Metodologia para Cálculo do Risco por Composição de Métodos

Érico Hoff do Amaral[1], Marisa M. Amaral[1], Raul C. Nunes[1]

[1]Programa de Pós Graduação em Informática (PPGI)
Universidade Federal de Santa Maria (UFSM)
Av. Roraima, 100 – CEP 91.501-970 – Santa Maria – RS - Brasil

ericoh@gmail.com, amarisa@cpd.ufsm.br, ceretta@inf.ufsm.br

Abstract. *The information became a valuable asset for organizations, and in computer systems is subject to various types of threats. To ensure the integrity, confidentiality and availability of this information is necessary to adopt risk management practices. This paper analyzes and compares different methods for calculating the risk, showing that there is diversity of results in the same area, and proposes a methodology for calculating simultaneously applying different methods to obtain more accurate results.*

Resumo. *A informação tornou-se um ativo valioso para as organizações, e em sistemas computacionais, está sujeita a diversos tipos de ameaças. Para garantir a integridade, a confidencialidade e a disponibilidade dessas informações se faz necessário adotar práticas de gestão de riscos. Este artigo analisa e compara diferentes métodos para o cálculo do risco, demonstrando que há diversidade de resultados em um mesmo domínio, e propõe uma metodologia de cálculo que aplica simultaneamente diferentes métodos para obter resultados mais precisos.*

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].

A quantificação dos riscos é muitas vezes subjetiva e pode ser difícil atribuir valores consistentes para estimá-los [Grandison 2003]. Por exemplo, valorações sobre informações, tais como *impacto* e *probabilidade*, são na maioria das vezes, estimados por pessoas com diferentes origens e personalidades, o que remete à incerteza dos valores estimados, em função destas individualidades. Para resolver o problema da subjetividade, técnicas matemáticas são utilizadas para calcular valores de probabilidade e impacto. Além disso, muitas metodologias de análise de riscos divergem

significativamente entre si, podendo resultar em quantificações classificatórias divergentes. Porém, elas não exploram a composição de metodologias para minimizar a probabilidade de classificação divergente.

Este artigo analisa e compara diferentes métodos para o cálculo do risco com escalas distintas, e propõe uma metodologia que os aplica simultaneamente para obter resultados mais precisos, cujo risco de maior gravidade é aquele indicado pela maioria dos métodos. O cenário de aplicação escolhido foi o Centro de Processamento de Dados (CPD) da instituição de ensino. Como resultado, obteve-se indicadores de risco potencialmente mais precisos, uma vez que refletem a predominância apontada por diferentes técnicas.

O artigo está organizado da seguinte forma: a seção 2 apresenta um referencial teórico sobre a gestão de riscos. A seção 3 aborda os métodos existentes para cálculo do risco. A seção 4 demonstra a metodologia utilizada para calcular o risco nos diferentes métodos analisados. A seção 5 apresenta os resultados obtidos e por fim, na seção 6, as considerações finais.

2. Gestão de Riscos

Segundo [Zhigang *et al.* 2009] 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. 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. Seu objetivo é administrar, priorizar e controlar os riscos de segurança. Através da gestão de riscos são identificados os principais impactos, ameaças e vulnerabilidades que cercam um sistema de informação [Kroll e Dornellas 2010]. Este artigo concentra-se na análise do risco e na sua quantificação para avaliação dos riscos.

2. 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.

Nesse contexto, é necessário que cada instituição e os seus diversos níveis organizacionais consigam enumerar seus ativos, incluindo as vulnerabilidades e as ameaças inerentes aos mesmos, com a finalidade de entender a natureza e a relevância dos riscos relacionados aos diferentes processos. 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. Assim, convém que o ativo de informação seja classificado para indicar a necessidade, prioridade e o nível esperado de proteção.

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.

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]. 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, ou seja, um risco.

O risco é então, 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].

2. 2. Quantificação do risco

De uma forma geral, existem duas metodologias para a análise de riscos: a qualitativa e a quantitativa. Ambas envolvem cálculos, embora a qualitativa utilize cálculos mais simples, os quais fornecem resultados subjetivos, enquanto a quantitativa apresenta resultados baseados em valores objetivos.

3. Métodos para cálculo do risco

Vários métodos já foram implementados para realizar a gestão de riscos, dentre os quais se destacam: ISRAM [Karabacak e Sogukpinar 2005], AURUM [Ekelhart *et al.* 2009], ARIMA [Leitner e Schaumuller-Bichl 2009] e FMEA [Rotondaro *et al*. 2006]. Cada método apresenta características específicas e fórmulas distintas para realizar o cálculo do risco. A seguir, é apresentado o referencial dos métodos utilizados nessa análise, explicando de forma detalhada as variáveis utilizadas, as escalas de valores e a fórmula proposta para o cálculo do risco.

3.1. O método ISRAM

O ISRAM (*Information Security Risk Analysis Method)* [Karabacak e Sogukpinar 2005] é um método de análise de riscos, utilizado para avaliar 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).

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

O ISRAM consiste em sete etapas principais:

1. Identificar os problemas de segurança que envolve 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 fator de risco do ISRAM é um valor numérico entre 1 e 25, que corresponde a um valor qualitativo (alto, médio ou baixo). O valor qualitativo é então utilizado como fator de decisão.

3.2. O método AURUM

O AURUM (*Automated Risk and Utility Management*) 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. Seu objetivo é minimizar a interação necessária entre usuário e sistema, fornecendo aos gestores uma solução intuitiva que pode ser utilizada sem conhecimento aprofundado sobre o domínio da segurança da informação [Ekelhart *et al.* 2009].

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 a seguinte:

Tabela 1. Escala de riscos - AURUM

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

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], atualmente, nenhum método satisfaz inteiramente os sub-processos 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 realizar o cálculo do 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	O impacto é controlável e não há efeitos subsequentes para a organização
M	O impacto não pode ser totalmente compensado
H	O impacto tem efeitos significativos sobre a organização

Tabela 3. Escala de Probabilidade – ARIMA

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

Após identificar o impacto e a probabilidade, ARIMA usa uma matriz (Tabela 4) para determinar o nível de 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

3.4. O método FMEA

O 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].

Conforme [Puente *et al.* 2002], o método *FMEA* é útil para definir ações que visam reduzir ou eliminar o risco associado a cada falha. 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; e
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 1.

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 Aruais	S	O	D	RPN	Estratégia	Ações Recomendadas	Situação

Figura 1. Formulário FMEA

O método FMEA estabelece três índices para pontuar o risco, podendo ser realizado com base no julgamento pessoal, por empirismo, 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):

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

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.

4. Metodologia para Cálculo do Risco por Composição de Métodos

Nesta seção, será apresentada a metodologia utilizada para realizar a análise e comparação entre os métodos ISRAM, AURUM, ARIMA e FMEA. O cenário adotado para realizar e aplicar o estudo foi o Centro de Processamento de Dados (CPD) da instituição de ensino.

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.

Inicialmente, foi feito um levantamento juntamente com os funcionários do CPD, utilizando técnicas de *brainstorming* para identificar os ativos da organização, suas vulnerabilidades e possíveis ameaças.

4.1. Identificação e classificação dos ativos

A identificação dos ativos consiste em determinar os bens relevantes para a organização dentro do escopo de projeto no cenário definido. Para realizar o levantamento dos ativos, este estudo utilizou técnicas de *brainstorming*, envolvendo os setores de desenvolvimento, suporte e atendimento ao usuário do CPD. Os ativos identificados foram agrupados de acordo com sua classificação, como mostra a Tabela 5.

4.2. Detecção das vulnerabilidades

O processo de detecção das vulnerabilidades tem por objetivo verificar a existência de falhas de segurança associadas aos ativos. Para cada ativo identificado na fase anterior foi realizado um levantamento das possíveis falhas de segurança que poderiam estar associadas a ele. Na Tabela 5 é possível visualizar algumas dessas vulnerabilidades.

4.3. 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. A Tabela 5 demonstra parte dos ativos, suas vulnerabilidades e ameaças.

Tabela 5. Lista de Ativos, Vulnerabilidades e Ameaças

Grupo de Ativos	Lista de Ativos	Vulnerabilidades	Ameaças
Ativos de Informação	Banco de Dados	Compartilhamento e quebra de senhas	Acesso indevido
			Alterações maliciosas - perda da integridade
			Vazamento de informações
		Testes de carga insuficientes	Sobrecarga no banco
	Documentação do sistema	Indefinição de regras e padrões de documentação	Inexistência de documentação do sistema
	Código-fonte	Compartilhamento de senhas	Acesso indevido
			Alterações maliciosas - perda da integridade
Ativos de Software	Ferramentas de desenvolvimento	Manual de instalação incompleto	Demora na instalação
		Falta de treinamento	Uso incorreto das ferramentas de desenvolvimento
Ativos Humanos	Funcionários	Insatisfação e Doença	Baixa na Produtividade
		Falta de capacitação	Erros nos processos de trabalho
	Usuários	Falta de treinamento	Erro na utilização do sistema

4.4. Utilização dos métodos para o cálculo do risco

Após a identificação dos ativos, suas vulnerabilidades e suas ameaças, 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.

Quantificar o risco é atribuir valores consistentes para estimá-los, e nesse contexto, vários métodos como ISRAM, AURUM, ARIMA e FMEA já foram desenvolvidos e avaliados com a finalidade de auxiliar neste processo. Variáveis como probabilidade e impacto são utilizadas para realizar os cálculos, no entanto, mesmo utilizando técnicas matemáticas para esses cálculos, os valores são estimados por pessoas, de forma subjetiva, portanto, não há uma garantia de que esses valores representam efetivamente a realidade.

Uma forma de amenizar este problema é utilizar mais de um método para estimar o risco e, com base nos resultados obtidos, calcular a média entre eles. Desta maneira, é possível obter valores mais próximos da realidade, já que o risco de maior gravidade será aquele apontado pela maioria dos métodos. Assim, a organização conhecendo o nível de risco 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.

Neste estudo, para aplicar simultaneamente os quatro métodos, foi necessário padronizar a coleta dos dados e realizar um mapeamento entre eles.

4.4.1. Padronização da coleta de informações

Com o objetivo de padronizar a entrada de informações, foi elaborado um questionário, onde o entrevistado deveria selecionar dentre uma lista de opções (Muito Baixa, Baixa, Média, Alta e Muito Alta) aquela que melhor representasse sua opinião, considerando as variáveis de Probabilidade, Detecção, Ocorrência e Impacto (Severidade) para cada ameaça identificada, como mostra a Tabela 6.

Tabela 6. Questionário aplicado aos participantes da pesquisa

Ativos	Ameaças	Probabilidade	Detecção	Ocorrência	Impacto (Severidade)
Banco de Dados	Acesso indevido	Média	Muito Baixa	Baixa	Média
	Vazamento de informações	Baixa	Baixa	Muito Baixa	Muito Alta
	Sobrecarga no banco	Média	Média	Alta	Alta
Funcionários	Baixa na Produtividade	Baixa	Muito Baixa	Muito Baixa	Baixa
	Erros nos processos de trabalho	Muito Baixa	Muito Baixa	Muito Baixa	Baixa
	Erro na utilização do sistema	Média	Média	Média	Alta

Considerando que cada método utiliza uma escala específica e possui variáveis diferentes para realizar o cálculo, foi necessário realizar um mapeamento entre eles. Para automatizar este processo foi utilizado o aplicativo Microsoft Excel.

4.4.2. Mapeamento dos métodos

Para se alcançar um resultado efetivo, no uso de diferentes métodos para estimar o risco, foi necessário realizar um mapeamento entre eles. Com exceção do FMEA, os outros métodos utilizam somente as variáveis de Probabilidade e Impacto para determinar o risco. O FMEA é o único que utiliza três variáveis: Severidade, Ocorrência e Detecção.

A escala *Likert* foi adotada como padrão para os métodos FMEA e ISRAM, em função de que os mesmos não possuem uma escala precisa, na definição do uso do método. No entanto, os métodos AURUM e ARIMA possuem sua própria escala para

Probabilidade e Impacto. Desta forma, foi necessário realizar um mapeamento entre a escala padrão e as escalas específicas. Veja a Tabela 7.

Tabela 7. Mapeamento dos métodos

FMEA e ISRAM		AURUM		ARIMA	
Escala Padrão	**Probabilidade e Impacto**	**Probabilidade**	**Impacto**	**Probabilidade**	**Impacto**
Muito Baixa	1	0,1	10	VL	L
Baixa	2	0,1	10	L	L
Média	3	0,5	50	M	M
Alta	4	1	100	H	H
Muito Alta	5	1	100	VH	H

O método AURUM considera somente três valores (Baixa, Média e Alta) para as variáveis de Probabilidade e Impacto. Deste modo, foi necessário estabelecer uma relação das opções "Muito Baixa" e "Muito Alta" para "Baixa" e "Alta", 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), como mostra a Tabela 7. 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).

Para resolver o problema do uso de escalas distintas foi utilizada a conversão para o percentual em relação ao total de cada método. Desta forma, identificou-se o valor máximo possível para o risco em cada método analisado, conforme sua escala (Tabela 8).

Tabela 8. Valores máximos obtidos em 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), podemos perceber que este é o valor máximo que pode ser obtido da interseção da linha Probabilidade com a coluna de Impacto.

O método ISRAM utiliza o produto de duas variáveis, que podem assumir como valor máximo 5, portanto, o seu produto final será 25. O AURUM também utiliza o produto de duas variáveis e 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 obter o resultado percentual, em relação ao total de cada método, foi utilizada uma regra de três simples, considerando o valor máximo equivalente a 100%. Assim, os valores foram calculados de acordo com as seguintes fórmulas:

$$ARIMA = ((P \cap I) * 100)/5 \quad (3)$$

$$ISRAM = ((P * I) * 100)/25 \quad (4)$$

$$AURUM = ((P*I) *100)/100 \quad (5)$$

$$FMEA = ((S*O*D)*100)/125 \quad (6)$$

O objetivo deste cálculo é permitir a comparação entre os métodos, pois os resultados obtidos estarão na mesma escala percentual.

5. Resultados e considerações

Após aplicar as fórmulas específicas de cada método, foi possível obter o valor do risco estimado. Na tabela 9, é possível visualizar a média das respostas de todos os participantes da pesquisa.

Tabela 9. Resultado da Pesquisa

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

Os resultados obtidos demonstraram divergências entre os métodos analisados. O método ISRAM foi o que obteve valores mais próximos da média, enquanto o método ARIMA apresentou o percentual mais alto que a maioria, consequência de sua escala pouco precisa (5 é o valor máximo para o risco).

Os métodos AURUM e FMEA mantiveram índices baixos se comparados aos demais, o que também se justifica em decorrência de sua escala (valores máximos 100 e 125 respectivamente).

Como podemos observar, os valores obtidos apresentaram divergências, o risco de maior gravidade (indicado na cor vermelha na Tabela 9) pelo método AURUM foi "Sobrecarga no banco", enquanto que para os demais foi "Sobrecarga nos servidores". O segundo risco de maior gravidade (indicado na cor azul na Tabela 9) 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 método, corre-se o risco de obterem-se resultados inconsistentes.

Ao utilizarmos mais de um método para o cálculo do risco, têm-se indicadores de risco potencialmente mais precisos, uma vez que refletem a predominância apontada pela maioria dos métodos. Na Figura 2, é possível visualizar os riscos que obtiveram o maior número de prioridade de risco com base na média calculada.

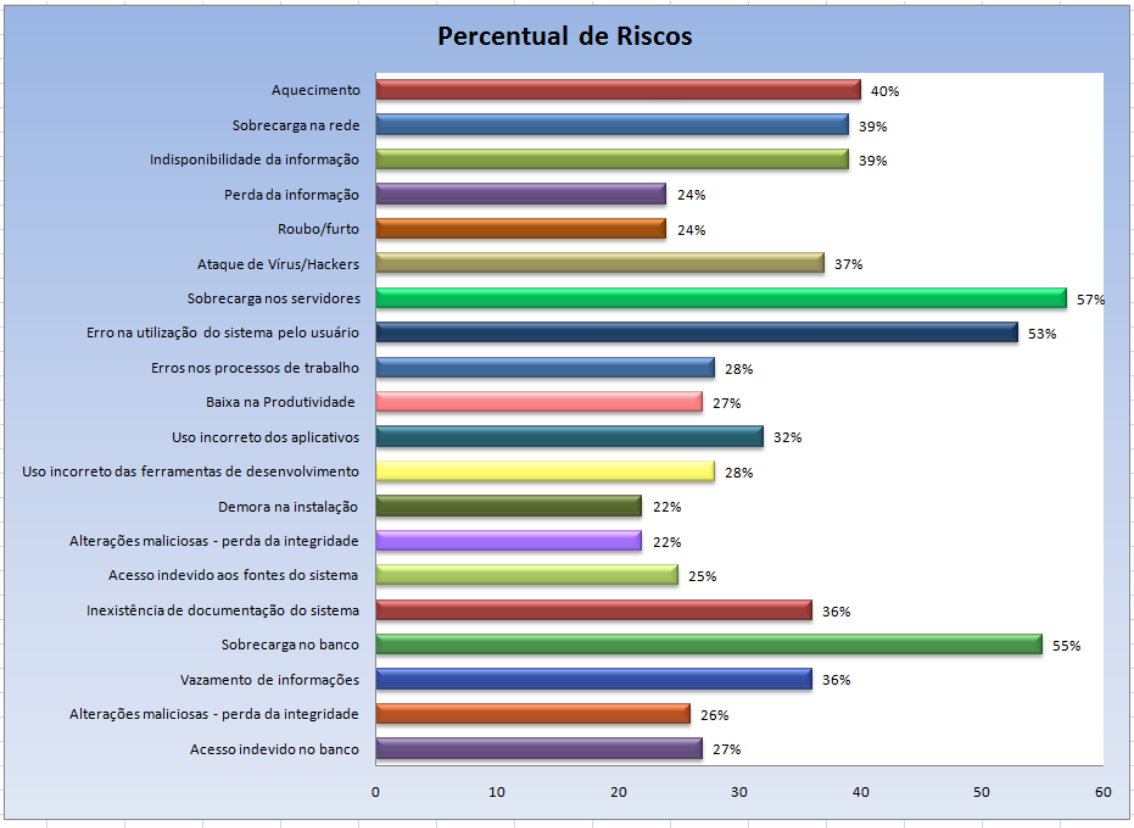

Figura 2. Gráfico com o percentual de riscos calculados com base na média

Analisando o gráfico da Figura 2 é possível perceber que as ameaças que obtiveram o maior percentual de risco foram: "Sobrecarga nos servidores" com 57%, "Sobrecarga no banco" com 55% e "Erro na utilização do sistema pelo usuário" com 53%. Esses resultados foram obtidos com base na média dos valores calculados em cada

um dos métodos analisados. Os riscos com maior prioridade são os que devem ser minimizados.

6. Conclusão

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.

Atualmente, existem vários métodos para estimar o risco, no entanto, cada um com suas peculiaridades. O presente artigo, apresenta uma metodologia que propõe a utilização de métodos diferentes para quantificar o risco, através da análise dos ativos, suas vulnerabilidades e suas ameaças. Na elaboração desse estudo, foram utilizados os métodos ISRAM, AURUM, ARIMA e FMEA.

Analisando os resultados obtidos podemos concluir que, os métodos utilizados para calcular o risco apresentaram divergências em seus resultados, mesmo tendo sido aplicados sob um mesmo domínio. Este estudo propõe como alternativa para minimizar estas divergências, a utilização de mais de um método para estimar o risco e, a aplicação de uma metodologia eficiente para o cálculo da média entre eles, o que permite, portanto, obter valores mais precisos.

Atualmente está sendo desenvolvida uma ferramenta computacional que automatiza a utilização de métodos diferentes para estimar o risco, o que deverá proporcionar agilidade e eficiência no processo de análise de risco de segurança da informação.

Referências

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

Dias, C. (2000). Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books.

Ekelhart, A., Fenz, S. and Neubauer, T. (2009). AURUM: A Framework for Information Security Risk Management. *42nd Hawaii International Conference on System Sciences*, HICSS '09.

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

Grandison, T.W.A. (2003). Trust Management for Internet Applications. Tese. University of London. London.

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

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

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

Leitner, A. and Schaumuller-Bichl, I. (2009). ARIMA - A new approach to implement ISO/IEC 27005. *Logistics and Industrial Informatics*. LINDI'09. 2nd International, 10-12 September.

Martins, A. B. and Santos, C.A.S. (2005). 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.

NBR ISO/IEC 17799:2005 (2005*).* Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro.

Oliveira, M. A. F., Nunes, R. C. and Ellwanger, C. (2009). 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.

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

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

Santos, A.M.R.C. (2007). Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação. Tese. Universidade do Minho – Escola de Engenharia.

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

Stoneburner, G., Goguen, A. and Feringa, A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800-30*.

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