metodologia, para dar suporte a técnicas diferentes para cada uma das etapas, com a única limitante que os resultados devem ser expressados no mesmo intervalo de valores que as metodologias atuais.

As simulações demonstraram que a ênfase nas opiniões confiáveis incrementa a precisão das estimativas de riscos e reduz a priorização de riscos altos fora da zona de tratamento. Porém a efetividade da abordagem é dependente da proporção entre a quantidade de avaliadores de

riscos confiáveis e a quantidade total de avaliadores de riscos, já que foi conseguida uma redução de 15% com uma proporção de 0.25, de 34% com uma proporção de 0.5 e de 38% com uma proporção de 0.75.

Apesar dos inconvenientes da efetividade proporcional, foi observado que a relação entre os riscos altos priorizados fora da zona de tratamento mediante a composição original e a composição com confiança, apresentou, durante todas as simulações, valores menores ou iguais a 1, o que significa que em todas as ocasiões as estimativas da composição suportada por confiança tiveram um melhor desempenho em comparação com a composição de métodos original.

A atualização de confiança foi capaz de eliminar e penalizar opiniões errôneas de risco a partir da segunda execução consecutiva e de eliminar-las definitivamente a partir da quarta execução. Na mesma linha, a atualização foi capaz de reproduzir a dinâmica de atualização de confiança frente a uma ausência total de informação de testemunhas (WI) para a quantificação da confiança inicial, mediante o estabelecimento de valores fixos e homogêneos de confiança entre os membros da rede social. Finalmente, e ante mudanças aleatórias na efetividade das opiniões dos avaliadores, a abordagem reagiu de forma correta.

Em suma, o refinamento constante dos coeficientes de confiança gerou um "efeito memória", onde os resultados do tratamento de riscos são condensados como consequência da modificação da função de atualização de TrustWebRank, conservando as propriedades desejadas durante os testes de efetividade na redução de desvios e durante os testes da dinâmica de evolução de confiança. O resultado é um modelo de análise/avaliação de risco mais robusto e consequentemente um gerenciamento de riscos mais consistente.

6.1 Limitantes e trabalhos futuros

Além da limitação intrínseca que representa a proporcionalidade entre a quantidade de opiniões boas e a efetividade da abordagem, foram identificadas duas limitantes. A primeira é a impossibilidade de avaliar a proposta frente a um período ideal de convergência para à atualização da confiança, dado que cada organização pode ter as suas próprias políticas de execução de gestão de riscos -e.g. mensual, semestral, anual, aperiódica-. Mesmo assim, com a alteração dos valores dos parâmetros κ e γ a convergência da proposta pode ser acelerada ou atrasada para cumprir com os requisitos de cada organização. A segunda limitante é o fato que a solução atualiza a confiança baseando-se unicamente em resultados de desempenho do tratamento de riscos, motivado principalmente porque era almejado um processo com etapas

independentes, o que pode não ser suficiente no caso que estes indicadores sejam considerados como limitados e não representativos da realidade.

Para trabalhos futuros, sugere-se:

1. A criação de atualizações de confiança baseadas em noções de confiança mais complexas que considerem outros fatores, tais como integridade, complacência, competências, egoísmo, reciprocidade e outras;

2. A avaliação do modelo proposto com diferentes modelos de quantificação de confiança e metodologias de análise/avaliação de riscos, visando suporte para outros contextos com caraterísticas diferentes;

3. A introdução de uma reconfiguração dinâmica do comitê de avaliação de riscos, já que ate o momento o processo foi testado assumindo que os participantes do comitê de análise/avaliação de riscos serão os mesmos durante todas as execuções do ciclo de gestão de riscos.

REFERÊNCIAS

ALLEN, J.; JAMES, A. D.; GAMLEN, P. Formal versus informal knowledge networks in R&D: a case study using social network analysis. **R&D Management**, v. 37, n. 3, p. 179–196, jun. 2007. ISSN 0033-6807. Disponível em: <http://doi.wiley.com/10.1111/j.1467-9310-.2007.00468.x>.

AMARAL, E. H.; AMARAL, M. M.; NUNES, R. C. Metodologia para Cálculo do Risco por Composição de Métodos. In: **Simpósio Brasileiro de Segurança de Informação e de Sistemas Computacionais**. [s.n.], 2010. p. 461–473. Disponível em: <http://labcom.inf.ufrgs-.br/labcom/ceseg/anais/2010/06_artigos_completos/artigo_37.pdf>.

ANDRESS, J. **The basics of information security: understanding the fundamentals of InfoSec in theory and practice**. [S.l.: s.n.], 2011. ISBN 9781597496537.

aO, A. P. P.; NUNES, R. C.; LóPEZ, V. L. O. Definition Risk Assessment Committee Based on Competencies. In: **XII SEPROSUL Semana de Engenharia de Produção Sulamericana**. Assunción-Paraguay: [s.n.], 2012. p. 01–10.

AUBIGNY, M. **Risk Modelling and Simulation for Critical Information Infrastructure Protection**. Tese (Doutorado) — Université Du Luxembourg, 2009. Disponível em: <http://www.micie.eu/documents/Aubigny_Master_2009.pdf>.

BACHMANN, R. **Handbook of trust research**. [S.l.: s.n.], 2006.

BAGHERIAN, R. et al. Community participation in watershed management programs. **Journal of Social Sciences**, v. 5, n. 3, p. 251–256, 2009. Disponível em: <http://thescipub-.com/abstract/10.3844/jssp.2009.251.256>.

BALKE, T.; KöNIG, S.; EYMANN, T. A survey on reputation systems for artificial societies. 2009. Disponível em: <http://www.econstor.eu/handle/10419/52616>.

BANERJEE, A. Equivalence of Risk: A Mathematical Approach. In: **The 29th International System Safety Conference**. [s.n.], 2011. Disponível em: <http://www.system-safety.org-/conferences/2011/papers/Equivalence of Risk - A Mathematical Approach.pdf>.

BERNSTEIN, L.; YUHAS, C. M. **Trustworthy Systems through Quantitative Software Engineering**. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2005. ISBN 9780471750338. Disponível em: <http://doi.wiley.com/10.1002/0471750336>.

BOEHM, B. W. Software risk management: principles and practices. **Software, IEEE**, IEEE Software Magazine, 1991. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all-.jsp?arnumber=62930>.

BOREALE, M.; CELESTINI, A. Asymptotic risk analysis for trust and reputation systems. **SOFSEM 2013: Theory and Practice of Computer**, p. 1–12, 2013. Disponível em: <http://link.springer.com/chapter/10.1007/978-3-642-35843-2_16>.

BURT, R. S.; KILDUFF, M.; TASSELLI, S. Social network analysis: foundations and frontiers on advantage. **Annual review of psychology**, v. 64, p. 527–47, jan. 2013. ISSN 1545-2085. Disponível em: <http://www.ncbi.nlm.nih.gov/pubmed/23282056>.

BUSKENS, V. The social structure of trust. **Social Networks**, v. 20, n. 3, p. 265–289, jul. 1998. ISSN 03788733. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii-/S0378873398000057>.

CARCHIOLO, V. et al. A Distributed Algorithm for Personalized Trust Evaluation in Social Networks. In: ESSAAIDI, M.; MALGERI, M.; BADICA, C. (Ed.). **Studies in Computational Intelligence**. Springer Berlin / Heidelberg, 2010, (Studies in Computational Intelligence, v. 315). p. 99–108. ISBN 978-3-642-15210-8. Disponível em: <http://dx.doi.org/10.1007/978-3-642-15211-5_11>.

CARCHIOLO, V. et al. Trust assessment: a personalized, distributed, and secure approach. **Concurrency and Computation: Practice and Experience**, John Wiley & Sons, Ltd, v. 24, n. 6, p. 605–617, 2012. ISSN 1532-0634. Disponível em: <http://dx.doi.org/10.1002/cpe.1856 http://onlinelibrary.wiley.com/doi/10.1002/cpe.1856/full>.

CARTER, C. R.; KAUFMANN, L.; MICHEL, A. Behavioral supply management: a taxonomy of judgment and decision-making biases. **International Journal of Physical Distribution & Logistics Management**, v. 37, n. 8, p. 631–669, 2007. ISSN 0960-0035. Disponível em: <http://www.emeraldinsight.com/10.1108/09600030710825694>.

CHAN, K.; CHO, J.-H.; ADALI, S. Composite Trust Model for an Information Sharing Scenario. **2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing**, Ieee, p. 439–446, set. 2012. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper-.htm?arnumber=6332033>.

CHANDRA, J. et al. A Tunable Mechanism for Identifying Trusted Nodes in Large Scale Distributed Networks. In: **2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications**. IEEE, 2012. p. 722–729. ISBN 978-1-4673-2172-3. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6296041 http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6296041>.

CHANG, B.-J. et al. Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks. **2008 IEEE Asia-Pacific Services Computing Conference**, Ieee, p. 156–161, dez. 2008. Disponível em: <http://ieeexplore.ieee-.org/lpdocs/epic03/wrapper.htm?arnumber=4780669>.

CHOROMANSKI, K.; MATUSZAK, M.; MIEKISZ, J. Scale-Free Graph with Preferential Attachment and Evolving Internal Vertex Structure. **Journal of Statistical Physics**, v. 151, n. 6, p. 1175–1183, abr. 2013. ISSN 0022-4715. Disponível em: <http://link.springer.com/10-.1007/s10955-013-0749-1>.

CLARKE, L. Politics and bias in risk assessment. **The Social Science Journal**, v. 25, n. 2, p. 155–165, 1988. Disponível em: <http://www.sciencedirect.com/science/article/pii-/0362331988900031>.

CLEMEN, R. T.; WINKLER, R. L. Combining Probability Distributions From Experts in Risk Analysis. **Risk Analysis**, Springer Netherlands, v. 19, n. 2, p. 187–203, 1999. ISSN 02724332. Disponível em: <http://www.springerlink.com/content/u03574n6440117t1/>.

COLEMAN, T. S. **A Practical Guide to Risk Management**. Research Foundation of CFA Institute, 2011. 228 p. ISBN 1934667412. Disponível em: <http://www.amazon.com/A-Practical-Guide-Risk-Management/dp/1934667412>.

CROSS, R.; PARKER, A.; BORGATTI, S. **A bird's-eye view: Using social network analysis to improve knowledge creation and sharing**. [S.l.], 2002. 18 p. Disponível em: <https://www.gslis.utexas.edu/~i385q/spring2005/readings/Cross_2002_using_social_network.pdf>.

DAILAMI, M.; LIPKOVICH, I.; DYCK, V. J. INFRISK: A Computer Simulation Approach to Risk Management in Infrastructure Project Finance Transactions. The World Bank, mar. 1999. Disponível em: <http://elibrary.worldbank.org/doi/book/10.1596/1813-9450-2083>.

DALTON, D. et al. Number of directors and financial performance: a meta-analysis. **Academy of Management Journal**, v. 42, n. 6, p. 674–686, 1999.

DAVIES, J. et al. **Key risk indicators–their role in operational risk management and measurement**. [S.l.], 2006. 1–32 p. Disponível em: <http://d.yimg.com/kq/groups/12093474-/1290864495/name/McLenaghenTara3.pdf>.

EKELHART, A.; FENZ, S.; NEUBAUER, T. AURUM : A Framework for Information Security Risk Management. **SciencesNew York**, IEEE, v. 0, n. September 2008, p. 1–10, 2009. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4755409>.

FENG, N.; LI, M. An information systems security risk assessment model under uncertain environment. **Applied Soft Computing**, v. 11, n. 7, p. 4332–4340, out. 2011. ISSN 15684946. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S1568494610001419>.

GOLBECK, J. Computing with trust: Definition, properties, and algorithms. In: **Securecomm and Workshops, 2006**. [s.n.], 2006. p. 1–7. ISBN 1424404231. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4198839>.

GRANDISON, T. Trust management for internet applications. 2003. Disponível em: <http://www.doc.ic.ac.uk/~mss/Papers/Grandison-phd.pdf>.

HE, F. et al. Chain of Trust Testing Based on Model Checking. **2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing**, Ieee, p. 273–276, 2010. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper-.htm?arnumber=5480664>.

IMMANENI, A.; MASTRO, C.; HAUBENSTOCK, M. A Structured Approach to Building Predictive Key Risk Indicators. n. May, p. 42–47, 2004.

ISACA. **The Risk IT Framework**. ISACA, 2009. 107 p. ISBN 9781604201116. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf>.

ISO/IEC. **ISO/IEC 27001:2011 – Information technology – Security techniques – Information security management systems – Requirements**. Geneva, Switzerland: ISO/IEC, 2011.

ISO/IEC. **ISO/IEC 27002:2011 Information technology – Security techniques – Information security risk management**. [S.l.: s.n.], 2011.

ISO/IEC. **ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management**. Geneva, Switzerland: ISO/IEC, 2011.

JONES, K. Trust as an affective attitude. **Ethics**, v. 107, n. 1, p. 4–25, 1996. Disponível em: <http://www.jstor.org/stable/10.2307/2382241>.

JONKER, C.; TREUR, J. Formal analysis of models for the dynamics of trust based on experiences. In: **9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World, MAAMAW'99**. [s.n.], 1999. p. 221–231. Disponível em: <http://link.springer.com/chapter/10.1007/3-540-48437-X_18>.

JOSANG, A.; GRAY, E.; KINATEDER, M. Analysing Topologies of Transitive Trust. In: **Proceedings of the Workshop of Formal Aspects of Security and Trust (FAST)**. [S.l.: s.n.], 2003.

KALBERS, L.; FOGARTY, T. Audit committee effectiveness: an empirical investigation of the contribution of power. **Auditing: A Journal of Practice and Theory**, v. 12, p. 24–49, 1993.

KAMVAR, S. D.; SCHLOSSER, M. T.; GARCIA-MOLINA, H. The Eigentrust algorithm for reputation management in P2P networks. In: **Proceedings of the 12th international conference on World Wide Web**. New York, NY, USA: ACM, 2003. (WWW '03), p. 640–651. ISBN 1-58113-680-3. Disponível em: <http://doi.acm.org/10.1145/775152.775242>.

KARABACAK, B.; SOGUKPINAR, I. ISRAM: information security risk analysis method. **Computers Security**, Elsevier, v. 24, n. 2, p. 147–159, 2005. ISSN 01674048. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0167404804001890>.

KESSEL, P. van; ALLAN, K. **Under cyber attack: EY's Global Information Security Survey**. [S.l.], 2013.

KHAMBHAMMETTU, H. et al. A Framework for Risk Assessment in Access Control Systems. **Computers & Security**, Elsevier Ltd, n. Sec 2012, p. 1–18, abr. 2013. ISSN 01674048. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0167404813000552>.

KLEINBERG, J. The small-world phenomenon. In: **Proceedings of the thirty-second annual ACM symposium on Theory of computing - STOC '00**. New York, New York, USA: ACM Press, 2000. p. 163–170. ISBN 1581131844. Disponível em: <http://dl.acm.org/citation-.cfm?id=335325 http://portal.acm.org/citation.cfm?doid=335305.335325>.

KO, D.; KIRSCH, L.; KING, W. Antecedents of knowledge transfer from consultants to clients in enterprise system implementations. **MIS quarterly**, v. 29, n. 1, p. 59–85, 2005. Disponível em: <http://www.jstor.org/stable/10.2307/25148668>.

LEITNER, A.; SCHAUMULLER-BICHL, I. ARiMA - A New Approach to Implement ISO/IEC 27005. In: **2009 2nd International Symposium on Logistics and Industrial Informatics**. IEEE, 2009. p. 1–6. Disponível em: <http://ieeexplore.ieee.org/articleDetails-.jsp?arnumber=5258624>.

LIU, H. et al. Predicting trusts among users of online communities: an epinions case study. **Proceedings of the 9th ACM conference on Electronic commerce**, p. 310–319, 2008. Disponível em: <http://dl.acm.org/citation.cfm?id=1386838>.

LIU, M. **Efficient simulation in financial risk management**. Tese (Doutorado) — Northwestern University, 2010. Disponível em: <http://users.iems.northwestern.edu/~staum-/Ming_Liu_Thesis.pdf>.

LOPEZ, J.; ALCARAZ, C.; ROMAN, R. Smart control of operational threats in control substations. **Computers & Security**, Elsevier Ltd, v. 38, p. 14–27, out. 2013. ISSN 01674048. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0167404813000588>.

LUKAS, C.; WALGENBACH, P. Trust me, it is High Trust: On Trust and its Measurement. 2010. Disponível em: <http://www.uni-konstanz.de/FuF/wiwi/workingpaperseries-/WP_Lukas-Walgenbach-9-10.pdf>.

LUND, M.; SOLHAUG, B. r.; LEN, K. S. Evolution in relation to risk and trust management. **Computer**, p. 49–55, 2010. Disponível em: <http://heim.ifi.uio.no/~ketils/kst/Articles/2010-.Computer.pdf>.

MANCHALA, D. W. E-commerce trust metrics and models. **Internet Computing, IEEE**, v. 4, n. April, p. 36–44, 2000. ISSN 1089-7801. Disponível em: <http://ieeexplore.ieee.org-/xpls/abs_all.jsp?arnumber=832944>.

MARSH, S. **Formalising Trust as a Computational Concept, in Computing Science and Mathematics**. Tese (Doutorado) — University of Stirling: Stirling, 1994.

MARTIN, A. **The ten-page introduction to Trusted Computing**. [S.l.], 2008.

MCKNIGHT, D. H.; CHERVANY, N. L. The meanings of trust. **Measurement**, Citeseer, v. 55455, n. 612, p. 86, 1996. ISSN 0277786X. Disponível em: <http://citeseerx.ist.psu.edu-/viewdoc/summary?doi=10.1.1.155.1213>.

MCNULTY, T.; FLORACKIS, C.; ORMROD, P. **Corporate Governance and Risk: A Study of Board Structure and Process**. Liverpool, UK, 2012.

MCPHERSON, M.; SMITH-LOVIN, L.; COOK, J. Birds of a feather: Homophily in social networks. **Annual review of sociology**, 2001. Disponível em: <http://www.jstor.org/stable-/10.2307/2678628>.

MOELLER, R. R. **COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes (Wiley Corporate F&A)**. Wiley, 2011. Disponível em: <http://www.amazon.com/COSO-Enterprise-Risk-Management-ebook-/dp/B005HF2HO0>.

NG, T.-H.; CHONG, L.-L.; ISMAIL, H. Is the risk management committee only a procedural compliance?: An insight into managing risk taking among insurance companies in Malaysia. **The Journal of Risk Finance**, v. 14, n. 1, p. 71–86, 2013. ISSN 1526-5943. Disponível em: <http://www.emeraldinsight.com/10.1108/15265941311288112>.

O'MADADHAIN, J.; FISHER, D.; SMYTH, P. **Analysis and visualization of network data using JUNG**. [S.l.], 2005. VV, n. Ii. Disponível em: <http://www.ics.uci.edu/~smyth-/kddpapers/UCI_KD-D_JUNG_preprint.pdf>.

PAOLUCCI, M.; BALKE, T.; CONTE, R. **Review of internet user-oriented reputation applications and application layer networks**. [S.l.], 2006. Disponível em: <http://papers-.ssrn.com/sol3/papers.cfm?abstract_id=1475424>.

PAPAGEORGIOU, A.; PASKOV, S. Deterministic simulation for risk management. **The Journal of Portfolio Management**, n. November, p. 1–11, 1999. Disponível em: <http://www.iijournals.com/doi/pdfplus/10.3905/jpm.1999.319698>.

PINYOL, I.; SABATER-MIR, J. Computational trust and reputation models for open multi-agent systems: a review. **Artificial Intelligence Review**, v. 40, n. 1, p. 1–25, jul. 2011. ISSN 0269-2821. Disponível em: <http://www.springerlink.com/index/10.1007/s10462-011-9277-z http://link.springer.com/10.1007/s10462-011-9277-z>.

PME, D. e. r. E. **As Pequenas e Médias Empresas que Mais Crescem no Brasil**. [S.l.], 2013. Disponível em: <https://www.deloitte.com/view/pt_BR/br/Conteudos/estudosepesquisas-/PMEs/fd6f50ce2dd70410VgnVCM2000003356f70aRCRD.htm>.

PRICEWATERHOUSECOOPERS. **A practical guide to risk assessment***. 2008. Disponível em: <http://www.pwc.com/us/en/issues/enterprise-risk-management/publications/guide-to-risk-assessment-risk-management-from-pwc.jhtml>.

PRICEWATERHOUSECOOPERS. **Pesquisa Global de Segurança da Informação 2013**. [S.l.], 2013. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets-/pesquisa-seguranca-inforrmacao-13.pdf>.

PUJOL, J. M.; SANGüESA, R.; DELGADO, J. Extracting reputation in multi agent systems by means of social network topology. In: **Proceedings of the first international joint conference on Autonomous agents and multiagent systems part 1 - AAMAS '02**. New York, New York, USA: ACM Press, 2002. p. 467. ISBN 1581134800. Disponível em: <http://dl.acm.org-/citation.cfm?id=544853 http://portal.acm.org/citation.cfm?doid=544741.544853>.

ROMER, P. M. Thinking and Feeling. **The American Economic Review**, American Economic Association, v. 90, n. 2, p. pp. 439–443, 2000. ISSN 00028282. Disponível em: <http://www.jstor.org/stable/117265>.

SABATER, J.; SIERRA, C. Review on Computational Trust and Reputation Models. **Artificial Intelligence Review**, v. 24, n. 1, p. 33–60, set. 2005. ISSN 0269-2821. Disponível em: <http://link.springer.com/10.1007/s10462-004-0041-5>.

SEARS, D. O. The Person-Positivity Bias. **Journal of Personality and Social Psychology**, v. 44, n. 2, p. 233–250, 1983. ISSN 00223514. Disponível em: <http://psycnet.apa.org-/journals/psp/44/2/233/>.

SEBRAE/SC. **SEBRAE/SC - Legislação - CRITÉRIOS DE CLASSIFICAÇÃO DE EMPRESAS: EI - ME - EPP**. 2014. Disponível em: <http://www.sebrae-sc.com.br/leis-/default.asp?vcdtexto=4154>.

SEGUDOVIC, H. Qualitative risk analysis method comparison. In: INFIGO INFORMATION SECURITY. **International ICT Convention MIPRO**. [S.l.], 2006. p. 1–17.

SEN, S.; SAJJA, N. Robustness of reputation-based trust: boolean case. In: **Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1**. New York, NY, USA: ACM, 2002. (AAMAS '02), p. 288–293. ISBN 1-58113-480-0. Disponível em: <http://doi.acm.org/10.1145/544741.544808>.

SENIK, C. Income distribution and well-being: what can we learn from subjective data? **Journal of Economic Surveys**, v. 19, n. 1, p. 43–63, fev. 2005. ISSN 0950-0804. Disponível em: <http://doi.wiley.com/10.1111/j.0950-0804.2005.00238.x http://dx.doi.org/10.1111/j-.0950-0804.2005.00238.x>.

SHERCHAN, W.; NEPAL, S.; PARIS, C. A survey of trust in social networks. **ACM Computing Surveys**, v. 45, n. 4, p. 1–33, ago. 2013. ISSN 03600300. Disponível em: <http://dl.acm.org/citation.cfm?doid=2501654.2501661>.

STAMATIS, D. H. **Failure mode and effect analysis: FMEA from theory to execution**. ASQ Quality Press, 2003. 80 p. ISSN 00401706. ISBN 0873895983. Disponível em: <http://www.jstor.org/stable/1268911>.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology. **Nist Special Publication**, Citeseer, v. 800-30, n. SP 800-30, p. 55, 2002. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.6062>.

TALBOT, M. J. **How to Performance Benchmark Your Risk Management: A practical guide to help you tell if your risk management is effective**. CreateSpace Independent Publishing Platform, 2012. 52 p. ISBN 1466377577. Disponível em: <http://www.amazon-.com/Performance-Benchmark-Your-Risk-Management/dp/1466377577>.

The Institute of Operational Risk. **KRI Guidance**. [S.l.], 2010. Disponível em: <https://www-.ior-institute.org/ior-news/the-ior-publishes-third-sound-practice-guidance-paper>.

TRIFUNOVIC, S.; LEGENDRE, F.; ANASTASIADES, C. Social Trust in Opportunistic Networks. In: **2010 INFOCOM IEEE Conference on Computer Communications Workshops**. IEEE, 2010. p. 1–6. ISBN 978-1-4244-6739-6. Disponível em: <http:/-/ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5466696>.

TRUNITS, C. Trust as a tradable commodity: a foundation for safe electronic marketplaces. v. 26, n. 2, 2010.

TSVETOVAT, M.; KOUZNETSOV, A. **Social Network Analysis for Startups: Finding Connections on the Social Web**. 1. ed. [S.l.]: O'Reilly Media, 2011. 192 p. ISBN 1449306462.

WALTER, F. E. Trust as the basis of coalition formation in electronic marketplaces. **Advances in Complex Systems**, v. 14, n. 02, p. 111–131, 2011. Disponível em: <http://www.worldscientific.com/doi/abs/10.1142/S0219525911003049>.

WALTER, F. E.; BATTISTON, S.; SCHWEITZER, F. Personalised and dynamic trust in social networks. **Proceedings of the third ACM conference on Recommender systems - RecSys '09**, ACM Press, New York, New York, USA, p. 197, 2009. Disponível em: <http://portal.acm.org/citation.cfm?doid=1639714.1639747>.

WATTS, D. J. Networks, dynamics, and the small-world phenomenon 1. **American Journal of Sociology**, v. 105, n. 2, p. 493–527, 1999. Disponível em: <http://www.jstor.org/stable/10-.1086/210318>.

WATTS, D. J. **Six Degrees: The Science of a Connected Age**. W. W. Norton & Company, 2003. 368 p. ISBN 0393041425. Disponível em: <http://www.amazon.com/Six-Degrees-The-Science-Connected/dp/0393041425>.

WINSHIP, C.; MARE, R. D. Models for Sample Selection Bias. **Annual Review of Sociology**, Annual Reviews, v. 18, p. pp. 327–350, 1992. ISSN 03600572. Disponível em: <http://www.jstor.org/stable/2083457>.

WORKMAN, M. Validation of a biases model in strategic security decision making. **Information Management & Computer Security**, v. 20, n. 2, p. 52–70, 2012. ISSN 0968-5227. Disponível em: <http://www.emeraldinsight.com/journals.htm?articleid=17036088 http://www.emeraldinsight.com/10.1108/09685221211235599>.

XIONG, L.; LIU, L. A reputation-based trust model for peer-to-peer e-commerce communities. In: **IEEE International Conference on E-Commerce, 2003. CEC 2003.** [s.n.], 2003. p. 275 – 284. ISBN 0769519695. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all-.jsp?arnumber=1210262>.

ZAHED-BABELAN, A. Attitudes of Payme Noor University Students toward Distance Education. **International Research Journal of Applied and Basic Sciences**, v. 3, n. 5, p. 1040–1044, 2012. Disponível em: <http://www.irjabs.com/files_site/paperlist-/r_412_121110143603.pdf>.

ZHENG, R. et al. An IOT Security Risk Autonomic Assessment Algorithm. **TELKOMNIKA Indonesian Journal of Electrical Engineering**, v. 11, n. 2, p. 819–826, 2013. Disponível em: <http://www.iaesjournal.com/online/index.php/TELKOMNIKA/article/view/2030>.

ZHOU, R.; HWANG, K.; CAI, M. GossipTrust for Fast Reputation Aggregation in Peer-to-Peer Networks. **Knowledge and Data Engineering, IEEE Transactions on**, v. 20, n. 9, p. 1282–1295, set. 2008. ISSN 1041-4347. Disponível em: <http://ieeexplore.ieee-.org/lpdocs/epic03/wrapper.htm?arnumber=4459326 http://ieeexplore.ieee.org/xpls/abs_all-.jsp?arnumber=4459326>.