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

METODOLOGIA PARA ANÁLISE E AVALIAÇÃO DE RISCOS POR COMPOSIÇÃO DE MÉTODOS

DISSERTAÇÃO DE MESTRADO

Marisa Munaretto Amaral

Santa Maria, RS, Brasil

2011

METODOLOGIA PARA ANÁLISE E AVALIAÇÃO DE RISCOS POR COMPOSIÇÃO DE MÉTODOS

Marisa Munaretto Amaral

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

Orientador: Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS, Brasil

2011

A485m Amaral, Marisa Munaretto
Metodologia para análise e avaliação de riscos por composição de métodos / por Marisa Munaretto Amaral. – 2011.
74 p.: il.; 31 cm.

Orientador: Raul Ceretta Nunes.
Dissertação (mestrado) – Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Informática, RS, 2011.

1. Sistemas computacionais 2. Gestão da Informação 3. Segurança da Informação 4. Informação digital 5.Sistemas de Informação 6. Análise de riscos 7.Cálculo do risco 8.Abordagem Seis Sigma I. Nunes, Raul Ceretta II.Título.

CDU: 004:658

Ficha catalográfica elaborada por Simone G. Maisonave – CRB 10/1733
Biblioteca Central da UFSM

Endereço Eletrônico: marisa.munaretto@gmail.com

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

A comissão Examinadora, abaixo assinada,
Aprova a Dissertação de Mestrado

METODOLOGIA PARA ANÁLISE E AVALIAÇÃO DE RISCOS POR COMPOSIÇÃO DE MÉTODOS

elaborada por
Marisa Munaretto Amaral

como requisito parcial para obtenção do grau de
Mestre em Computação

COMISSÃO EXAMINADORA:

_____
Raul Ceretta Nunes, Dr.
(Presidente/Orientador)

_____
Taisy Silva Weber, Dra. (UFRGS)

_____
Lisandra Manzoni Fontoura, Dra. (UFSM)

Santa Maria, 02 de Agosto de 2011.

À minha filha Julia e ao meu marido Cezar, aos meus pais, Creci e Brasil, e aos meus irmãos, Mara, Magda e Flavio pela compreensão e estímulo constante, dedico esta obra.

Agradecimentos

Agradeço, em primeiro lugar, a Deus, por esta oportunidade, pela experiência adquirida, pelo convívio com os colegas, pela força e determinação que me levaram a conclusão de mais uma etapa de aprendizado.

Ao Professor Raul Ceretta Nunes, pelo apoio e estímulo, pelas considerações feitas para o desenvolvimento deste trabalho.

Aos professores e colegas do Curso de Pós-Graduação em Informática e ao Grupo de Pesquisa de Gestão e Tecnologia em Segurança da Informação da UFSM.

À Universidade Federal de Santa Maria, pela oportunidade, permitindo o meu aperfeiçoamento profissional.

Ao Centro de Processamento de Dados pelo apoio que sempre obtive durante estes 14 anos.

Aos meus colegas de trabalho, que sempre estiveram presentes com palavras de incentivo.

À minha filha Julia e ao meu marido Cezar, pelo apoio incondicional em todas às horas, pela compreensão, pelo amor e pelo incentivo.

Aos meus pais Creci e Brasil, que me ensinaram a importância do estudo, do esforço, da humildade e da honestidade.

Agradeço também, aos meus irmãos, que sempre estiveram ao meu lado incentivando e apoiando.

RESUMO

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

METODOLOGIA PARA ANÁLISE E AVALIAÇÃO DE RISCOS POR COMPOSIÇÃO DE MÉTODOS

Autora: Marisa Munaretto Amaral
Orientador: Prof. Dr. Raul Ceretta Nunes
Data e Local de Defesa: Santa Maria, 02 de Agosto de 2011.

A informação tornou-se um ativo valioso para as organizações e, em sistemas computacionais, está sujeita a diversos tipos de ameaças. A gestão de riscos é responsável por garantir a integridade, a confidencialidade e a disponibilidade dessas informações, identificando as principais vulnerabilidades e ameaças que cercam um sistema de informação.

Para assegurar a proteção dos ativos e diminuir a incidência de falhas de segurança, é necessário adotar práticas de gerenciamento de riscos. Vários métodos já foram propostos com esse objetivo, no entanto, alguns divergem significativamente entre si, podendo resultar em quantificações classificatórias divergentes, mesmo sendo aplicados em um mesmo domínio.

Este trabalho propõe uma metodologia para análise/avaliação de riscos, que utiliza a composição de métodos para obter resultados mais precisos, onde o risco de maior prioridade é obtido através da ponderação dos métodos analisados. Com o objetivo de validar a metodologia proposta, foi desenvolvida uma ferramenta computacional que automatiza todas as fases da metodologia e realiza os cálculos necessários para priorizar os riscos existentes.

O cenário de aplicação foi o Centro de Processamento de Dados da Universidade Federal de Santa Maria. Como resultado, obteve-se indicadores de risco potencialmente mais precisos, uma vez que refletem os riscos priorizados com base na ponderação dos métodos analisados.

Palavras-chave: Análise de Riscos, Segurança da Informação, Metodologia, Cálculo do Risco.

ABSTRACT

Master Dissertation
Computer Science Graduate Program
Federal University of Santa Maria

A METHODOLOGY FOR ANALYSIS AND RISKS ASSESSMENT BY METHODS COMPOSITION

Author: Marisa Munaretto Amaral
Advisor: Prof. Dr. Raul Ceretta Nunes
Santa Maria, August 02, 2011.

The information has become a valuable asset for organizations, and computer systems, is subject to various types of threats. Risk management is responsible for ensuring the integrity, confidentiality and availability of this information, identifying key vulnerabilities and threats that surround an information system.

To ensure the protection of assets and reduce the incidence of security breaches, it is necessary to adopt risk management practices. Several methods have been proposed for this purpose, however, some differ significantly from each other and may result in classifying different measurements, even when applied to the same domain.

This thesis proposes a methodology for analysis and risk assessment, which uses the composition of methods for more accurate results, where the risk of higher priority is obtained by weighting the methods analyzed. In order to validate the proposed methodology, we developed a computational tool that automates all stages of the process and performs the calculations necessary to prioritize the risks.

The application scenario was the Data Processing Center, Federal University of Santa Maria. As a result, we obtained risk indicators potentially more accurate, since they reflect the risks prioritized based on weighting of the methods analyzed.

Keywords: *Risk Analysis, Information Security, Methodology, Risk Calculation.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

ARIMA	*Austrian Risk Management Approach*
AURUM	*Automated Risk and Utility Management*
CCTA	*Central Communication and Telecom Agency*
CPD	Centro de Processamento de Dados
DMAIC	Definir-Medir- Implementar- Controlar
FMEA	*Failure Model and Effect Analysis*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ISRAM	*Information Security Risk Analysis Method*
MAAR	Metodologia para Análise e Avaliação de Riscos
MER	Modelo Entidade Relacionamento
NBR	Norma Brasileira Reguladora
NIST	*The National Institute of Standards and Technology*
NPR	Número de Prioridade de Risco
OCTAVE	*Operationally Critical Threat, Asset and Vulnerability Evaluation*
OGC	*Office of Government Commerce*
SGSI	Sistema de Gestão da Segurança da Informação
TCU	Tribunal de Contas da União
TIC	Tecnologia de Informação e Comunicação
UFSM	Universidade Federal de Santa Maria

SUMÁRIO

1 INTRODUÇÃO

O uso da informação digital nas organizações tornou-se um recurso vital e estratégico para aumentar a eficiência da operacionalização dos processos produtivos e de gestão. Em alguns casos, o sistema de informação é o principal patrimônio da empresa, o que o torna um ativo crítico que necessita ser protegido, pois está sujeito a ameaças internas e/ou externas (SANTOS, 2007).

Dessa forma, para garantir a segurança (integridade, disponibilidade e confidencialidade) das informações, se faz necessário gerenciar e identificar as ameaças que colocam em risco os ativos da organização. Assim, analisar os riscos de ocorrência de incidentes é uma tarefa essencial para a gestão da segurança da informação, pois permite identificar o grau de proteção que os ativos necessitam (CAMPOS, 2007) (OLIVEIRA, NUNES e ELLWANGER, 2009).

No entanto, a quantificação dos riscos é muitas vezes subjetiva e pode ser difícil atribuir valores consistentes para estimá-los (GRANDISON, 2003). Segundo Karabacak e Sogukpinar (2005), em função da complexidade da estrutura dos sistemas de informações atuais, os métodos qualitativos são mais adequados para estimar os riscos, pois não envolvem cálculos matemáticos. Entretanto, o próprio autor afirma que essa prática pode gerar resultados subjetivos, que dependem muito da opinião das pessoas que conduzem o processo de análise do risco.

De acordo com Ekelhart *et al. (*2009) as abordagens existentes para a implementação da gestão de riscos sugerem melhores práticas e definições muito abstratas, o que dificulta sua aplicação prática, as organizações acabam mapeando manualmente esses conhecimentos e diretrizes para sua infra-estrutura real.

Para Kroll (2010) muitos modelos de gestão de riscos podem ser encontrados na literatura, mas nenhum deles tem se consagrado e tornado-se referência para as organizações.

Desta forma, trabalhos atuais, tais como: Karabacak e Sogukpinar (2005), Ekelhart *et al. (*2009) , Leitner e Schaumuller-Bichl (2009) estão sendo propostos com o objetivo de minimizar estes problemas, porém, alguns divergem significativamente entre si, podendo resultar em quantificações classificatórias divergentes. No entanto, tais estudos não exploram a composição de métodos para minimizar a probabilidade de classificação divergente.

Diante destas constatações, este trabalho visa preencher esta lacuna, apresentando uma metodologia para análise/avaliação de riscos, que utiliza a composição de métodos para

priorizar os riscos relacionados à segurança da informação. A proposta fornece uma definição clara das fases do processo, estabelecendo diretivas para a sua aplicação prática.

Para apoiar a aplicação e validação da metodologia, foi desenvolvida uma ferramenta computacional que automatiza todas as fases da metodologia, realizando os cálculos matemáticos necessários para obter o percentual de risco. O resultado final é uma lista de riscos priorizados com base na ponderação dos métodos analisados.

O cenário de aplicação da metodologia foi o Centro de Processamento de Dados (CPD) da Universidade Federal de Santa Maria. A pesquisa contou com a participação de 70% dos funcionários, incluindo pessoas de diferentes setores.

Os resultados demonstraram que ao aplicar simultaneamente métodos distintos sob um mesmo domínio, é possível ocorrer divergências nas priorizações dos riscos. Desta forma, ao utilizar a composição de métodos, obtém-se indicadores de risco potencialmente mais precisos, pois refletem a ponderação entre os métodos analisados.

1.1 Contexto e motivação

Com o aumento das ameaças que podem provocar a perda da confidencialidade, integridade e disponibilidade das informações, as organizações estão buscando adotar práticas e medidas de segurança que protejam seus ativos. Através da gestão de riscos, são identificadas as principais vulnerabilidades e ameaças que cercam um sistema de informação e que podem resultar em falhas de segurança.

Com o objetivo de entender como está a governança dos sistemas públicos na área de Tecnologia de Informação e Comunicação (TIC), o Tribunal de Contas da União (TCU) vem analisando a infra-estrutura e sistemas de informação dos órgãos federais, sob várias perspectivas, desde 2007, de uma forma sistemática. Desta forma, em 2010 foi realizada uma pesquisa com 300 órgãos públicos que, de acordo com o TCU apontou a total ausência de comprometimento dos altos escalões com a área de TICs do governo federal, o resultado da pesquisa mostrou que (MEIRA, 2011):

53% NÃO têm processo de software ao menos gerenciado.

63% NÃO aprovam e publicam PDTI[1] interna ou externamente.

65% NÃO possuem política corporativa de segurança da informação.

74% NÃO inventariam todos os ativos de informação.

75% NÃO gerenciam os incidentes de segurança da informação.

[1] PDTI – Plano Diretor de Tecnologia da Informação

83% NÃO analisam os riscos aos quais a informação está submetida.

89% NÃO classificam a informação para o negócio.

97% NÃO possuem plano de continuidade de negócio em vigor.

> Mais da metade das instituições públicas faz software de forma amadorística; mais de 60% não possuem política e estratégia para sua informática e segurança da informação; 74% não têm nem mesmo as bases de um processo de gestão de ciclo de vida de informação; 75% não gerenciam incidentes de segurança de informação, como invasão de *sites* e sistemas ou perdas; 83% não faz idéia dos riscos a que a informação sob sua responsabilidade está sujeita, quase 90% não classifica informação para o negócio, o que significa que a instituição está sob provável e permanente caos informacional e quase 100% não tem um plano de continuidade de negócio em vigor. (MEIRA, 2011)

Neste contexto, destaca-se a importância de adotar medidas de segurança, priorizar os riscos e definir ações corretivas para diminuir a ocorrência de incidentes. Entretanto, Ekelhart *et al. (*2009) afirmam que as abordagens existentes para a implementação da gestão de riscos sugerem definições muito abstratas, o que dificulta sua aplicação prática. Segundo Grandison (2003), pode ser difícil atribuir valores consistentes para estimar os riscos, pois a quantificação muitas vezes é subjetiva. Outro fator relevante é com relação à dificuldade em estimar o risco de maneira quantitativa em função da complexidade dos sistemas de informações atuais e dos cálculos necessários para a obtenção dos índices de riscos (KARABACAK e SOGUKPINAR, 2005).

Desta forma, a metodologia proposta visa suprir esta necessidade, definindo um padrão para a execução da análise/avaliação de riscos e utilizando a composição de métodos para obter resultados mais precisos.

1.2 Contribuições

Este trabalho propõe uma metodologia que realiza a análise e avaliação de riscos, através da composição de métodos, priorizando os riscos indicados pela maioria dos métodos. Para isso, a metodologia estabelece sete fases para a sua execução, e em cada fase são definidos os passos necessários para sua aplicação prática.

A vantagem em utilizar mais de um método neste processo é a redução da probabilidade de erro na priorização dos riscos, ou seja, os resultados não dependem exclusivamente de um método, mas sim da ponderação entre os métodos analisados. Desta forma, os riscos priorizados representam com maior precisão a realidade da organização.

Além disso, a metodologia estabelece um padrão para a entrada de informações e o mapeamento entre os métodos, através de critérios de pontuação. Assim, é possível obter valores mais precisos, resultantes da combinação de várias técnicas.

Para apoiar o uso da metodologia proposta, foi desenvolvida uma ferramenta computacional que automatiza todas as fases da metodologia e executa os cálculos matemáticos necessários para a obtenção dos índices de risco. A ferramenta foi projetada com o objetivo de auxiliar a equipe responsável pelo processo de análise/avaliação de riscos na organização, mesmo que esta equipe não tenha um amplo conhecimento sobre o domínio da segurança da informação. Desta forma, cada organização pode configurar o sistema da maneira que melhor se adapta ao seu processo de trabalho, utilizando os métodos de análise/avaliação de riscos que julgar necessário para a obtenção de resultados mais efetivos.

1.3 Organização do trabalho

Este trabalho está organizado da seguinte forma: o Capítulo 2 descreve o referencial teórico relacionado à gestão da segurança da informação e ao processo de gerenciamento de riscos. Ainda neste capítulo, são detalhados alguns métodos existentes para análise quantitativa de riscos.

O Capítulo 3 propõe uma metodologia para análise e avaliação do risco com base na composição de métodos. O Capítulo 4 apresenta detalhes sobre a implementação da ferramenta desenvolvida, que tem como objetivo apoiar a aplicação da metodologia proposta.

O Capítulo 5 realiza a avaliação da metodologia e discute os resultados obtidos, e, finalmente, o Capítulo 6, descreve as conclusões e trabalhos futuros.

2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Com objetivo de melhor elucidar o tema segurança da informação e sua importância no contexto atual, este capítulo realiza uma revisão literária dos principais conceitos que abrangem a segurança da informação (Seção 2.1), apresenta uma metodologia para a implantação da gestão da segurança da informação (Seção 2.2) e aborda a problemática associada à gestão do risco, bem como alguns métodos propostos para o seu gerenciamento (Seção 2.3).

2.1 Segurança da Informação

Os sistemas de informações das organizações são expostos a diversos tipos de ameaças, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Estes danos também podem ser causados por códigos maliciosos, que estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (NBR/ISO IEC 17799:2005)

Cada vez mais os sistemas de informações (SI) assumem um papel estratégico e relevante, tornando-se vitais para a organização. Sendo assim, é necessária e obrigatória a existência de um conjunto de mecanismos que os protejam (KARABACAK e SOGUKPINAR, 2005).

> A segurança da informação é obtida pela utilização de controles: políticas, práticas, procedimento, estruturas organizacionais e infra-estruturas de hardware e software. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização (NBR ISO/IEC 17799:2005).

Conforme NBR/ISO IEC 17799:2005, os princípios básicos para garantir a segurança da informação em uma organização, são:

- **Confidencialidade**: a informação deve ser acessada por pessoas explicitamente autorizadas;
- **Integridade**: a informação deve ser encontrada em sua forma original, sendo mantida a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas;
- **Disponibilidade**: toda informação deve estar disponível a qualquer momento que for necessário.

Para compreender a Gestão da Segurança da informação é necessária a introdução e a definição de alguns dos seus conceitos básicos, os quais compreendem os ativos da informação, vulnerabilidades, ameaças, incidentes e riscos.

2.1.1 Ativo de Informação

Conforme ISO/IEC TR 13335-1: 2004, ativo é tudo aquilo que agrega valor para a organização. Ele pode ser representado por uma informação, processo, produto, base de dados, software, hardware, entre outros. O valor de um ativo corresponde à sua importância para a organização e deve refletir os custos que decorrem de sua indisponibilidade.

2.1.2 Vulnerabilidade

Segundo NBR ISO/IEC 17799: 2005, a vulnerabilidade é uma fragilidade de um ativo ou um grupo de ativos que pode ser explorada por uma ou mais ameaças, o que permite a ocorrência de incidentes. A análise de vulnerabilidades examina um sistema e determina as falhas existentes, tendo como referência normas, políticas e procedimentos estabelecidos pela organização.

2.1.3 Ameaça

A ameaça é entendida como a causa potencial de um incidente que poderá resultar em danos para um sistema, processo ou organização (ISO/IEC TR 13335-1, 2004), podendo advir de diferentes formas, sejam elas naturais ou tecnológicas (DIAS, 2000).

2.1.4 Incidente de Segurança

A norma NBR ISO/IEC 17799: 2005 define incidente de segurança da informação, como sendo um ou mais eventos indesejados ou inesperados, que tenham alguma probabilidade de comprometer as operações ou os processos do negócio e ameaçar a segurança da informação.

2.1.5 Impacto

O Impacto é o resultado de um incidente de segurança da informação (ISO/IEC 13335-1, 2004).

2.1.6 Risco

O risco é, no escopo da gestão da segurança da informação, a possibilidade de uma ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos, do qual pode resultar prejuízo para o sistema. É medido em termos de combinação da probabilidade de um evento ocorrer (ISO/IEC TR 13335-1, 2004).

O processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização é definido como Gerenciamento de Riscos (STONEBURNER, 2002).

2.2 Metodologia para a GSI através da abordagem Seis Sigma

Com a disseminação das normas e padrões de segurança, o interesse das organizações preocupadas em proteger o seu maior ativo, a informação, é cada dia maior. Muitos estudos vêm sendo publicados, e com eles são apresentadas novas metodologias, *frameworks* e recomendações para a implementação da gestão de segurança da informação (OLIVEIRA, 2009).

No entanto, pesquisas atuais apontam para uma nova preocupação, o da sustentação da segurança da informação, principalmente por que para minimizar os riscos e controlar as melhorias é necessário que a organização esteja apoiada em uma base sólida que gere esta sustentação. O modelo *Seis Sigma* é visto como uma das soluções que direcionam a essa sustentação, por ser considerada uma abordagem que promove a qualidade através do princípio da melhoria contínua, sendo as pessoas o principal agente para esta promoção (OLIVEIRA *et al.*, 2008).

Neste contexto, Oliveira (2009) propõe um processo de implantação de um SGSI, que utiliza a abordagem *Seis Sigma* e o ciclo de melhoria DMAIC, o qual resulta na padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas.

O termo *Seis Sigma* corresponde à variação mínima desejada dos processos que tem impacto para o cliente (interno ou externo), tendo como meta a redução de defeitos em produtos ou serviços em 3,4 defeitos (6σ) por milhão de oportunidades (BLAUTH, 2003).

Para a implantação do *Seis Sigma*, a metodologia tem como alicerce o método de gerenciamento DMAIC, que significa "*Define, Measure, Analyse, Improve and Control*", na qual evidencia claramente suas etapas de aplicação (FERNANDES & ABREU, 2006), conforme ilustra a Figura 1. As fases do método DMAIC são:

1) Definir: tem como objetivo o conhecimento sobre os processos, definindo pontos críticos para a organização e quais processos são mais relevantes;
2) Medir: tem como objetivo medir o problema que foi definido na primeira fase, procurando identificar as características críticas para a qualidade;
3) Analisar: identificar o que será melhorado e priorizado, desenvolvendo soluções para atender esses pontos resultantes da fase de medição;
4) Implementar ou Melhorar: tem como objetivo implementar melhorias que venham atender requisitos que foram identificados e medidos nas fases anteriores, a fim de obter a solução ou a minimização do problema;
5) Controlar: controla e avalia as ações que foram tomadas para atender as melhorias, sendo nesta fase realizado o recomeço do ciclo do processo de melhoria DMAIC.

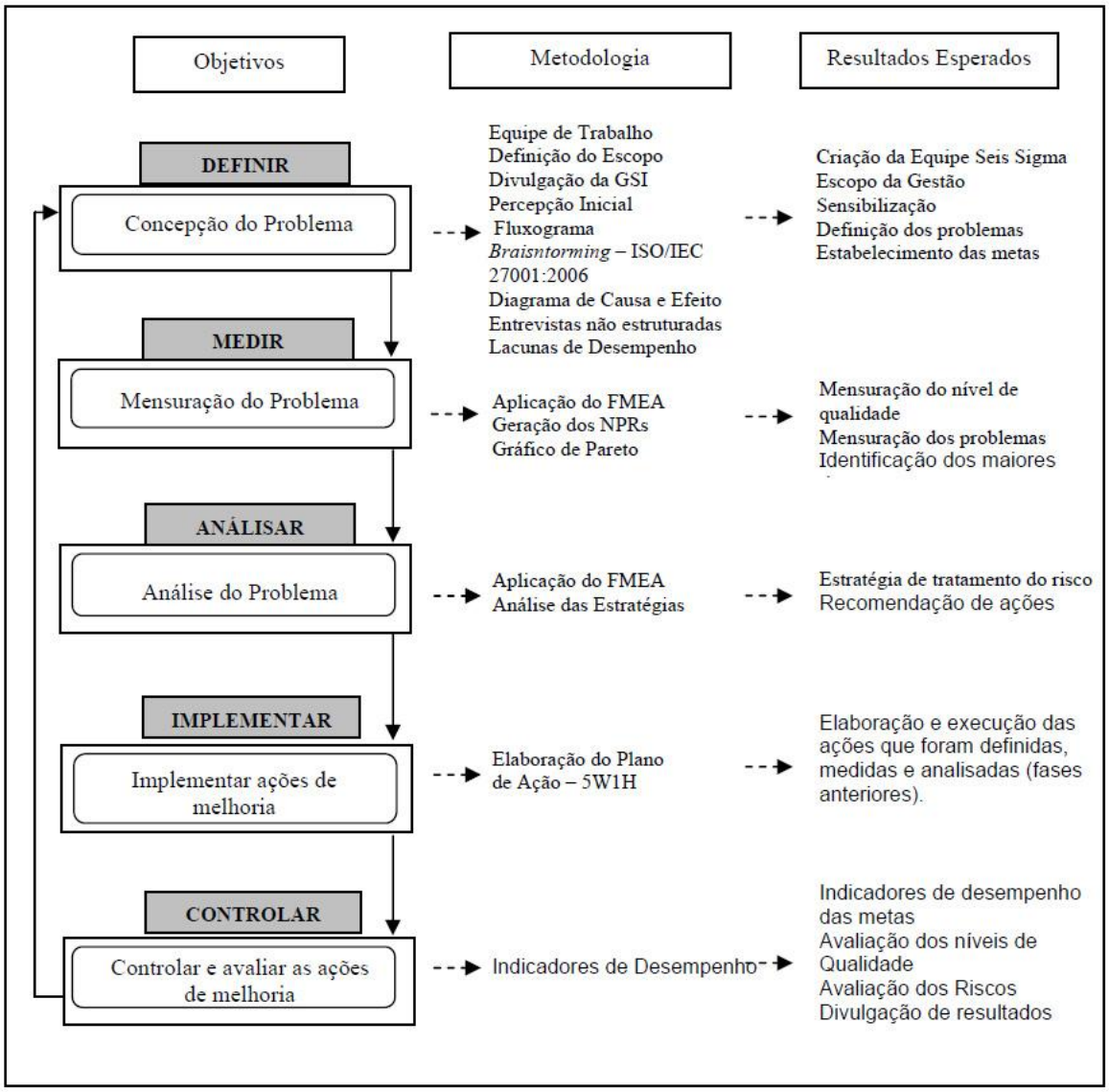


Figura 1 – Metodologia para implantação de um SGSI
Fonte: OLIVEIRA, 2009.

Cada fase estabelecida pelo método DMAIC está relacionada com uma etapa do projeto, onde são recomendadas ações que podem ser executadas conforme sugeridas pelo método. As ferramentas e técnicas propostas para cada fase visam atender as expectativas dos clientes e gerar os resultados esperados.

A metodologia proposta por Oliveira (2009) traz como contribuição o alinhamento de todas as fases do método DMAIC, estabelecendo em cada fase de execução as ferramentas, técnicas e procedimentos que podem ser utilizados durante todo o processo de implantação da gestão da segurança da informação usando a abordagem *Seis Sigma.* Esta abordagem estabelece a criação de uma equipe de trabalho, denominada "Equipe *Seis Sigma*".

A equipe *Seis Sigma* é responsável por conduzir todo o processo de implantação da gestão da segurança da informação. Possuem responsabilidades e funções definidas (ROTONDARO et al. 2006):

− *Executivo líder*: normalmente é composto pela alta gerência e é responsável pela condução, incentivo e supervisão da aplicação da metodologia na organização e também por selecionar os executivos que irão fazer parte da equipe;

− *O Campeão*: essa função é mais comum em organizações de grande porte com várias divisões. Sua responsabilidade é organizar e guiar o começo e o desdobramento da implementação do *seis sigma* por toda a organização;

− *Master Black Belt*: essa função também é mais comum em empresas de grande porte. São pessoas que já possuem experiência na implantação do *Sei Sigma*. Suas responsabilidades são: criar mudanças na organização, oferecer ajuda aos campeões, treinar e instruir os *Black Belts* e *Green Belts*;

− *Black Belts*: são, juntamente com os *Green Belts*, elementos chaves do sistema. Suas responsabilidades são aplicar as ferramentas e os conhecimentos do *Seis Sigma* em projetos específicos e orientar os *Green Belts* na condução dos grupos;

− *Green Belts*: sua responsabilidade é auxiliar os *Black Belts* na coleta de dados e no desenvolvimento de experimentos.

De acordo com a metodologia proposta por Oliveira (2009), a fase responsável pela mensuração dos problemas é a fase Medir. Nela, a metodologia propõe o uso do FMEA[2] (*Failure mode and effects analysis)* para a geração do Número de Prioridade de Risco (NPR). No processo de gestão de riscos, os problemas sobre os quais serão tomadas ações devem ser aqueles com valores de NPRs mais altos (ROTONDARO et al. 2006). Desta forma, a geração

[2] Técnica utilizada para definir, identificar e eliminar falhas conhecidas ou potenciais.

do NPR define uma maneira para hierarquizar os riscos e com isso priorizar ações mais urgentes para saná-los ou mitigá-los. A gestão de riscos compreende uma das etapas do processo de Gestão da Segurança da Informação, e será abordado na seção 2.3.

2.3 Gestão de Riscos

A Gestão de Riscos é um processo dinâmico, que inclui a identificação, a análise, a avaliação e o controle do risco. Seu objetivo é reduzir o risco inerente à segurança da informação a um nível aceitável pela organização (ZHIGANG *et al.*, 2009). Para isso, é necessário compreender as vulnerabilidades existentes e avaliar as consequências resultantes das possíveis ameaças (FENG e ZHANGN, 2004). Dessa forma, a gestão de riscos tornou-se um processo fundamental para suprir as necessidades de segurança da informação.

Através da gestão de riscos, são identificados os principais impactos, ameaças e vulnerabilidades que cercam um sistema de informação (KROLL e DORNELLAS, 2010). No entanto, Zapater e Suzuki (2005), ressaltam o quão trabalhoso e custoso pode se tornar o processo de mitigar tais vulnerabilidades, pois a complexidade e a sofisticação dos ataques contribuíram de maneira direta para o aumento dos incidentes de segurança. A tendência é que as ameaças à segurança continuem a crescer não apenas em ocorrência, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e mitigação de riscos, cada vez mais difícil e sofisticado.

Para Mayer e Fagundes (2008), as empresas precisam implementar a gestão de riscos de forma consistente e sistematizada. Porém, não há um modelo de maturidade voltado à Gestão de Riscos em Segurança da Informação, que meça ou avalie o nível de maturidade desse processo dentro das organizações, conforme os requisitos de um SGSI.

De acordo com a NBR ISO/IEC 27005:2008 o processo de gestão de riscos de segurança da informação (vide Figura 2) consiste nas seguintes etapas:

- *Definição do contexto*: determina os critérios básicos para a condução do processo, o escopo, limites e a equipe de gestão de riscos de segurança da informação;
- *Análise/Avaliação de riscos*: etapa que identifica, qualifica, quantifica e prioriza os riscos em função dos critérios de avaliação da organização;
- *Tratamento do risco*: seleciona controles para reduzir, reter evitar ou transferir os riscos priorizados na etapa anterior;
- *Aceitação de riscos*: é a decisão formal de aceitar o risco;

- *Comunicação do risco*: comunicação das informações de riscos entre o tomador de decisão e os interessados;
- *Monitoramento e análise crítica de riscos*: processo contínuo para identificar rapidamente mudanças contextuais na organização que possam afetá-la futuramente.

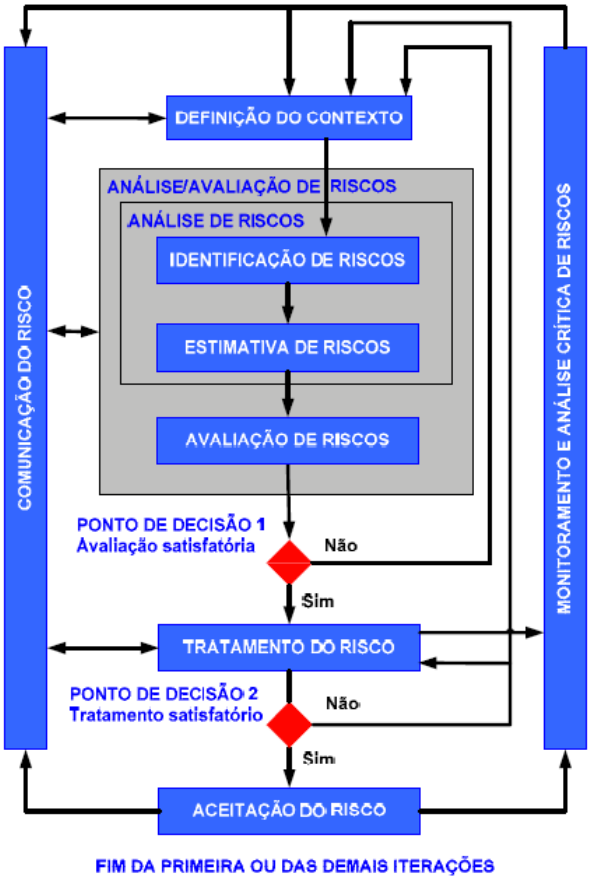


Figura 2 – Processo de Gestão de Riscos
Fonte: NBR ISO/IEC 27005:2008.

Ao analisar a Figura 2, percebe-se que o processo de Análise/Avaliação de riscos é subdividido em Análise de Riscos (Identificação e Estimativa) e Avaliação de Riscos, que serão detalhados nas seções 2.3.1 e 2.3.2, respectivamente.

2.3.1 Análise de Riscos

A prática da análise de riscos consiste em verificar a probabilidade de perda causada por uma ameaça contra um bem específico. No âmbito da segurança da informação, ela está associada à possibilidade da perda de algum dos seus princípios, seja a disponibilidade, a

integridade ou a confidencialidade (MARTINS e SANTOS, 2005). Deste modo, a análise de riscos possibilita identificar o grau de proteção que os ativos de informação necessitam.

A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização (NBR ISO/IEC 27005:2008).

Uma maneira simples e objetiva de mostrar à alta administração a verdadeira necessidade de investimentos em Segurança da Informação é através da análise de riscos, pois permite detectar falhas, que não eram percebidas, e que podem acarretar prejuízos para a organização. Assim, é possível aplicar controles objetivos nos pontos mais críticos e com real necessidade de investimento.

Durante esta etapa, deve ser feita a quantificação dos riscos, mensurando o impacto que um determinado risco pode causar ao negócio. Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços gastos com segurança.

De acordo com uma pesquisa realizada em organizações públicas austríacas (com foco em tecnologia da informação), descrita por Leitner e Schaumuller-Bichl (2009), a situação atual a respeito das experiências com métodos de análise de riscos indicou que a maioria das organizações utiliza uma abordagem própria para gerenciar os riscos de TI, fazendo uma combinação de uma abordagem individual com outros métodos existentes para a análise de riscos. Segundo os entrevistados, essa abordagem é mais adequada para definir o risco corretamente, pois o processo de análise do risco deve ser personalizado, expansível e adequado às necessidades da organização. Outro fator indicado pelos entrevistados é a preferência por uma abordagem qualitativa para determinar o nível atual do risco na organização. A razão para a aversão à escala quantitativa é a complexidade associada ao esforço para a sua realização. O problema é que a prática de adoção de uma abordagem própria pode levar a resultados não precisos.

Visando uma análise detalhada, o processo de análise de riscos é formado pelas etapas de identificação e estimativa de riscos.

2.3.1.1 Identificação de Riscos

O objetivo desta etapa é identificar as fontes de risco, suas causas e possíveis consequências, e com isso obter uma lista completa dos riscos existentes (ISO/IEC

31000:2008). A identificação de riscos é a tentativa de especificar todos os riscos que podem afetar a segurança da informação durante o seu ciclo de vida. Essa fase é muito importante, pois os riscos não identificados não serão analisados nem tratados. Assim, é necessário determinar os eventos que podem causar perdas potenciais e deixar claro como, onde e por que a perda pode ocorrer.

Durante essa etapa deve ser realizada uma análise para identificar também as ameaças e vulnerabilidades. Esta análise inicial pode ser tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada no conhecimento de especialistas.

Segundo a NBR ISO/IEC 27005:2008, para uma organização estabelecer o valor de seus ativos, é necessário primeiramente identificá-los num nível de detalhamento adequado. Dois tipos de ativos podem ser distinguidos:

a) **Ativos primários:**
   - Processos e atividades do negócio
   - Informação

b) **Ativos de suporte e infra-estrutura** (sobre os quais os elementos primários do escopo se apóiam), de todos os tipos:
   - Hardware
   - Software
   - Rede
   - Recursos humanos
   - Instalações físicas
   - A estrutura da organização

Desta forma, convém que sejam relacionados os ativos, vulnerabilidades e ameaças considerando os vários elementos descritos, com o objetivo de contemplar o maior número possível de ameaças relacionadas ao escopo definido.

A ISO/IEC 27001:2006 propõe os seguintes passos para a identificação dos riscos:

1) identificar os ativos dentro do escopo do SGSI e seus proprietários;

2) identificar as ameaças a esses ativos;

3) identificar as vulnerabilidades que podem ser exploradas pelas ameaças;

4) identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

Para auxiliar neste processo de identificação, recomenda-se a utilização de algumas ferramentas tais como *brainstorming*, entrevistas, *checklists*, entre outros.

2.3.1.2 Estimativa de Riscos

Estimativa de Riscos é o processo utilizado para atribuir valores à probabilidade e consequências de um risco (NBR ISO/IEC 27005:2008).

De uma forma geral, existem duas metodologias para estimativa de riscos: a qualitativa e a quantitativa. A qualitativa utiliza uma escala com atributos qualificadores para descrever o risco, já a quantitativa apresenta resultados baseados em valores numéricos.

Segundo a NBR ISO/IEC 27005:2008, uma metodologia para a estimativa de riscos pode ser qualitativa ou quantitativa ou uma combinação de ambas, dependendo das circunstâncias:

- **Estimativa qualitativa**: utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo: Pequena, Média e Grande) e a probabilidade dessas consequências ocorrerem. A estimativa qualitativa tem como vantagem a facilidade de compreensão por todas as pessoas envolvidas, porém, sua desvantagem é a dependência a escolha subjetiva da escala. As escalas podem ser adaptadas ou ajustadas, de acordo com a necessidade. Na prática, a estimativa qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos.
- **Estimativa quantitativa**: a estimativa quantitativa utiliza uma escala com valores numéricos tanto para consequências quanto para a probabilidade, usando dados de diversas fontes. A estimativa quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização. Sua desvantagem é a falta de tais dados sobre novos riscos ou sobre fragilidades da segurança da informação. Uma desvantagem da abordagem quantitativa ocorre quando dados factuais e auditáveis não estão disponíveis. Nesse caso, a exatidão da análise/avaliação de riscos e os valores associados tornam-se ilusórios.

Desta forma, quantificar os riscos é uma tarefa que exige bastante cuidado, pois a qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados (NBR ISO/IEC 27005:2008).

2.3.2 Avaliação de Riscos

A fase de Avaliação é responsável pela classificação dos riscos de acordo com sua criticidade, em função da importância dos ativos para a realização dos objetivos de negócios da organização. O processo de avaliação de riscos tem como entrada uma lista de riscos com níveis de valores designados e como saída uma lista de riscos ordenados por prioridades (NBR ISO/IEC 27005:2008).

A priorização dos riscos é necessária, pois um risco de nível alto, com baixo impacto financeiro, não necessariamente deva ser tratado antes de um risco de nível médio, porém com grande impacto financeiro. Desta forma, os riscos com prioridades maiores deverão ser minimizados.

De acordo com a norma ISO/IEC 31000:2008, o objetivo da avaliação de riscos é auxiliar na tomada de decisão, com base nos resultados da análise de riscos, priorizando os riscos que requerem um tratamento prioritário ou mantendo os controles existentes.

2.3.3 Métodos para estimativa quantitativa do risco

Várias metodologias já foram propostas com o objetivo de auxiliar no processo de gerenciamento de riscos, tais como OCTAVE (ALBERTS, 2003), NIST SP 800 (STONEBURNER, GOGUEN e FERINGA, 2002), entre outras.

O NIST (*National Institute of Standards & Technology*) SP (*Special Publication*) 800-30 é uma abordagem destinada para avaliação qualitativa dos riscos, que foi baseada em trabalhos já realizados por analistas de segurança com sistemas proprietários. Essa abordagem trabalha para identificar, avaliar e gerenciar os riscos em sistemas de TI (STONEBURNER, GOGUEN e FERINGA, 2002).

A metodologia *Operationally Critical Threat, Asset and Vulnerability Evaluation Methodology* (OCTAVE) versão 2.0, datada de 2001, foi desenvolvida pelo *Software Engineering Institute* como uma metodologia de análise qualitativa do risco, com a finalidade de identificar: ativos críticos de informação; ameaças que afetam os ativos; vulnerabilidades associadas a tais ativos e níveis atuais de risco referentes aos ativos (ALBERTS, 2003).

Segundo Stoneburner, Goguen e Feringa (2002), a desvantagem em utilizar a abordagem qualitativa para estimar o risco é não fornecer medições quantificáveis específicas da magnitude dos impactos, o que dificulta a priorização dos riscos.

Desta forma, este trabalho utilizou métodos de análise quantitativa, que possuem fórmula definida para calcular e obter o índice do risco, tornando o processo de priorização de

riscos mais eficaz, onde a magnitude dos impactos pode ser quantificada. Os métodos encontrados na literatura foram: o ISRAM (KARABACAK e SOGUKPINAR, 2005), o AURUM (EKELHART et al., 2009), o ARIMA (LEITNER e SCHAUMULLER-BICHL, 2009) e o FMEA (ROTONDARO et al., 2006), os quais foram utilizados para compor a lista de métodos analisados no estudo proposto por esta dissertação.

A seguir, é apresentado o referencial teórico destes métodos, explicando de maneira detalhada suas variáveis, escala de valores e fórmulas utilizadas para calcular o risco.

2.3.3.1 O método ISRAM

O ISRAM (*Information Security Risk Analysis Method)* (KARABACAK e SOGUKPINAR, 2005) é um método utilizado para analisar o risco causado por problemas de segurança da informação. O método propõe a determinação do risco com base em questionários relacionados com os problemas de segurança e recorre a uma fórmula específica para o cálculo do índice do risco. Este método adota uma fórmula simples, frequentemente usada por muitos autores, em que o risco é o produto da probabilidade de ocorrer uma quebra de segurança pelo valor das consequências a ela associadas, e é expresso como segue (Fórmula 1).

$$Risco = \begin{bmatrix} \text{Probabilidade de ocorrer} \\ \text{uma quebra de segurança} \end{bmatrix} \text{x} \begin{bmatrix} \text{Consequência da ocorrência} \\ \text{da quebra de segurança} \end{bmatrix} \quad (1)$$

O ISRAM consiste em sete etapas principais:

1. Identificar os problemas de segurança que envolvem a organização em estudo;
2. Listar todos os fatores que podem influenciar a ocorrência de uma quebra de segurança;
3. Elaborar um questionário com base nos fatores identificados na fase anterior;
4. Elaborar a tabela de conversão das respostas obtidas em função de valores quantitativos e qualitativos para a probabilidade de ocorrer uma quebra de segurança e para as consequências de uma quebra de segurança;
5. Aplicação dos questionários aos utilizadores;
6. Cálculo do índice do risco;
7. Análise dos resultados com o intuito de tentar apontar medidas que corrijam o problema de segurança.

O ISRAM é essencialmente um método quantitativo, embora apresente a possibilidade de o risco ser traduzido por uma expressão qualitativa. Este método apresenta uma formulação matemática para o cálculo do índice do risco, sendo esta formulação sustentada por um conjunto de questionários.

Na definição do método, Karabacak e Sogukpinar (2005) utilizaram uma escala quantitativa de 1 a 5, tanto para a probabilidade como para o impacto. Desta forma, o fator de risco do ISRAM é um valor numérico entre 1 e 25.

2.3.3.2 O método AURUM

O AURUM (*Automated Risk and Utility Management*) (EKELHART *et al.*, 2009) é uma ferramenta utilizada para automatizar a gestão de riscos e apoiar os gestores na escolha das medidas de segurança, de acordo com requisitos técnicos e econômicos. Ela foi projetada para apoiar a NIST SP 800-30 (STONEBURNER, GOGUEN e FERINGA, 2002) que estabelece um padrão de gerenciamento de risco para sistemas de tecnologia da informação.

Essa ferramenta baseia-se no uso de uma matriz de risco, sendo uma técnica valiosa para o cálculo do risco. O objetivo dessa matriz e do nível de pontuação de risco é fornecer uma metodologia consistente e objetiva para priorizar as ameaças. A orientação do NIST SP 800-30 é construir uma matriz 3x3 baseada nos atributos da probabilidade (Alto, Médio e Baixo) e o impacto de ameaças (Alto, Médio e Baixo).

Nesta aplicação, os níveis de riscos possíveis podem ser: Alto, Médio e Baixo, sendo que, ao determinar esses níveis, a probabilidade para cada ameaça é expressa da seguinte forma: 1,0 para Alta, 0,5 para Média e 0,1 para a Baixa. Com relação ao impacto da ameaça os seguintes valores são atribuídos: 100 para Alto, 50 para Médio, e 10 para Baixo.

Após essas definições, multiplica-se a probabilidade da ameaça pelos valores de impacto. A escala de risco para interpretar os resultados é apresentada na Tabela 1, conforme definição do NIST SP 800-30:

Tabela 1 – Escala de Riscos AURUM

Valores obtidos	Escala de Riscos
(> 50 a 100)	Alta
(> 10 a 50)	Média
(1 a 10)	Baixa

Fonte: EKELHART *et al.*, 2009.

2.3.3.3 O método ARIMA

O método ARIMA (*Austrian Risk Management Approach)* foi desenvolvido de acordo com os processos da norma ISO/IEC 27005 e com o objetivo de satisfazer os requisitos de gestão de riscos das autoridades públicas austríacas. Segundo os seus autores, Leitner e Schaumuller-Bichl (2009), de acordo com uma pesquisa realizada os resultados indicaram que, atualmente, nenhum método satisfaz inteiramente as exigências das autoridades públicas ou os subprocessos da ISO/IEC 27005.

O método ARIMA foi desenvolvido para atender essa necessidade e combina vantagens de alguns métodos analisados, no entanto, ele simplifica alguns passos para aumentar a transparência. Para obter o risco segundo este método é necessário utilizar a escala de Impacto e Probabilidade apresentada nas Tabelas 2 e 3, respectivamente.

Tabela 2 – Escala de Impacto – ARIMA

Sigla	Escala do impacto
L	Impacto controlável e não há efeitos subsequentes para a organização
M	Impacto não pode ser totalmente compensado
H	Impacto tem efeitos significativos sobre a organização

Fonte: LEITNER; SCHAUMULLER-BICHL, 2009.

Tabela 3 - Escala de Probabilidade – ARIMA

Sigla	Probabilidade
VL	Muito baixa
L	Baixa
M	Média
H	Alta
VH	Muito alta

Fonte: LEITNER; SCHAUMULLER-BICHL, 2009.

Após identificar o impacto e a probabilidade, ARIMA usa uma matriz (Tabela 4) para determinar o índice do risco obtido através da interseção da linha da probabilidade com a coluna do impacto. Por exemplo, se o impacto de uma ameaça for alto (H) e sua probabilidade for muito baixa (VL), então o valor do risco será 3, conforme Tabela 4.

Tabela 4 – Matriz de riscos ARIMA

Probabilidade	Impacto		
	L	**M**	**H**
VL	1	2	3
L	2	3	4
M	3	3	4
H	3	4	5
VH	4	5	5

Fonte: LEITNER; SCHAUMULLER-BICHL, 2009.

2.3.3.4 O método FMEA

O método FMEA (*Failure Mode and Effect Analysis*) é uma técnica utilizada para definir, identificar e eliminar falhas conhecidas ou potenciais, de sistemas, projetos, processos e/ou serviços, antes que essas atinjam o cliente (STAMATIS, 2003).

Segundo Puente *et al.* (2002), o FMEA inicialmente foi utilizado pela Nasa (*National Aeronautics and Space Administration*) em 1963, e então expandido para a indústria automobilística, onde foi utilizado para quantificar e ordenar possíveis defeitos potenciais no estágio de projeto de produtos, antes de chegarem ao consumidor final, através de sessões de *brainstormings* que buscam levantar falhas que podem ocorrer. Desta forma, esse método avalia a severidade do impacto do efeito de uma falha, a probabilidade de ocorrência da mesma e uma maneira pró-ativa de detecção, a fim de evitar transtornos para os clientes.

De acordo com Rotondaro *et al*. (2006), as etapas para a execução do *FMEA* são:

1. Identificar modos de falha conhecidos e potenciais;
2. Identificar os efeitos de cada modo de falha e a sua respectiva severidade;
3. Identificar as causas possíveis para cada modo de falha e a sua probabilidade de ocorrência;
4. Identificar os meios de detecção do modo de falha e sua probabilidade de detecção;
5. Avaliar o potencial de risco de cada modo de falha e definir medidas para sua eliminação ou redução. Isto é possível através de ações que aumentam a probabilidade de detecção ou reduzam a probabilidade de ocorrência da falha.

A realização do FMEA é feita usando-se um formulário padronizado, como mostra a Figura 3.

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas											
Projeto:				Cliente:							
Gerente do Projeto:				Data do FMEA:							
Data início Projeto:				Data Conclusão Projeto:							
Controle	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	RPN	Estratégia	Ações Recomendadas	Situação

Figura 3 – Formulário FMEA
Fonte: Adaptado de ROTONDARO, 2006.

O método FMEA estabelece três índices para pontuar o risco, podendo ser realizado com base no julgamento pessoal, empírico, com base em dados históricos ou testes. Estes índices são:

Ocorrência - define a frequência da falha.

Severidade - corresponde à gravidade do efeito da falha.

Detecção - é a habilidade para detectar a falha antes que ela atinja o cliente.

Com base nestes três elementos, severidade, ocorrência e detecção, o método *FMEA* leva à priorização de quais modos de falhas acarretam os maiores riscos ao cliente e que, portanto, merecem atenção. Para determinar o risco associado a cada modo de falha, multiplica-se a pontuação da Severidade (S) pela Ocorrência (O) e pela Detecção (D). Isso irá gerar um Número de Prioridade de Risco (NPR):

$$NPR = S \times O \times D \quad (2)$$

Para classificar os riscos, pode-se ter, por exemplo, uma escala que vai de 1 a 1000 pontos, sendo 1 um baixíssimo risco e 1000 um risco crítico ao cliente. Essa escala pode ser modificada de acordo com as necessidades da organização. A falha mais crítica será a que obtiver o maior NPR e, portanto, será a primeira do *ranking* para a aplicação de ações de melhoria. O resultado gerado com o NPR define uma maneira mais precisa para hierarquizar os riscos e com isso priorizar ações mais urgentes para saná-los ou mitigá-los.

2.4 Conclusões Parciais

Cada vez mais os sistemas de informações (SI) assumem um papel estratégico e relevante dentro das organizações, no entanto, estão expostos a diversos tipos de ameaças.

Para garantir a integridade, disponibilidade e confidencialidade das informações, se faz necessário gerenciar e identificar as ameaças que colocam em risco os ativos da organização. Entretanto, os métodos atuais para estimativa de riscos apresentam classificações divergentes ao priorizar os riscos da organização, o que pode comprometer o resultado final.

3 METODOLOGIA PARA ANÁLISE E AVALIAÇÃO DE RISCOS

Este capítulo apresenta a metodologia proposta para realizar o processo de análise e avaliação de riscos, através da composição de métodos. A seção 3.1 descreve as características da metodologia proposta e a seção 3.2 detalha cada uma de suas fases. Ao final, na seção 3.3 são apresentadas as conclusões parciais do capítulo.

3.1 Características da metodologia proposta

O objetivo da metodologia proposta é estabelecer uma orientação prática para a implantação da análise/avaliação de riscos em uma organização, explorando o uso da composição de métodos para minimizar a probabilidade de classificação divergente, pois os resultados representam a ponderação entre os métodos analisados.

Como qualquer metodologia, a metodologia proposta identifica os ativos, suas vulnerabilidades e possíveis ameaças dentro do escopo definido para realizar a análise/avaliação de riscos. Entretanto, ao utilizar a composição de métodos, a coleta de informações é padronizada, pois cada método possui suas próprias variáveis e escalas específicas. Desta forma, para não desanimar os entrevistados com vários questionários repetitivos (um de cada método) é utilizado um questionário único com base nas ameaças identificadas e nas variáveis de cada método.

Para estabelecer uma relação entre os métodos e permitir uma comparação entre eles, é realizado um mapeamento da escala padrão adotada para as escalas específicas de cada método. Assim, cada resposta pode assumir um peso diferente de acordo com o método utilizado. Entretanto, alguns métodos não possuem uma escala específica, então é utilizada a própria escala padrão.

Após o mapeamento, é possível então calcular o risco de acordo com as fórmulas definidas em cada método e por fim obter a ponderação entre os métodos analisados.

A priorização dos riscos é a última fase da metodologia proposta, nesta etapa os NPRs gerados devem ser colocados em ordem decrescente de valor.

Finalmente, de forma geral, a metodologia proposta estabelece um processo com sete etapas para a execução do processo de análise e avaliação de riscos em uma organização. A descrição de cada uma das fases é apresentada a seguir. A Figura 4 apresenta uma síntese

deste processo e define a sequência de passos que devem ser empregados para obter os resultados esperados.

1. *Identificação dos Ativos*: realizar o levantamento dos bens relevantes para a organização dentro do escopo definido, ou seja, os ativos que serão analisados.
2. *Detecção das Vulnerabilidades:* detectar as fragilidades associadas aos ativos que podem ser exploradas.
3. *Identificação das Ameaças:* identificar as ameaças que podem explorar as vulnerabilidades e causar prejuízos para a organização.
4. *Padronização da coleta de informações:* padronizar a entrada de informações através de um questionário único para a aplicação simultânea dos diferentes métodos que serão analisados. Para isso é necessário utilizar um questionário padrão, onde a resposta de cada participante é transformada em valores quantitativos, embora ele utilize uma escala qualitativa para responder.
5. *Mapeamento dos métodos:* mapear a escala padrão adotada para as escalas específicas de cada método. O mapeamento entre os métodos permite a conversão entre escalas específicas e a escala padrão adotada (Escala Likert[3]). Assim, cada resposta pode assumir um peso diferente de acordo com o método utilizado. Alguns métodos estabelecem um peso específico para suas respostas, outros não, desta forma, se faz necessário adotar um padrão de conversão a fim de realizar os cálculos necessários para obtenção do índice do risco.
6. *Cálculo do Risco:* realizar o cálculo do risco de acordo com a fórmula e a escala específica de cada método. Calcular a ponderação final entre os métodos analisados.
7. *Priorização dos Riscos:* classificar os riscos em ordem decrescente dos índices gerados. Os riscos com maiores índices devem ser priorizados, pois através da mensuração é que se descobre o que de fato é importante para a organização e que necessita de maior atenção.

[3] É um tipo de escala de resposta usada comumente em questionários. Normalmente, utiliza cinco valores possíveis para as respostas (1 – 5).

Figura 4 – Metodologia para análise e avaliação de riscos

Ao relacionar este trabalho com a metodologia proposta por Oliveira (2009) para a implantação da gestão da segurança da informação (seção 2.2), é possível afirmar que este estudo concentra-se na primeira e segunda fase do método DMAIC, ou seja, nas fases Definir e Medir. Seu objetivo é estabelecer o escopo e auxiliar no processo de avaliação de riscos, priorizando os riscos que representam maior prejuízo para a organização.

Oliveira (2009) propõe o uso do FMEA para a geração dos NPRs (Número de Prioridade de Risco), o que difere um pouco da metodologia proposta neste trabalho, que sugere a utilização de mais de um método de cálculo para a obtenção dos NPRs. Para isso, na pesquisa realizada foram utilizados quatro métodos, incluindo o FMEA.

Desta forma, conhecendo o nível de risco, a organização tem a oportunidade de decidir o que fazer em relação a ele: reduzir, aceitar, evitar ou transferir, tomando decisões de acordo com a gravidade identificada e as possíveis perdas.

O detalhamento das fases é apresentado na seção 3.2, que descreve os procedimentos realizados em cada uma das etapas.

3.2 Fases da Metodologia

Nesta seção serão detalhadas as fases da metodologia proposta, definindo um roteiro para a aplicação prática da metodologia.

3.2.1 Identificação dos ativos

Inicialmente, é preciso determinar os bens relevantes para a organização dentro do escopo de projeto no cenário definido. A NBR ISO/IEC 27005:2008 recomenda (vide seção 2.3.1.1) que os ativos sejam identificados num nível de detalhamento adequado, considerando os ativos primários e os de suporte e infra-estrutura. Como esta metodologia utiliza como ativo primário a "Informação", os seguintes elementos de suporte e infra-estrutura devem ser considerados no momento de elencar os ativos da organização: Hardware, Software, Rede, Recursos humanos, Instalações físicas, estrutura da organização, dentre outros.

É possível realizar o levantamento de ativos utilizando técnicas de *brainstorming*, entrevistas, *checklists*, diagramas de causa e efeito, entre outros. No entanto, o padrão adotado por esta metodologia foi o uso do *brainstorming*, por ser uma técnica que busca a diversidade de opiniões e idéias. Desta forma, a lista de ativos é resultante dos *brainstormings* realizados.

Com o objetivo de envolver a organização como um todo, é recomendável que os participantes do *brainstorming* sejam de setores e competências diferentes, pois suas experiências diversas podem colaborar para a obtenção de informações mais abrangentes e realmente importantes para o processo de análise de riscos. Porém, para se chegar à lista definitiva dos ativos, é necessário estabelecer um consenso entre os participantes, selecionando os ativos relevantes para a organização. A Tabela 5 apresenta o exemplo de uma lista de ativos, considerando os elementos de suporte e infra-estrutura.

Tabela 5 – Lista de Ativos

Lista de Ativos
Banco de Dados
Código Fonte
Computadores
Equipamentos de Rede
Equipamentos Servidores
Funcionários
Sala de Servidores
Usuários

3.2.2 Detecção das vulnerabilidades

O processo de detecção das vulnerabilidades tem por objetivo verificar a existência de falhas de segurança associadas aos ativos. Desta forma, para cada ativo identificado na fase anterior deve ser realizado um levantamento, através da técnica de *brainstorming,* das possíveis vulnerabilidades relacionadas a este ativo, conforme mostra a Tabela 6. Um ativo pode ter inúmeras vulnerabilidades associadas.

Tabela 6 – Lista de Vulnerabilidades

Lista de Ativos	Lista das Vulnerabilidades
Banco de Dados	Compartilhamento de senhas
Banco de Dados	Políticas de segurança inadequadas
Cabeamento	Incidência de roedores
Código Fonte	Testes Insuficientes
Computadores	Políticas de segurança inadequadas
Equipamentos de Rede	Equipamentos antigos e precários
Equipamentos Servidores	Ausência de redundância de servidores
Funcionários	Quadro reduzido de funcionários
Funcionários	Insatisfação ou Doença
Sala de Servidores	Ausência de mecanismos de acesso
Usuários	Usuários sem treinamento no sistema

3.2.3 Identificação das ameaças

As ameaças podem explorar vulnerabilidades inerentes aos ativos e acarretar perdas à organização. Desta forma, para identificar as ameaças é preciso analisar as vulnerabilidades existentes, considerando seus ativos. Para cada vulnerabilidade identificada na fase anterior é feito um levantamento das possíveis ameaças.

É interessante trabalhar com ameaças mais genéricas ao invés de criar uma infinidade de ameaças relacionadas à indisponibilidade de um sistema, pois isto pode acabar desperdiçando muito tempo. O conjunto de ameaças que assola um ativo tende ao infinito. Um dos maiores desafios é conseguir otimizar o tempo que se leva no processo sem deixar passar informações importantes e, ao mesmo tempo, maximizar os resultados obtidos. Não existe uma forma de cobrir todas as situações. Desta forma, na Tabela 7 é possível visualizar algumas dessas ameaças. Uma vulnerabilidade pode ter inúmeras ameaças associadas.

Tabela 7 – Lista de Ameaças

Lista de Ativos	Lista das Vulnerabilidades	Lista de Ameaças
Banco de Dados	Compartilhamento de senhas	Vazamento de informações sigilosas
Banco de Dados	Políticas de segurança inadequadas	Acesso Indevido
Cabeamento	Incidência de roedores	Rompimento do cabeamento
Código Fonte	Testes Insuficientes	Geração de aplicações com erros
Computadores	Políticas de segurança inadequadas	Ataque de Vírus/Hackers
Equipamentos de Rede	Equipamentos antigos e precários	Instabilidade da rede
Equipamentos Servidores	Ausência de redundância de servidores	Indisponibilidade da informação
Funcionários	Quadro reduzido de funcionários	Demanda excessiva de trabalho
Funcionários	Insatisfação ou Doença	Baixa na produtividade
Sala dos Servidores	Ausência de mecanismos de acesso	Acesso indevido a sala dos servidores
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema

3.2.4 Padronização da coleta de informações

Após a identificação dos ativos, vulnerabilidades e ameaças, torna-se possível então, elaborar um questionário único contendo todas essas informações. O propósito do questionário é padronizar a coleta dos dados, através de uma interação única com os participantes, independente do número de métodos utilizados para calcular o risco.

O questionário foi projetado na forma tabular como mostra a Tabela 8, a primeira coluna representa os ativos, a segunda as vulnerabilidades e a terceira as ameaças. Ao lado delas, foram adicionadas as colunas representando as variáveis: Probabilidade, Detecção, Ocorrência e Impacto (ou Severidade).

Os participantes devem responder o questionário analisando o cruzamento das variáveis com as possíveis ameaças e assim optar pela resposta que melhor representa a sua opinião, considerando as definições de cada variável:

Probabilidade – é a probabilidade da ameaça se concretizar.

Detecção – é a dificuldade em detectar a ameaça antes que ela atinja o cliente.

Ocorrência – é a frequência com que a ameaça ocorre.

Impacto/Severidade – é impacto negativo que irá ocorrer caso a ameaça se concretize.

Tabela 8 – Formulário padrão para a coleta de informações

Ativos	Vulnerabilidades	Ameaças	Probabilidade	Detecção	Ocorrência	Impacto (Severidade)
Banco de Dados	Políticas de Segurança Inadequadas	Perda da integridade dos dados	Baixo (Muito Baixo, Baixo, Médio, Alto, Muito Alto)			
	Compartilhamento de senhas	Vazamento de informações sigilosas				
Código Fonte	Testes Insuficientes	Geração de aplicações com erros				
Funcionários	Quadro reduzido de funcionários	Demanda excessiva de trabalho				
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema				

Para padronizar as respostas dos participantes foi adotada a escala *Likert*, que varia de 1 a 5, como mostra a Tabela 9. Desta forma, o entrevistado deve selecionar a opção (Muito Baixo, Baixo, Médio, Alto e Muito Alto) que melhor descreve a sua opinião com relação à ameaça e a variável em análise.

Tabela 9 – Escala Likert

Opção	Peso
Muito Baixo	1
Baixo	2
Médio	3
Alto	4
Muito Alto	5

Para responder o questionário foi padronizado o uso da escala padrão. No entanto, como alguns métodos utilizam escalas específicas para as suas variáveis, é necessário realizar um mapeamento entre eles, explicado na seção 3.2.5.

3.2.5 Mapeamento dos métodos

Considerando que cada organização pode utilizar diferentes métodos para calcular o risco, com escalas totalmente distintas, se faz necessário estabelecer um mapeamento entre

eles. Por exemplo, alguns métodos como o AURUM consideram que avaliar as variáveis de probabilidade e impacto somente considerando uma matriz 3x3 (Baixa, Media e Alta) já é o suficiente para obter o índice do risco. No entanto, outros como o ISRAM consideram que utilizar uma matriz 5x5 proporciona uma estimativa mais precisa.

Ao utilizar mais de um método para estimar o risco, é necessário realizar um mapeamento entre eles, pois é comum apresentarem escalas distintas, o que contribui para a elaboração de uma tabela de mapeamento, conforme ilustra a Tabela 10.

Tabela 10 – Mapeamento entre os métodos

FMEA e ISRAM		**AURUM**		**ARIMA**	
Escala Padrão	**Probabilidade, Impacto, Detecção**	**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

A escala padrão adotada utiliza valores de 1 a 5 (Escala *Likert*), e é a mesma utilizada pelo método ISRAM. Essa escala também foi atribuída ao método FMEA, para padronizar em cinco opções as possíveis respostas. Os métodos AURUM e ARIMA possuem escalas próprias, como mostra a tabela de mapeamento (Tabela 10).

O método AURUM considera somente três valores (Baixo, Médio e Alto) para as variáveis de Probabilidade e Impacto. No entanto a escala padrão utiliza cinco valores. Assim, foi necessário estabelecer a conversão das respostas, transformando as opções “Muito Baixo” e “Muito Alto” para “Baixo” e “Alto”, respectivamente.

O método ARIMA também utiliza uma escala de três valores para o Impacto (L, M, H) e cinco valores para a Probabilidade (VL, L, M, H, VH). No entanto, para calcular o risco esse método utiliza uma matriz de Probabilidade versus Impacto. A interseção da linha Probabilidade com a coluna Impacto é que irá determinar o valor do risco (Tabela 4).

Com exceção do FMEA, os outros métodos utilizam somente variáveis de Probabilidade e Impacto para determinar o risco. FMEA é o único que utiliza três variáveis: Severidade/Impacto, Ocorrência e Detecção.

3.2.6 Cálculo do risco

Após o mapeamento, torna-se possível então, calcular a probabilidade do risco. Este cálculo é baseado na potencialidade de uma ameaça se concretizar e explorar as vulnerabilidades de um ativo, causando impactos negativos para a organização.

Os valores são calculados com base nas fórmulas definidas em cada método e considerando sua escala específica de pesos. No entanto, para que os valores obtidos possam ser comparados, é necessário que estejam na mesma escala. Desta forma, para atingir esse propósito foi calculado o valor percentual de cada método em relação ao seu total, identificando o valor máximo possível para o risco em cada método analisado, conforme sua escala, como mostra a Tabela 11.

Tabela 11 – Valores máximos permitido para cada Método

Métodos	Valor máximo para o Risco
ARIMA	5
ISRAM	25
AURUM	100
FMEA	125

No método ARIMA o valor máximo permitido é 5, pois analisando a Tabela 4 (Matriz de riscos) percebe-se que esse é o valor máximo obtido da interseção da linha Probabilidade com a coluna Impacto (P ∩ I).

O método ISRAM utiliza o produto de duas variáveis (P x I), que podem assumir como valor máximo 5, portanto, o seu produto final será 25. O AURUM também utiliza o produto de duas variáveis (P x I), entretanto, o seu produto final pode chegar a 100.

O FMEA é o único que utiliza três variáveis e cada uma delas pode assumir o valor máximo 5, portanto, seu produto final poderá chegar a 125.

Para que os valores estejam na mesma escala, é aplicada uma regra de três simples, que multiplica o resultado da fórmula por 100 e divide pelo total obtido em cada método, considerando o peso máximo aplicado a fórmula.

Considerando P a Probabilidade, I o Impacto, S a Severidade, O a Ocorrência e D a Detecção, os resultados obtidos são calculados com base nas fórmulas descritas pelos métodos e acrescidos das modificações necessárias para obter o valor percentual, conforme apresenta as expressões 3, 4, 5 e 6.

$$\text{ARIMA} = ((\mathbf{P} \cap \mathbf{I}) * 100)/5 \quad (3)$$

$$\text{ISRAM} = ((\mathbf{P} * \mathbf{I}) * 100)/25 \quad (4)$$

$$\text{AURUM} = ((\mathbf{P} * \mathbf{I}) * 100)/100 \quad (5)$$

$$\text{FMEA} = ((\mathbf{S} * \mathbf{O} * \mathbf{D}) * 100)/125 \quad (6)$$

O método ARIMA, descrito na expressão 3, utiliza a interseção entre as variáveis Probabilidade e Impacto. No entanto, para calcular o valor do risco automaticamente pela ferramenta, foi necessário transformar a expressão 3 em uma fórmula com operações básicas da matemática (adição, subtração, multiplicação e divisão). Assim, foi elaborada a fórmula da expressão 7, que ao ser executada resulta exatamente nos mesmos valores definidos na Tabela 4. Para se chegar a esta fórmula foram realizadas várias tentativas, atribuindo pesos diferentes para as variáveis de forma que os valores finais fossem iguais aos da Tabela 4.

$$\text{ARIMA} = ((\mathbf{I} + \mathbf{((P - 1) * 0,5)}) * 100)/5 \quad (7)$$

Assim, atribuindo os valores (L = 1.2, M= 2.1, H= 3) para o Impacto e os valores (VL= 1, L=2.6, M=3.6, H=5, VH=5.9) para a Probabilidade, ao substituir esses valores na fórmula 7 e aplicar a regra de arredondamento, é possível obter o resultado igual ao da matriz de riscos ARIMA (Tabela 4).

Depois de obter o risco percentual em cada método, foi dado o mesmo peso para todos os métodos e calculado a média entre eles, de acordo com a Fórmula 8.

$$\mathbf{Risco\% = \frac{(\Sigma\ (M1 + M2 + Mn))}{n}} \quad (8)$$

onde

M - Resultado percentual do método
n - número de métodos utilizados

3.2.7 Priorização dos riscos

Após calcular a média entre os métodos é possível então classificar os riscos existentes, pois estarão na mesma escala percentual. Os riscos são priorizados em ordem decrescente das médias obtidas. Desta forma, os NPRs com maiores índices devem ser avaliados primeiramente pela organização para que esta decida o que fazer: reduzir, aceitar, evitar ou transferir o risco identificado.

3.3 Conclusões Parciais

A metodologia proposta define um padrão para a implantação do processo de análise e avaliação de riscos em uma organização. Para isso, ela adota a composição de métodos, com o objetivo de minimizar a probabilidade de classificação divergente. Desta forma, os riscos são priorizados de acordo com a ponderação entre os métodos analisados e não considerando o resultado de apenas um método. A ponderação tem como vantagem o aumento da precisão.

Além disso, a metodologia também apresenta definições claras e objetivas do que deve ser feito em cada uma de suas fases, facilitando a sua aplicação prática. O resultado final é uma lista de riscos priorizados que auxilia a organização a tomar decisões com base em informações mais precisas.

4 MAAR – UMA FERRAMENTA PARA ANÁLISE E AVALIAÇÃO DE RISCOS

Este capítulo descreve detalhes da implementação da ferramenta MAAR (Método para Análise e Avaliação de Riscos), que tem como objetivo apoiar a aplicação e validação da metodologia proposta no Capítulo 3, automatizando os processos de cálculo. A Seção 4.1 descreve as características da ferramenta, a Seção 4.2 apresenta o modelo de dados e a Seção 4.3 descreve as funcionalidades desenvolvidas. Ao final são apresentadas as conclusões parciais do capítulo (Seção 4.4).

4.1 Características da ferramenta

O processo de análise e avaliação de riscos pode se tornar oneroso em organizações onde o número de participantes é expressivo, principalmente quando é utilizado mais de um método, pois a complexidade dos cálculos matemáticos aumenta. Desta forma, o objetivo da ferramenta desenvolvida é apoiar a aplicação e validação da metodologia proposta no capítulo 3, automatizando todas as suas fases e realizando os cálculos matemáticos necessários para obter o percentual de risco. O resultado final é uma lista de riscos priorizados com base na ponderação dos métodos analisados.

O uso da composição de métodos através da ferramenta é um procedimento simples e facilmente parametrizável, pois basta cadastrar o método desejado. Portanto, qualquer método para estimativa de riscos pode ser utilizado pela ferramenta, desde que tenha uma fórmula definida para calcular o risco. As funcionalidades previstas na ferramenta permitem executar todas as fases da metodologia proposta.

A ferramenta contempla parte da metodologia proposta por Oliveira (2009) para a Gestão de Segurança da Informação, pois auxilia no processo de mensuração e priorização dos possíveis problemas, exatamente o que estabelece a fase Medir do método DMAIC.

Para o desenvolvimento da ferramenta MAAR utilizou-se a linguagem de programação Java EE[4] e o banco de dados PostgreeSQL[5].

[4] Java Enterprise Edition (Plataforma de programação na linguagem java).
[5] Sistema gerenciador de banco de dados, desenvolvido como projeto de código aberto.

4.2 Modelo de dados

O modelo entidade relacionamento (MER)[6], apresentado na Figura 5, foi elaborado para dar suporte às funcionalidades da ferramenta MAAR.

Cada projeto pode ter inúmeros ativos vinculados, como mostra a Figura 5, sendo que cada ativo pode ter várias vulnerabilidades e uma vulnerabilidade pode ter inúmeras ameaças. Assim, é possível relacionar todos estes itens a um mesmo projeto.

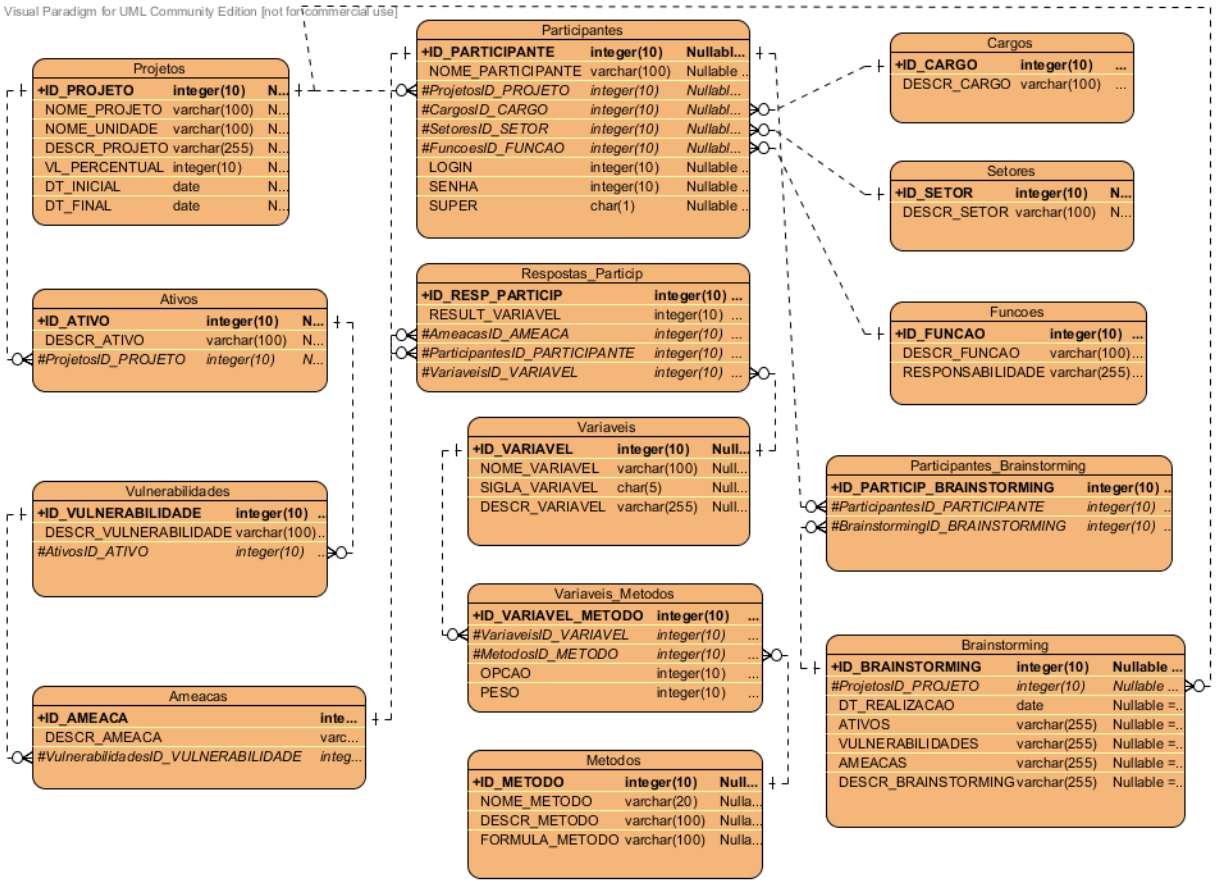


Figura 5 – Modelo ER da ferramenta

O projeto também possui vários participantes, onde cada participante deve ter um cargo associado, o setor onde trabalha e a função que desempenha dentro da equipe *Seis Sigma*, caso ele faça parte. Os *brainstormings* também estão associados a um projeto, e cada *brainstorming* pode ter vários participantes.

Os métodos podem ter inúmeras variáveis associadas, e vice-versa, sendo que nesta relação é possível estabelecer o peso da variável para cada opção de resposta.

A seguir serão apresentadas as funcionalidades da ferramenta desenvolvida.

[6] É um modelo abstrato cuja finalidade é descrever, de maneira conceitual, os dados a serem utilizados em um sistema de informações.

4.3 Funcionalidades

A ferramenta MAAR possui várias funcionalidades para dar suporte ao processo de análise e avaliação de riscos em uma instituição. A seguir estas funcionalidades serão descritas, considerando sua aplicação prática dentro das fases da metodologia proposta.

4.3.1 Cadastro de Projetos

Um projeto pode ser definido como o processo de análise e avaliação de riscos, realizado em um determinado local durante um período de tempo. Ele é o ponto de entrada para realizar a análise e avaliação de riscos, como ilustra o exemplo da Figura 6, onde aparece uma lista com o nome de vários projetos cadastrados.

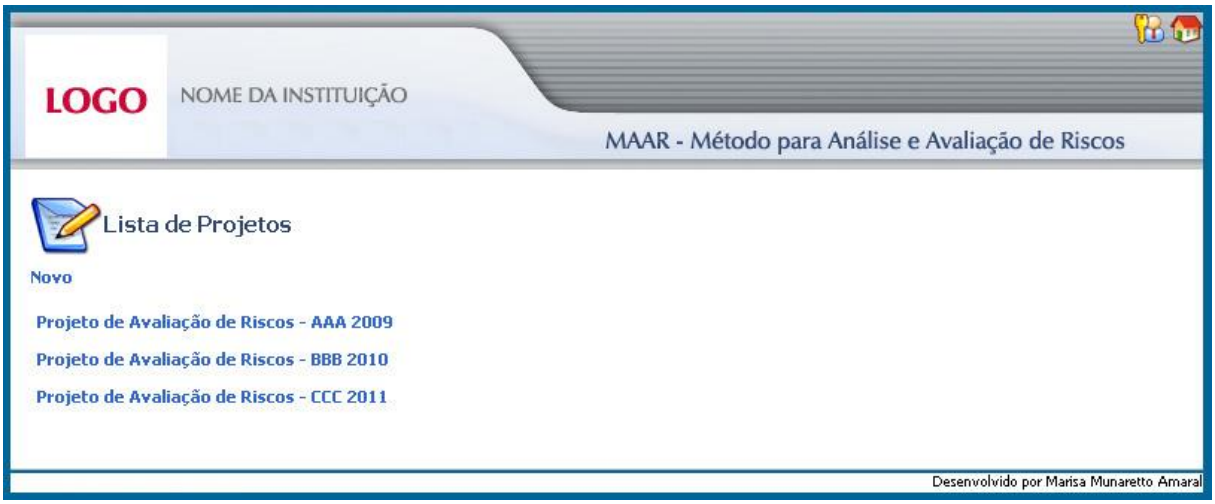


Figura 6 – Lista de Projetos

Ao selecionar um projeto é possível visualizar todas as funcionalidades associadas a ele, como mostra a Figura 7. Essas funcionalidades estão dispostas exatamente na ordem de execução das fases da metodologia proposta. Entretanto, algumas delas são informações básicas de apoio a metodologia e devem ser informadas previamente para que o processo de análise/avaliação de riscos seja executado com sucesso. Assim, inicialmente é necessário cadastrar um projeto e seus participantes, para então prosseguir e dar início as fases da metodologia proposta.

Figura 7 – Menu Inicial

Um projeto possui um nome, um período de duração e a unidade ou organização onde será aplicada a análise e avaliação de riscos, como pode ser visualizado na Figura 8.

Cada projeto deve ter a liberdade de escolher o percentual de riscos que quer considerar em seu processo de análise/avaliação. Desta forma, foi projetada uma parametrização no sistema que permite que cada projeto estabeleça o percentual de risco que deseja priorizar. Assim, ao mostrar a lista de priorização de riscos o sistema irá destacar na cor vermelha os que estiverem dentro do percentual configurado.

Figura 8 – Cadastro de Projetos

4.3.2 Participantes do Projeto

Os participantes do projeto são as todas as pessoas envolvidas no processo de análise/avaliação de riscos de um projeto. Cada participante deve ter um *login* e uma senha de acesso ao sistema, além do nome, setor onde trabalha e cargo que ocupa dentro da instituição, como ilustrado na Figura 9.

Outra informação importante é com relação à função que o participante terá no projeto, ou seja, ele pode fazer parte da equipe *Seis Sigma*, que irá gerenciar o processo de análise/avaliação de riscos. Neste caso, ele terá funções definidas dentro do projeto e deverá se responsabilizar por elas.

As informações sobre cargos e setores também são importantes para aplicar filtros nos resultados finais da pesquisa, pois permite identificar certas particularidades. Por exemplo, determinados setores podem priorizar riscos diferentes dos demais, dependendo do que as pessoas que trabalham neste setor consideram como um risco grave para a organização. Por isso, é importante envolver todos os setores, para que o resultado final da avaliação de riscos represente a realidade da instituição. Na Figura 9, é possível visualizar a lista dos participantes cadastrados, os setores e os cargos que ocupam. O botão ao lado do nome do participante permite visualizar suas respostas, considerando o projeto selecionado.

Figura 9 – Cadastro de Participantes

Caso os participantes queiram responder novamente a pesquisa ou se os responsáveis pela avaliação (equipe *seis sigma)* julgarem algumas respostas tendenciosas, é possível excluí-las, entretanto, o resultado final não irá representar a totalidade dos participantes.

4.3.3 Registro do *Brainstorming*

Com o objetivo de identificar os ativos, vulnerabilidades e ameaças existentes é necessário realizar um *brainstorming* entre os participantes do projeto. Nem todos precisam participar, porém, deve ter no mínimo um representante de cada setor da organização para que as informações obtidas sejam o mais abrangente possível.

É possível realizar várias sessões de *brainstorming*, e em cada uma delas informar os participantes, os ativos, as vulnerabilidades e as ameaças identificadas durante as sessões de discussões. A equipe *Seis Sigma* responsável pelo processo de análise/avaliação de riscos deve acompanhar e conduzir a reunião, e se necessário, estabelecer um consenso na definição dos principais ativos, vulnerabilidades e ameaças que podem estar presentes no cenário alvo. Na Figura 10, é possível visualizar o exemplo de um *brainstorming* para o levantamento de ativos.

Figura 10 – Registro do *Brainstorming*

Para cada *brainstorming* realizado, é necessário informar os participantes que auxiliam no levantamento das informações, como mostra a Figura 11. Esse registro é importante para identificar se pessoas de diferentes setores estão sendo envolvidas no processo.

Figura 11 – Participantes do *Brainstorming*

O uso da técnica de *brainstorming* é muito importante, pois ela reflete a opinião de todos os participantes. Ao envolver pessoas de diferentes setores é possível obter uma visão geral dos ativos, vulnerabilidades e ameaças presentes na organização.

Esta funcionalidade "Registro do *Brainstorming"* é utilizada pelas fases "Identificação de Ativos", "Detecção das Vulnerabilidades" e "Identificação das Ameaças" da metodologia proposta.

4.3.4 Cadastro de Ativos

Após a identificação dos ativos através da técnica de *brainstorming*, os responsáveis pelo processo de análise/avaliação de riscos dentro da organização, devem registrar no sistema o resultado obtido a partir do levantamento feito. Os ativos pertencem a um projeto e serão utilizados posteriormente para identificar as vulnerabilidades associadas a eles. Na Figura 12, é possível visualizar um exemplo de ativos identificados e cadastrados no sistema.

A funcionalidade "Cadastro de Ativos*"* é utilizada na fase "Identificação de Ativos" da metodologia proposta.

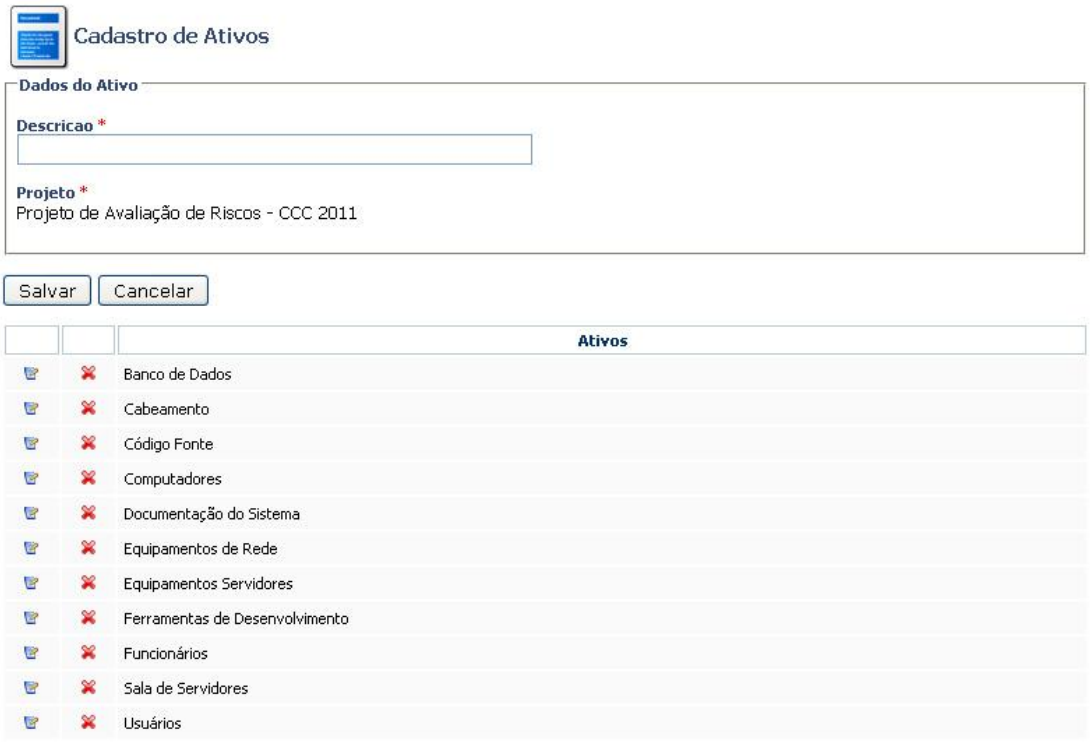


Figura 12 – Cadastro de Ativos

4.3.5 Cadastro de Vulnerabilidades

As vulnerabilidades representam as fragilidades de um ativo, que podem ser exploradas por ameaças. A Figura 13 apresenta as vulnerabilidades associadas aos ativos.

Figura 13 – Cadastro de Vulnerabilidades

Para detectar as vulnerabilidades existentes deve ser utilizada a técnica de *brainstorming*, analisando os ativos já identificados. Um ativo pode ter inúmeras vulnerabilidades associadas. A funcionalidade "Cadastro de Vulnerabilidades*"* é utilizada na fase "Identificação de Vulnerabilidades" da metodologia proposta.

4.3.6 Cadastro de Ameaças

Uma ameaça é qualquer coisa que possa danificar ou causar prejuízos em um sistema ou em uma organização. Ela está diretamente relacionada à vulnerabilidade de um ativo. Na Figura 14, é possível visualizar essa relação.

		Ameaças	Vulnerabilidades	Ativos
		Perda da Integridade dos dados	Políticas de Segurança Inadequadas	Banco de Dados
		Vazamento de Informações sigilosas	Compartilhamento de senhas	Banco de Dados
		Rompimento do cabeamento	Incidência de roedores	Cabeamento
		Sobrecarga nos Servidores	Testes de carga insuficientes	Código Fonte
		Geração de aplicações com erros	Testes insuficientes	Código Fonte
		Ataque de Vírus/Hackers	Políticas de Segurança Inadequadas	Computadores
		Instabilidade da Rede	Equipamentos antigos e precários	Equipamentos de Rede
		Indisponibilidade da Informação	Ausência de espelhamento	Equipamentos Servidores
		Demanda excessiva de trabalho	Quadro reduzido de funcionários	Funcionários
		Baixa produtividade	Insatisfação ou Doença	Funcionários
		Acesso Indevido	Ausência de mecanismos de acesso	Sala de Servidores
		Mau uso do sistema	Usuários sem treinamento no sistema	Usuários

Figura 14 – Cadastro de Ameaças

A funcionalidade "Cadastro de Ameaças*"* é utilizada na fase "Identificação das Ameaças" da metodologia proposta.

4.3.7 Métodos e Variáveis

Como visto anteriormente, existem diferentes métodos para realizar o cálculo do risco, cada um com sua fórmula específica. Para tornar o sistema flexível, foi desenvolvido um

"Cadastro de Métodos", ilustrado na Figura 15, que permite incluir novos métodos, alterar e excluir os já existentes. Cada método recebe um nome e uma descrição, além da fórmula que será usada para realizar os cálculos.

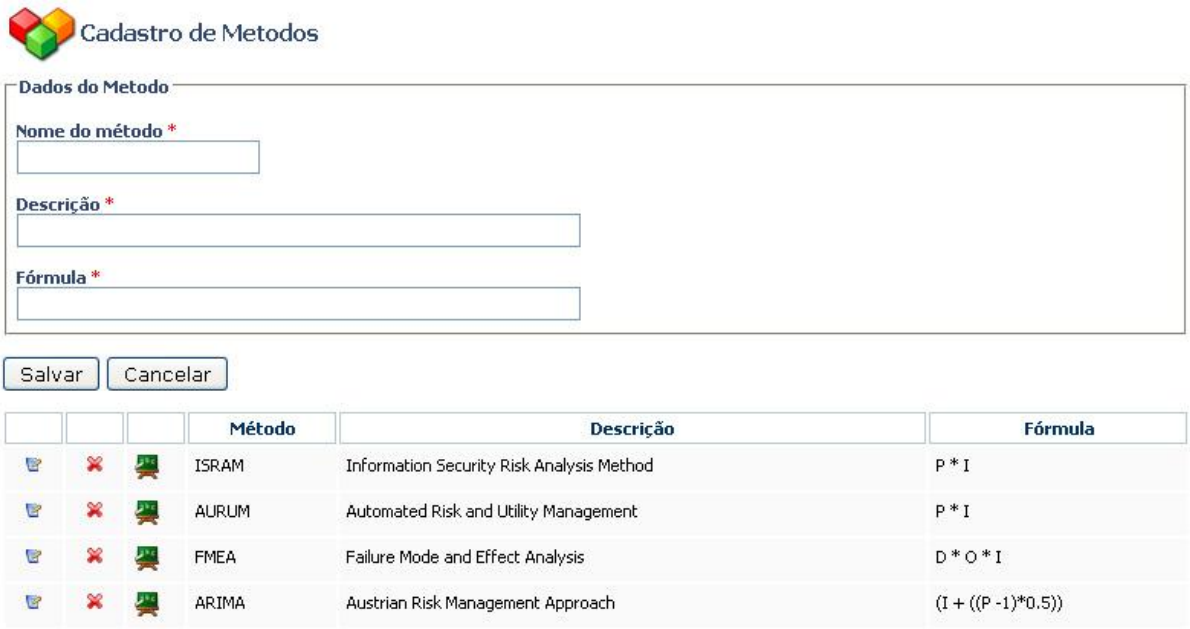


Figura 15 – Cadastro de Métodos

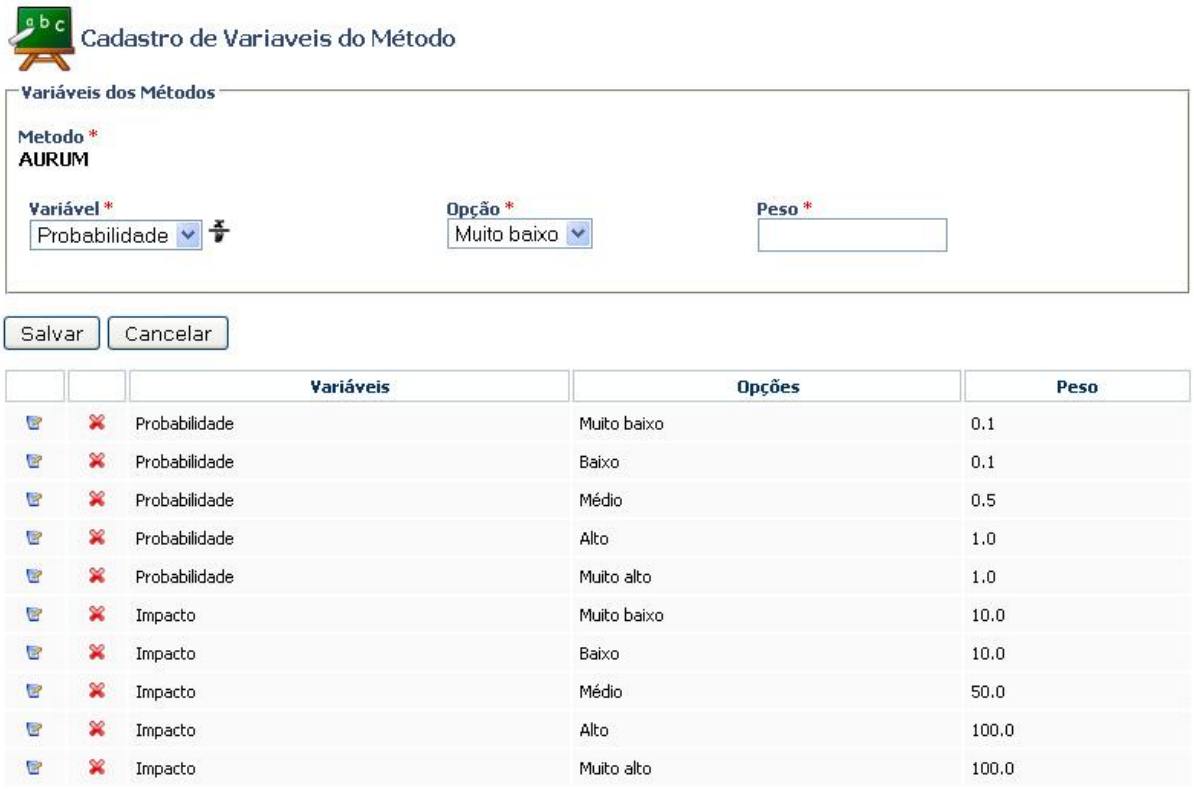
As variáveis utilizadas pelos métodos devem estar cadastradas no sistema, como ilustra a Figura 16. Cada variável deve ter um nome, uma sigla (usada para substituir o valor na fórmula) e uma descrição que será usada como legenda para auxiliar o participante a entender o significado da variável durante o preenchimento do questionário.

Figura 16 – Cadastro de Variáveis

Um método pode utilizar inúmeras variáveis em sua fórmula e elas podem assumir valores distintos. No entanto, para padronizar a entrada de informações foi necessário definir as opções de respostas que o participante poderia selecionar para atribuir um peso às ameaças identificadas.

A escala padrão adotada foi a *Likert*, que utiliza valores de 1 a 5 (Muito Baixo, Baixo, Médio, Alto, Muito Alto). Desta forma, ao vincular a variável a um método é preciso atribuir um peso para cada uma das opções possíveis, como ilustra a Figura 17.

No exemplo da Figura 17, o método AURUM estabelece pesos diferentes para as variáveis de Probabilidade e Impacto, considerando as opções (Baixo, Médio e Alto). Nesse caso, o método utiliza somente três opções, que devem ser mapeadas em cinco. Assim, foi atribuído para as opções "Muito Baixo" e "Muito Alto" o mesmo peso das opções "Baixo" e "Alto", respectivamente. Desta forma, ao preencher o questionário e atribuir o impacto "Muito Baixo" para uma ameaça, será considerado o mesmo peso do impacto "Baixo".



Variáveis	Opções	Peso
Probabilidade	Muito baixo	0.1
Probabilidade	Baixo	0.1
Probabilidade	Médio	0.5
Probabilidade	Alto	1.0
Probabilidade	Muito alto	1.0
Impacto	Muito baixo	10.0
Impacto	Baixo	10.0
Impacto	Médio	50.0
Impacto	Alto	100.0
Impacto	Muito alto	100.0

Figura 17– Variáveis dos Métodos

Aos demais métodos que não definem pesos para as variáveis, cadastrou-se os valores da escala *Likert* (1-5), considerando 1 como "Muito Baixo" e 5 como "Muito Alto".

A funcionalidade "Métodos e Variáveis" é utilizada pela fase "Mapeamento dos métodos" da metodologia proposta. Nesta fase é necessário mapear a escala padrão adotada

para as escalas específicas de cada método, pois as respostas podem assumir um peso diferente de acordo com o método utilizado, como ilustra a Figura 17.

4.3.8 Questionário

A coleta dos dados é feita através de um questionário, criado dinamicamente de acordo com as ameaças identificadas e as variáveis cadastradas. Para preencher o questionário, o participante já deve estar cadastrado no sistema. Ao analisar as ameaças existentes, o participante deve indicar a resposta que melhor representa a sua opinião considerando cada uma das variáveis listadas, como mostra a Figura 18.

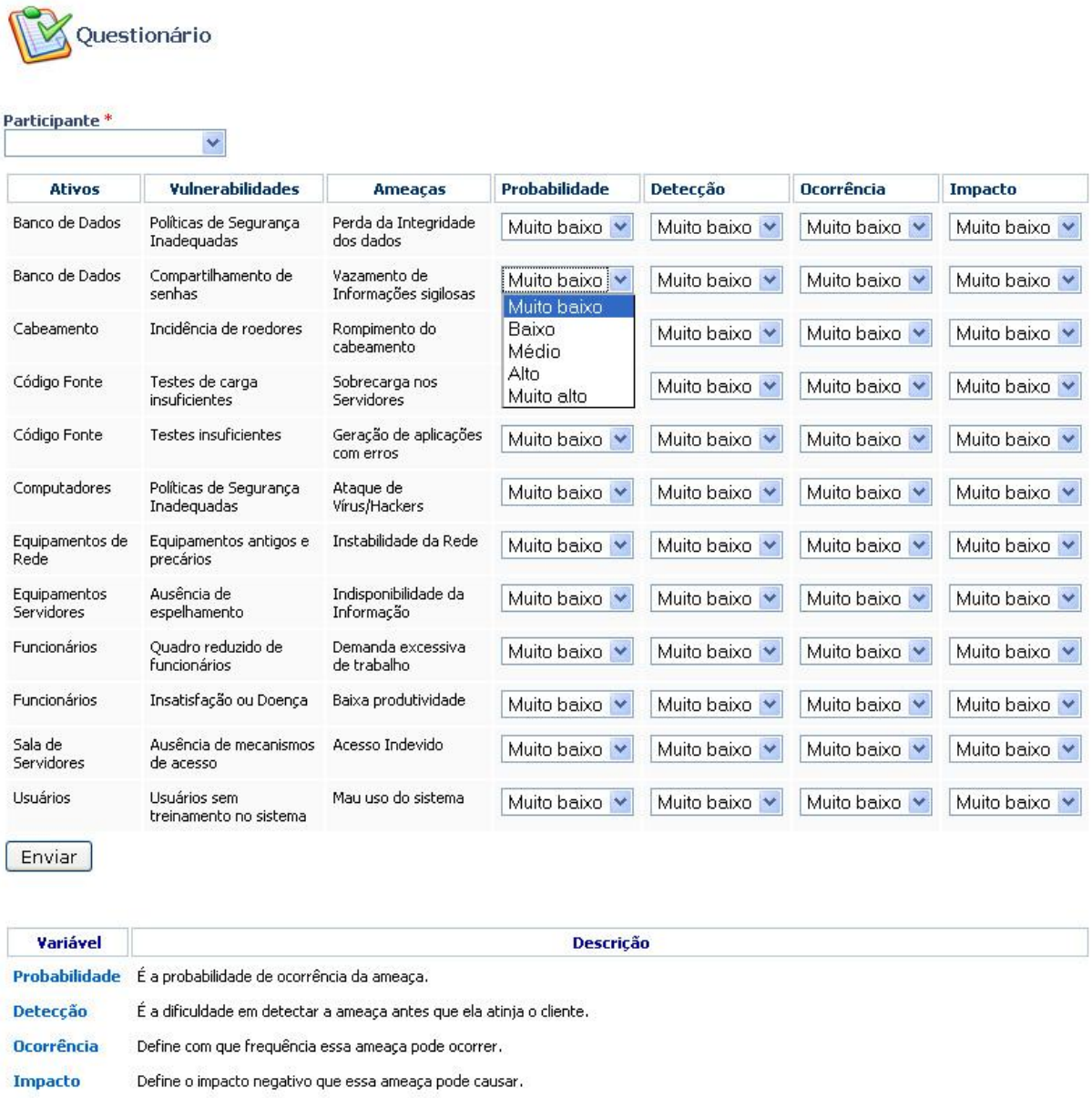


Figura 18– Questionário

Para facilitar o entendimento do participante, sobre o significado de cada variável, foi adicionada uma legenda logo abaixo do questionário, com a descrição definida no Cadastro de Variáveis (Figura 16).

Quando uma nova variável é cadastrada, o sistema a insere automaticamente no questionário, o mesmo acontece com as ameaças. Essa flexibilidade permite que a organização utilize vários métodos em seu processo de análise/avaliação de riscos de forma simples e rápida. É possível utilizar as mesmas respostas no cálculo do risco de um método novo, desde que ele utilize variáveis que já foram preenchidas anteriormente pelos participantes. Esta funcionalidade corresponde à fase "Padronização da coleta de informações" da metodologia proposta.

4.3.9 Cálculo e Priorização do Risco

O cálculo do risco é realizado com base nas fórmulas e variáveis dos métodos, seguindo as regras da metodologia proposta. Assim, o sistema calcula o valor do risco em cada método e obtém o valor percentual em relação ao total, para só depois calcular a média final entre os métodos. O risco é então priorizado em ordem decrescente de valor. Estas funcionalidades correspondem às fases "Cálculo do Risco" e "Priorização do Risco" da metodologia proposta. A Figura 19 apresenta os resultados já calculados e priorizados considerando as respostas de um participante.

Participante

Ativos	Vulnerabilidades	Ameaças	ARIMA	AURUM	FMEA	ISRAM	Média
Banco de Dados	Compartilhamento de senhas	Vazamento de Informações sigilosas	78.90 %	50.00 %	20.00 %	60.00 %	52.22
Equipamentos de Rede	Equipamentos antigos e precários	Instabilidade da Rede	75.23 %	50.00 %	21.60 %	48.00 %	48.71
Código Fonte	Testes de carga insuficientes	Sobrecarga nos Servidores	62.39 %	25.00 %	24.00 %	36.00 %	36.85
Computadores	Políticas de Segurança Inadequadas	Ataque de Vírus/Hackers	68.81 %	10.00 %	16.00 %	32.00 %	31.70
Equipamentos Servidores	Ausência de espelhamento	Indisponibilidade da Informação	55.05 %	10.00 %	20.00 %	20.00 %	26.26
Código Fonte	Testes insuficientes	Geração de aplicações com erros	58.72 %	10.00 %	12.00 %	16.00 %	24.18
Sala de Servidores	Ausência de mecanismos de acesso	Acesso Indevido	38.53 %	5.00 %	36.00 %	12.00 %	22.88
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema	45.87 %	5.00 %	12.00 %	12.00 %	18.72
Funcionários	Insatisfação ou Doença	Baixa produtividade	45.87 %	5.00 %	7.20 %	12.00 %	17.52
Funcionários	Quadro reduzido de funcionários	Demanda excessiva de trabalho	45.87 %	5.00 %	2.40 %	12.00 %	16.32
Banco de Dados	Políticas de Segurança Inadequadas	Perda da Integridade dos dados	38.53 %	5.00 %	7.20 %	12.00 %	15.68
Cabeamento	Incidência de roedores	Rompimento do cabeamento	38.53 %	5.00 %	2.40 %	12.00 %	14.48

Figura 19– Resultado do Participante

Cada participante pode visualizar o resultado obtido considerando somente as suas respostas, como mostra a Figura 19.

4.4 Conclusões Parciais

Neste capítulo foram descritas as características da ferramenta desenvolvida MAAR, seu modelo de dados e suas funcionalidades.

O objetivo da ferramenta é permitir que vários métodos sejam utilizados simultaneamente, o que contribui para a obtenção de resultados mais precisos, pois os valores representam a ponderação entre os métodos analisados. Além disso, a ferramenta não restringe os métodos que devem ser utilizados, portanto, fica a critério da organização decidir quais métodos deseja utilizar no seu processo de análise e avaliação de riscos. Para isso, basta cadastrar os métodos e as variáveis, e de acordo com as respostas dos participantes, os cálculos são realizados automaticamente, substituindo as respostas pelos pesos definidos para cada variável.

Com o auxílio de uma ferramenta automatizada o processo de análise de riscos torna-se bem mais simples e menos oneroso para a organização, facilitando a tomada de decisão.

5 AVALIAÇÃO

Neste capítulo é apresentado o resultado final da pesquisa que apontou os principais riscos da instituição avaliada. A seção 5.1 apresenta o cenário de aplicação da metodologia proposta, a seção 5.2 faz uma análise dos resultados obtidos e ao final na seção 5.3 são apresentadas as conclusões parciais do capítulo.

5.1 Cenário de aplicação da metodologia

A metodologia proposta foi aplicada no Centro de Processamento de Dados (CPD) da Universidade Federal de Santa Maria. O CPD é o órgão responsável pela análise e desenvolvimento de sistemas, suporte e atendimento aos usuários. Seus serviços devem estar sempre disponíveis e os dados íntegros e confidenciais, o que exige um controle maior com relação à segurança da informação e justifica a escolha como laboratório de pesquisa.

O processo de avaliação foi realizado no mês de janeiro de 2011. No total 70% dos funcionários (23 pessoas) participaram da pesquisa, incluindo os setores de Desenvolvimento, Suporte, Atendimento ao Usuário e Direção.

Os percentuais de riscos foram calculados com base nas respostas dos participantes, de acordo com o peso definido para as variáveis dos métodos analisados. Os riscos foram classificados em ordem decrescente de média, com a finalidade de auxiliar a priorização dos índices mais altos.

5.2 Análise de Resultados

Ao analisar os resultados da pesquisa, foram consideradas as respostas de todos os participantes envolvidos. Depois foram aplicados alguns filtros, tais como: o setor de lotação do participante e o cargo de ocupação dentro da instituição, a fim de verificar as variações existentes.

5.2.1 Risco Total

O Risco Total representa a opinião de todos os participantes da pesquisa, ou seja, os riscos que devem ser priorizados dentro da organização. Para salientar os riscos com maiores

índices, a ferramenta exibe-os na cor vermelha, de acordo com o percentual configurado no Cadastro de Projetos, conforme ilustra a Figura 20.

Risco Total

Setor

Cargo

Filtrar

Ativos	Vulnerabilidades	Ameaças	ARIMA	AURUM	FMEA	ISRAM	Média
Funcionários	Quadro reduzido de funcionários	Demanda excessiva	84.90 %	80.67 %	40.87 %	62.33 %	67.19
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema	85.13 %	74.58 %	41.77 %	64.83 %	66.58
Código Fonte	Testes de carga insuficientes	Sobrecarga nos Servidores	78.98 %	61.25 %	34.83 %	56.00 %	57.76
Código Fonte	Testes insuficientes	Geração de aplicações com erros	76.64 %	57.17 %	30.40 %	53.17 %	54.34
Equipamentos de Rede	Equipamentos antigos e precários	Instabilidade da Rede	69.30 %	44.67 %	28.77 %	45.33 %	47.02
Banco de Dados	Compartilhamento de senhas	Vazamento de Informações sigilosas	73.01 %	43.58 %	20.33 %	49.83 %	46.69
Computadores	Políticas de Segurança Inadequadas	Ataque de Vírus/Hackers	71.98 %	42.33 %	23.73 %	47.33 %	46.34
Equipamentos Servidores	Ausência de espelhamento	Indisponibilidade da Informação	69.38 %	34.46 %	23.20 %	41.67 %	42.18
Sala de Servidores	Ausência de mecanismos de acesso	Acesso Indevido	67.39 %	40.08 %	18.40 %	40.33 %	41.55
Funcionários	Insatisfação ou Doença	Baixa produtividade	64.56 %	29.83 %	17.00 %	36.00 %	36.85
Banco de Dados	Políticas de Segurança Inadequadas	Perda da Integridade dos dados	63.34 %	19.67 %	17.40 %	33.67 %	33.52
Cabeamento	Incidência de roedores	Rompimento do cabeamento	53.36 %	14.04 %	11.57 %	26.50 %	26.37

Figura 20 – Risco Total

Observando a Figura 20, é possível perceber que os métodos utilizados para calcular o risco apresentaram divergências em seus resultados, mesmo tendo sido aplicados sob um mesmo domínio.

Ao analisar individualmente cada um dos métodos, percebe-se que ARIMA, FMEA e ISRAM indicaram como o primeiro lugar no *ranking* dos riscos com maior prioridade a ameaça “Mau uso do sistema”, relacionada ao ativo “Usuários” e a vulnerabilidade “Usuários sem treinamento no sistema”. Já o método AURUM apontou a ameaça “Demanda excessiva de trabalho”, relacionada ao ativo “Funcionários” e a vulnerabilidade “Quadro reduzido de funcionários”.

Em segundo lugar, os métodos ARIMA, FMEA e ISRAM apontaram a ameaça “Demanda excessiva de trabalho”, enquanto AURUM apontou “Mau uso do sistema”.

Em terceiro e quarto lugar, os quatro métodos apontaram as mesmas ameaças “Sobrecarga nos servidores” e “Geração de aplicações com erros”, respectivamente.

Em quinto lugar, os métodos ARIMA e ISRAM indicaram a ameaça “Vazamento de informações sigilosas”, enquanto os métodos AURUM e FMEA indicaram “Instabilidade na rede”.

Com base nos resultados da Figura 20, foi possível elaborar o gráfico da Figura 21, que apresenta o percentual de risco total obtido.

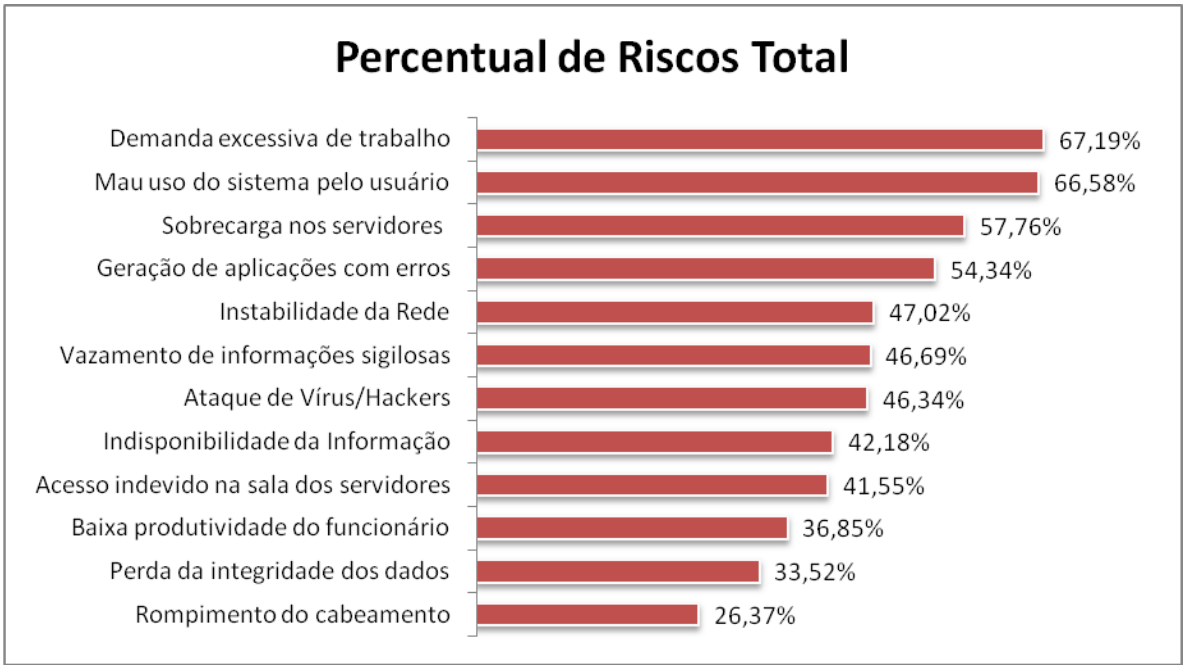


Figura 21 – Gráfico do Percentual total de risco obtido

O gráfico ilustra que 67% consideram a ameaça "Demanda excessiva de trabalho" como sendo o maior risco para a instituição analisada, seguido por "Mau uso do sistema pelo usuário", "Sobrecarga nos servidores" e "Geração de aplicações com erros". Para os participantes o impacto e a probabilidade desses riscos são altos. Esta preocupação pode ser observada pelos mais altos NPRs obtidos na avaliação.

Para facilitar a visualização das divergências entre os métodos analisados, foi elaborada a Tabela 12, que contém a ordem de classificação dos riscos e as ameaças priorizadas em cada método. Assim, é possível obter uma visão linear de quais riscos estão no mesmo lugar de classificação considerando todos os métodos.

Percebe-se que somente na terceira, quarta e última linha de classificação, os mesmos riscos foram indicados por todos os métodos. As colunas pintadas representam os riscos que se enquadraram no mesmo lugar de classificação. Desta forma, "Sobrecarga nos servidores", "Geração de aplicações com erros" e "Rompimento do cabeamento" foram as três ameaças indicadas no mesmo lugar de classificação por todos os métodos. As demais ameaças apresentaram divergências classificatórias.

Tabela 12 – Classificação dos riscos priorizados em cada método

Classificação	ARIMA	AURUM	FMEA	ISRAM
1º Lugar	Mau uso do sistema	Demanda excessiva	Mau uso do sistema	Mau uso do sistema
2º Lugar	Demanda excessiva	Mau uso do sistema	Demanda excessiva	Demanda excessiva
3º Lugar	Sobrecarga nos servidores	Sobrecarga nos servidores	Sobrecarga nos servidores	Sobrecarga nos servidores
4º Lugar	Geração de aplicações com erro	Geração de aplicações com erro	Geração de aplicações com erro	Geração de aplicações com erro
5º Lugar	Vazamento de Informações Sigilosas	Instabilidade da rede	Instabilidade da rede	Vazamento de Informações Sigilosas
6º Lugar	Ataque de Vírus/Hackers	Vazamento de Informações Sigilosas	Ataque de Vírus/Hackers	Ataque de Vírus/Hackers
7º Lugar	Indisponibilidade da Informação	Ataque de Vírus/Hackers	Indisponibilidade da Informação	Instabilidade da rede
8º Lugar	Instabilidade da rede	Acesso Indevido	Vazamento de Informações Sigilosas	Indisponibilidade da Informação
9º Lugar	Acesso Indevido	Indisponibilidade da Informação	Acesso Indevido	Acesso Indevido
10º Lugar	Baixa Produtividade	Baixa Produtividade	Perda da integridade dos dados	Baixa Produtividade
11º Lugar	Perda da integridade dos dados	Perda da integridade dos dados	Baixa Produtividade	Perda da integridade dos dados
12º Lugar	Rompimento do cabeamento	Rompimento do cabeamento	Rompimento do cabeamento	Rompimento do cabeamento

Desta forma, é possível concluir que os métodos utilizados resultaram em listas de priorização de riscos distintas. Neste caso, a lista é pequena, mas em organizações maiores essa lista pode aumentar consideravelmente, resultando em um número maior de classificações divergentes.

Em pesquisa prévia realizada em julho de 2010 (AMARAL, AMARAL e NUNES, 2010), no mesmo cenário, ou seja, no CPD da UFSM, a aplicação da metodologia também apresentou divergências classificatórias na priorização dos riscos. Naquele momento participaram 9 pessoas e foram utilizados os mesmos métodos para estimativa de riscos já descritos (ISRAM, AURUM, ARIMA e FMEA). Porém o que se observou foi que o trabalho dispensado para obter os percentuais de riscos foi bem maior, pois a ferramenta MAAR ainda não estava implementada. Desta forma, todos os cálculos matemáticos foram feitos utilizando o Excel[7]. Cada resposta enviada por um participante era anexada à planilha original para que

[7] Programa de planilha eletrônica de cálculo.

o resultado final fosse calculado. Na Tabela 13 é possível visualizar os resultados obtidos. A Média representa o risco final, com base nos métodos analisados.

Tabela 13 – Percentual de Risco obtido em pesquisa anterior

Ameaças	Percentual de Risco (%)				
	P * I	P * I	Intersecção P - I	S * D * O	Média
	ISRAM	*AURUM*	*ARIMA*	*FMEA*	*Média*
Acesso indevido no banco	28	13	57	8	27
Alterações maliciosas - perda da integridade	22	9	60	12	26
Vazamento de informações	39	25	71	8	36
Sobrecarga no banco	**52**	**61**	**83**	23	**55**
Acesso indevido nos fontes do sistema	27	11	54	7	25
Uso incorreto dos aplicativos	30	27	54	16	32
Baixa na Produtividade	28	13	57	11	27
Erros nos processos de trabalho	29	16	54	12	28
Erro na utilização do sistema pelo usuário	49	55	80	**27**	53
Sobrecarga nos servidores	**53**	**59**	**86**	**29**	**57**
Ataque de Vírus/Hackers	36	23	71	16	37
Roubo/furto	23	9	54	8	24
Perda da informação	22	7	60	7	24
Indisponibilidade da informação	37	32	71	17	39
Sobrecarga na rede	37	40	63	17	39

Fonte: AMARAL; AMARAL; NUNES, 2010.

Ao analisar o resultado da Tabela 13, percebe-se que os valores obtidos apresentaram divergências, o risco de maior prioridade (indicado na cor vermelha na Tabela 13) pelo método AURUM foi “Sobrecarga no banco”, enquanto que para os demais foi “Sobrecarga nos servidores”. O segundo risco de maior prioridade (indicado na cor azul na Tabela 13) também apresentou divergências, pois para os métodos ISRAM e ARIMA o segundo lugar foi “Sobrecarga no banco”, para o FMEA “Erro na utilização do sistema pelo usuário” e para o AURUM “Sobrecarga nos servidores”. Estes resultados demonstram que, mesmo utilizando-se um mesmo domínio para efetuar a pesquisa, a ordem de priorização dos riscos pode variar de método para método, e ao seguir somente um deles, corre-se o risco de priorizar ameaças que não representam grande risco para a organização e acabar deixando outras relevantes de lado.

5.2.2 Risco Parcial por Setor

O risco parcial por setor demonstra que dentro da organização é possível obter visões distintas dos principais riscos envolvidos, conforme Figura 22. Cada setor prioriza os riscos que no seu dia-a-dia julga ser mais importante. Por isso, é necessário envolver no processo de análise/avaliação de riscos o maior número de pessoas de todos os setores da organização.

Setor: Divisão de Suporte | Cargo: | Filtrar

Ativos	Vulnerabilidades	Ameaças	ARIMA	AURUM	FMEA	ISRAM	Média
Funcionários	Quadro reduzido de funcionários	Demanda excessiva de trabalho	91.74 %	100.00 %	39.20 %	64.00 %	73.74
Computadores	Políticas de Segurança Inadequadas	Ataque de Vírus/Hackers	82.34 %	76.25 %	40.00 %	58.00 %	64.15
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema	83.49 %	75.00 %	30.40 %	56.00 %	61.22
Equipamentos Servidores	Ausência de espelhamento	Indisponibilidade da Informação	82.11 %	62.50 %	29.80 %	55.00 %	57.35
Banco de Dados	Compartilhamento de senhas	Vazamento de Informações sigilosas	73.62 %	42.50 %	23.40 %	49.00 %	47.13
Sala de Servidores	Ausência de mecanismos de acesso	Acesso Indevido	75.46 %	40.00 %	19.20 %	47.00 %	45.42
Código Fonte	Testes de carga insuficientes	Sobrecarga nos Servidores	68.12 %	32.50 %	27.60 %	39.00 %	41.80
Código Fonte	Testes insuficientes	Geração de aplicações com erros	67.20 %	27.50 %	25.20 %	38.00 %	39.48
Cabeamento	Incidência de roedores	Rompimento do cabeamento	62.16 %	27.75 %	15.20 %	34.00 %	34.78
Banco de Dados	Políticas de Segurança Inadequadas	Perda da Integridade dos dados	63.76 %	13.75 %	17.00 %	31.00 %	31.38
Equipamentos de Rede	Equipamentos antigos e precários	Instabilidade da Rede	54.82 %	20.25 %	17.80 %	31.00 %	30.97
Funcionários	Insatisfação ou Doença	Baixa produtividade	53.90 %	15.25 %	15.00 %	28.00 %	28.04

Figura 22 – Risco Parcial por Setor

Ao analisar individualmente o resultado dos métodos na Figura 22, percebe-se que novamente houve variação na lista de priorização de riscos. Considerando o resultado obtido no setor “Divisão de Suporte” o risco com maior prioridade para os métodos ARIMA, AURUM e ISRAM foi “Demanda excessiva de trabalho”. Entretanto, para o método FMEA foi “Ataque de Vírus/Hackers”.

Em segundo lugar o risco de maior prioridade para o método ARIMA foi “Mau uso do sistema”, enquanto que para os métodos AURUM, FMEA e ISRAM foi “Ataque de Vírus/Hackers”.

A ordem de classificação dos riscos pode ser melhor visualizada na Tabela 14, onde são apresentadas as ameaças e o seu lugar de classificação considerando cada um dos métodos analisados.

Tabela 14 – Classificação dos riscos priorizados no setor Divisão de Suporte

Classificação	ARIMA	AURUM	FMEA	ISRAM
1º Lugar	Demanda excessiva	Demanda excessiva	Ataque de Vírus/Hackers	Demanda excessiva
2º Lugar	Mau uso do sistema	Ataque de Vírus/Hackers	Demanda excessiva	Ataque de Vírus/Hackers
3º Lugar	Ataque de Vírus/Hackers	Mau uso do sistema	Mau uso do sistema	Mau uso do sistema
4º Lugar	Indisponibilidade da Informação	Indisponibilidade da Informação	Indisponibilidade da Informação	Indisponibilidade da Informação
5º Lugar	Acesso Indevido	Vazamento de Informações Sigilosas	Sobrecarga nos servidores	Vazamento de Informações Sigilosas
6º Lugar	Vazamento de Informações Sigilosas	Acesso Indevido	Geração de aplicações com erro	Acesso Indevido
7º Lugar	Sobrecarga nos servidores	Sobrecarga nos servidores	Vazamento de Informações Sigilosas	Sobrecarga nos servidores
8º Lugar	Geração de aplicações com erro	Rompimento do cabeamento	Acesso Indevido	Geração de aplicações com erro
9º Lugar	Perda da integridade dos dados	Geração de aplicações com erro	Instabilidade da rede	Rompimento do cabeamento
10º Lugar	Rompimento do cabeamento	Instabilidade da rede	Perda da integridade dos dados	Perda da integridade dos dados
11º Lugar	Instabilidade da rede	Baixa Produtividade	Rompimento do cabeamento	Instabilidade da rede
12º Lugar	Baixa Produtividade	Perda da integridade dos dados	Baixa Produtividade	Baixa Produtividade

Os resultados apresentados na Tabela 14, demonstram que houve uma variação ainda maior entre os métodos na priorização dos riscos considerando somente as respostas dos participantes lotados no setor “Divisão de Suporte”. As colunas pintadas representam os riscos que se repetiram no mesmo lugar de classificação, sendo que a única posição que apresentou o mesmo risco para todos os métodos foi o quarto lugar com a ameaça “Indisponibilidade da Informação”. Em todas as outras posições ocorreram divergências. Assim, ao filtrar pelo setor, o nível de variação nas classificações de riscos entre os métodos foi maior do que considerando as respostas de todos os participantes. Desta forma, os resultados demonstram que ao realizar a análise/avaliação de riscos em uma organização é possível obter visões distintas entre os riscos que devem ser priorizados. Isto é consequência da subjetividade no processo de coleta de informações, pois os resultados dependem exclusivamente das respostas dos participantes e de sua opinião pessoal.

Para auxiliar na visualização das divergências dos riscos priorizados em cada setor, foi elaborado o gráfico da Figura 23, com base nos resultados obtidos pela ferramenta MAAR.

O gráfico apresenta uma legenda com os setores analisados e para cada ameaça identificada é mostrado o percentual obtido em cada setor.

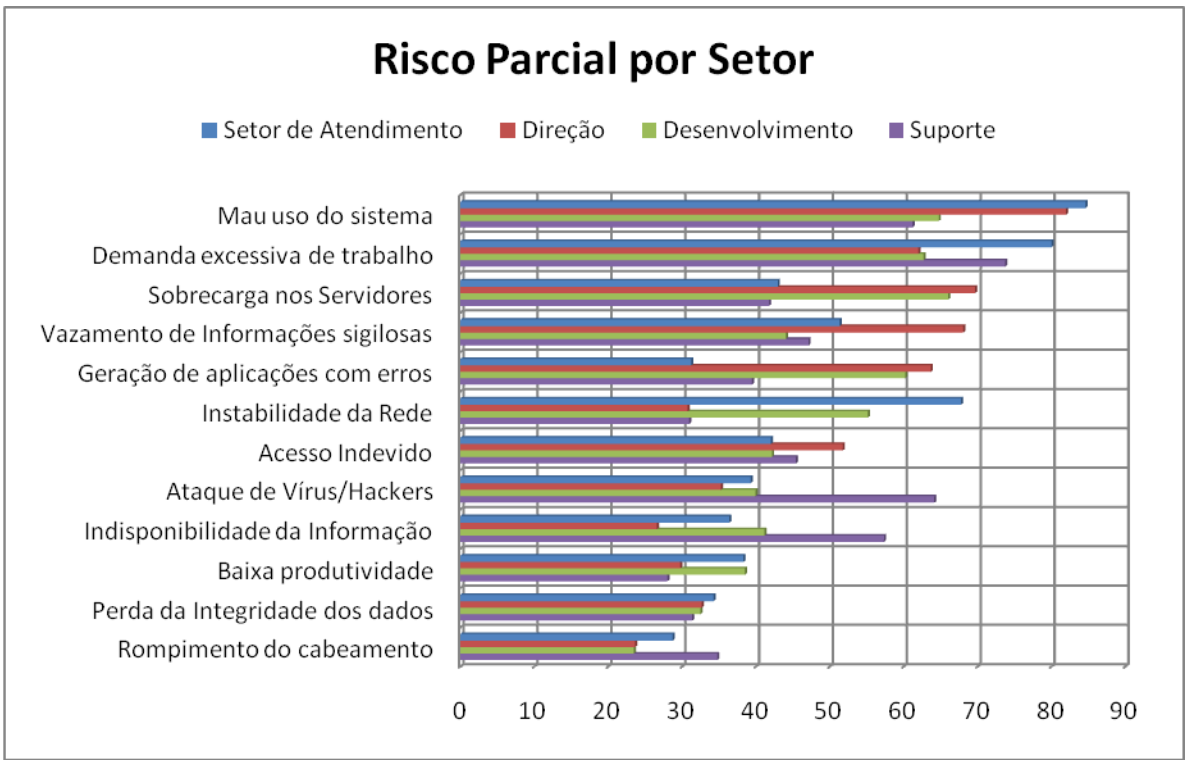


Figura 23 – Gráfico de Comparação dos riscos priorizados em cada Setor

Ao analisar o gráfico da Figura 23, percebe-se que houve variação nos riscos priorizados em cada setor. Para o setor de Suporte a ameaça "Ataque de Vírus/Hackers" é considerada de alto risco para a organização, enquanto que para os demais setores esta ameaça não representa um risco elevado.

A ameaça "Sobrecarga nos servidores" também apresentou variações. Para o setor de Desenvolvimento e de Direção, essa ameaça é considerada de alto risco, no entanto, para os setores de Suporte e Atendimento esta ameaça é de baixo risco.

Desta forma, percebe-se que os setores priorizaram riscos diferentes em sua avaliação, isto é resultado da convivência diária com problemas específicos ao setor, por isso a importância de envolver todos no processo de análise/avaliação de riscos, para que ameaças importantes sejam identificadas.

5.2.3 Risco Parcial por Cargo

Outra forma de obter o risco parcial é filtrando os resultados por Cargo. As pessoas que ocupam diferentes cargos na instituição também apresentam opiniões distintas, ilustrado na Figura 24.

Risco Parcial por Cargo

Setor

Cargo: Assistente de TI

Filtrar

Ativos	Vulnerabilidades	Ameaças	ARIMA	AURUM	FMEA	ISRAM	Média
Usuários	Usuários sem treinamento no sistema	Mau uso do sistema	91.74 %	100.00 %	80.00 %	80.00 %	87.94
Funcionários	Quadro reduzido de funcionários	Demanda excessiva de trabalho	95.87 %	100.00 %	38.40 %	82.00 %	79.07
Equipamentos de Rede	Equipamentos antigos e precários	Instabilidade da Rede	89.45 %	75.00 %	27.60 %	74.00 %	66.51
Banco de Dados	Compartilhamento de senhas	Vazamento de Informações sigilosas	77.52 %	55.00 %	11.20 %	58.00 %	50.43
Funcionários	Insatisfação ou Doença	Baixa produtividade	66.97 %	30.00 %	26.40 %	34.00 %	39.34
Sala de Servidores	Ausência de mecanismos de acesso	Acesso Indevido	66.97 %	30.00 %	20.80 %	32.00 %	37.44
Banco de Dados	Políticas de Segurança Inadequadas	Perda da Integridade dos dados	50.46 %	25.50 %	36.00 %	32.00 %	35.99
Computadores	Políticas de Segurança Inadequadas	Ataque de Vírus/Hackers	65.60 %	17.50 %	16.80 %	38.00 %	34.48
Código Fonte	Testes de carga insuficientes	Sobrecarga nos Servidores	57.34 %	15.00 %	18.00 %	30.00 %	30.08
Equipamentos Servidores	Ausência de espelhamento	Indisponibilidade da Informação	57.34 %	15.00 %	18.00 %	30.00 %	30.08
Cabeamento	Incidência de roedores	Rompimento do cabeamento	42.20 %	13.00 %	5.60 %	20.00 %	20.20
Código Fonte	Testes insuficientes	Geração de aplicações com erros	28.90 %	1.00 %	2.80 %	10.00 %	10.68

Figura 24– Risco Parcial por Cargo

Para o cargo “Assistente de Tecnologia da Informação”, a ameaça que representa o maior risco é “Mau uso do sistema”, o que difere do risco identificado pela maioria dos participantes como primeiro lugar “Demanda excessiva de trabalho”. Isto se deve ao fato de que as pessoas que possuem esse cargo na instituição, estão exercendo funções de atendimento ao usuário, por isso sua preocupação é maior com relação a esta ameaça.

Percebe-se que a ameaça “Geração de aplicações com erros” aparece em último lugar na lista de priorização dos riscos para o cargo “Assistente de TI”. No entanto, considerando as respostas de todos os participantes, essa mesma ameaça ficou em quarto lugar.

No gráfico da Figura 25, é possível visualizar os riscos filtrados pelos cargos da instituição avaliada. Os valores obtidos demonstram a diferença de opinião entre pessoas que possuem cargos distintos.

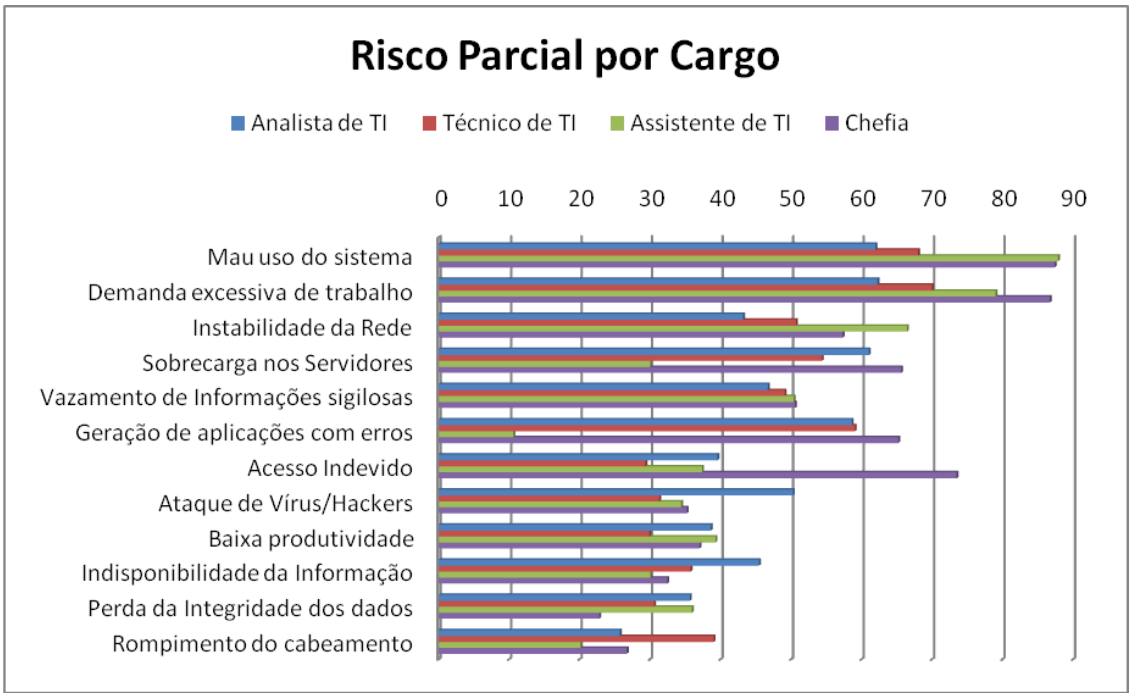


Figura 25– Gráfico de Comparação dos riscos priorizados por Cargo

O Risco parcial por cargo também apresentou divergências em seus resultados. A ameaça "Acesso Indevido" foi considerada pela chefia como sendo uma ameaça de alto risco. Entretanto, para os analistas, técnicos e assistentes, esta mesma ameaça foi considerada de baixo risco.

Outra ameaça que também apresentou uma variação significativa foi "Mau uso do sistema". Para a chefia e assistentes esta ameaça representa um alto risco para a instituição, no entanto, para analistas e técnicos a ameaça "Demanda excessiva de trabalho" tem prioridade.

5.2.4 Comparação entre os métodos

Os dados coletados durante o processo de análise/avaliação de riscos são expressos através de valores percentuais, que servirão de apoio nas decisões gerenciais do negócio, na elaboração de políticas, procedimentos e mudanças operacionais e gerenciais, necessárias para reduzir a probabilidade de ocorrência de incidentes.

Os valores de impacto e probabilidade atribuídos ao risco são baseados na opinião subjetiva dos participantes. Assim, riscos graves podem não ser diferenciados o suficiente se utilizado um único método. Ao usar a composição de métodos, os valores obtidos irão representar a ponderação dos métodos analisados, o que reduz a probabilidade de erro.

A comparação entre os métodos também auxilia na tomada de decisão, pois permite verificar tendências e variações existentes. Na Figura 26, é possível visualizar a comparação

entre os métodos analisados. Os valores obtidos simbolizam o percentual de risco calculado, e a média representa a soma dos resultados de cada método dividido pelo número de métodos.

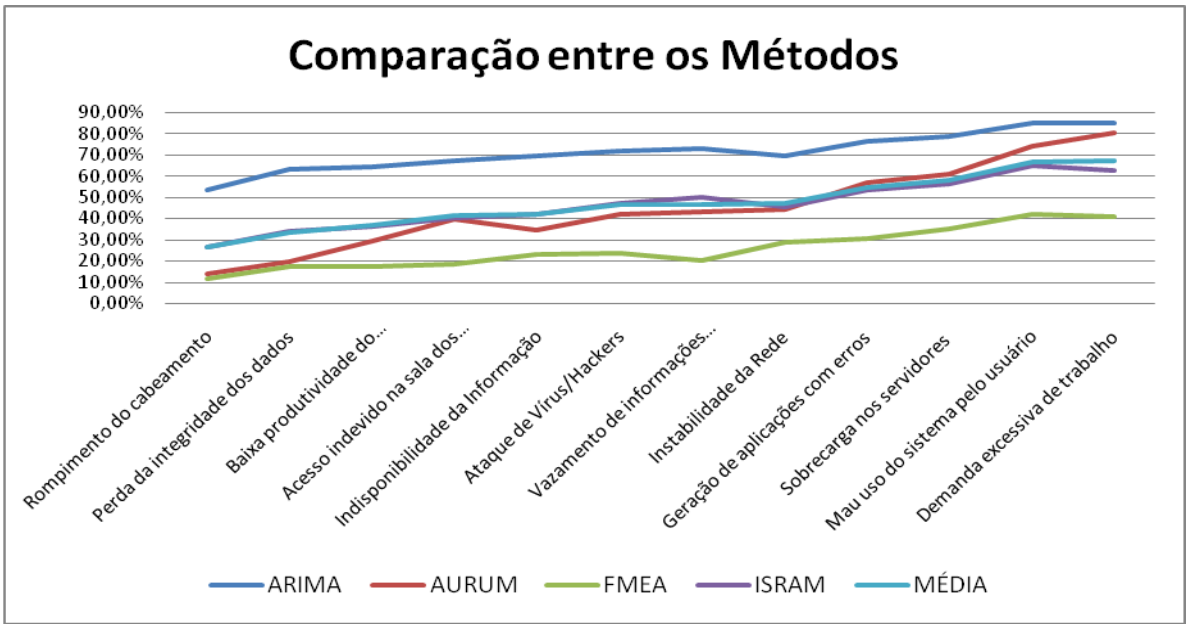


Figura 26 – Gráfico de Comparação entre os métodos

Observa-se que o método ISRAM é o mais próximo da média e que o método ARIMA é o mais afastado. Porém, o ARIMA mantém a mesma variação da média ao longo do gráfico, o que resulta em uma lista de priorização bastante similar.

Os métodos AURUM e FMEA, apresentam pequenas quedas em seus resultados, demonstrando que a priorização de riscos diverge em alguns pontos da média. Este fato permite concluir que a priorização de riscos pode ter variações dependendo do método utilizado.

5.3 Conclusões Parciais

Neste capítulo foram apresentados os resultados obtidos com a aplicação da metodologia proposta no Capítulo 3. O uso de vários métodos possibilitou realizar uma análise comparativa com o objetivo de identificar possíveis divergências na priorização de riscos, o que de fato ocorreu.

Os resultados demonstraram que houve uma variação na lista de priorização dos riscos considerando os métodos ISRAM, AURUM, ARIMA e FMEA. Desta forma, riscos graves podem não ser diferenciados o suficiente se utilizado um único método. Ao usar a composição de métodos, os valores obtidos irão representar a ponderação dos métodos analisados, o que reduz a probabilidade de classificação divergente.

6 CONCLUSÕES

Com o aumento de ameaças que podem explorar vulnerabilidades e gerar incidentes de segurança, tornou-se necessário a prática da gestão de riscos, com o objetivo de reduzir a probabilidade da ocorrência de incidentes a um nível aceitável pela organização. Entretanto, o processo de análise/avaliação de riscos pode se tornar oneroso, pois demanda tempo das pessoas envolvidas e exige vários cálculos matemáticos para mensuração dos riscos.

Atualmente, existem vários métodos para estimar o risco, no entanto, nem sempre estabelecem a escala a ser utilizada ou o padrão para a coleta das informações, o que acaba dificultando a sua aplicação prática. Além disso, utilizar somente um método pode resultar em quantificações classificatórias divergentes.

Esta dissertação apresentou uma metodologia que propõe a composição de métodos para quantificar o risco, através da análise dos ativos, suas vulnerabilidades e ameaças. Na elaboração do estudo, foram utilizados os métodos quantitativos ISRAM, AURUM, ARIMA e FMEA.

A metodologia propôs sete etapas para a obtenção do valor do risco, calculado com base na ponderação dos métodos analisados. Para isso, foi necessário padronizar a coleta de informações e realizar um mapeamento para colocá-los na mesma escala.

O cenário de aplicação foi o CPD da Universidade Federal de Santa Maria. No total 70% dos funcionários (23 pessoas) participaram da pesquisa, incluindo os setores de Desenvolvimento, Suporte, Atendimento ao usuário e Direção.

Os resultados demonstraram que ao aplicar simultaneamente métodos distintos sob um mesmo domínio, é possível ocorrer divergências nas priorizações dos riscos, o que pode resultar em decisões baseadas em valores incertos, que não representam a realidade da organização.

Para auxiliar nos processos de cálculo e na utilização da metodologia proposta, foi desenvolvida uma ferramenta computacional, com várias funcionalidades, o que facilitou o processo de implantação da análise/avaliação de riscos no cenário adotado. A ferramenta assegurou a eficiência do processo, contribuiu para a avaliação da metodologia proposta, automatizou os cálculos matemáticos e assegurou confiabilidade e agilidade para os gestores que buscam tomar decisões com base em relatórios gerados.

6.1 Trabalhos Futuros

Como sugestão para trabalhos futuros, sugere-se a expansão da ferramenta desenvolvida para auxiliar de forma integral no processo de gestão de riscos definido pela NBR ISO/IEC 27005:2008, que inclui outras etapas: tratamento do risco, monitoramento, comunicação e aceitação, e por questões de cronograma foram deixadas de lado, mas podem tornar-se matéria-prima para trabalhos futuros.

Outra contribuição importante para este trabalho é a geração de gráficos, com base nos resultados obtidos, permitindo que gestores analisem de forma gráfica os riscos existentes em sua organização.

A subjetividade no processo de coleta das informações também pode ser explorada em trabalhos futuros, com o objetivo de minimizar esse problema.

Além disso, a ferramenta também pode ser expandida para um sistema informatizado de gestão de segurança da informação, implementando outras fases do método DMAIC da metodologia proposta por Oliveira (2009).

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:2005.** Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2005.

_____. **NBR ISO/IEC 27001:2006.** Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Rio de Janeiro, 2006.

_____. **NBR ISO/IEC 27005:2008.** Tecnologia da Informação. Técnicas de Segurança. Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

ALBERTS, C., *et al*. **Introduction to the OCTAVE® Approach**. Pittsburgh: Carnegie Mellon University, 2003. Disponível em: <http://www.cert.org/octave>. Acesso em: jun. 2011.

AMARAL, E. H., AMARAL, M.M. e NUNES, R.C. **Uma metodologia para Cálculo do Risco por Composição de Métodos**. X Simpósio Brasileiro de Segurança da Informação-SBSEG '10. Fortaleza - CE. 2010.

BLAUTH , Regis. **Seis Sigma: uma estratégia para melhorar resultados**. Revista FAE Business**,** n.5, abr. 2003. Disponível em: <http://www.est.ipcb.pt/psi/psi_OG/>. Acesso em: 13 abr. 2011.

CAMPOS, A. (2007). **Sistema de Segurança da Informação: Controlando os Riscos.** Florianópolis: Visual Books, 2. Ed.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

EKELHART, A., FENZ, S. and NEUBAUER, T. **AURUM: A Framework for Information Security Risk Management**. *42nd Hawaii International Conference on System Sciences*, HICSS '09. 2009.

FENG, D. and ZHANG, Y. **Survey of information security risk assessment**. *Journal of China Institute of Communications*, 25(7):10-18. 2004.

FERNANDES, A. A., ABREU, V. F. **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: Brasport, 2006.

GRANDISON, T.W.A. **Trust Management for Internet Applications**. Tese. University of London. London. 2003.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC TR 13335-1.** Guidelines for the Management of IT Security(GMITS) - Techniques for the management of IT Security. 1st Edition. Switzerland, 2004.

_____. **ISO/IEC 31000:2008.** Risk management — Principles and guidelines on implementation. International Organization for Standardization, 2008.

KARABACAK, B. and SOGUKPINAR, I. **ISRAM: information security risk analysis method**, In: Computers & Security 24 (2) 147-159. 2005.

KROLL, J. and DORNELLAS, M. C. **Aplicação da Metodologia de Avaliação de Riscos para o Gerenciamento Estratégico da Segurança da Informação**. *XLI Simpósio Brasileiro de Pesquisa Operacional*, Porto Seguro - BA. 2009.

KROLL, J. **Um modelo conceitual para especificação da gestão de riscos de Segurança em Sistemas de Informação**. 2010. 138 f. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de Santa Maria, 2010.

LEITNER, A. and SCHAUMULLER-BICHL, I. **ARIMA - A new approach to implement ISO/IEC 27005**. *Logistics and Industrial Informatics*. LINDI'09. 2nd International, 10-12 September. 2009.

MARTINS, A. B. and SANTOS, C.A.S. **Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação**. *Revista de Gestão e Tecnologia e Sistema de Informação*. Vol. 2, No. 2, pp. 121-136. 2005.

MAYER, J; FAGUNDES, L. L. **Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.** VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, São Leopoldo-RS, 2008.

MEIRA, S. **E-gov: os problemas e o tamanho da oportunidade**. 2011. Disponível em <http://smeira.blog.terra.com.br/2011/05/30/e-gov-os-problemas-e-o-tamanho-da-oportunidade/>. Acesso em: jun. 2011.

OLIVEIRA, M. A. F., NUNES, R. C. and ELLWANGER, C. **Uma Metodologia Seis Sigma para Implantação de uma Gestão de Segurança da Informação Centrada na Percepção dos Usuários**. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, SBSeg'09, Campinas, Porto Alegre: SBC, pp.173-186. 2009.

OLIVEIRA, M. A. F. **Implantação de uma gestão de Segurança da Informação através da abordagem Seis Sigma**. 2009. 187 f. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de Santa Maria, Santa Maria, 2009.

OLIVEIRA, M.A.F., et al. **Uma Metodologia de Gestão da Informação Direcionada a Riscos baseado na Abordagem Seis Sigma**. XXVIII ENEGEP, Rio de Janeiro. 2008.

PUENTE, J., et al. **A decision support system for applying failure mode and effects analysis**. *International Journal of Quality & Reliability Management*, n.2, v. 19. 2002.

ROTONDARO, R.G., et al. **Seis Sigma. Estratégia Gerencial para a Melhoria de Processos, Produtos e Serviços**. São Paulo: Atlas. 2006.

SANTOS, A. M. R. C. **Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação**. 2007. 277 f. Tese (Doutorado em Engenharia) - Universidade do Minho – Escola de Engenharia, Portugal, 2007.

STAMATIS, D.H. **Failure Mode and Effect Analysis: FMEA from theory to execution**. Milwaukee, Winsconsin: ASQ Quality Press, second edition. 2003.

STONEBURNER, G., GOGUEN, A. e FERINGA, A. **Risk Management Guide for Information Technology Systems**: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800-30*. 2002.

ZAPATER, M.; SUZUKI, R. **Segurança da Informação – Um diferencial determinante na competitividade das corporações.** Promon Business & Technology Review, 2005. Disponível em: http://www.promon.com.br. Acesso em: mar. 2011.

ZHIGANG, L., et al. **Study on Efficiency of Risk Management for Information Security Based on Transaction**. *Second International Symposium on Electronic Commerce and Security*, pp. 356 – 360. 2009.