Proposta de um modelo para auxílio na gestão de riscos da informação – Integrando métodos e normas

Mariana Freitas[1], Gerson Nunes[1], Patrícia Lopes[1], Thiago Dantas[1], Érico Amaral[1]

[1]Universidade Federal do Pampa (UNIPAMPA)
Caixa Postal – Bagé – RS – Brazil

{maripompeof,padulalopes,thiagodantas923}@gmail.com,
{gersonnunes,ericoamaral}@unipampa.edu.br

Abstract. *Information is considered a valuable asset to businesses, and is subject to several types of threats. To ensure the necessary protection and avoid incidents, it is necessary to adopt risk management practices that ensure business continuity, minimize risk and maximize return of investment. As a simplified way of identifying threats that could put at risk the organization's assets, this paper proposes the study and creation of a model for the analysis of potential risks based on international norms and standards of security. This work has results, among which are cited: creation and validation of a new model of risk analysis and implementation of a pilot software to automate the model created.*

Resumo. A informação é considerada um ativo valioso para as empresas, e está sujeita a diversos tipos de ameaças. Para assegurar a proteção necessária e evitar incidentes é necessário adotar práticas de gerenciamento de riscos, que garantem a continuidade do negócio, minimiza o risco e maximiza o retorno do investimento. Como uma maneira de identificar, de forma simplificada, as ameaças que possam colocar em risco os ativos da organização, este trabalho propõe o estudo e criação de um modelo para análise de potenciais riscos baseada em normas e padrões internacionais de segurança. Este trabalho possui resultados, dentre os quais citam-se: criação e validação de um novo modelo de análise de riscos e implementação de um software piloto para automatizar o modelo criado.

1. Introdução

Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança dos clientes, o relacionamento com parceiros e fornecedores e, pode impedir, direta ou indiretamente, a organização de cumprir sua missão e de gerar algum lucro. Para enfrentar essas ameaças, as empresas devem adotar atividades proativas, evitando os prejuízos. Isto pode ser obtido através do gerenciamento de riscos, que contribui para o sucesso dos negócios, pois protege a disponibilidade, integridade e privacidade das informações (ABBASS et al, 2014). A aplicação das abordagens existentes para a gestão de riscos se concentra, em sua maioria, em conceitos e princípios (TALABIS & MARTIN, 2013), o que dificulta sua implantação.

Diante desse cenário, este trabalho vislumbra implementar e validar um modelo para avaliação de potenciais riscos encontrados em ativos de informação em instituições públicas e privadas, a fim de garantir o cumprimento dos princípios básicos da segurança da informação. A construção do modelo utilizou-se das normas de segurança da informação NBR ISO/IEC, em especial a NBR ISO/IEC 27005 (ABNT, 2011) e o processo de avaliação e gerenciamento de riscos do domínio de Planejamento e Organização do COBIT 4.1 (IT GOVERNANCE INSTITUTE, 2007). Este trabalho concentra-se na fase de avaliação de riscos.

A estrutura textual adotada neste artigo é composta de seis seções organizadas da seguinte forma: a seção 2 apresenta a metodologia adotada, a seção 3 apresenta dois trabalhos correlatos, a seção 4 demonstra a pesquisa e a análise dos resultados obtidos, a seção 5 expõe a implementação do Projeto Piloto, e, por fim têm-se as conclusões e os trabalhos futuros.

2. Metodologia

A metodologia adotada neste trabalho se enquadra no método hipotético-dedutivo. Com relação aos procedimentos técnicos adotou-se os tipos bibliográfica, documental e experimental, além disso, de acordo com os tipos de pesquisa descritos por GIL (2010), esse trabalho se classifica como exploratório. Baseado na taxonomia de VERGARA (2006), esta pesquisa pode ser classificada como de natureza aplicada.

3. Trabalhos Correlatos

Nesta seção são apresentados 2 trabalhos correlatos, a fim de identificar o estado da arte nesta área de estudo: O trabalho de dissertação intitulado “Metodologia para Análise e Avaliação de Riscos por Composição de Métodos” de autoria de AMARAL (2011) propõe uma metodologia para análise/avaliação de riscos que utiliza a composição de métodos já conceituados, tais como ISRAM, AURUM, ARIMA e FMEA para exibição dos valores de risco. Estes foram calculados com base nas fórmulas definidas em cada método e considerando sua escala específica. A fim de validar a metodologia proposta, foi implementado a ferramenta MAAR. O trabalho conclui que os métodos utilizados resultaram em listas de priorização de riscos distintas, o que levou a conclusão que riscos graves poderiam não ser diferenciados o suficiente se utilizado um único método. O modelo proposto nesse trabalho se difere do apresentado por AMARAL (2011) em vários aspectos técnicos tais como a forma como é calculada a probabilidade da ameaça ser explorada e portanto, a forma como os riscos são calculados entre outros.

O documento “Metodologia de Gestão de Riscos de Segurança da Informação - Desenvolvimento de metodologia e ferramenta de software público de arquitetura aberta para gestão de riscos de segurança da informação na Administração Pública Federal” (FACTI, 2015), apresenta a Metodologia de Gestão de Riscos de Segurança da Informação do SISP (MGR-SISP). Este visa descrever métodos para padronizar e sistematizar a gestão de riscos de segurança da informação na Administração Pública Federal (APF) e objetivou atingir níveis satisfatórios de segurança da informação, bem como racionalizar os investimentos na área de segurança da informação. As informações necessárias para a realização dos processos da metodologia proposta foram obtidas por meio de questionários, através destes, foi possível apurar uma lista de ativos primários e respectivos valores de criticidade para cada um dos atributos. Este trabalho correlato é voltado para um órgão em específico, diferente do que é proposto nesse projeto, que deve ser genérico e servir de apoio para qualquer tipo de empresa.

4. Apresentação da Pesquisa e Análise de Resultados

A NBR ISO/IEC 27005 (ABNT, 2011) propõe os seguintes passos para a identificação dos riscos:

1) Identificar os ativos;
2) Identificar as ameaças a esses ativos;
3) Identificar as vulnerabilidades que podem ser exploradas pelas ameaças;
4) Identificar os impactos que possam ser causados aos ativos. Sabendo disso, foi construído o modelo ilustrado na Figura 1 que consiste em 8 passos. Apesar de o modelo seguir uma série de passos, a ideia é possibilitar ao usuário editar as informações fornecidas em passos anteriores (o que pode ser percebido nas flechas azuis da Figura 1).

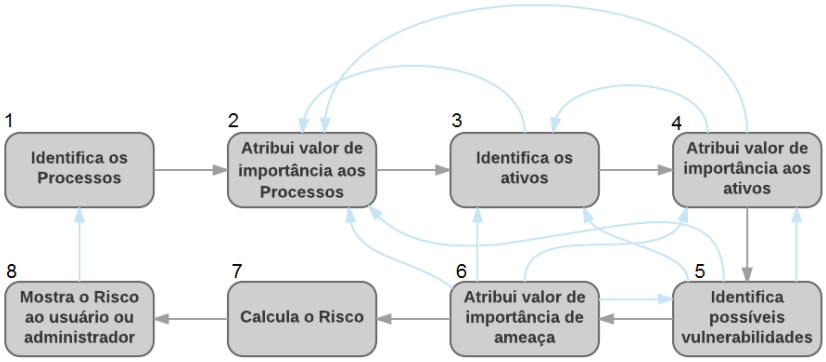

Figura 1: Passos do modelo

O modelo funciona da seguinte forma:

1) Identifica os Processos;
2) Atribui o valor de importância com base em uma escala de 3 pontos, conforme Tabela 1.
3) Identifica os ativos;
4) Atribui o valor de importância com base em uma escala de 3 pontos;
5) Identifica as vulnerabilidades;

Tabela 1: Nota e descrição de importância de Processo

Nota	Descrição da Nota
1	Pouco importante (alterações no processo não impedem o cumprimento da missão da organização);
2	Importante (alterações podem afetar de forma significativa o cumprimento da missão da organização);
3	Muito importante (sua interrupção torna impossível cumprir a missão da organização);

Tabela 2: Nota e descrição de importância do Ativo

Nota	Descrição da Nota
1	Pouco importante (ativo pode ser substituído/recriado com facilidade);
2	Importante (ativo pode ser substituído/recriado com dificuldade);
3	Muito importante (ativo não pode ser substituído/recriado);

6) Atribui o valor de importância do impacto da vulnerabilidade (se explorada) com base em uma escala de 5 pontos, conforme Tabela 3;
7) Calcula risco;
8) Apresenta o índice de risco para o usuário;

Tabela 3: Nota e descrição de importância de impacto

Nota	Descrição da Nota
1	Insignificante (nenhum prejuízo na imagem, perdas financeiras irrelevantes, sem impactos sobre os negócios);
2	Menor (pequenos efeitos e facilmente reparados, solução imediata local, perdas financeiras médias);
3	Moderado (efeitos sobre algumas atividades de negócios, possui solução com ajuda externa, perdas financeiras moderadas);
4	Maior (grandes abalos na imagem, interrupção temporária da atividade de negócio, ajuda externa para tratamento, perdas financeiras elevadas);
5	Catastrófico (morte, interrupção total das atividades, solução externa, danos de difícil reparação, perdas financeiras elevadas).

Tabela 4: Média de Risco para a Empresa

	Valor de Risco
Ativo de Hardware	80
Ativo de Software	225
Ativo de Redes	48
Risco Médio para a Empresa	225

Para o cálculo do Risco foram propostas duas equações. Estas foram desenvolvidas levando em conta possíveis incidentes e vulnerabilidades, além disso, considerou-se os valores de importância dos ativos, dos processos e das ameaças. Objetivando determinar um único valor de risco total para a empresa optou-se por comparar os índices de riscos calculados a partir das Equações na análise e fornecer ao usuário como risco final o maior valor encontrado. Essa escolha teve como embasamento os testes realizados na validação do modelo, fornecer uma média por exemplo, retornava muitas vezes um valor de risco baixo ou médio, o que poderia dar ao usuário uma falsa ideia de bom nível de segurança, quando na verdade alguns ativos necessitavam de medidas que diminuíssem o valor do risco. Da mesma forma, o valor retornado como risco médio da empresa (valor considerando todos os ativos analisados) será o maior valor encontrado entre os ativos, tal fato pode ser melhor visualizado na Tabela 4.

Além de um valor quantitativo, os riscos podem assumir um valor qualitativo. Neste trabalho para classificação de riscos quantitativos será adotado a escala *Likert*. Os valores correspondentes aos riscos são mostrados ao usuário de forma qualitativa conforme descrito na Tabela 5.

Tabela 5: Classificação Qualitativa e Quantitativa dos Riscos

Classificação Qualitativa	Classificação Quantitativa
Risco Muito Baixo	0 – 25
Risco Baixo	26 – 40
Risco Médio	41 – 60
Risco Alto	61 – 100
Risco Muito Alto	Acima de 100

As classificações, bem como os intervalos quantitativos para cada risco qualitativo descritos na Tabela 5 foram obtidos por método de tentativa e erro e foram validadas.

Para avaliar de forma preliminar o modelo proposto foram realizados testes. Estes são constituídos de três passos, detalhados a seguir:

1) Foram elencadas cinco empresas reais para testar o modelo;
2) Os profissionais das empresas responderam ao questionário criado pelos autores e baseado na norma ISO;
3) Foi realizada a análise de risco considerando as respostas fornecidas no questionário. O resultado final está na Tabela 6.

Os ativos escolhidos para validação do modelo e implementação do Projeto Piloto foram definidos por meio de pesquisas, através de questionários web. Profissionais de diversas empresas com diferentes ramos de atuação (financeiro, comércio, indústria, educação, órgão/instituição pública e prestação de serviços) responderam aos questionários. Por meio destes, foram obtidos os ativos existentes nas organizações. O resultado da pesquisa pode ser observado no gráfico ilustrado na Figura 2. Foram implementados os 3 ativos mais presentes de acordo com a pesquisa.

Figura 2: Identificação dos Ativos presentes nas organizações

Tabela 6: Resultado dos Testes do Modelo criado

Empresa	Ativo Hardware	Ativo Software	Ativo Redes	Risco Final
Empresa 1 (Órgão Público Federal)	40	100	60	100 (Alto)
Empresa 2 (Privada)	10	8	4	10 (Muito Baixo)
Empresa 3 (Privada)	18	18	16	18 (Muito Baixo)
Empresa 4 (Órgão Público Estadual)	80	120	60	120 (Muito Alto)
Empresa 5 (Privada)	80	64	48	80 (Alto)

A validação do modelo foi realizada de forma manual. Para cada resposta dada pelo usuário, era verificado se aquilo que o modelo retornava era aceitável considerando a quantidade de vulnerabilidades encontradas e os valores atribuídos aos ativos e ameaças. Considerando os resultados encontrados na análise de risco do modelo criado, pode-se concluir que o modelo foi validado com sucesso. Assim parte-se para a próxima fase – a implementação do projeto piloto.

5. Implementação

Após os testes do modelo proposto, se fez necessário automatizá-lo, a fim de facilitar a análise de risco. Foram implementadas as seguintes funcionalidades até o presente momento: Cadastro de administrador; Cadastro de Empresa; Cadastro de usuários; Análise de Risco;

O funcionamento do protótipo pode ser melhor entendido com Diagrama de Sequências ilustrado na Figura 3.

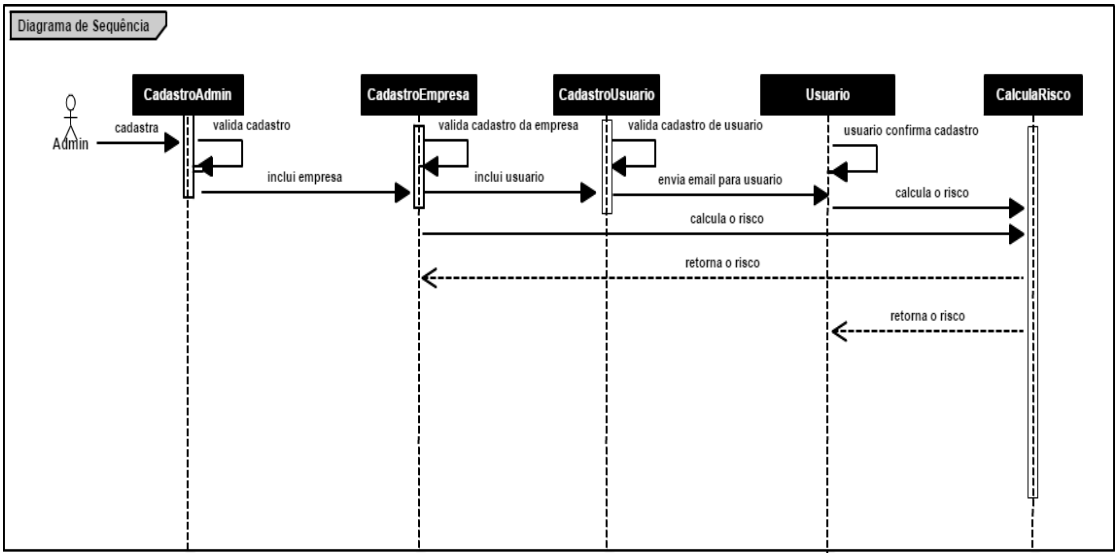

Figura 3: Diagrama de Sequências

Após a implementação das funcionalidades citadas, foram determinados os casos de testes visando validar o programa do projeto piloto. Para cada um dos Casos de Teste foram determinados objetivos, os passos necessários para atingir o objetivo proposto e os critérios de êxito. Os resultados de análise de risco fornecidos pelo programa para todos os ativos de todas as empresas coincidiram com os obtidos nos testes manuais de validação do modelo, como era esperado, visto que o programa é a implementação do modelo, portanto o software do Projeto Piloto foi validado com sucesso.

6. Conclusões e Trabalhos Futuros

Serão expostos alguns pontos importantes relacionados ao modelo criado, ao software piloto e a norma NBR ISO/IEC 27005 (ABNT, 2011) e o *framework* COBIT.

A norma NBR ISO/IEC 27005 (ABNT, 2011) estabelece na seção 7 alguns critérios para avaliação de riscos. Foram considerados no desenvolvimento deste modelo, os seguintes itens: O valor estratégico do processo que trata as informações de negócios; A criticidade dos ativos de informação envolvidos. Para critérios de impacto, o modelo desenvolvido atendeu aos seguintes itens: Perdas de negócio e de valor financeiro; Dano a reputação, entre outros. No que diz respeito ao escopo e os limites da organização para a gestão de riscos, o modelo atendeu aos seguintes itens previstos na norma: Processos de negócios; Funções e estrutura da organização; Ativos de informação. A seção 8 que trata do processo de avaliação de riscos prevê as seguintes atividades consideradas no modelo: Identificação dos ativos, das ameaças e das vulnerabilidades. Também é sugerido que seja considerada durante a análise de risco a importância do processo de negócios ou da atividade suportada por um determinado ativo. Tal sugestão é atendida no modelo criado visto que o valor de importância do processo dado pelo usuário ou administrador é levado em consideração na equação do cálculo de risco, e, quanto maior o valor, maior será o nível de risco retornado. Seguindo o *framework* COBIT 4.1 e os Processos relacionados a Avaliação e Gerenciamento de Riscos de TI, o modelo desenvolvido neste trabalho atendeu aos seguintes processos: PO9.2 Estabelecimento do Contexto de Risco; PO9.3 Identificação de Eventos; PO9.4 Avaliação de Risco. Pode-se afirmar que o modelo criado, além de ter sido validado de forma manual com empresas reais, retornando os resultados esperados, assim como o software piloto, de fato atende à norma NBR ISO/IEC 27005(ABNT, 2011) e o COBIT como proposto inicialmente. Como trabalho futuro propõe-se implementar outras funcionalidades importantes, tais como exclusão de administradores e usuários, possibilidade de inclusão de ativos, entre outros, além disso, pretende-se colocar o software online para facilitar o acesso aos interessados.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.

_____**NBR ISO/IEC 27005:** Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro/RJ, 2011.

ABBASS, Wissam; BAINA, Amine; BELLAFKIH, Mostafa. **Improvement of Information System Security Risk Management**, IEEE, 2014.

AMARAL, Marisa Munaretto. **Metodologia para Análise e Avaliação de Riscos por Composição de Métodos.** Dissertação de Mestrado. Santa Maria, 2011.

FACTI. **Metodologia de Gestão de Riscos de Segurança da Informação.** Relatório RM2, 2015.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2010.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**. 2007. Disponível em: https://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cobit4-1.aspx

MAYER, Janice; FAGUNDES, Leonardo Lemes. **A Model to Assess the Maturity Level of the Risk Management Process in Information Security**. IEEE, 2009.

TALABIS, Mark Ryan M; MARTIN, Jason L. **Information Security Assessment Tolkit**. Elsevier, 2013.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2006.