PROCEDIMENTO PARA AVALIAÇÃO E DIAGNÓSTICO DO NÍVEL DE CRITICIDADE EM SEGURANÇA DA INFORMAÇÃO.

Thiago Poleto
Universidade Federal de Pernambuco
Av, Professor Moraes Rego, 1235, Cidade Universitária
thiagopoleto@hotmail.com

Lúcio Câmara e Silva
Universidade Federal de Pernambuco, Campus Agreste
Rodovia BR-104 km 59 - Nova Caruaru
lucio_camara@hotmail.com

Maísa Mendonça Silva
Universidade Federal de Pernambuco, Campus Agreste
Rodovia BR-104 km 59 - Nova Caruaru
maisa@ufpe.br

Ana Paula Henrique Gusmão
Universidade Federal de Pernambuco, Campus Agreste
Rodovia BR-104 km 59 - Nova Caruaru
anagusmao@ufpe.com

Ana Paula Cabral Seixas Costa
Universidade Federal de Pernambuco
Av, Professor Moraes Rego, 1235, Cidade Universitária
apcabral@ufpe.br

RESUMO

Este artigo apresenta um procedimento para diagnóstico a avaliação de empresas com relação ao nível de segurança da informação, através do uso da lógica *Fuzzy* e da abordagem multicritério. Para esse diagnóstico foram analisados 25 modos de falhas associadas a cinco dimensões: gestão de segurança, segurança da comunicação, infraestrutura, acesso e controle e desenvolvimento de sistema. Para ilustrar a aplicabilidade do procedimento, foi realizada uma simulação contendo 5 empresas, obtendo-se um ordenamento final em nível de criticidade. Foi feita uma análise de sensibilidade, porém sem nenhuma mudança de cenário. Ao final da aplicação, pode-se constatar como as empresas estão, perante as demais, com relação aos riscos em segurança da informação, servindo de input para avaliação dos níveis de maturidade em segurança da informação.

PALAVARAS CHAVE. Segurança da Informação, FMEA, Multicritério, *Fuzzy*, Nível de Criticidade.

ABSTRACT

This article presents a procedure for diagnostic and evaluation of companies with the level of information security using fuzzy logic and multi-criteria approach. For this diagnostic were analyzed 25 failure modes associated with five dimensions: security management, communication security, infrastructure, and access control and system development. To illustrate the applicability of the procedure, a simulation was performed containing five companies to give a final level of criticality order. A sensitivity analysis was performed, but without any change of scenario. At the end of the application, it can be seen how companies are compared to each other, with respect to risks in information security, serving as input for the assessment of levels of maturity in information security.

KEYWORDS. Information Security, FMEA, Multicriteria, Fuzzy, Criticality Level.

1. Introdução

De acordo com Petrović *et al.* (2014) a segurança da informação desempenha um papel cada vez mais importante nas empresas, tornando-se um fator fundamental para garantir que as informações se mantenham acessíveis e disponíveis na organização. Porém, um dos maiores desafios que os pesquisadores de segurança e analistas enfrentam atualmente, devido os altos índices de incidentes, são os ataques realizados contra as organizações (Huang *et al.*, 2009). Segundo esses mesmos autores, esses ataques podem afetar e causar danos ao processo de comunicação de informações, como também, vazamento de informações pessoais, e perdas financeiras geradas pelas interrupções do sistema.

Desta forma, as organizações têm se preocupado em minimizar sua vulnerabilidade por meio da adoção de políticas de segurança da informação. Essa adoção de um conjunto políticas, normas e procedimentos visam alcançar um nível de segurança desejado, o qual este deve ser seguido e mantido (Anderson e Choobineh, 2008). A partir desse nível alcançado é possível obter dimensionados os riscos a que a organização está exposta, como também identificar ações prioritárias e emergenciais a serem executadas, visando a proteção das informações.

Diante da necessidade de proteger as informações contra possíveis falhas, diferentes pesquisas têm sido desenvolvidas nas áreas de segurança da informação, tais como: tecnologia de autenticação (Kim *et al.*, 2015), acesso inteligente por biometria (Cao e Ge, 2015), certificado digital (Xing *et al.*, 2014), políticas de criptografia no processo de terceirização de TI (Celdrán *et al.*, 2015), autodetecção contra invasores ou arquivos não reconhecidos (Kawanaka *et al*. 2014).

Além disso, a segurança da informação também é pesquisada com extrema importância no contexto de *Big Data*, uma vez que estes dois conceitos estão associados. De um lado a segurança com a questão da detecção de fraude, de outro lado *Big Data* com identificação, visualização e analises de dados. Embora seja uma área de pesquisa pouco explorada, Hsu *et al.* (2014) apresentam um proposta para atuar e minimizar os ataques sobre grande quantidade de dados. Ainda neste contexto, Hipgrave (2013) propõe o uso do *Big Data* para monitoramento de tráfego de rede, analisados em tempo real, com a proposta de identificar o risco e fraude e descobrir tendências e padrões em grandes quantidades de dados, estruturados e não estruturados, e, assim, não apenas resolver a questão dos ataques e espionagem, mas também prevenir a criminalidade no ambiente virtual.

Portanto, segurança da informação possui extrema relevância para as organizações, visto que os impactos causados pelos ataques podem ocasionar danos diretos e indiretos as organizações. Nesse sentido, é importante realizar uma avaliação e monitoramento dos níveis de criticidades das empresas, de forma abrangente, para prover conhecimento que pode ser aplicado para auxiliar os gestores na identificação de possíveis falhas e, portanto, tomar providências a fim de prevenir e mitigar as ameaças ao negócio.

Neste contexto, a proposta deste trabalho é o desenvolvimento de um procedimento para diagnóstico e avaliação do nível de criticidade nas empresas, em relação à segurança da informação, que proporcione as mesmas identificarem os pontos de riscos que impactam diretamente ao seu negócio. Para essa avaliação foram incorporadas diferentes dimensões, baseadas em Silva *et al* (2014), que associam a integridade, confiabilidade e disponibilidade das informações. Para cada uma dessas dimensões foram analisados possíveis modos de falha através do uso do FMEA (*Failure Mode and Effects Analysis*) conforme descrito em detalhes na seção 2.2, no qual cada modo foi avaliado em termos do nível de severidade, ocorrência e detecção. Cada avaliação foi realizada por meio de lógica *Fuzzy*, através de uma escala verbal. Por fim, as empresas foram ordenadas com relação ao nível de criticidade, utilizando-se a abordagem multicritério.

O restante deste artigo se divide da seguinte forma: a Seção 2 apresenta um referencial teórico sobre segurança da informação, FMEA, lógica *Fuzzy* e decisão multicritério; a Seção 3 apresenta o procedimento para avaliação e diagnóstico proposto; a Seção 4 apresenta a aplicação da proposta; a Seção 5 apresenta a conclusão deste trabalho com a proposta para trabalhos futuros.

2. Base Metodológica

2.1 Segurança da Informação

A segurança da informação é um tema que tem sido pesquisado em diferentes aspectos, por exemplo, ataques e ameaças interna (Alam *et al.*, 2015), ataques externos (Ahmad *et al.*, 2014; Asri e Pranggono, 2015), crimes cibernéticos (Ak *at al.* 2015), cultura organizacional (Da Veiga e Martins, 2015), incidentes causados a partir de vulnerabilidade (Tondel *at al*, 2014).

Porém, a principal finalidade em adotar a segurança da informação é garantir a continuidade dos negócios e minimizar os ataques que possam impactar em destruição, alteração ou roubo das informações, os quais são discutidos nas categorias de autenticação, confidencialidade, integridade e disponibilidade da informação (Iizuka *et al.* 2007). De uma maneira geral, um evento contra a segurança da informação pode ser definido como uma série única ou de eventos indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações de negócio (Anderson e Choobineh, 2008).

Neste contexto, tem sido destacado nos últimos anos, na literatura, vários aspectos relacionados a segurança da informação, conforme Tabela 1.

Tabela 1 – Identificações de questões referente a segurança da informação

Questões de Segurança da informação	**Descrição**	**Referencias**
Proteção dos dados organizacionais	Refere-se adoção de ferramentas que visam manter os dados contra acesso não autorizado, a fim de minimizar o vazamento das informações	(Iizuka *et al.*, 2007; Shin e Shin, 2011)
Controle de acesso	Refere-se a gestão de identificação pessoal físico e lógico	(Kim *et al.*, 2015)
Ameaças para Segurança	Refere-se a ataques de códigos maliciosos, como por exemplo; *Malware*, *Trojan*, *spyware*, *worms*.	(Ahmad, *at al.* 2014; Vida *et al*, 2015)
Segurança de Infraestrutura de Rede	Refere-se a adoção de monitoramento de rede interna contra acesso e recebimento de objetos indevido	(Chen e Hsieh, 2012)

Desta forma, na busca pela mitigação de ataques e implementação da gestão de segurança da informação é importante destacar o enfoque no planejamento de segurança, formalização das políticas, gestão de risco, seleção de tecnologias de segurança, avaliação de ameaças e vulnerabilidades e monitoramento de desempenho (Nazareth e Choi, 2015). Entretanto, a implementação bem-sucedida de políticas e práticas de segurança da informação requer apoio e envolvimento dos gestores, que por sua vez têm responsabilidade de formular e adequar as políticas da segurança da informação às estratégias da organização (Anderson e Choobineh, 2008).

2.2 *Failure Mode and Effects Analysis*- FMEA

FMEA é um método sistemático para analisar os modos de falhas de um sistema, auxiliando no processo de desenvolvimento de produto ou serviço a encontrar potenciais problemas, evitando, assim, desperdícios em estágios posteriores no processo (Teng e Ho, 1996). Dessa forma, este método identifica os efeitos de falhas que podem impedir o funcionamento ideal e explora o impacto da falha no sistema permitindo que, em seguida, execute as medidas necessárias para implementar políticas preventivas.

A FMEA é um método que tem sido aplicado em diferentes áreas: Liao and Ho (2014) utilizam o FMEA para analisar os potenciais riscos dos resíduos biomédicos descartados. No setor de serviço, Geum *at al.* (2011) propõem uma sistemática para a identificação e avaliação de potenciais modos falhas adotando características especificas do serviço ao FMEA. Petrović *et al.* (2014) apresentam um modelo de avaliação de risco de falha do equipamento de mineração. Silva *et al.* (2014) utilizaram o FMEA para identificar os modos de falhas em segurança da informação.

Primeiramente, para aplicação do FMEA são identificados os possíveis modo de falha e

efeito, estimando o nível de (S) severidade. Em seguida, a causa potencial de falhas é determinado o nível de (O) ocorrência e, em seguida, a possibilidade de (D) detecção dessa falha. Com base nesses três indicadores, o valor de risco obtido (*Risk Priority Number* – RPN) é calculado multiplicando-se a severidade pela ocorrência e detecção do risco.

Nesse contexto, o objetivo deste trabalho é o de ampliar a aplicação do FMEA no âmbito da segurança da informação, baseado em Silva *et al* (2014), a fim de diagnosticar os possíveis modos de falhas na organização. Neste caso, cada falha é considerada individualmente como um evento independente, relacionada com outras falhas do sistema de avaliação, baseado nos três critérios: ocorrência, severidade e detecção (Braglia *at al*. 2003).

2.3 Lógica Fuzzy

A teoria dos conjuntos *fuzzy* foi proposta (Zadeh, 1965) e tem sido considerada como base para abordagens linguísticas (ou numéricas) e de caráter impreciso (Zadeh, 1965). Sua aplicação tem se expandido, por exemplo, para modelos decisão para contratação de pessoal (Petrovic-Lazarevic, 2001) e seleção de fornecedor de serviço de TI (Chen *at al*. 2011).

A utilização da teoria dos conjuntos *fuzzy* permite auxiliar na solução de problemas multicritério onde há ambiguidade na medição de performances e na determinação de pesos de critérios (Hatami-Marbini eTavana, 2011).

O conjunto fuzzy é caracterizado por uma função de pertinência, que associa a cada ponto de X a um número real, no intervalo de [0,1]. A forma da função pertinência reflete o problema em questão e, no caso do presente artigo, o número *fuzzy* trapezoidal A, pode ser descrito de acordo com a seguinte função conforme a Equação 1:

$$\mu_A(x) = \{0 \text{ se } x < a_1, \frac{x-a_1}{b_1-a_1} \text{ se } a_1 \leq x \leq b_1, 1 \text{ se } b_1 \leq x \leq b_2, \frac{x-b_2}{b_2-a_2} \text{ se } b_2 \leq x \leq a_2, 0 \text{ se } x > a_2. \quad (1)$$

onde A pode também ser representado pela figura 1.

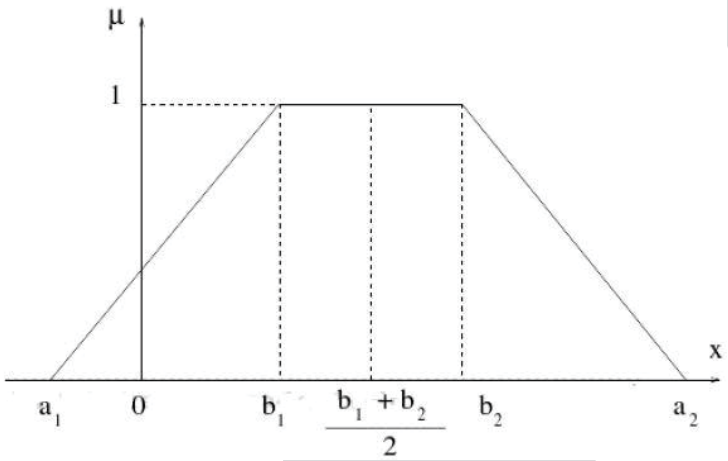

Figura 1: Numero Trapezoidal *fuzzy* adaptado de (Bojadziev e Bojadziev, 2007),

$$A = (a_1, b_1, b_2, a_2). \quad (2)$$

Se $b_1 = b_2 = b_A$, A é um número *fuzzy* trapezoidal: $A = (a_1, b_A, b_A, a_2) = (a_1, b_A, a_2)$.

Operações básicas da teoria dos conjuntos *fuzzy* podem ser revistos como a extensões dos números correspondentes *crisp*, que suportam a determinação do número *fuzzy*. Para mais detalhes (Bojadziev e Bojadziev, 2007; Zadeh, 1965).

O conjunto $\tilde{A}_1 = (a_1, b_1, c_2, d_2)$ e $\tilde{A}_2 = (a_3, b_3, c_4, d_4)$ é representado por números *fuzzy* trapezoidais conforme a Equação 3:

(i) $\tilde{A}_1 + \tilde{A}_2 = (a_1, b_1, c_2, d_2) + (a_3, b_3, c_4, d_4) = (a_1 + a_3, b_1 + b_3, c_2 + c_4, d_2 + d_4)$

(ii) $\tilde{A}_1 - \tilde{A}_2 = (a_1, b_1, c_2, d_2) - (a_3, b_3, c_4, d_4) = (a_1 - a_3, b_1 - b_3, c_2 - c_4, d_2 - d_4)$

(iii) $-\tilde{A}_1 = -(a_1, b_1, c_2, d_2) = (-c_2, -d_2, -a_1, -b_1)$

(iv) $\tilde{A}_1 \otimes \tilde{A}_2 = (a_1, b_1, c_2, d_2) \otimes (a_3, b_3, c_4, d_4) \cong (a_1 a_3, b_1 b_3, c_2 c_4, d_2 d_4)$

(3)

2.4 Apoio a Decisão Multicritério

O apoio multicritério a decisão pode ser visto como um conjunto de métodos que auxiliam o entendimento de um problema, no qual as alternativas são avaliadas por múltiplos critérios, muitas vezes, conflitantes entre si (Vincke, 1992).

Há vários métodos de decisão multicritério. Dentre eles, a família de métodos PROMETHEE (*Preference Ranking Method for Enrichment Evaluation*) foi desenvolvida inicialmente por Brans (1982), sendo expandida posteriormente por Brans e Vincke (1985). Conforme Brans e Mareschal (2002), os métodos dessa família possuem duas fases: construção de uma relação de sobreclassificação com a agregação entre alternativas e entre critérios, e exploração das relações.

De uma maneira geral, a estrutura de avaliação dos métodos PROMETHEE baseia-se na definição de pesos para cada critério, a partir do qual pode ser o grau de sobreclassificação de uma alternativa em relação a outra, para cada par de alternativas (Brans e Vincke, 1985). Este grau de sobreclassificação, representado por $\pi(a,b)$, pode ser obtido através da Equação 4.

$$\pi(a, b) = \sum_{i=1}^{n} p_i F_i(a, b) \quad (4)$$

Onde:

$\sum_{i=1}^{n} p_i = 1$;

p_i representa o peso de cada critério;

$F_i(a,b)$, que assume valores entre 0 e 1, representa a função da diferença $[g_i(a) - g_i(b)]$ entre o desempenho das alternativas para cada critério *i*.

Dentre os métodos dessa família, o PROMETHEE II estabelece uma pré-ordem completa entre as alternativas (Brans, Vincke e Mareschal, 1986), baseando-se na utilização do fluxo liquido (Equação 5), que representa a diferença entre o fluxo positivo (Equação 6) e o fluxo negativo (Equação 7).

$$\phi(a) = \phi^{+}(a) + \phi^{-}(a) \quad (5)$$

$$\phi^{+}(a) = \sum_{x \in A} \pi(a, x) \quad (6)$$

$$\phi^{-}(a) = \sum_{x \in A} \pi(x, a) \quad (7)$$

Portanto, utilizando-se o indicador $\Phi(a)$ pode-se organizar as alternativas em ordem decrescente, definindo a ordem completa entre as alternativas com base nas relações de Preferência (aPb) se $\Phi(a) > \Phi(b)$ e Indiferença (aIb) se $\Phi(a) < \Phi(b)$. Mais detalhes sobre algoritmo do PROMETHEE II podem ser vistos em Brans e Vincke (1985), Brans e Mareschal (2002).

3. Procedimento para diagnóstico do nível de criticidade das empresas

O procedimento proposto visa apoiar as empresas na avaliação de risco em segurança da informação. Embora tenha sido realizado um estudo hipotético, a proposta pode ser adaptada às empresas no contexto real. O procedimento é dividido em 3 etapas conforme descrito na Figura 2.

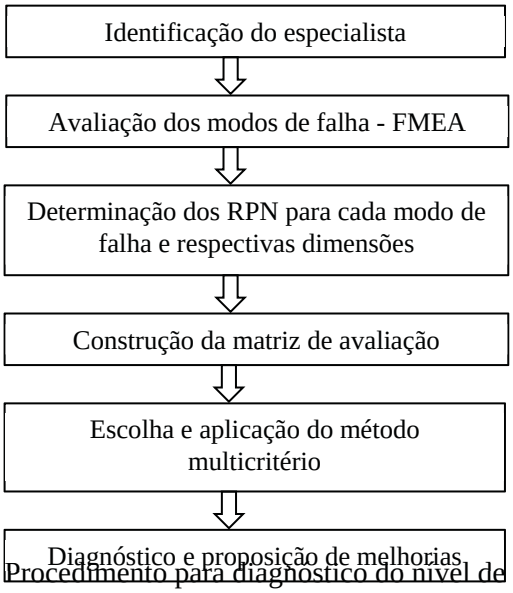

Figura 2 – Procedimento para diagnóstico do nível de criticidade

A primeira etapa da abordagem consiste na identificação especialista. O auditor em segurança é a pessoa que conhece os sistemas corporativos e suas vulnerabilidades, sendo capaz, portanto, de avaliar os riscos da organização. Para essa avaliação são consideradas cinco dimensões em segurança da informação: gestão de segurança, processo de comunicação seguro, infraestrutura, acesso e controle e desenvolvimento de sistema de informação.

Em seguida são identificados, baseado na proposta de Silva *et al.* (2014), os possíveis modos de falha, utilizando-se o FMEA. Cada modo de falha é associado a cada uma das cinco dimensões. Após essa identificação, determina-se o RPN de cada modo, utilizando-se a lógica *Fuzzy*, que permite uma visão mais próxima da realidade do problema.

Em seguida, determina-se o RPN de cada dimensão, que será o input na aplicação do método multicritério. Nessa etapa, cada dimensão será considerada como um critério para avaliação. Nesse caso empresas foram avaliadas quanto à gestão de segurança da informação, processo de comunicação seguro, infraestrutura, acesso e controle de segurança da informação e desenvolvimento de sistema de informação. Estas avaliações apresentadas na forma matricial dão origem ao que comumente se chama de matriz de desempenho dos critérios. Para essa avaliação, observou-se a necessidade de utilização de um método de agregação com caráter não-compensatório, pois não é relevante para organização com desempenho muito alto no aspecto de acesso e controle, mas com baixa performance no critério de comunicação segura. Portanto, os métodos de sobreclassificação são adequados para este problema de segurança da informação.

4. Aplicação do procedimento proposto para avaliação de segurança da informação

Objetivando validar a proposta, uma ilustração numérica foi desenvolvida através da simulação de características de cinco empresas fictícias em relação à segurança da informação.

Com a ajuda de um especialista, foram identificados e avaliados, com relação à ocorrência(O), severidade (S) e detecção (D), cada um dos modos de falha, conforme ilustra a Tabela 2. Essa avaliação foi utilizada as variáveis linguísticas (Muito Alto- VH, Alto-H, médio-M, Baixo-L, Muito Baixo-VL) para os números *fuzzy* trapezoidais, de forma que possa capturar e converter a informação imprecisa do decisor.

Tabela 2 – Analise dos modos de falhas

Dimensões	Modos de Falhas potencial	(O)	(S)	(D)
A1- Gerenciamento de Segurança da informação	A1.1:Falta de auditoria de segurança da informação	VH	M	M
	A1.2:Falta de documentação para a segurança de informação	M	H	H
	A1.3:Falta de pessoal responsável pela segurança da informação	H	L:	H
	A1.4:Falta de manutenção de hardware e software	L	H	L
	A1.5:Falta de revisão das políticas de segurança da informação	M	H	M
A2 – Processo de comunicação Seguro	A2.1:Falta de segurança das mensagens de correio electrónico	H	H	H
	A2.2:Falta de ambiente interno de comunicação	H	M	VH
	A2.3:Falta de gerenciamento de controle de criptografia	VH	H	H
	A2.4:Falta de controle de acesso aos conteúdos da internet	M	H	H
	A2.5:Falta de treinamento em segurança da informação	H	M	M
A3- Infraestrutura	A3.1:Falta de back-up das informações	H	M	L
	A3.2:Falta de certificação interna da rede	M	M	L
	A3.3:Falta de software original	L	H	L
	A3.4:Falta de software defesa a segurança	VH	H	H
	A3.5:Falta de servidor Cluster	L:	M	M
	A3.6:Falta de gerador elétrico	VL	H	M
A4–Acesso e controle de segurança da informação	A4.1:Falta de gerenciamento de mídias removíveis	VH	M	M
	A4.2:Falta de controle de senha do usuário	M	H	H
	A4.3:Falta de registro por usuário	H	L:	H
	A4.4:Falta de reconhecimento automático de terminal	L:	H	L
	A4.5:Falta de autenticação ID de usuário	M	H	M
	A4.6:Falta de gestão de acesso externo	VH	M	M
A5- Desenvolvimento de Sistema de Informação Seguro	A5.1:Falta de padronização e documentação do processo de desenvolvimento de software	L:	H	L
	A5.2:Falta de teste contra vulnerabilidade do código fonte	M	M	H
	A5.3:Falta de monitoramento de alterações no código	VH	M)	H

Em seguida, identificou-se o RPN para cada modo de falha e, consequentemente, para cada dimensão. Para essa etapa, foi utilizado o procedimento de Adamo's (1980). Dessa forma, cada dimensão foi considerada como um critério para a matriz de avaliação, conforme a Tabela 3.

Tabela 3 – Matriz de avaliação

	D1:Gestão de segurança da informação	*D2:Segurança da comunicação*	*D3:Infraestrutura*	*D4: Acesso e controle de segurança da informação*	*D5:Desenvolvimento de sistema de Informação seguro*
Empresa 1	700,03	506,24	971,48	754,89	1422,40
Empresa 2	280,03	450,49	383,78	266,49	329,41
Empresa 3	547,33	484,34	752,78	515,44	434,81
Empresa 4	985,38	742,49	551,93	494,64	406,56
Empresa 5	984,75	1283,50	1152,50	843,00	849,75

Como exposto anteriormente, nosso problema consiste em atribuir prioridades, consideradas como nível de criticidade, às empresas e ordená-las. Dessa forma, optamos pela aplicação do PROMETHEE II, mais adequado a nossa problemática. Aplicando o este método, calculamos o valor de Φ(a) (Eq. 5), como descrito anteriormente, e obtemos a ordenação das

empresas, conforme a Tabela 4. Vale salientar que, para aplicação do modelo, foi considerada função de critério usual, onde não há parâmetro a ser definido.

Tabela 4 – Ranking das empresas

Ranking	*Empresa*	*Fluxo Líquido*
1	Empresa 5	0,80
2	Empresa 1	0,40
3	Empresa 4	0,00
4	Empresa 3	-0,20
5	Empresa 2	-1,0

Com base na Tabela 4, percebe-se que a empresa 5 foi considerada a mais crítica com relação a segurança da informação. Com base nessa informação, o gestor tem uma noção de como sua empresa está perante as outras, com relação a segurança da informação. Essa informação possibilita, num estágio posterior, enquadrar a empresa num determinado nível de maturidade em segurança da informação, que trata-se de uma proposta para trabalhos futuros.

Para validação da aplicação, foi realizada uma análise de sensibilidade, variando o peso de alguns critérios em ± 5%, porém não foi encontrada nenhuma mudança de ordem.

4.1 Ações propostas para a segurança da informação

Como complemento do procedimento, a análise permite apresentar algumas ações requeridas para melhorar a questão da segurança da informação nas empresas, conforme Tabela 5.

Tabela 5: Recomendações de políticas de segurança da informação

Dimensões	***Ações requeridas para segurança da informação***
Gestão de segurança da informação	Adequação as políticas de acordo com estratégia da organização
	Auditória de segurança da informação e conteúdo de registros de auditoria
	Adoção de implementação do monitoramento incidente
	Automatizar o Backup e recuperação das informações
Comunicação segura	Adoção de portais coorporativos e software de comunicação interna
	Gerenciamento de mídias removíveis
	Segurança de comunicação com terceiros
	Adoção de políticas de Segurança de e-mail eletrônico
Infraestrutura	Adoção de Controle de Rede
	Sistema de detecção de intrusões de host (contra código maliciosos, vírus)
	Monitoramento de Sistemas de informação
	Proteção física e ambiental
Acesso e controle de segurança da informação	Adoção de gerenciamento de acesso do colaborador
	Adoção de políticas de identificação do usuário e autenticação
	Gestão de usuário e senha
	O controle de acesso para dispositivos portáteis e móveis

	Adoção de política de segurança de acesso a terceiros (Fornecedor)
	A autenticação do usuário para conexões externas
Desenvolvimento de sistema de informação seguro	Controle de acesso de rede sem fio Sistemas de notificação de incidente funcionamento do software
	Gestão de Teste de software
	Teste de vulnerabilidade no código fonte do Software
	Documentação e padronização do processo de desenvolvimento de Software
	Adoção de sistema de acompanhamento de correção das falhas encontradas na operação

É importante destacar que à medida que a empresa adota novas tecnologias da informação ou modifica determinado processo interno é necessário à manutenção das políticas a fim de garantir informação íntegra, disponível e acessível.

5. Conclusão

Com o constante aumento da utilização de meios digitais que dão suporte aos negócios, faz-se necessária a utilização de políticas que visam a segurança da informação, garantindo o sigilo e a inteireza da operação, uma vez que proteger os ativos de informação é uma atividade crítica para as organizações. Neste cenário, as organizações devem refletir sobre potenciais riscos de ataque, como também melhorar os pontos fracos.

A importância deste trabalho reside em apresentar um procedimento para mensurar o nível de criticidade em segurança da informação das empresas quanto ao risco, de uma maneira robusta e sistemática, através do uso do FMEA, Lógica *Fuzzy* e abordagem multicritério. Como resultado da proposta, apresenta-se uma ordenação das empresas em grau de criticidade em segurança da informação, ou seja, que apresenta maior vulnerabilidade e possibilidade de ameaça.

Para isso, foi realizada uma avaliação levando-se em consideração gestão de segurança da informação, segurança da comunicação, infraestrutura, acesso e controle de segurança da informação e desenvolvimento de sistema de informação seguro. O procedimento proposto é capaz de avaliar os possíveis modos de falha da organização, alertando o gestor para possíveis medidas de prevenção contra vulnerabilidade e ameaças. Além disso, foram recomendados políticas de segurança para mitigação de ameaças, a nível estratégico, a fim de minimizar o risco contra o negócio.

Dentre as propostas para trabalhos futuros, considera-se a inserção ao modelo dos aspectos relacionados aos usuários, como também o desenvolvimento de um modelo de maturidade em segurança da informação.

Agradecimentos

Agradecemos ao GPSID (Grupo de Pesquisa Sistema de Informação e Decisão) pelo suporte prestado ao desenvolvimento da pesquisa.

Referências

Adamo, J. M. (1980), Fuzzy decision trees, *Fuzzy Sets and Systems*, 4(3): 207–219.

Ahmad, A. Maynard, S.B. e Park, S. (2014), Information security strategies: Towards an organizational multi-strategy perspective, *Journal of Intelligent Manufacturing*, 25(2): 357–370.

Ak, Ş. Özdemir, Y. e e Kuzucu, Y. (2015), Cybervictimization and cyberbullying: The mediating role of anger, don't anger me! *Computers in Human Behavior*,49: 437–443.

Alam, S. Horspool, R.N. Traore, I. e Ibrahim, S. (2015), A framework for metamorphic malware analysis and real-time detection, *Computers & Security*, 48: 212–233.

Anderson, E.E. e Choobineh, J. (2008), Enterprise information security strategies, *Computers & Security*, 27: 22–29.

Asri, S. e Pranggono, B. (2015), Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure, *Wireless Personal Communications*.

Braglia, M. Frosolini, M. e Montanari, R. (2003), Fuzzy criticality assessment model for failure modes and effects analysis, *International Journal of Quality & Reliability Management*, 20(4): 503–524.

Brans, J. P. L. (1982),'ingenierie de la decision. Elaboration d'instruments d'aide a la decision. Methode PROMETHEE. In: NADEAU, R.; LANDRY, M. (Eds.). L'aide a la Decision: Nature, Instruments et Perspectives D'avenir. Quebec: Presses de Universite Laval, 183–214.

Brans, J.P. e Mareschal, B. (2002), Promethee-Gaia, une Methodologie d´Aide à la Décision em Présence de Critères Multiples. Éditions Ellipses, Bruxelles

Brans, J. P. Vincke, P. Mareschal, B. (1986), How to select and how to rank projects: The PROMETHEE method, *European Journal of Operational Research*, 24, 228-238.

Brans, J. P.; Vincke, P. A. (1985), Preference Ranking Organisation Method: The PROMETHEE Method for Multiple Criteria Decision-Making, *Management Science*, 31, 647–656.

Cao, L. e Ge, W. (2015), Analysis and improvement of a multi-factor biometric authentication scheme, *Security and communication networks*, 8(4): 617–625.

Chen, Y-H. Wang, T-C. e Wu, C-Y. (2011), Strategic decisions using the fuzzy PROMETHEE for IS outsourcing, *Expert Systems with Applications*, 38(10): 13216–13222.

Bojadziev, G. e Bojadziev, M. (2007), *Fuzzy Logic for Business, Finance, and Management*, 2nd ed, *Management*, World Scientific Publishing Company.

Geum, Y. Cho, Y.e Park, Y. (2011), A systematic approach for diagnosing service failure: Service-specific FMEA and grey relational analysis approach, *Mathematical and Computer Modelling*, 54(11-12): 3126–3142.

Hatami-Marbini, A. e Tavana, M. (2011), An extension of the Electre I method for group decision-making under a fuzzy environment, *Omega*, 39(4): 373–386.

Hipgrave, S. (2013), Smarter fraud investigations with big data analytics, *Network Security*, 2013(12): 7–9.

Hsu, C. Zeng, B. e Zhang, M. (2014), A novel group key transfer for big data security, *Applied mathematics and computation*, 249(2013): 436–443.

Huang, Y-L. Cárdenasa, A. A. Aminb, S. Linc, Z-S. Tsaic, H.-Y. e Sastrya, S. (2009), Understanding the physical and economic consequences of attacks on control systems, *International Journal of Critical Infrastructure Protection*, 2(3): 73–83.

Celdrán , H. A. Tormo, D.G. Mármol, G. F. Pérez, G. M, e Pérez G. M. (2015), Resolving privacy-preserving relationships over outsourced encrypted data storages, *International Journal of Information Security*.

Iizuka, S. Ogawa, K. e Nakajima, S. (2007), Factors Affecting User Reassurance When Handling Information in a Public Work Environment, *International Journal of Human-Computer Interaction*, 23(1-2): 163–183.

ISO/IEC-27035. (2011), Information technology e Security techniques e Information security incident management.

Kawanaka, T. Matsumaru, M. e Rokugawa, S. (2014), Software measure in cyber-attacks on production control system, *Computers & Industrial Engineering*,76: 378–386.

Kim, YS. Tague, P. Lee, H. e Kim, H. (2015), A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control, *Wireless Networks*.

Liao, CJ. e Ho, CC. (2014), Risk management for outsourcing biomedical waste disposal - Using the failure mode and effects analysis, *Waste Management*, 34(7): 1324–1329.

Nazareth, DL. e Choi, J. (2015), A system dynamics model for information security management, *Information & Management*, 52(1): 123–134.

Petrović, D. V. Tanasijevićb, M. Milić, V. Lilić, N. Stojadinović, S. e Svrkotaa, I. (2014), Risk assessment model of mining equipment failure based on fuzzy logic, *Expert Systems with Applications*, 41(18): 8157–8164.

Petrovic-Lazarevic S. (2001), Personnel Selection Fuzzy Model, *International Transactions in Operational Research*, 8(1): 89–105.
Puente, J. Pino, R. Priore, P. Fuente, e DD La. (2002), A decision support system for applying failure mode and effects analysis, *International Journal of Quality & Reliability Management*, 19(2): 137–150.
Chen, R.-M. e Hsieh, K-T. (2012), Effective allied network security system based on designed scheme with conditional legitimate probability against distributed network attacks and intrusions, *International Journal of Communication Systems*, 25(5): 672–688.
Shin, D-H. e Shin, Y-J. (2011), Consumers' Trust in Virtual Mall Shopping: The Role of Social Presence and Perceived Security, *International Journal of Human-Computer Interaction*, 27(5): 450–475.
Shirtz, D. e Elovici, Y. (2011), Optimizing investment decisions in selecting information security remedies, *Information Management & Computer Security*, 19(2): 95–112.
Silva, M.M. Gusmão, A.P.H. Poleto, T. Silva, L.C.E. e Costa, A.P.C.S. (2014), A multidimensional approach to information security risk management using FMEA and fuzzy theory, *International Journal of Information Management*, 34(6): 733–740.
Teng, S-H. e Ho, S-Y. (1996), Failure mode and effects analysis An integrated approach for product design and process control, *International journal of quality & reliability management*, 13(5): 8–29.
Tondel, IA. Line, MB. e Jaatun, MG. (2014), Information security incident management: Current practice as reported in the literature, *Computers & Security*, 45: 42–57.
Da Veiga, A. Martins, N. (2015), Information security culture and information protection culture: A validated assessment instrument, *Computer Law & Security Review*, 31(2): 243–256.
Vida, R. Galeano, J. e Cuenda, S. (2015), Vulnerability of multi-layer networks under malware spreading, *Physica A*, 421(1): 134–140.
Xing, L. Jiang, L. Yang, G. e Wen, B. (2014), A novel trusted computing model for network security authentication, *Journal of Networks*, 9(2): 339–343.
Vincke, P. (1992), Multicriteria decision aid. Bruxelles: Jonh Wiley & Sons.
Zadeh, La. (1965), Fuzzy sets. *Information and Control*, 8(3): 338–353.