Uso da abordagem multicritério para seleção de ferramenta de Gerenciamento Unificado de Ameaças

Juliano Stiegemeier

julianostiegem@gmail.com

Abstract. *Faced with the challenges posed by the increase in cyber threats on the Internet, organizations have been successful in their information security strategy by means of Unified Threat Management tools. However, they face difficulties in identifying the most appropriate alternative. Given this, this work proposes the development of a model to support decision making, based on the VIKOR multicriteria analysis method, to help them improve their selection process. The application of the suggested model determined the ranking of the evaluated alternatives, choosing a compromise solution capable of solving this decision problem.*

Resumo. *Frente aos desafios impostos pelo aumento das ameaças cibernéticas presentes na Internet, as organizações têm obtido êxito na sua estratégia de segurança da informação por meio do emprego de ferramentas de Gerenciamento Unificado de Ameaças. Entretanto, enfrentam dificuldades no momento de identificar a alternativa mais adequada. Diante disso, este trabalho propõe o desenvolvimento de um modelo de apoio a tomada de decisão, baseado no método de análise multicritério VIKOR, a fim de auxiliá-las a aprimorar o seu processo de seleção. A aplicação do modelo sugerido determinou a ordenação das alternativas avaliadas, elegendo uma solução de compromisso capaz de resolver este problema de decisão.*

1. Introdução

A informação é considerada um ativo crítico dentro das organizações, capaz de agregar valor a processos, produtos e serviços, na medida em que permite o cumprimento da missão e o atingimento dos objetivos organizacionais [Beal 2008]. Neste contexto, surge a segurança da informação, que, de acordo com a norma NBR ISO/IEC 27002 de 2005 da Associação Brasileira de Normas Técnicas (ABNT), "consiste na proteção da informação de vários tipos de ameaças para garantir continuidade ao negócio, minimizar riscos e maximizar o retorno sobre investimentos e oportunidades".

Segundo Galvão (2015), a chegada da Internet acelerou as comunicações e permitiu a fácil troca de informações. Entretanto, trouxe inconvenientes como o acesso indevido a essas informações. Na década de 1990 e início dos anos 2000, as tecnologias de segurança tradicionais para controle de ameaças cibernéticas, como *firewall* e IPS (*Intrusion Prevention System*), eram implementadas de forma isolada na rede. Esta abordagem de segurança acabava por aumentar a complexidade e o custo envolvido, visto que cada nova tecnologia exigia a implantação de um novo dispositivo, a configuração de novas políticas e uma nova interface de gerenciamento para monitorar. Outra deficiência apresentada neste cenário era a falta de integração entre os produtos, permitindo assim a existência de pontos cegos e potenciais ameaças de segurança da rede [Tittel 2014].

Em resposta aos novos desafios trazidos por novas ameaças e aos problemas apresentados anteriormente, um novo conceito de ferramenta de segurança foi introduzido no mercado em 2004 pelo IDC[1], o Gerenciamento Unificado de Ameaças (UTM - *Unified Threat Management*). Esta ferramenta apresenta-se na forma de *appliance*, combinando *hardware*, software e variadas tecnologias de segurança de rede capazes de operar de forma unificada. Inicialmente, para que um dispositivo de segurança fosse incluído nesta categoria, deveria oferecer as funcionalidades de *firewall*, IPS e antivírus de *gateway*. Porém, segundo o *Gartner*[2], empresa líder mundial em pesquisa de tecnologia da informação, com o passar dos anos novas funcionalidades como VPN (*Virtual Private Network)*, *Web Filtering*, *Application Control*, WAF (*Web Application Firewall)*, *AntiSpam* passaram a fazer parte desta solução.

Segundo Scarfone (2016) o UTM é uma ferramenta que permite uma abordagem de proteção em camadas, consolidando diversas tecnologias de segurança em um só produto, consequentemente é capaz de oferecer uma estratégia de defesa mais efetiva. Entretanto, na medida em que aumentaram as funcionalidades trazidas por esta ferramenta, a complexidade no momento de selecionar a opção mais adequada para cada organização, frente à multiplicidade de critérios envolvidos, também cresceu. Adicionalmente, os crescentes números de novos desenvolvedores de solução aumentam consideravelmente o número de alternativas disponíveis para avaliação no momento da aquisição.

Nos casos onde as organizações não possuem um processo de seleção adequado no momento de adquirir uma ferramenta de UTM e, suas decisões são pautadas de maneira empírica sem levar em consideração todos os critérios envolvidos no problema, a escolha de um produto que não atenda completamente as necessidades pode colocar em risco a segurança das suas informações.

Diante de um problema de decisão tão complexo, composto por múltiplos critérios de difícil mensuração, inúmeras alternativas no que diz respeito a fornecedores e produtos presentes no mercado, e a falta de um processo de decisão estruturado por parte das organizações. Este trabalho propõe o desenvolvimento de um modelo de apoio a tomada de decisão, baseado em um método de análise multicritério, que possibilite auxiliar as organizações a aprimorar seu processo de seleção ao adquirir uma ferramenta de segurança baseada em UTM.

A análise de decisão multicritério é tema de estudo da área do conhecimento denominada como Pesquisa Operacional (PO). Seu objetivo é estudar, desenvolver e aplicar métodos analíticos avançados para auxiliar a tomada de melhores decisões nas mais diversas áreas de atuação humana [Hillier e Lieberman 2014].

Sob o ponto de vista da literatura, existe uma falta de estudos que fundamentem a utilização de um modelo de análise de decisão multicritério para apoiar o processo de seleção de uma ferramenta de UTM nas organizações. Por outro lado, estes métodos têm sido amplamente utilizados na área de TI, principalmente na seleção de sistemas ERP, como pode ser observado nos estudos de [Efe 2015], [Kilic, Zaim e Delen 2014], [Jafarnejad et al. 2012]. Assim sendo, esta pesquisa contribui para o estado atual do conhecimento, ao desenvolver um modelo de decisão multicritério baseado no método

[1] http://www.idc.com
[2] http://www.gartner.com

VIKOR, um método de decisão multicritério, em um contexto ainda não tratado desta forma.

Este artigo está organizado da seguinte maneira: os conceitos básicos relacionados às ferramentas de segurança baseadas em UTM e aos métodos de análise multicritério são definidos na Seção 2. A Seção 3 descreve a metodologia empregada com a apresentação do modelo de decisão proposto. A Seção 4 exibe os experimentos e resultados obtidos com o uso do método de análise multicritério. Por fim, as conclusões são apresentadas na Seção 5.

2. Fundamentação Teórica

Esta seção tem por finalidade apresentar os principais conceitos teóricos relacionados aos objetivos definidos neste trabalho. Serão caracterizados os princípios e teorias mais relevantes que envolvem a Segurança da Informação, bem como a definição de uma solução de UTM. Posteriormente, serão descritos os conceitos que envolvem o processo de tomada de decisão e as definições dos métodos de análise de decisão multicritério.

2.1. Segurança da Informação

São diversas as definições para segurança da informação na literatura. Dentre elas, segundo Fontes (2001) "segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada". Já para Moraes (2010) "a segurança da informação pode ser definida como um processo de proteger a informação do mau uso tanto acidental como intencional, por pessoas internas ou externas à organização, incluindo empregados, consultores e hackers".

Analisando os conceitos apresentados por Fontes (2001) e Moraes (2010), é possível concluir que a segurança da informação é de suma importância para as organizações, visto que minimiza os riscos inerentes ao negócio quanto ao uso dos recursos de informação para o funcionamento da organização. A informação incorreta ou até mesmo a falta dela podem comprometer significativamente o funcionamento de um negócio.

Para [Beal 2008], a segurança da informação visa a proteger a informação garantindo três aspectos fundamentais:

- **Confidencialidade:** garantir que a informação seja acessada e utilizada exclusivamente por usuários que necessitam dela, mediante autorização prévia;
- **Integridade:** garantir que a informação, ao longo de todo seu ciclo de vida, esteja correta, verdadeira e não seja corrompida;
- **Disponibilidade:** garantir que a informação e os recursos que estejam associados a ela estejam disponíveis para os usuários devidamente autenticados, possibilitando o atingimento dos objetivos e missão das organizações.

Outros autores, como Fontes (2001), acrescentam aos três objetivos previamente citados os princípios da:

- **Legalidade:** o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e pela sociedade;
- **Auditabilidade:** possibilidade de identificação de quem fez o acesso e do que foi feito com a informação através de registros;
- **Não repudio de autoria:** implementação de mecanismos que garantam a autoria da criação ou alteração de uma informação.

2.2 Gerenciamento Unificado de Ameaças (UTM)

Conforme Tittel (2014), o UTM pode ser definido como uma ferramenta de segurança que unifica diversos recursos de segurança de rede em um único dispositivo. À proporção que as ameaças evoluem, a segurança precisa adaptar-se para continuar protegendo as redes de computadores. Essa constante mudança torna difícil definir quais recursos de segurança fazem parte de uma solução de UTM. Ao longo do tempo, a presença de recursos de segurança segue aumentando e, atualmente, as melhores soluções de UTM do mercado incluem as seguintes funcionalidades: *Firewall*, IPS, VPN, *Web Filtering*, *Application Control*, Antivírus, *Antispam*, WAF, DLP (*Data Loss Prevention*), ATP (*Advanced Threat Prevention*) e *Sandbox*.

2.3. Problema, modelo e métodos de decisão multicritério

A concepção e a solução de problemas de decisão são alvo de constante preocupação dentro das organizações. O desempenho na análise dos problemas pelos tomadores de decisão, comumente gerentes e executivos, exerce forte impacto na competitividade das empresas frente ao mercado.

Alguns destes problemas de decisão podem ser classificados como problemas de decisão multicritério. Segundo Almeida (2013), problemas desta natureza surgem no momento em que existem pelo menos duas alternativas a serem escolhidas, e essa escolha é pautada pelo propósito de atender múltiplos objetivos, muitas vezes conflitantes entre si. A esses objetivos são associadas variáveis que os representam e possibilitam a avaliação de cada alternativa, com base em cada objetivo. Essas variáveis podem ser chamadas de critérios.

A fim de alcançar a resolução de um problema multicritério, apresenta-se a necessidade da construção de um modelo de decisão multicritério. Um modelo de decisão multicritério equivale a uma representação formal e com simplificação do problema de decisão com múltiplos objetivos enfrentado pelo tomador de decisão. Esse modelo de decisão deve reunir o conjunto de preferências do tomador de decisão para o problema a ser resolvido [Gomes e Gomes 2014].

Em geral, um modelo de decisão é elaborado com base em um método de apoio a decisão multicritério. Para Ishizaka e Nemery (2013), um método de apoio a decisão multicritério (MCDA - *Multi-Criteria Decision Analysis*) pode ser conceituado como uma fórmula metodológica ou uma teoria, que pode ser usado para construir um modelo de decisão que aponta a solução de um determinado problema de decisão.

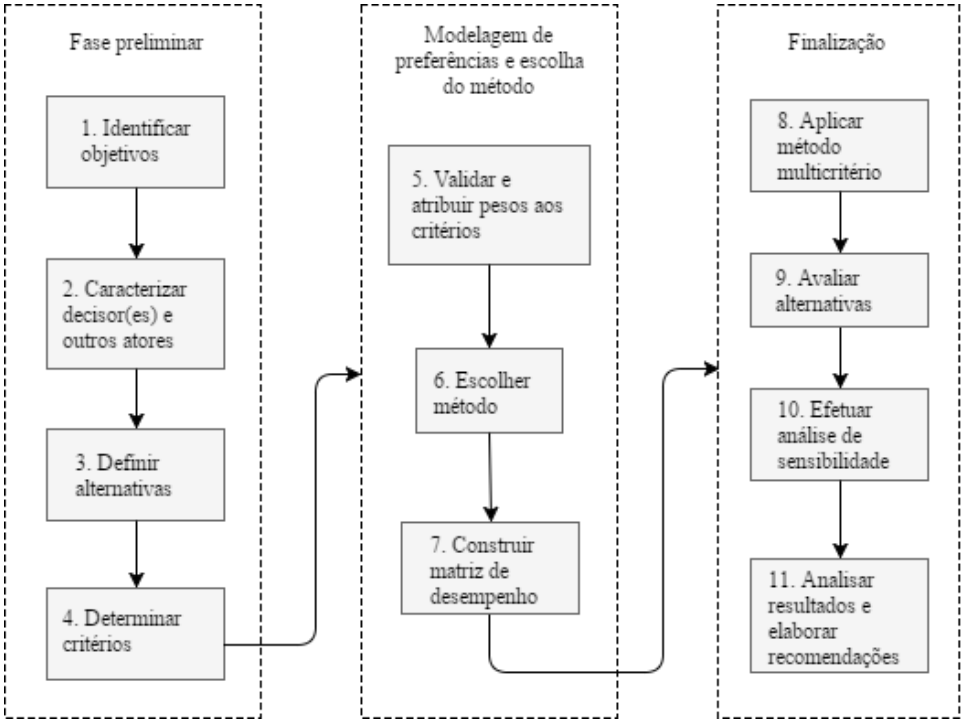
2.4. Processo de construção do modelo de decisão

Segundo Bana e Costa (1988), o processo de tomada de decisão é composto por duas fases fundamentais. Na primeira, conhecida como fase de análise, são identificados e estabelecidos os atores, alternativas e critérios que fazem parte do problema de decisão. Em um segundo momento, na fase de síntese da análise, recorre-se à aplicação de um método multicritério, para identificação da alternativa preferencial.

Com base no estudo de Almeida (2013), a sequência de etapas apresentada a seguir descreve o passo a passo da construção de um modelo de decisão:

1. **Identificar objetivos:** O processo de identificação dos objetivos é a razão principal de interesse no problema de decisão e responsável por guiar os esforços em situações de decisão e avaliação de alternativas.
2. **Caracterizar decisor(es) e outros atores:** Nesta etapa, acontece a caracterização dos principais atores que fazem parte do processo de decisão nas organizações. Tendo em vista as diferentes estruturas hierárquicas presentes em cada empresa, diversos atores, ou seja, aqueles que detêm responsabilidade e dever no processo de tomada de decisão, fazem parte deste processo;
3. **Definir alternativas:** Nesta etapa, deve ser definido um conjunto de alternativas que serão avaliadas no problema de decisão em questão;
4. **Determinar critérios:** O estabelecimento de critérios, quantitativos e/ou qualitativos, objetiva identificar variáveis que possam medir o grau de desempenho de cada alternativa a ser avaliada;
5. **Validar e atribuir pesos aos critérios:** Etapa responsável por atribuir pesos aos critérios de modo que possam representar as preferências dos decisores envolvidos no processo;
6. **Escolher método:** Neste momento será definido o método multicritério mais adequado ao problema em questão;
7. **Construção da matriz de desempenho:** A matriz será composta pelas alternativas, critérios, pesos e o desempenho de cada alternativa em relação a cada critério;
8. **Aplicar método multicritério:** a fim de identificar a melhor alternativa a ser escolhida, o método multicritério será aplicado nesta etapa;
9. **Avaliar alternativas:** Essa etapa consiste na avaliação global das alternativas;
10. **Efetuar análise de sensibilidade:** Com base no resultado obtido na etapa anterior, chega-se a uma recomendação prévia que requer uma análise para avaliar sua robustez em relação aos dados de entrada e aos critérios empregados no modelo de decisão;
11. **Analisar resultados e elaborar recomendações:** Nessa etapa, os dados são novamente analisados e as recomendações são elaboradas. É apresentada uma ordenação das alternativas baseada no seu desempenho e no grau de importância de cada critério.

Para que possa ser melhor compreendido, as etapas e o fluxo do processo de tomada de decisão estão representadas na Figura 1.



Fonte: Adaptado pelo autor de Almeida (2013).

Figura 1. Fluxograma do processo de tomada de decisão

2.5. O método VIKOR

O método VIKOR (*VIseKriterijumska Optimizacija I Kompromisno Resenje*), cujo significado pode ser interpretado como "Otimização Multicritério e Solução de Compromisso", foi desenvolvido como um método de decisão multicritério para solucionar problemas de decisão discreto com critérios não-mensuráveis e conflitantes. Este método determina uma ordenação das soluções de compromisso, uma solução de compromisso e os intervalos de estabilidade ponderados para a estabilidade da preferência por uma solução de compromisso obtida com os pesos iniciais dados. O método emprega um índice de ordenação multicritério baseado na medida particular de proximidade a uma solução ideal ou desejada [Opricovic e Tzeng 2004].

Segundo Opricovic e Tzeng (2004), o algoritmo de ordenação de compromisso VIKOR possui as seguintes etapas:

Etapa 1: Determinar os melhores valores f_i^* e os piores valores f_i^- em relação a todos os critérios $i = 1, 2, \dots, n$:

$$f_i^* = \max_j f_{ij}, \qquad f_i^- = \min_j f_{ij},$$

se o critério i representar um benefício, e

$$f_i^- = \min_j f_{ij}, \qquad f_i^* = \max_j f_{ij},$$

se o critério i representar um custo;

Etapa 2: Calcular os valores S_j e R_j para $j = 1, 2, \dots, J$, por meio das relações:

$$S_j = \sum_{i=1}^{n} w_i \left(f_i^* - f_{ij}\right) / \left(f_i^* - f_i^-\right) \quad (1)$$

$$R_j = \max_i [w_i \left(f_i^* - f_{ij}\right) / \left(f_i^* - f_i^-\right)], \quad (2)$$

onde w_i são os pesos dos critérios, representando a sua respectiva importância relativa.

Etapa 3: Calcular os valores $Q_j, j = 1, 2, \ldots, J$, pela relação

$$Q_j = v(S_j - S^*)/(S^- - S^*) + (1 - v)(R_j - R^*)/(R^- - R^*) \quad (3)$$

onde

$$S^* = \min_j S_j, \qquad S^- = \max_j S_j, \qquad R^* = \min_j R_j, \qquad R^- = \max_j R_j,$$

e v é introduzido para efetuar o balanço entre a estratégia de máxima utilidade do grupo e a medida de não conformidade individual. Neste trabalho, foi assumido $v = 0.5$.

Etapa 4: Ordenar as alternativas em ordem crescente, pelos valores obtidos para os índices S, R, e Q, obtendo como resultado três listas ordenadas.

Etapa 5: Propor como solução de compromisso a alternativa a' que é classificada como a melhor pela medida Q (mínima) se as seguintes condições forem atendidas:

Condição 1 - Vantagem aceitável:

$$Q(a'') - Q(a') \geq DQ \quad (4)$$

onde a'' é a alternativa na segunda posição na lista de ordenação Q; onde $DQ = 1/(J - 1)$; e J é o número de alternativas.

Condição 2 - Estabilidade aceitável na tomada de decisão: Alternativa a' também deve ser a melhor categorizada pelas ordenações S, e/ou R. Esta solução de compromisso é estável dentro de um processo de tomada de decisão, que poderia estar baseado: ou na "escolha pela regra da maioria" (quando $v > 0.5$), ou no "consenso" $v \approx 0.5$, ou no "veto" ($v < 0.5$). Aqui, v é considerado como o peso da estratégia de tomada de decisão baseada na máxima utilidade do grupo.

Se uma das duas condições anteriores não for atendida, então um conjunto de soluções de compromisso é proposto, consistindo em:

- Alternativas a' e a'' se somente a Condição 2 não for atendida;
- Alternativas $a', a'', \ldots, a^{(M)}$ se a Condição 1 não for atendida, onde $a^{(M)}$ é determinada pela relação $Q(a^{(M)}) - Q(a') < DQ$ para o maior valor de M , isto é, de forma que as posições dessas alternativas sejam próximas.

3. Metodologia

O uso de uma ferramenta de segurança baseado em UTM é recomendado para as organizações manterem, no que tange à segurança da sua rede de computadores, uma estratégia de segurança da informação mais eficiente, capaz de dar continuidade aos seus negócios e minimizar o impacto gerado pelas ameaças cibernéticas presentes no contexto atual da Internet.

No entanto, no momento de escolher a ferramenta ideal a ser adquirida, as organizações se deparam com um mercado repleto de alternativas, composto por inúmeros fornecedores e produtos, cada qual com suas próprias implementações das diversas funcionalidades de segurança que compõem uma solução de UTM.

Por isso, a fim de evitar a tomada de decisão de maneira empírica, sem a correta fundamentação dos critérios relevantes envolvidos, este trabalho propõe a construção de um modelo de decisão, capaz de apoiar o processo de avaliação e seleção das opções disponíveis, garantindo maior assertividade na escolha final.

A seguir, as etapas que compõem o modelo de decisão proposto, descrito de forma genérica na Seção 2.4, são descritas visando a resolver o problema de decisão objeto de estudo deste trabalho.

3.1. Identificação dos objetivos

O objetivo geral deste trabalho, conforme descrito na Seção 1, é ajudar as organizações na tomada de decisão em um processo de seleção de uma ferramenta de segurança da informação baseada em UTM.

3.2. Caracterização do(s) decisor(es) e outros atores

A tomada de decisão nas organizações pode ser considerada uma das atividades mais relevantes exercidas por seus gerentes e executivos, uma vez que o desempenho desses interventores no processo de decisão impacta diretamente na competitividade da organização e até na sua sobrevivência.

No contexto atual das organizações, diversos atores podem fazer parte deste processo decisório, desde um gestor da área de TI até um diretor geral, porém cabe ressaltar a importância de considerar a opinião de um especialista da área de segurança da informação, profissional capaz de realizar o levantamento das necessidades do projeto e uma avaliação adequada das alternativas propostas.

Neste trabalho, o autor assumirá o papel de decisor conhecendo e avaliando as alternativas selecionadas através da comparação dos critérios pré-estabelecidos. Porém, o modelo desenvolvido pode servir como ferramenta de auxílio a gestores responsáveis pela tomada de decisão relativa a este objeto de estudo.

3.3. Definição das alternativas

As empresas de pesquisa de mercado da área de tecnologia desempenham um papel relevante auxiliando executivos da área de TI, à medida em que indicam o que deve ser considerado ao tomar decisões na aquisição de produtos ou serviços. Por meio de equipes, compostas por analistas, pesquisadores e consultores, publicam relatórios regulares avaliando as empresas mais importantes de cada setor. Atualmente, destacam-se o *Gartner*, o IDC e a *Forrester*[3] como as principais companhias que entregam tais serviços ao mercado.

O autor elegeu a empresa de pesquisa e consultoria *Gartner* como parâmetro para seleção das alternativas a serem consideradas neste modelo de decisão. O *Gartner* é uma

[3] https://go.forrester.com/

empresa reconhecida mundialmente pela qualidade de suas informações e pela publicação de seus relatórios, que muitas vezes revelam as principais tendências na área de TI.

O Quadrante Mágico (Figura 2) é o principal relatório publicado anualmente pela empresa. Nele, é apresentada a posição de cada concorrente dentro de um determinado segmento de mercado, com base nos critérios de capacidade de execução de cada fornecedor, juntamente com seus pontos fortes e fracos, prezando pela neutralidade das suas classificações. Seu objetivo final é funcionar exclusivamente como uma ferramenta de pesquisa para embasar decisões a partir de necessidades específicas de cada negócio.

Figura 2. Quadrante Mágico do ***Gartner*** para UTM

O *Gartner* define o mercado de UTM como sendo um mercado composto por produtos de segurança de rede multifuncionais usados por pequenas e médias empresas, onde classifica as médias como empresas que possuem de 100 a 1.000 empregados. Dado que essas empresas possuem equipes reduzidas e com menor nível de especialização, características apresentadas pelas ferramentas de UTM como: gerenciamento baseado em interface web, facilidade de configuração, presença de relatórios embarcados na solução, são preferidas.

As ferramentas selecionadas para esta avaliação foram:

- ***FortiGate*** - nome dado à família de produtos de segurança baseados em UTM produzidos pela empresa americana *Fortinet*. São comercializados nas plataformas física e virtual. O primeiro modelo desta linha foi lançado no ano de 2002.
- ***Sonicwall*** - os produtos de segurança baseados em UTM da empresa americana *Sonicwall* levam o mesmo nome do seu fabricante. Possuem uma variedade de

modelos que podem atender desde pequenas empresas até aquelas de grande porte. A empresa foi fundada em 1991 e foi de propriedade da *Dell* no período de 2012 a 2016.

- ***XG Firewall*** - A linha de produtos de UTM da empresa inglesa *Sophos* é nomeada *XG Firewall*. Os produtos desta família foram lançados em 2015 após a fusão do seu antigo produto com o produto da empresa indiana *Cyberoam*, adquirida pela *Sophos* em 2014.

3.4. Definição dos critérios

O estabelecimento de critérios válidos e abrangentes é uma etapa fundamental do processo de construção do modelo de decisão, visto que os mesmos servirão de base para a avaliação das alternativas previamente definidas, influenciando diretamente na qualidade da decisão a ser tomada.

Por meio de revisão bibliográfica e pesquisa da opinião de especialistas publicadas em sites referentes ao assunto, foram elencados uma série de critérios capazes de classificar as alternativas deste problema de decisão [Tittel 2014], [Basile et al. 2013], [Snyder 2006], [Scarfone 2014], [Poklandnik e Santander 2007].

Em virtude da complexidade, do alto número de critérios e da limitação de tempo envolvidos neste trabalho, foram levados em consideração apenas critérios de caráter técnico. Eles foram organizados de maneira hierárquica conforme pode ser observado na Figura 3.

O critério A é formado por recursos de segurança básicos que fazem parte da maioria das soluções de UTM presentes no mercado. As alternativas serão avaliadas mediante análise dos subcritérios pertencentes a este grupo. A seguir, os subcritérios pertencentes a este critério são brevemente descritos:

1. ***Firewall*** - Considerada uma funcionalidade básica das soluções de UTM, seu papel é inspecionar todo tráfego de rede que passa através de suas interfaces e, mediante a configuração de políticas de segurança, é capaz de permitir ou bloquear o seu conteúdo;
2. **IPS** - Este recurso atua como uma segunda camada de proteção além do *firewall*, é responsável por monitorar toda a atividade de entrada e saída da rede e identificar quaisquer padrões suspeitos que possam indicar um ataque de rede ou sistema.
3. **VPN** - Este componente permite criptografar o tráfego de rede utilizando a Internet como meio de interligação entre matriz e filiais de uma organização, ou dispositivos remotos à rede corporativa, impedindo que qualquer intruso intercepte seu conteúdo.
4. ***Web Filtering*** - Esta funcionalidade permite controlar qual tipo de conteúdo web pode ser visto mediante a interceptação das solicitações dos usuários. Seu uso reduz a exposição da rede à malwares e sites inapropriados, melhorando inclusive a produtividade dos colaboradores.
5. ***Application Control*** - Este recurso fornece visibilidade e controle das aplicações utilizadas na rede das organizações, investigando seu comportamento e conteúdo, oferecendo proteção contra ameaças e aumento de produtividade.

6. **Antivírus -** Este item de segurança oferece uma ferramenta de varredura e detecção de infecções a nível de gateway, capaz de proteger os dispositivos por meio da checagem dos pacotes antes mesmo de entrarem na rede.
7. ***Antispam*** - Esta ferramenta é responsável por analisar o tráfego de mensagens de e-mail que entram e saem da rede. Por meio da implementação de regras e tecnologias, é possível classificar as mensagens indesejadas como *spam*.
8. **WAF** - Este recurso é utilizado para proteger sites ou aplicações baseadas na web que ficam localizadas dentro da infraestrutura de rede das organizações, porém visíveis na Internet. Tais aplicações podem conter vulnerabilidades e estarem expostas a diversos tipos de ataques como *SQL injection*, *cross-site scripting*, *session hijacking*, dentre outros.

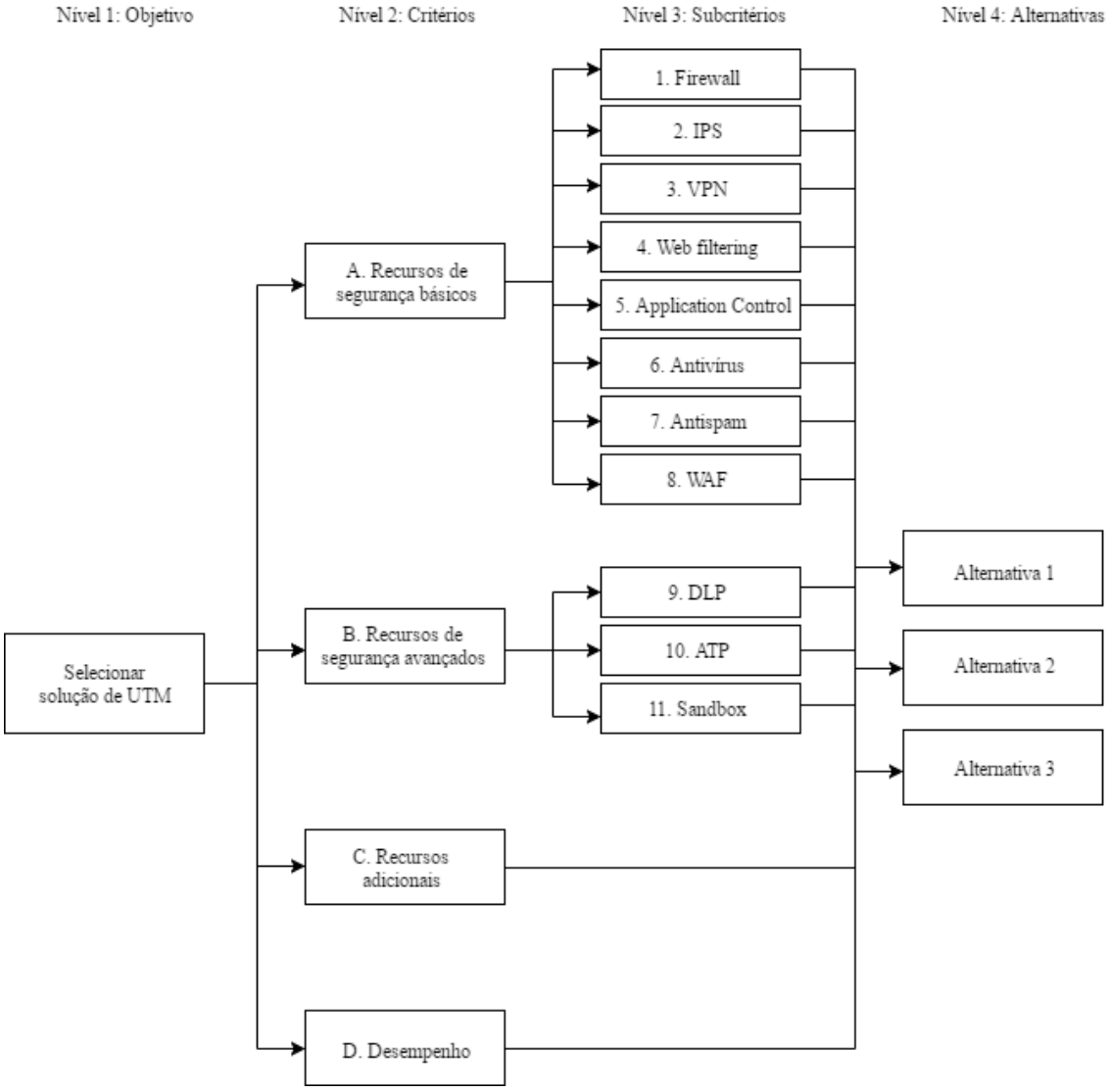


Figura 3. Diagrama de critérios

Por sua vez, o critério B compreende recursos de segurança considerados avançados, que nem sempre são encontrados nas soluções de UTM, porém exercem um papel muito importante no que diz respeito à proteção contra-ataques de segurança

avançados e perda de dados confidenciais. A seguir, os subcritérios pertencentes a este critério são brevemente descritos:

9. **DLP** - Esta funcionalidade permite controlar dados confidenciais que não podem sair da rede da empresa. Seu uso pode evitar o vazamento acidental ou intencional de informações sigilosas.
10. **ATP** - Este recurso fornece proteção contra tipos de ataque direcionados e persistentes.
11. ***Sandbox*** - Este serviço permite que programas suspeitos possam ser executados em um ambiente isolado e seguro, a fim de compreender sua finalidade sem colocar a rede da organização em perigo.

Já o critério C leva em consideração recursos adicionais que fazem, ou não, parte das soluções de UTM. Tais recursos aumentam a oferta de opções disponíveis para uso na infraestrutura de rede das organizações. Os seguintes recursos adicionais serão considerados nesta pesquisa: suporte a alta disponibilidade, ferramenta de logs e relatórios embarcada, balanceamento de links WAN (*Wide Area Network*), gerenciamento de banda (QoS - *Quality of Service*), gerenciamento de solução de redes sem fio, gerenciamento de solução de *endpoint*, autenticação baseada em serviço de diretório, gerenciamento centralizado de múltiplos dispositivos, suporte à encriptação de e-mails, suporte a protocolos de roteamento dinâmico, suporte a VLAN (*Virtual Local Area Network*), gerenciamento baseado em função, e duplo fator de autenticação.

Por último, outro critério fundamental para a seleção de uma ferramenta de UTM é o seu desempenho, que está relacionado à velocidade de tratamento dos pacotes que trafegam através das suas interfaces de rede. Geralmente, o UTM está posicionado na borda da rede, filtrando todo tráfego entre a rede interna da empresa e a Internet e, caso não estiver corretamente dimensionado pode tornar-se um gargalo, prejudicando a velocidade da conexão dos usuários ou deixando ameaças passarem. Ao avaliar os produtos de diferentes fabricantes, as principais métricas de desempenho precisam ser comparadas. Segundo [Snyder 2006], as quatro métricas mais utilizadas são: taxa de conexão, limite de conexão simultânea, *throughput* (taxa de transferência) e latência. Para [Pokladnik e Santander 2007], itens de hardware como processador, número e tipos de portas de rede, tamanho da memória e espaço em disco também devem ser verificados.

3.5. Validação e atribuição de pesos aos critérios

A validação e atribuição de pesos aos critérios foi construída mediante a análise dos resultados de um questionário aplicado à profissionais da área de TI. Os profissionais sugeriram qual o grau de importância que cada um dos critérios elencados nesta pesquisa exerce ao avaliar uma ferramenta de segurança baseada em UTM.

As respostas foram apresentadas mediante uma escala de avaliação composta pelas alternativas: nada importante, pouco importante, relativamente importante, muito importante e extremamente importante, cujos pesos respectivamente usados para contabilizar as repostas serão 0, 2.5, 5, 7.5 e 10.

3.6. Escolha do método

O método de análise multicritério escolhido como base para este problema de decisão foi o método VIKOR, cujo conceito, etapas e equações foram descritos na Seção 2.5. A

escolha por este método justifica-se pela sua capacidade em identificar uma solução de compromisso avaliando, simultaneamente, uma medida de utilidade de grupo (desempenho global) e uma medida individual de disparidade em relação a uma configuração ideal (desempenho individual).

3.7. Construção da matriz de desempenho

A partir da definição das alternativas e da determinação e validação dos critérios, uma matriz de desempenho pode ser construída. A matriz de desempenho contém as notas, expressadas em valores numéricos e/ou escala verbal, fornecidas pela avaliação quantitativa e/ou qualitativa do decisor, referente a cada alternativa em relação a cada critério.

O cenário construído para solução deste problema de decisão em específico classificou os critérios em dois níveis, conforme pôde ser observado na Figura 3. Isso, por sua vez, motivou a construção de três matrizes de desempenho, uma para os critérios e outras duas para cada conjunto de subcritérios. A primeira matriz possui os valores de desempenho referentes aos critérios de nível 2, enquanto as outras duas os valores de desempenho referentes aos dois conjuntos de subcritérios de nível 3.

4. Experimentos e resultados

Esta seção mostra os resultados obtidos através da execução do modelo de decisão previamente descrito. Inicialmente os resultados da aplicação do questionário aos profissionais de TI são exibidos. Em seguida são apresentadas as avaliações de desempenho das alternativas por meio das matrizes de desempenho, seguidas pela aplicação do método multicritério determinando a ordenação das alternativas e sugerindo uma solução de compromisso para este problema de decisão. Por fim, uma análise de sensibilidade é efetuada com intenção de experimentar o resultado obtido simulando uma alteração de parâmetro.

4.1. Questionário

O questionário foi criado usando a ferramenta gratuita *Google Forms* e ficou disponível *on-line* no período de 23/05/2017 a 23/06/2017. No total, 31 profissionais de 16 empresas responderam ao questionário. Observou-se que os principais cargos dos respondentes são: analista de suporte, diretor de TI, diretor comercial, gerente e professor. A média do tempo de atuação dos profissionais entrevistados nos respectivos cargos foi de 5,4 anos.

A Figura 4 apresenta o número de votos obtidos por cada critério usando a escala de avaliação.

Outra análise possível de ser feita a partir dos resultados apresentados pelo questionário foi o fato de que todos os critérios e subcritérios elencados no modelo de decisão se mostraram relevantes, ao passo que foram validados por parte dos profissionais respondentes.

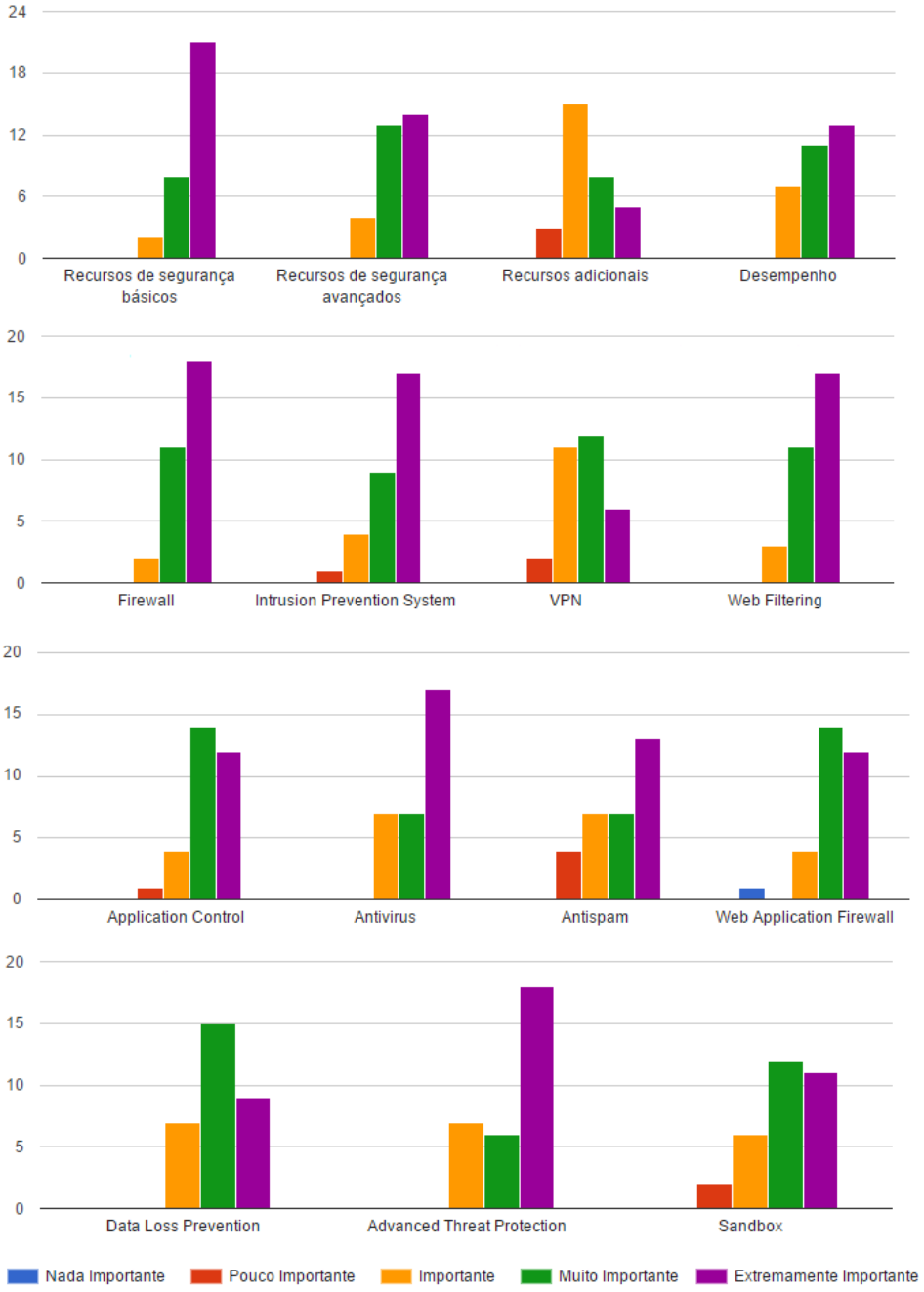


Figura 4. Gráficos de resultados

Para definição dos pesos de cada critério/subcritério, foram utilizados os valores definidos para cada opção da escala de avaliação descrita na seção 3.5 e realizada uma média ponderada. Os pesos extraídos para cada critério e subcritério são apresentados na Tabela 1.

Tabela 1. Lista de pesos dos critérios e subcritérios

Critérios e subcritérios	Peso
A) Recursos de segurança básicos	0,286445013
B) Recursos de segurança avançados	0,26342711

C) Recursos adicionais	0,196930946
D) Desempenho	0,253196931
A1) *Firewall*	0,137106918
A2) IPS	0,13081761
A3) VPN	0,105660377
A4) *Web Filtering*	0,134591195
A5) *Application Control*	0,124528302
A6) Antivírus	0,129559748
A7) *Antispam*	0,114465409
A8) WAF	0,12327044
B9) DLP	0,324232082
B10) ATP	0,354948805
B11) *Sandbox*	0,320819113

4.2. Matrizes de desempenho

A fim de atender a etapa de construção da matriz de desempenho, descrita na Seção 3.7, o autor realizou a avaliação de desempenho das alternativas apresentadas na Seção 3.3, em relação a cada critério apresentado na Seção 3.4.

A avaliação realizada levou em consideração diversos aspectos como: características de hardware, performance, método de implementação, número de ameaças conhecidas, frequência de atualização, dentre outras, observadas nas versões de avaliação disponíveis e nos documentos explicativos fornecidos pelos seus fabricantes. Os resultados obtidos podem ser visualizados nas Tabelas 2, 3 e 4, onde ALT1, ALT2 e ALT3 correspondem às alternativas *Fortigate*, *Sonicwall* e *Sophos XG Firewall*, respectivamente.

Tabela 2. Matriz de desempenho dos critérios

Critérios/Alternativas	ALT1	ALT2	ALT3
A) Recursos de segurança básicos	-	-	-
B) Recursos de segurança avançados	-	-	-
C) Recursos adicionais	9,0	8,5	9,5
D) Desempenho	8,5	6,0	9,0

Tabela 3. Matriz de desempenho dos subcritérios do critério A

Critérios/Alternativas	ALT1	ALT2	ALT3
A1) *Firewall*	9,2	7,8	8,8
A2) IPS	8,5	6,5	9,0
A3) VPN	9,5	8,8	9,3
A4) *Web Filtering*	8,2	7,1	8,6
A5) *Application Control*	7,9	6,2	8,2
A6) Antivírus	8,3	7,8	9,1

A7) *Antispam*	7,9	6,2	8,2
A8) WAF	8,6	7,1	8,9

Tabela 4. Matriz de desempenho dos subcritérios do critério B

B9) DLP	7,7	4,1	8,6
B10) ATP	8,4	7,6	9,2
B11) *Sandbox*	7,1	4,6	8,9

4.3. Aplicação do método multicritério

A próxima etapa do modelo de decisão consiste em aplicar o método de análise multicritério VIKOR.

No método VIKOR, os valores de S_j são calculados usando a Equação (1), para determinar uma medida global de distância de cada alternativa para uma alternativa ideal. Por sua vez, a alternativa ideal é estabelecida a partir dos melhores desempenhos obtidos pelas alternativas em todos os critérios. Já os valores de R_j são calculados, conforme a Equação (2), para avaliar a maior medida de disparidade de cada alternativa em relação à medida ideal para cada critério considerado no modelo de decisão.

Em seguida, os valores de Q_j são calculados, conforme a Equação (3). Esta medida determina a ordenação final com base em uma expressão que realiza o balanço entre a medida de desempenho global e compensatória S_j e a medida de desempenho individual e não-compensatória R_j.

Os resultados de S, R e Q para cada alternativa, obtidos pela aplicação do método são apresentados na Tabela 5.

Tabela 5. Resultados obtidos pelo VIKOR

	ALT1	ALT2	ALT3
S	0,296643158	1	0,019868423
R	0,099211178	0,286445013	0,019868423
Q	0,290010578	1	0

A ordenação das alternativas, ou *ranking*, é um dos resultados esperados após a aplicação do método VIKOR. Sua resposta é conhecida através da ordenação crescente dos valores de S, R e Q, conforme descrito pela etapa 4 do método, apresentada na Seção 2.5. Logo, as classificações obtidas pelas alternativas deste problema de decisão são apresentadas na Tabela 6.

Tabela 6. ***Ranking*** das alternativas

	Ranking
S	ALT3, ALT1, ALT2
R	ALT3, ALT1, ALT2
Q	ALT3, ALT1, ALT2

A etapa final do método VIKOR prevê a determinação de uma solução de compromisso identificando o seu nível de superioridade em relação às demais, de acordo

com a sua adequação às duas condições apresentadas na etapa 5 do método. Portanto, dado que somente a condição 2 foi atendida, o método VIKOR propõe um conjunto de soluções de compromisso composto pelas alternativas ALT3 e ALT1, pois os resultados apresentados pela segunda colocada não foram suficientemente distantes para eleger apenas a primeira alternativa como uma solução de compromisso.

4.4. Análise de sensibilidade

A análise de sensibilidade tem como objetivo avaliar a robustez da solução de compromisso identificada pelo modelo de decisão original. Na análise aqui realizada, foi imposta uma alteração no parâmetro v, isto é, uma alteração no balanço entre o desempenho global e individual de cada uma das alternativas, a fim de verificar o impacto sobre a ordenação Q. A solução do modelo de decisão é avaliada para diferentes valores de v assumidos no intervalo [0, 1]. A Figura 5 apresenta o gráfico gerado a partir desta análise.

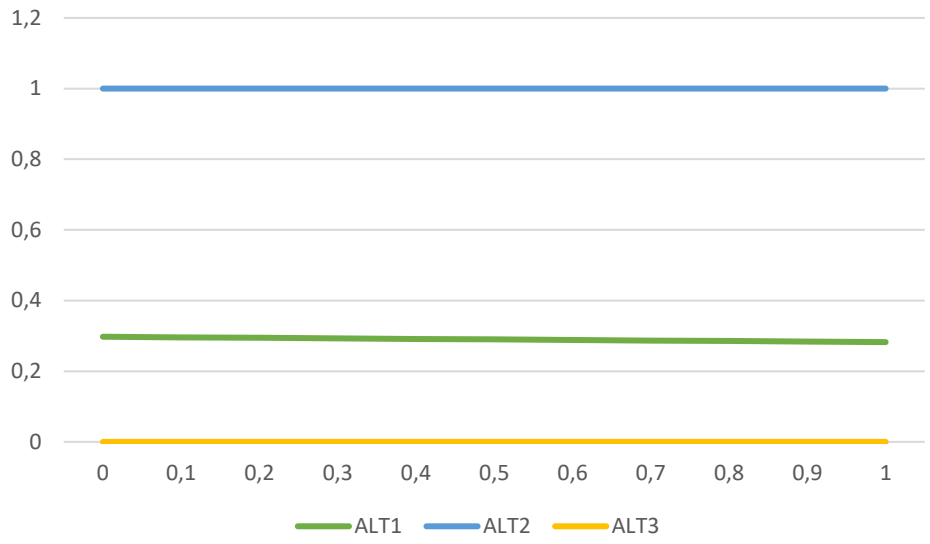


Figura 5. Gráfico da análise de sensibilidade

Com base na interpretação do gráfico apresentado na Figura 5, podemos concluir que mesmo após aplicar uma variação no parâmetro v, não houveram alteração significativas nos resultados apresentados anteriormente.

5. Conclusão

Com base no estudo realizado, é possível afirmar que o uso de uma ferramenta de segurança baseada em UTM como principal tecnologia de segurança de borda da rede de computadores das organizações se tornou um padrão de mercado, tamanho sua eficiência no que diz respeito à detecção de ameaças sofisticadas. Tal efetividade se dá pelo grande número de recursos de segurança presentes na solução, que atuam, inclusive de forma integrada e permitem detectar os ataques em todos seus ciclos de vida.

Para auxiliar as organizações a aprimorar seu processo de seleção ao adquirir uma ferramenta de UTM, este trabalho identificou a necessidade do emprego de um método científico. Para tanto, foi apresentada a construção de um modelo de decisão apoiado no uso do método de análise de decisão multicritério VIKOR.

Os resultados demonstraram que a aplicação do modelo de decisão foi capaz de estruturar este problema de decisão, por meio da correta identificação dos critérios envolvidos, assim como sua atribuição de pesos e desempenhos. Por fim, foi possível ordenar as alternativas e elaborar a recomendação de um conjunto de soluções de compromisso composto pelas duas ferramentas de UTM que obtiveram os melhores resultados na avaliação.

Espera-se que este estudo possa servir de apoio às organizações que desejam adquirir ou até mesmo substituir suas soluções de UTM. Da mesma forma, existe a expectativa de que o modelo de decisão proposto aqui possa auxiliar o processo de tomada de decisão em outros contextos.

Este estudo se limitou apenas à análise de critérios técnicos, portanto para trabalhos futuros abre-se a possiblidade de avaliar outros critérios envolvidos na problemática, como por exemplo: custos, fornecedores e suporte técnico.

Referências

Almeida, A. T. de (2013) "Processo de decisão nas organizações: construindo modelos de decisão multicritério". São Paulo: Atlas.

Associação Brasileira de Normas Técnicas (ABNT) (2005). "ABNT NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação". Rio de Janeiro.

Bana e Costa, C. A. (1988) "Introdução geral às abordagens multicritério de apoio à tomada de decisão". Investigação Operacional, v. 8, p. 117–139.

Basile, R. et al. (2013) "UTM Security with Fortinet: Mastering FortiOS". Waltham: Elsevier.

Beal, A. (2008) "Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações". São Paulo: Atlas.

Efe, B. (2016) "An integrated fuzzy multi criteria group decision making approach for ERP system selection". Applied Soft Computing. v. 38, p. 106-117.

Fontes, E. (2001) "Segurança da Informação: O usuário faz a diferença". São Paulo: Saraiva.

Forouzan, B. A. (2010) "Comunicação de dados e redes de computadores". 4. ed. Porto Alegre: AMGH.

Gomes, L. F. A. M. e Gomes, C. F. S. (2014) "Tomada de decisão gerencial: Enfoque Multicritério". 5. Ed. São Paulo: Atlas.

Hillier, F. S. e Lieberman, G. J. (2014) "Introduction to Operations Research". 10. Ed. Mcgraw-Hill.

IDC Press Release (2016). Disponível em:<https://www.idc.com/getdoc.jsp?Containerid=prus41078516> Acesso em: 31 ago.

Ishizaka, A. e Nemery, P. (2013) "*Multi-Criteria Decision Analysis Multi-Criteria Decision Analysis"*. [S.l: s.n.].

Jafarnejad, A. et al. (2012) "A hybrid MCDM approach for solving the ERP system selection problem with application to steel industry". International Journal of

Enterprise Information Systems. V. 8, p. 54-73.

Kilic, H. S., Zaim, S. e Delen, D. (2014) “Selecting ‘‘The Best’’ ERP system for smes using a combination of ANP and PROMETHEE methods”. Expert Systems with Applications Journal.

Moraes, A. F. de (2010) “Segurança em Redes: Fundamentos”. São Paulo: Érica.

Opricovic, S. e Tzeng, G. (2004). “Compromise solution by MCDM methods: a comparative analysis of VIKOR and TOPSIS”. European Journal of Operational Research, n. 156, p. 445-455.

Pokladnik, M. e Santander, M. (2016) “UTM (Unified Threat Management) – Validating a UTM Device”. Disponível em: <<http://www.sans.edu/student- files/projects/20070 9_003.doc> Acesso em: 30 ago.

Scarfone, K. (2016) “Unified Threat Management - From Business Problem to Technical Solution”. Disponível em: <http://searchsecurity.techtarget.com/ebooK/Unified-threat -management-What-UTM-product-fits-your-organization>. Acesso em: 30 ago.

Snyder, J. (2016) “Evaluating Unified Threat Management Products for Enterprise Networks”. Disponível em: <http://www.opus1.com/www/whitepapers/utm-eval.pdf eval.pdf> Acesso em: 10 out.

Tittel, E. (2014) “Unified Threat Management for dummies”. Hoboken: Wiley.