ABORDAGEM MULTICRITÉRIO PARA IMPLANTAÇÃO DE AÇÕES DE SEGURANÇA DA INFORMAÇÃO: UMA APLICAÇÃO NO SETOR DE SAÚDE

Lúcio Camara e Silva, Thiago Poleto, Jadielson Alves de Moura, Suzana França Dantas Daher, Ana Paula Cabral Seixas Costa.
Universidade Federal de Pernambuco - UFPE
lucio_camara@hotmail.com, thiagopoleto@hotmail.com, dielson10@hotmail.com, suzanadaher@gmail.com, apcabral@ufpe.br

RESUMO

Segurança da informação está relacionada com a proteção de um conjunto de dados, de forma a preservar seu valor para um indivíduo ou organização e vem sendo adotada, através de diferentes estratégias, por várias empresas. Conforme um estudo anteriormente realizado pelos autores no setor de saúde, foi constatada a existência de uma diferença com relação ao desempenho em segurança da informação entre uma empresa pública e uma privada. A análise dessa diferença foi o ponto de partida para elaboração desse trabalho, cujo objetivo é dar suporte na priorização de políticas e/ou ações de segurança da informação que atendam às necessidades, preferências e restrições de um hospital público situado em Recife. Para tanto se fez uso de uma combinação de um modelo multicritério e da programação inteira. Os resultados servirão de base para que as ações sejam implantadas de forma mais eficiente em face de restrições de tempo e recursos financeiros.

PALAVRAS CHAVE. Segurança da informação, políticas de segurança, saúde, PROMETHEE II, programação inteira.

Área principal (ADM – Apoio a Decisão Multicritério, SE – PO em Serviços, SA – PO na área de Saúde)

ABSTRACT

Information security is a concept related to data protection, in order to preserve its value for an individual or organization, which has been adopted by several companies through different strategies. In accordance with a previous study in health sector developed by the authors, a difference with respect to the performance in information security between a public company and a private one was detected. The analysis of this difference was the start point for development of this study in which the main goal is support a public hospital to prioritize security policies and/or actions considering needs, preferences and constraints of the organization. Facing this objective, a combination of multicriteria model and integer programming was conducted. The results gives a basis for implement the actions in a more efficient way considering time and financial constraints.

KEYWORDS. Information security, security policies, health, PROMETHEE II, integer programming.

1. Introdução

Conforme pode ser visto em Syamsuddin e Hwang (2010), o conceito de segurança da informação - SegInf – está associado a um conjunto de leis, regras e práticas que regularizam como uma organização gerencia, protege e distribui recursos para alcançar os objetivos das políticas de segurança. Entretanto, dentre os requisitos para planejamento, implementação e manutenção da SegInf em uma organização, têm-se as Políticas de SegInf (Pathari e Sonar, 2012), as quais, segundo Zakaria (2005), correspondem a formas de manter dados e sistemas de informação de forma segura.

De acordo com Shirtz e Elovici (2010), existem quatro dimensões que estão associadas com as políticas de SegInf, a saber: confidencialidade, integridade, disponibilidade e não-repúdio. Confidencialidade significa que toda informação deve ser protegida de acordo com o grau de confidencialidade do seu conteúdo e, portanto, o caminho no qual seus conteúdos são ilustrados devem ser limitados. Integridade está associada ao estado da informação no tempo em que foi gerada e recebida. Deverá ser considerado um recebimento completo se a informação for fiel ao seu estado original. Disponibilidade assegura que apenas usuários autorizados tem acesso a informação e ao correspondente sistema quando precisarem. Não-repúdio é a garantia de que alguém não pode negar alguma coisa e refere-se à capacidade de garantir que uma parte de um contrato ou uma comunicação não pode negar a autenticidade de seu/sua assinatura em um documento ou o envio de uma mensagem de impressão que o usuário originou.

Uma vez que uma determinada organização contém quantidades significativas de informações pessoais, uma violação dos dados pode causar diversos danos (Renaud e Goucher, 2012). Esse é um exemplo em um setor de saúde, no qual a privacidade dessas informações tem sido mandatória por atos legislativos, através da imposição de normas rígidas sobre como as informações do cliente são protegidos (Johnston e Warkentin, 2008).

Com isso, a necessidade da aplicação de políticas de SegInf está atrelada à proteção contra possíveis ameaças. Esta tem se tornado, portanto, prática comum nas empresas e várias têm elaborado suas respectivas estratégias de segurança. Esse resultado pôde ser observado no estudo proposto por Silva et al. (2012), onde foi analisada a adoção de políticas de SegInf em duas empresas, pública e privada, do setor de saúde. Foi observado que cada empresa, de acordo com suas restrições, seja financeira, tecnológica, adotava um percentual de políticas de SegInf, com a privada levando certa vantagem em relação a pública.

Portanto, a análise dessa diferença serviu de base para elaboração desse trabalho, cujo objetivo é dar suporte na priorização de políticas SegInf e/ou ações de SegInf, que correspondem a um conjunto dessas políticas, que atendam às necessidades, preferências, restrições e limitações de cada organização, tornando-a mais desenvolvida nesse aspecto. Diante do cenário exposto, faz-se necessário a aplicação de um método que auxilie na tomada de decisão que envolve múltiplas alternativas e múltiplos critérios, alguns deles conflitantes entre si. Portanto, uma abordagem multicritério é extremamente útil para auxiliar nesse processo.

O restante do artigo está organizado da seguinte forma: a Seção 2 é dedicada a uma revisão da literatura sobre segurança da informação; Seção 3 apresenta o fluxograma referente às atividades do trabalho, bem como uma aplicação do método no contexto de saúde. Finalmente, as conclusões e discussão deste trabalho são apresentadas na Seção 4, que também faz recomendações para futuras pesquisas sobre o tema em questão.

2. Referencial Teórico

2.1 Segurança da Informação

Conforme pode ser observado na literatura, Segurança da Informação tem se tornado uma prática comum nas empresas e, com isso, vários modelos e *frameworks* têm sido sugeridos para o processo de tomada de decisão com relação às medidas corretivas quando os eventos inesperados de SegInf ocorrem.

Veiga e Eloff (2010) propuseram um *framework* para avaliar a cultura de SegInf em uma organização levando-se em consideração os aspectos técnicos, processuais e de comportamentos humanos. Este também fornece um ponto abrangente para o cultivo de uma

cultura em uma organização que minimiza os riscos decorrentes de comportamento dos usuários. Enquanto isso, Pathari e Sonar (2012) propuseram uma abordagem para analisar um conjunto de políticas de SegInf para estabelecer uma hierarquia implícita e importância relativa entre essas políticas.

No trabalho proposto por Silva et al. (2012), um *framework* foi desenvolvido para analisar o modelo de maturidade de segurança da informação (ISMM – *Information Security Maturity Model*) em duas organizações no setor de saúde: uma Pública e outra Privada. Foi assumido que cada organização adota um nível mínimo de políticas de SegInf com base nos aspectos de confidencialidade, integridade, disponibilidade e não repúdio. Com isso, o nível de maturidade foi analisado com relação ao percentual de políticas que uma organização apresenta em relação a todas as políticas citadas no modelo. O resultado mostrou um desempenho diferenciado da organização Publica (58,93 %), com relação a Privada (68,05%).

2.2 Apoio Multicritério a Decisão

De acordo com Almeida e Costa (2003), o apoio multicritério a decisão tem como princípio estabelecer uma relação de preferências entre as alternativas que estão sendo avaliadas de acordo com conjunto de critérios destacados no processo decisório. Ainda de acordo com os autores, existem vários métodos desenvolvidos para o tratamento de problemas envolvendo múltiplos objetivos. Wiecek et al. (2008) destaca que o desenvolvimento desses métodos foi motivado não apenas por uma variedade de problemas da vida real que exigem a consideração de múltiplos critérios, mas também pela vontade dos profissionais em propor técnicas avançadas de apoio a decisão.

Na literatura é comum encontrar um divisão entre os métodos multicritérios: a escola americana, baseada nos modelos únicos de síntese e donde pode-se destacar Teoria da Utilidade Multiatributo (MAUT); e a europeia, baseadas nos métodos de sobreclassificação que admitem incomparabilidade, destacando-se os métodos da família ELECTRE e PROMETHEE (Almeida e Costa, 2003). A escolha do método mais adequado depende da estrutura de preferência do decisor e do tipo de problemática a ser analisada, que segundo Roy (1996), pode ser identificada em 4 tipo: Escolha, Classificação, Ordenação e Descrição.

Segundo Brans e Mareschal (2002), os métodos da família PROMETHEE se baseiam na construção de uma relação de sobreclassificação, agregando informações entre alternativas e critérios, e a exploração dessa relação para o apoio a decisão. De acordo ALBADVI et al. (2007) a avaliação das alternativas em relação ao critério forma uma matriz de avaliação, considerada a entrada básica para a maioria dos métodos. Deve-se acrescentar a essa entrada alguns parâmetros, tais como: os pesos dos critérios e função preferência dos decisores, quando comparados a contribuição das alternativas em relação a cada critério.

Dentre esses métodos, o PROMETHEE II estabelece uma ordem decrescente de fluxo líquido e, com isso uma ordem completa entre as alternativas (Brans e Mareschal, 2002).

2.3 Uso da abordagem multicritério em Segurança da Informação

Syamsuddin e Hwang (2010) apresentam uma estrutura para orientar os decisores na avaliação do desempenho da política de SegInf, utilizando o método AHP (*Analytic Hierarchy Process*). Esta estrutura é baseada na hierarquia de quatro níveis (meta, critérios, sub-critérios e alternativas), representando diferentes aspectos da política de SegInf. Seus resultados mostraram que os decisores preferem como prioridade da SegInf a questão da disponibilidade, seguido de confidencialidade e integridade. Apesar das discussões acerca dos problemas axiomáticos (Dyer 1990) desse método, a estrutura hierárquica dos critérios de avaliação mostrada no trabalho traz a luz uma boa referência sobre a estruturação do problema.

Yang et al. (2013), por sua vez, propuseram um modelo de avaliação de controle de risco em SegInf que pudesse melhorar a segurança para as empresas. Nessa ocasião propuseram um modelo multicritério combinando VIKOR (do Sérvio - *Multicriteria Optimization and Compromise Solution*), DAMATEL (*Decision-making Trial and Evaluation Laboratory*) e ANP (*Analytic Network Process*) para solucionar o problema de critérios conflitantes que apresentam

dependência.

Imamverdiev e Derakshande (2011) desenvolveram um modelo para tratar do problema da escolha de medidas preventivas para a redução de riscos em SegInf, com base na metodologia *Fuzzy* e *OWA* (*Ordered Weighted Averaging*). Com isto é possível modificar os pesos associados aos critérios baseada na entropia da informação.

Com base na metodologia multicritério de apoio a decisão, cujo uso em problemas relacionados à segurança da informação já foi analisado, será desenvolvido o presente trabalho.

3. Metodologia

De acordo com dados da Secretaria de Saúde de Pernambuco, esta administra aproximadamente 32 hospitais, 14 Unidades de Pronto Atendimento (UPAs), fora laboratórios e outros mais, tornando-se a segunda maior secretaria estadual de saúde do Brasil. Dentre esses hospitais, destaca-se para a análise do hospital público, objeto do presente estudo, o qual oferece aproximadamente 33 especialidades e atende em média 12 mil pacientes por mês. Porém, conforme pode ser visto em Silva et al. (2012), a questão da segurança da informação não é enfatizada nessa organização. Com isso, a busca por novos investimentos em segurança da informação demonstra o interesse por parte do gestor de TI dessa empresa em melhorar essa deficiência.

Portanto, dada a complexidade no processo de decisão com relação a SegInf, o presente trabalho tem como objetivo utilizar uma abordagem multicritério para dar suporte na priorização de políticas e/ou ações de SegInf que atendam às necessidades e preferências das organizações.

O desenvolvimento deste trabalho foi estruturado em 4 etapas, conforme ilustrado na Figura 1.

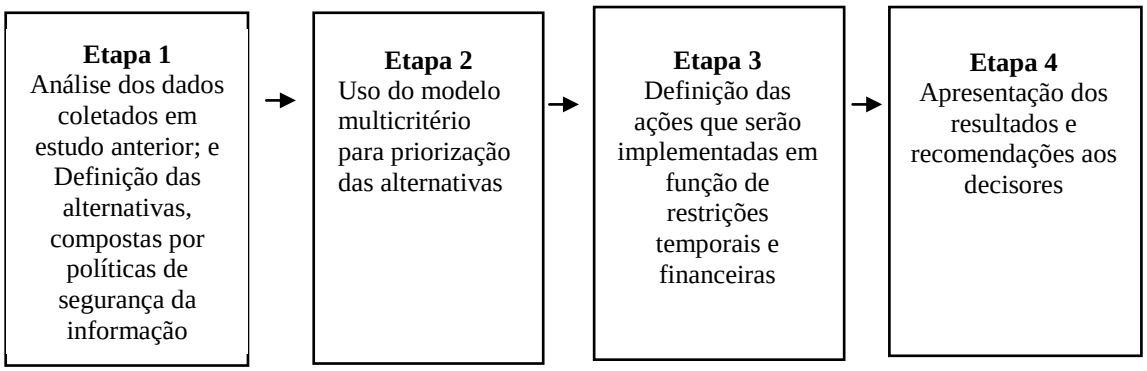

Figura 1 – Etapas para definição das ações de segurança da informação a serem adotadas

3.1 Etapa 1

A primeira etapa corresponde à análise do estudo comparativo de Silva et al. (2012) com relação ao desempenho na adoção de políticas de SegInf nas organizações Públicas e Privadas. Foram levantadas as políticas que ainda não tinham sido adotadas pela empresa que obteve desempenho mais fraco (no caso, o hospital público), dentre o total de políticas disponíveis, tornando-as subsídio para o desenvolvimento das ações estratégicas de SegInf a serem implementadas. A tabela 1 apresenta o conjunto de políticas de SegInf, associado aos critérios de confidencialidade, integridade, disponibilidade e não-repúdio, propostos em Silva et al (2012).

Tabela 1 – Definição das Políticas de Segurança da Informação (Fonte: Adaptado de Silva et al, 2012).

	Confidencialidade		**Integridade**
(PC_1)	Criptografia de dados em repouso	(PI_1)	Sistema de Monitoramento
(PC_2)	Autenticação de identificação do usuário para assinatura digital e conta bloqueada	(PI_2)	*Backup*

(PC_3)	Ao navegar na web, não permitir que os navegadores aceitem *cookies* de sites / Gerenciamento de sessão	(PI_3)	Servidor e estação de trabalho com antivírus
(PC_4)	Autenticação de Protocolo para Sistema de RFID	(PI_4)	Antivírus em Emails
(PC_5)	Digitalizar ataques	(PI_5)	Segurança Física do Ambiente
(PC_6)	Desenvolvimento de cenários hipotéticos sobre SI e riscos, aproveitando o conhecimento de especialistas.	(PI_6)	Aplicações e detectores de candidatos
(PC_7)	Criar um comitê de auditoria que compreenda claramente o seu papel na segurança da informação e como ele vai trabalhar com o gerenciamento e os auditores	(PI_7)	Estratégias de defesa de Rede *Wireless*
		(PI_8)	Aplicação do *Firewall*
		(PI_9)	Fortalecer toda a segurança, servidores críticos e plataformas de comunicação
	Disponibilidade		**Não-Repudiação**
(PD_1)	Identificação de contas de usuários	(PN_1)	Gerenciamento de Operações e Comunicação
(PD_2)	Controle e Acesso - Restrição nas contas dos usuários	(PN_2)	Classificação da Informação no valor da Organização
(PD_3)	Limitações no acesso e monitoramento externo	(PN_3)	Análise de Tráfego
(PD_4)	Toda sessão do computador requer único ID de usuário e senha	(PN_4)	Papéis e responsabilidades de políticas de segurança da informação
(PD_5)	Identificação por Rádio Frequência (RFID)	(PN_5)	Treinamento de empregados para segurança de computadores pessoais
(PD_6)	Avaliação dos efeitos de um programa de conscientização de segurança da informação	(PN_6)	Executar programas com capacidade de resposta de segurança, estabelecer linhas de base de segurança e verificar com rigor o seu cumprimento.
		(PN_7)	Avaliação de Riscos

De posse desse conjunto de políticas, foi feita uma avaliação de quais dessas cada organização, pública e privada, adotava. A Figura 2 abaixo ilustra a diferenciação da adoção nas empresas.

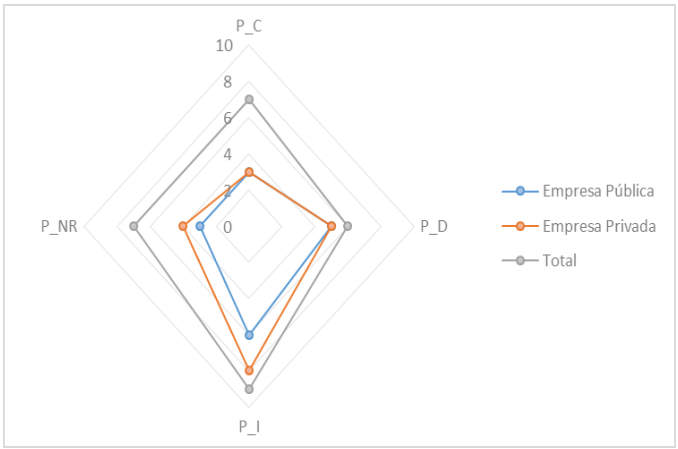

Figura 2 – Diferenciação do uso de políticas de SI nas Organizações

Com base no esquema da figura 2, pode-se notar que do total de políticas analisadas,

que corresponde à linha cinza, a empresa privada destaca-se positivamente com relação à pública. Fato este que pode ser descrito pela dificuldade em realizar investimentos por parte da empresa Pública.

3.2 Apoio Multicritério a Decisão (AMD) para priorização das alternativas

O problema associado ao presente trabalho baseia-se na tomada de decisão para priorização de ações de SegInf para melhorar o desempenho da organização no quesito de segurança. Como consequência dessa proposta, tem-se a possibilidade de redução de perdas/danos nos dados e/ou informações das empresas.

3.2.1 Características gerais do problema

Para aplicação do método multicritério escolhido para analisar os problema, estão apresentadas a seguir as tabelas com as alternativas (Tabela 2), baseadas em um conjunto de políticas não implementadas pela empresa pública do total de políticas disponíveis, e os critérios e os respectivos pesos relativos a cada critério (Tabela 3), todos estabelecidos diretamente pelo decisor, que corresponde ao gestor de TI.

Neste trabalho foram utilizados alguns dos critérios propostos por Syamsuddin e Hwang (2010) e que representam os interesses do decisor. Para cada critério, uma função específica da preferência foi definida e, com base na preferência do decisor foram utilizadas as funções de critério usual para todos.

De acordo com a estrutura de preferência do decisor foi adotado o método PROMETHEE II para a ordenação das alternativas e sua posterior combinação com um modelo de programação inteira. O PROMETHEE V também poderia ter sido adotado para essa mesma finalidade (Vetschera e Almeida 2012). Em outro trabalho, Almeida e Vetschera (2012) analisam o problema da transformação de escala no PROMETHEE V que foi comentado anteriormente neste texto.

Tabela 2 – Definição das Políticas de SI

Alternativa	Código	Alternativa
A1	PD_6	Avaliação dos efeitos de um programa de conscientização de SegInf
A2	PI_7	Estratégias de defesa de rede *Wireless*
A3	PD_5	Identificação por rádio frequência
A4	PN_5	Treinamento para os usuários
A5	PN_7	Avaliação dos riscos
A6	PN_1	Gerenciamento de operação/comunicação
A7	PD_3	Limitação de acesso/monitoramento externo
A8	PC_1	Criptografia dos dados
A9	PC_2	Autenticação de ID do usuário para assinatura digital
A10	PN_6	Executar programas com capacidade de resposta de segurança, estabelecer linhas de base de segurança e verificar com rigor seu cumprimento

Tabela 3 – Definição dos critérios utilizados

Critério	Definição	Pesos
Cr 1 (Gerenciamento)	Exigência no cumprimento de normas, bem como realização periódica de revisões.	0,4
Cr 2 (Complexidade)	Complexidade para implantação da política (tecnológicas, infraestrutura)	0,3
Cr 4 (Cultura)	Dificuldade de Conscientização / Adaptação dos usuários (educação)	0,3

A seguir, apresenta-se a Tabela 4 com a matriz de avaliação das alternativas e os critérios.

Tabela 4 – Matriz de Avaliação Critério x Alternativa

	Critério 1	**Critério 2**	**Critério 3**
Alternativas	Gerenciamento	Complexidade	Cultura
A1	3	4	3
A2	3	3	5
A3	4	3	4
A4	3	5	3
A5	4	4	4
A6	5	4	4
A7	5	3	3
A8	3	4	5
A9	3	5	3
A10	4	3	3

*Avaliação da alternativa com base na escala de Likert de 5 pontos

Na tabela 5 está apresentada a ordenação obtida pelo PROMETHEE II, através do fluxo líquido:

Tabela 5 – *Ranking* das Alternativas

	Ação	ϕ_i
1º	A6	0,52
2º	A5	0,3
3º	A8	0,11
4º	A3	0,03
5º	A7	-0,01
6º	A4	-0,12
7º	A9	-0,12
8º	A2	-0,15
9º	A10	-0,23
10º	A1	-0,32

3.3 Adaptando o problema às restrições de tempo e recursos financeiros

A terceira etapa corresponde ao uso dos fluxos líquido (ϕ_i) calculado pelo PROMETHEE II, conforme mostrado na Tabela 5, em um problema de otimização utilizando a programação inteira, o conhecido problema da mochila. Entretanto, bem como em Mavrotas et. al. (2006), estes fluxos não são adequados para representar os coeficientes das alternativas na função objetivo do problema de programação inteira 0-1, uma vez que alguns deles são negativos, fazendo com que estas alternativas nunca fossem aceitas, mesmo havendo folga das restrições. Com isso, conforme visto em Almeida (2012), são calculados os fluxos líquidos escalonados, que correspondem ao fluxo líquido das alternativas subtraído pelo menor valor entre os fluxos líquidos, acrescidos de um pequeno valor ε, a fim de tornar disponíveis todas as ações. Essa transformação é obtida através da seguinte equação:

$$\phi_i' = \phi_i + \left| min_i \phi_1 \right| + \varepsilon \quad (1)$$

Considerando ε = 0,02, tem-se os seguintes valores para os fluxos.

Tabela 6 – Fluxos Líquidos Escalonados

Ação	A6	A5	A8	A3	A7	A4	A9	A2	A10	A1
Φi escalonado	0,86	0,64	0,45	0,37	0,33	0,22	0,22	0,19	0,11	0,02

Desta forma, o objetivo dessa etapa é solucionar o problema de programação inteira, cuja função objetivo segue a forma (2).

$$Max \sum_{i=1}^{10} x_i \times \emptyset_i \quad (2)$$

Com isso, cada alternativa x_i receberá o valor 1 se for selecionada, e o valor 0 caso contrário. Nessa modelagem, também é levado em consideração não apenas o tempo limite para implementação das políticas, bem como o recurso disponível, que foram definidos pelo decisor com base numa verba disponível (R$ 7000,00) a ser utilizada num período de tempo específico (60 dias). Os valores abaixo são hipotéticos e foram utilizados para ilustrar como o problema foi tratado. As informações sobre o tempo de implantação de cada política, bem como seu custo associado estão descritas na Tabela 7.

Tabela 7 – Informações de Tempo e Custo das Políticas de SegInf

Alternativa	Tempo (Dias)	Custo (R$)
A1	10	950
A2	12	1700
A3	15	1800
A4	5	800
A5	8	1100
A6	12	2500
A7	7	500
A8	14	1600
A9	12	1000
A10	10	1500

Sendo assim, foram definidas as seguintes restrições de tempo e custo, respectivamente.

$$\sum_{i=1}^{10} x_i \times t_i \leq 60 \quad (3)$$

$$\sum_{i=1}^{10} x_i \times r_i \leq 7000 \quad (4)$$

Portanto, é através da aplicação da equação (2), sujeita às restrições (3) e (4), que irá definir a ação que a organização deverá executar para melhorar sua eficiência em SegInf. Como resultado, o gestor de TI deveria implementar, de acordo com as restrições da empresa, as

políticas A3, A5, A6 e A8. Nesse caso, destacam-se as políticas de não-repúdio, como Avaliação dos riscos (A5) e Gerenciamento de Operação/Comunicação (A6), representando a metade das políticas a serem implementadas. Esta última, A6, apresenta maior custo de implementação. Por outro lado, políticas relacionadas a confiabilidade (A8) e disponibilidade (A3) dos dados apresentam maior tempo necessário para implementação.

3.4 Apresentação dos resultados e recomendações ao decisor

A última etapa desse trabalho corresponde a apresentação dos resultados encontrado na etapa anterior. Para isto, foi organizada uma reunião para apresentação e entrega do relatório com os resultados do modelo utilizado. Entretanto, a implementação das políticas não faz parte do escopo desse trabalho.

4. Conclusão

O planejamento da segurança da informação (SegInf), principalmente no que se refere a adoção de políticas de SegInf apresenta-se bastante complexo pelas condições de tempo, custo e prioridade de implantação dessas políticas. Com isso, essa é uma questão que tem se tornado muito importante nas organizações, uma vez que a violação dos dados pode causar diversos danos às mesmas.

Essa importância foi notada no estudo elaborado anteriormente, através de empresas, uma pública e outra privada, do setor de saúde. Nesse estudo constatou-se que há uma diferença no desempenho das organizações no uso de políticas de SegInf, com a Privada relativa superioridade em relação a Pública. Foi com esse resultado, portanto, que motivou e deu embasamento para o desenvolvimento do presente trabalho. Este, por sua vez, tem por objetivo dar suporte a empresas a adotarem políticas de SegInf de acordo com suas preferências e restrições, revelando oportunidades ao decisor em aprimorar seu planejamento em SegInf.

A importância deste trabalho reside basicamente em apoiar os decisores, de uma maneira mais robusta, através do uso de técnicas de programação inteira e abordagem multicritério, na melhoria da eficiência no que diz respeito a SegInf para tomada de decisão de maneira a analisar potenciais alternativas em relação aos critérios, levando-se em consideração questões como restrições financeiras, de tempo e de prioridade na implantação dessas políticas.

Para trabalhos futuros, deixamos como sugestão a análise de um conjunto maior de empresas, bem como de segmentos distintos.

Referências

Albadvi, A., Chaharsooghi, S. K. e Esfahanipour, A. (2007), Decision making in stock trading: an application of PROMETHEE. *Eur. J. Oper. Res*. 177, 673–683.

Almeida, J. A. de. (2012), *Modelo multicritério para seleção de portfólio de projetos de sistema de informação*. Tese (Doutorado) - Universidade Federal de Pernambuco. Programa de Pós-Graduação em Engenharia de Produção.

Almeida, A. T. e Costa, A. P. C. S. (2003), *Aplicações com métodos multicritério à decisão*. Recife: Ed. Universitária UFPE.

Almeida, A. T. e Vetschera, R. (2012), A note on scale transformations in the PROMETHEE V method, *European Journal of Operational Research*, 219, 1, 198–200.

Brans, J.P. e Mareschal, B. (2002), *PROMETHEE – GAIA: une méthodologia d'aide à La décision em présence de critères multiples*. Bruxelles: Éditions de L'Université de Bruxelles.

Dyer, J.S. (1990), Remarks on the Analytic Hierarchy Process, *Management Science*, 36, 3, 249-258.

Imamverdiev, Y.N. e Derakshande, S. A. (2011), Fuzzy OWA Model for Information Security Risk Management, *Automatic Control and Computer Sciences*, 45, 1, 20–28.

Johnston, A. C. e Warkentin, M. (2008), Information Privacy Compliance in the Healthcare Industry: Do Healthcare Professionals Want to Comply with HIPAA? *Information Management & Computer Security*, 16, 1, 5-19

Mavrotas, G., Diakoulaki, D. e Caloghirou, Y. (2006), Project prioritization under policy restrictions. A combination of MCDA with 0–1 programming. *European Journal of Operational Research*, 171, 296–308.

Pathari, V. e Sonar, R. (2012), Identifying linkages between statements in information security policy, procedures and controls, *Information Management & Computer Security*, 20, 4, 264 – 280.

Renaud, K. e Goucher, W. (2012), Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security*, 20, 4, 296-311**.**

Roy, B. (1996), *Multicriteria Methodology Goes Decision Aiding*. Kluwer Academic Publishers.

Silva, L., Poleto, T., Moura, J. e Costa, A. P. C. S. (2012), An Analysis of and Perspective on the Information Security Maturity Model: a case study of a Public and a Private Sector Company. *AMCIS 2012 Proceedings*. Paper 11**.**

Shirtz, D. e Elovici, Y. (2010) Optimizing investment decisions in selecting information security remedies. *Optimizing investment decisions*, 19, 2, 95-112

Syamsuddin, I. e Hwang, J. (2010), The Use of AHP in Security Policy Decision Making: An Open Office Calc Application. *Journal of Software*, 5, 10.

Veiga, A. Da. e Eloff, J.H.P. (2010), A framework and assessment instrument for information security culture, *Computer & Security*, 29, 196–207.

Vetschera, R., e Almeida, A. T. (2012), A PROMETHEE-based approach to portfolio selection problems, *Computers & Operations Research*, 39, 5, 1010–1020**.**

Vincke, P. (1992), *Multicriteria Decision Aid*. New York: John Wiley.

Zakaria, O. (2005), Information Security Culture and Leadership, *Proceedings of the 4th European Conference on Information Warfare and Security*, Cardiff, Wales, pp 415-420, 2005.

Yang, YP., Shieh, HM. e Tzeng, GH.(2013), A VIKOR technique based on DEMATEL and ANP for information security risk control assessment, *Information Sciences*, 232, 482–500.

Wiecek, M. M., Ehrgott, M., Fadel, G. e Figueira, J.r. (2008), Multiple Criteria Decision Making for Engineering , *Omega*, 36, 337-339.