Método SAPEVO-M aplicado no processo de seleção de equipamento de proteção Firewall UTM para órgãos da Administração Pública Federal (APF)

Maxli Barroso Campos UNIVERSIDADE FEDERAL FLUMINENSE mcampos.2004@gmail.com
Anderson Gonçalves Portella UNIVERSIDADE VEIGA DE ALMEIDA andersonportella@yahoo.com.br

Professor Orientador: Marcos dos Santos
INSTITUTO MILITAR DE ENGENHARIA (IME) marcosdossantos@ime.eb.br

Resumo

Os avanços na área de tecnologia da informação e comunicação resultaram em uso intenso do espaço cibernético para as mais diversas atividades. Nessa direção, o crescimento de conectividade e o aumento da digitalização tornou a economia global mais eficiente e dinâmica, mas também mais suscetível a ataques cibernéticos. O Brasil tem se destacado no cenário nacional e internacional por suas ações nas áreas de segurança e defesa cibernéticas, mas nenhum órgão definiu até o presente momento uma norma padronizada com o mapeamento de requisitos mínimos para orientar gestores da Alta Administração Pública com relação a aquisição de soluções em tecnologia de segurança da informação. O estudo almeja apresentar um levantamento das principais soluções de firewall *Unified Threat Management* (UTM) do mercado para proteção das redes de computadores para órgãos da Administração Pública Federal (APF), atendendo requisitos relevantes que visam referenciar futuras aquisições. O trabalho emprega o método ordinal de grupo de decisão chamado SAPEVO-M, um acrônimo para *Simple Aggregation of Preferences Expressed by Ordinal Vectors Group Decision Making*, por meio da plataforma SADEMON, que permite a agregação das classificações de preferência dos tomadores de decisão (TD) em uma classificação de consenso, que expressa graus de importância por meio de uma classificação.

Palavras-Chaves: proteção de redes, Administração Pública Federal, SAPEVO-M, SADEMON.

1. INTRODUÇÃO

O tema Segurança Cibernética no Brasil foi tratado com uma abordagem inicial de Segurança da Informação e se materializou a partir da criação do Gabinete de Segurança Institucional da residência da República (GSI/PR), por meio da Medida Provisória nº 2.216-37, de 31 de agosto de 2001 (BRASIL, 2001), que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998 (BRASIL, 1998).

Pelo decreto nº 5772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar aos órgãos da APF, assim como orientação para a criação de comitês e verificação do nível de implementação da Política Nacional de Segurança da Informação (PNSI), assim como disposições sobre a instituição de políticas específicas para cada órgão (BRASIL, 2018).

O próprio Decreto levou a aprovação em 2020 da Estratégia Nacional de Segurança Cibernética, também chamada de E-Ciber, por meio do Decreto nº 10.222 (BRASIL, 2020), com o objetivo de orientar as ações de segurança cibernética planejadas pelo governo, em âmbito nacional e internacional e ainda busca fomentar a conscientização e o debate sobre cibersegurança, assim como a implementação de medidas fortes dentro das empresas.

O ambiente cibernético das redes de comunicação de dados é o principal vetor de circulação e transmissão de informações governamentais ostensivas ou sigilosas. Na medida em que são nestas redes que circulam as decisões políticas e estratégicas, bem como as ordens das operações militares, torna-se fundamental estabelecer padrões e estruturas mínimas para implementação da segurança das Organizações, visando garantir à circulação das informações sem interceptação ou interferência de outros atores, o que afiança a privacidade das informações de seus cidadãos e de empresas, a continuidade da prestação de serviços, além do sigilo das políticas e estratégias governamentais.

Soma-se a estes aspectos o fato de que a digitalização, apesar de ter tornado a economia global mais eficiente e dinâmica, tem provocado o aumento da camada de vulnerabilidades cibernéticas das instituições que acabam acarretando prejuízos e impactos de imagem e econômicos.

De acordo com o relatório da Smith *et al.* (2020) a economia global sofre um prejuízo de mais de 1 trilhão de dólares devido aos crimes cibernéticos e o Gartner (2021) apontou em seu relatório de que o impacto financeiro dos ataques cibernéticos que resultarão em prejuízos reais chegará a mais de US$ 50 bilhões até 2023.

Diante destes desafios fica claro que a aquisição de equipamentos de segurança de borda para proteção de rede de um órgão da Administração Pública Federal (APF) precisa seguir requisitos técnicos mínimos para garantir uma proteção eficiente e eficaz, sendo capaz de se interligar a rede de dados corporativa da organização de maneira segura.

Segundo Clarke (2015), para o domínio de um espaço cibernético, é preferível um sistema de proteção permanente e altamente capacitado a um sistema de ataque cibernético sofisticado, pois um país pode ser surpreendido por um ataque inicial e ter essa capacidade ofensiva anulada.

Os requisitos levantados no trabalho serão aplicados ao método SAPEVO-M para que os tomadores de decisão, neste caso, os Comandantes das Organizações Militares (OM) tenham subsídios para garantir os critérios necessários para condução de um processo de contratação.

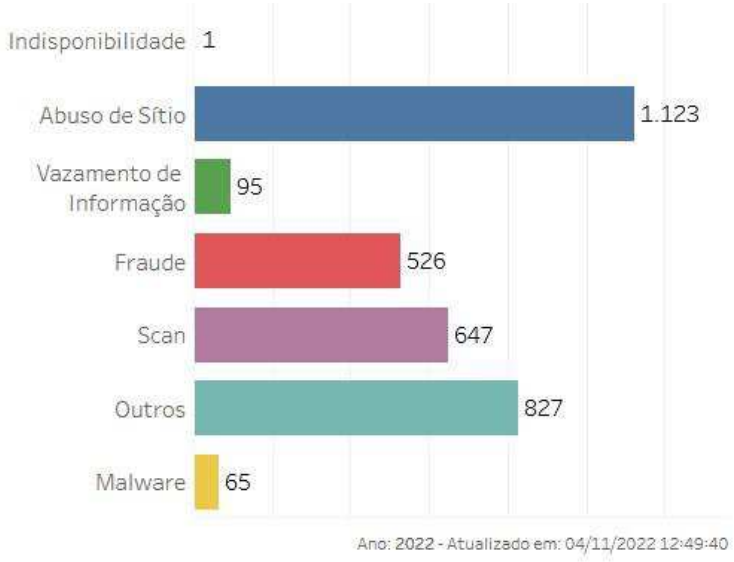
2. DESCRIÇÃO DO PROBLEMA

No Brasil, no que diz respeito à APF, o Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos (CTIR Gov) é o órgão do governo responsável por receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança cibernética.

Trata-se de um *Computer Security Incident Response Team* (CSIRT), ou Grupo de Resposta a Incidentes de Segurança (GRIS) de responsabilidade nacional de coordenação e tem por objetivo coordenar e integrar ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da APF. Um dos serviços providos pelo CTIR consiste na disponibilização de estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos.

De acordo com relatório disponibilizado pelo CTIR (2022) e os dados mostrados na Figura 1, até 04/11/2022, mais de 34,21% dos ataques foram do tipo Abuso de Sítio, também chamados de Desfiguração de Páginas ou *Defacement*. Ataques na modalidade *Scan* aparecem em segundo lugar, com 19,71% dos casos. Em terceiro lugar, com quase 17% dos casos relatados, encontra-se o incidente denominado como Fraude, seguidos pelo tipo de Vazamento de Informações (2,89%) e *Malware* (1,98%).

FIGURA 1: Incidentes confirmados por categoria em 2022



Fonte: CTIR.Gov (2022)

Diante deste cenário, fica cada vez mais evidente que os dados das organizações estão vulneráveis e suscetíveis a novas e sofisticadas ameaças cibernéticas, onde nos últimos anos se registra muitos casos de vazamento de informações e ataques direcionados a diversas organizações, sejam elas pequena, média ou grande porte. Com a Lei Geral de Proteção de Dados (LGPD) em vigor, várias organizações precisam se reestruturar e adotar soluções de segurança mais robustas.

Segundo Mckenzie (2017, p. 9) as atividades maliciosas na internet aumentam em frequência e gravidade, e à medida que os países se estruturam para defender suas redes e infraestruturas, essa capacidade de combater crimes no espaço cibernético ganha cada vez mais relevância internacional. E essas possibilidades de uso indevido transformaram o espaço cibernético em um ambiente estratégico para os governos, negócios e sociedade (TEN; MANIMARAN; LIU, 2010).

Dentre as soluções, destaca-se o equipamento Firewall, pelo fato de atuar na linha de frente da infraestrutura de redes, com a capacidade de identificar, mitigar e bloquear ameaças e ataques direcionados a rede interna.

E da mesma forma que outros equipamentos de segurança evoluíram ao longo dos anos, o Firewall vem agregando novas e importantes funcionalidades, com soluções mais integradas, especialmente de perímetro, que oferecem um conjunto de características de segurança, de alto valor agregado, em um produto único, com forte integração.

O termo Firewall UTM ou simplesmente UTM (Unified Threat Management, do inglês, Gerenciamento Unificado de Ameaças) é a nomenclatura dada a um dispositivo de hardware ou software capaz de reunir diversas funções de segurança, como filtro de pacotes, *proxy*, sistemas de detecção e prevenção de intrusão, proteção contra malwares, controle de aplicação, entre outros.

Para fins de aquisição, os órgãos da APF contam com a Instrução Normativa Nº 1, de 4 de abril de 2019 (BRASIL, 2019), que regula o processo de contratação de bens e serviços de tecnologia da informação e comunicação no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.

Apesar do novo modelo simplificar o processo ao incorporar o Plano Anual de Contratações (PAC) e eliminar documentos, não estabelece, recomenda ou padroniza requisitos mínimos de segurança cibernética para aquisição de soluções de segurança da informação, ficando a cargo de cada órgão a responsabilidade de adquirir, instalar e manter uma solução que pode ainda ser integrada com outros órgãos da APF e acabar sendo um vetor de entrada de ameaças para rede de governo.

A falta de uma definição padronizada de requisitos de segurança cibernética mínima favorece à condução de processos de licitação já viciados na origem, sem privilegiar aspectos importantes e necessários para uma correta integração segura de um novo equipamento de segurança à infraestrutura da rede de dados corporativa da organização. Estes equipamentos podem servir de vetor de entrada para rede corporativa da organização e comprometer a sua infraestrutura, assim como sua cadeia de suprimentos.

É neste sentido, que este trabalho busca mapear requisitos mínimos de segurança cibernética para, em um processo de tomada de decisão, orientar os gestores da APF com relação à aquisição ou contratação de soluções de segurança da informação, empregando o Método Multicritério Ordinal SAPEVO-M.

Este trabalho trata de uma pesquisa de campo, com visitas in loco e coleta de dados, interações com gestor da área de tecnologia e segurança da informação, a fim de entender quais os critérios relevantes na aquisição de um Firewall UTM. Entendendo que esses fatores são fundamentais para estruturar a base da condução deste estudo. Com base nos requisitos (critérios) levantados por especialistas, foi possível identificar algumas opções e, com auxílio do Software SADEMON (https://www.sademon.com/), foi aplicado o conceito do método SAPEVO-M.

3. FUNDAMENTAÇÃO TEÓRICA

Problemas de decisão do mundo real raramente são baseados em um único critério e geralmente envolvem uma variedade de critérios, muitas vezes contraditórios (GOMES *et al.*, 2020). De acordo com o mesmo autor:

> "a Tomada de Decisão Multicritério (TDMC) tem sido uma das áreas de Pesquisa Operacional (PO) que mais cresce nas últimas duas décadas, sendo ainda uma das metodologias de decisão mais utilizadas em ciência, negócios, governo e engenharia para apoiar a qualidade no processo de tomada de decisão." (AIRES & FERREIRA, 2018 apud GOMES *et al.*, p.2).

As técnicas de TDMC lidam com os problemas em que as alternativas são predefinidas e o decisor classifica as alternativas disponíveis com base em critérios predeterminados (TESFAMARIAM e SADIQ, 2006 apud MOFARRAH *et al.*, 2012). Os métodos ordinais foram os primeiros métodos de auxílio à tomada de decisão, desenvolvidos a partir de meados do século XVIII, pelos estudos de Jean-Charles de Borda, de acordo com Gomes *et al.* (2020). Esses métodos oferecem vantagens devido à relativa facilidade de compreensão e administração, bem como maior confiabilidade em termos de redução de inconsistências geradas no processo de elicitação de preferências.

O trabalho em análise tem por objetivo apresentar o método ordinal de grupo de decisão chamado SAPEVO-M para classificar alternativas com múltiplos critérios e tomadores de decisão (TD). O SAPEVO-M tem por objetivo estender o método desenvolvido por Gomes *et al.* (1997) para decisão de grupo, além de verificar sua consistência no processo de normalização da matriz.

Gomes *et al.* (2020) destaca que além do novo algoritmo proporcionar uma análise multicritério com múltiplos decisores, também foi integrado um processo de normalização das matrizes de avaliação, mediante a correção de pesos negativos e nulos dos critérios, incrementando assim a consistência do modelo.

De acordo com o modelo apresentado são necessários dois processos. Inicialmente é realizada a transformação da preferência ordinal entre critérios, a ser expressa por um vetor representando os pesos dos critérios. Em seguida, é realizada a transformação ordinal da preferência entre alternativas dentro de um determinado conjunto de critérios, expressa por uma matriz.

Uma série de comparações pareadas entre as opções quer seja critérios ou alternativas dentro de um determinado critério, denotam as informações de preferência individual de cada decisor.

Uma escala de sete pontos expressa a relação entre as alternativas, na qual são mensuradas, relativamente, a importância entre cada opção. A partir da avaliação entre alternativas, é obtido uma matriz com a representação numérica correspondente. A relação entre a escala de preferência e o valor numérico é expressa na Tabela 1.

TABELA 1: Escala ordinal de importância

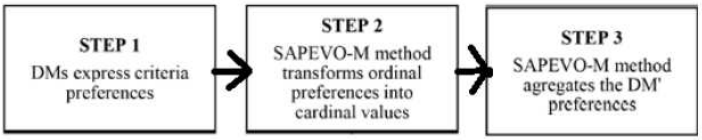
Indicação de Preferência	Pontuação
Absolutamente pior / Absolutamente menos importante	-3
Muito pior / Muito menos importante	-2
Pior / Menos importante	-1
Equivalente / Tão importante quanto	0
Melhor / Mais importante	1
Muito Melhor / Muito Mais Importante	2
Absolutamente Melhor / Absolutamente Mais Importante	3

Fonte: Adaptado de (GOMES *et al.*, 2020)

Gomes *et al.* (2020) afirmam que os métodos ordinais apresentados fornecem uma classificação sem uma medida escalar para cada alternativa. Muitos métodos que contabilizam informações ordinais sobre pesos e valores alternativos/utilidades dentro da Teoria da Utilidade Multiatributo (TUMA, também designado por MAUT – Multiattribute Utility Theory) podem ser encontrados na literatura; no entanto, o ranking da diferença entre os valores das alternativas consecutivas utilizadas para representar as preferências do MD não é tão comum na literatura.

Essa limitação foi superada, com restrições pelo método SAPEVO, proposto por Gomes *et al.* (1997). Assim sendo, o método SAPEVO-M permite agregar preferências de múltiplos tomadores de decisão (TD) em um processo ordinal, onde a primeira parte do método (Passo 1 ao Passo 3) pode ser utilizada de forma independente pelos TD para estabelecer pesos aos critérios de forma ordinal, conforme Figura 2.

FIGURA 2: Passos 1 a 3 do método SAPEVO-M

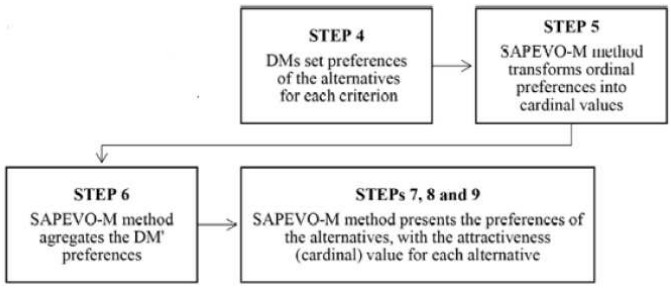


Fonte: GOMES *et al.* (2020)

Esses pesos podem ser aplicados posteriormente no SAPEVO-M ou outro método (escolhido pelos TD). Se os TD tiverem um vetor de preferência para os critérios e desejarem ordenar as

alternativas ordinariamente, eles podem descartar esse vetor e usar o método SAPEVO-M da etapa 4 à etapa 9, conforme Figura 3.

FIGURA 3: Passos 4 a 9 do método SAPEVO-M



Fonte: GOMES *et al.* (2020)

Embora o SAPEVO-M seja um método simples, envolve cálculos matriciais que podem se tornar trabalhosos dependendo do número de TD, critérios e alternativas. Este é principalmente o caso porque esta técnica requer a comparação pareada de todos os elementos.

O novo Método Multicritério Ordinal, chamado SAPEVO-M, é uma nova versão do método original SAPEVO. Agora ele possibilita a utilização de múltiplos decisores, além de ter introduzido um processo de normalização das matrizes de avaliação, que incrementou a sua consistência axiomática. O método foi publicado na Revista Pesquisa Operacional e já conta com dezenas de aplicações em problemas complexos de nível operacional, tático e estratégico.

Na aplicação do método foi utilizado o sistema SADEMON (NETO; SANTOS; GOMES, 2020), que foi desenvolvido no Instituto Militar de Engenharia (IME), com o objetivo de ser uma ferramenta dinâmica e interativa para os decisores que permite que eles incluam suas respectivas avaliações acerca dos critérios e das alternativas. O SADEMON, na qual a entrada de dados é feita está disponível no seguinte sítio da internet https://www.sademon.com/.

4. METODOLOGIA

A primeira técnica de pesquisa utilizada foi o *brainstorm*, para que se pudessem descobrir as emoções presentes na prestação dos serviços. Brown (2010) afirma que a utilização do *brainstorm* essencial para a criatividade, sendo o mesmo indispensável para ampliar a variedade de ideias e para a criação de escolhas nas organizações. A sessão de *brainstorm* realizada foi facilitada pelos próprios pesquisadores, sendo suas funções: o controle do tempo, o estímulo a perguntas e a reflexões, e o registro das ideias manifestadas pelos participantes.

A pesquisa contou com a participação efetiva de 5 profissionais de segurança da informação atuantes na AFP, podendo-se ter uma visão mais ampla da opinião dos mesmos sobre as suas percepções quanto as soluções e requisitos técnicos mínimos definidos no contexto do trabalho.

O trabalho emprega uma metodologia de pesquisa aplicada e exploratória, de caráter qualitativo. Para a pesquisa bibliográfica, foi utilizada as bases de dados SCOPUS. Já para busca de artigos foram utilizadas inicialmente as seguintes combinações: "multicriteria" OR "multiple criteria" AND "SAPEVO-M".

Quanto à sua natureza, a pesquisa pode ser classificada como aplicada, uma vez o assunto a ser pesquisado tem influência prática no emprego em processos de aquisição e contratação de soluções de segurança da informação ligados aos órgãos da APF. Ao final, servirá como referência para novos processos de aquisição e contratação. No que tange à classificação segundo as fontes de informação, pode-se afirmar que o trabalho será desenvolvido com base em pesquisas bibliográfica, documental e de campo (GONÇALVES, 2007).

5. PROPOSTA DE SOLUÇÃO

Para apoiar a decisão, o pesquisador optou por usar o método SAPEVO-M (Simple Aggregation of Preferences Expressed by Ordinal Vectors – Multi Decision Makers) e a interação foi processada através da plataforma computacional de acesso livre SADEMON (SAPEVO-M: Decision Making Online) (NETO; SANTOS; GOMES, 2020), disponível no sítio web https://www.sademon.com/. Para uso inicial da ferramenta, o analista precisa criar uma sessão destinada ao processo de decisão, conforme apresentado na Figura 4.

FIGURA 4: Página inicial do software SADEMON

Fonte: Elaborado pelo autor

E no contexto deste estudo de caso, o pesquisador juntamente com outros profissionais da área de segurança da informação elaboraram, por meio da técnica de *brainstorm*, uma tabela de

decisão para o problema de decisão multicritério, conforme compilação apresentada na Tabela 2.

TABELA 2: Tabela com a compilação da discussão e brainstorm inicial com os decisores

<table>
<tr><td>Regras
Utilizar o método SAPEVO-M para o processo de decisão de aquisição de uma nova solução de firewall SOHO</td><td>Desafio
- Coleta das informações sobre as alternativas
- Informações insuficientes
- Necessidade de Contato com fornecedores</td><td rowspan="2">Recompensa
- Será sempre a escolha ótima
- Melhora na identificação e proteção de ameaças
- Agregar Inteligência de ameaças</td><td>Alternativas
- CISCO
- Fortinet
- Blockbit
- Palo Alto
- Check Point
- Juniper
- Sonicwall
- Sophos</td><td>Decisão a fazer
- Ordenar os equipamentos UTM por meio da implementação do método de apoio multicritério à decisão SAPEVO-M</td></tr>
<tr><td>Jogadores
- Organizações PMEs
- Fornecedores</td><td>Recursos
Site http://www.sapevo-m.com/home.php</td><td>Indicadores
- Custo; Suporte na região; Atualização regular; Inteligência de Ameaças</td><td>Decisão a não fazer
- Quais alternativas não adquirir com base nos resultados?</td></tr>
<tr><td colspan="3">Cenário
- As Organizações PMEs precisam implementar soluções de segurança robustas (eficientes e eficazes) para segurança das redes
- São de extrema importância para evitar possíveis incidentes cibernéticos
- Padronizar os equipamentos de segurança (firewall UTM) e contribuir para segurança nas integrações entre redes.</td><td colspan="2">Estratégia
- Coletar dados; conseguir uma proposta comercial para as soluções alternativas selecionadas e que atendam a necessidade da OM; empregar o método SAPEVO-M para o auxílio na tomada de decisão.</td></tr>
</table>

Fonte: Elaborado pelo autor

Para aplicação do método foi proposto pelo pesquisador uma arquitetura de Firewall UTM padrão, conforme apresentado na Tabela 3 abaixo, que se adequa perfeitamente a necessidade e modelos para organizações conhecidas como pequenas e médias empresas (PME).

A ideia consiste em, a partir de uma arquitetura padrão, identificar as melhores soluções que atendam aos requisitos técnicos definidos neste trabalho, na medida em que seria praticamente impossível apontar a melhor solução para diferentes arquiteturas.

TABELA 3: Requisitos técnicos da solução proposta para o Firewall UTM

Descrição dos requisitos técnicos do Firewall UTM padrão	
Throughput	3Gbps
Throughput (UDP)	40 Gbps
VPN Throughput (IPSEC/SSL)	8Gbps
Webfilter Throughput (HTTP/HTTPS SSL Inspection)	10/3Gbps
Número de portas	Mínimo de 8 (oito) portas

Fonte: Elaborado pelo autor

A primeira etapa para resolução do problema proposto foi estabelecer os critérios e alternativas. Sendo as alternativas as opções de Firewall UTM a serem adquiridos e os critérios a serem julgados importantes. Destacamos abaixo os principais critérios a serem considerados no problema:

1. Suporte em âmbito nacional;
2. Arquitetura redundante e balanceada;
3. Possui NOC/SOC no Brasil;
4. Plataforma de Inteligência de Ameaças; e
5. Política de atualização.

Com a configuração da arquitetura padrão e os critérios definidos, o próximo passo consistiu na solicitação de uma proposta comercial aos 8 (oito) maiores fornecedores de soluções de Firewall UTM mapeados no mercado brasileiro, com indicação de material de referência para consulta (*datasheet*), em um prazo de duas semanas.

Além da proposta comercial, os fornecedores precisariam responder pontualmente o formulário apresentado no Anexo "A".

Após o término do período, 6 (seis) empresas retornaram declarando ter condições de atender a solicitação proposta e os critérios solicitados. Dentre as empresas que responderam, uma delas apresentou uma proposta diferente da arquitetura padrão definida no trabalho e outra apresentou um preço médio para a solução muito além das outras e foram descartadas das amostras deste estudo de caso.

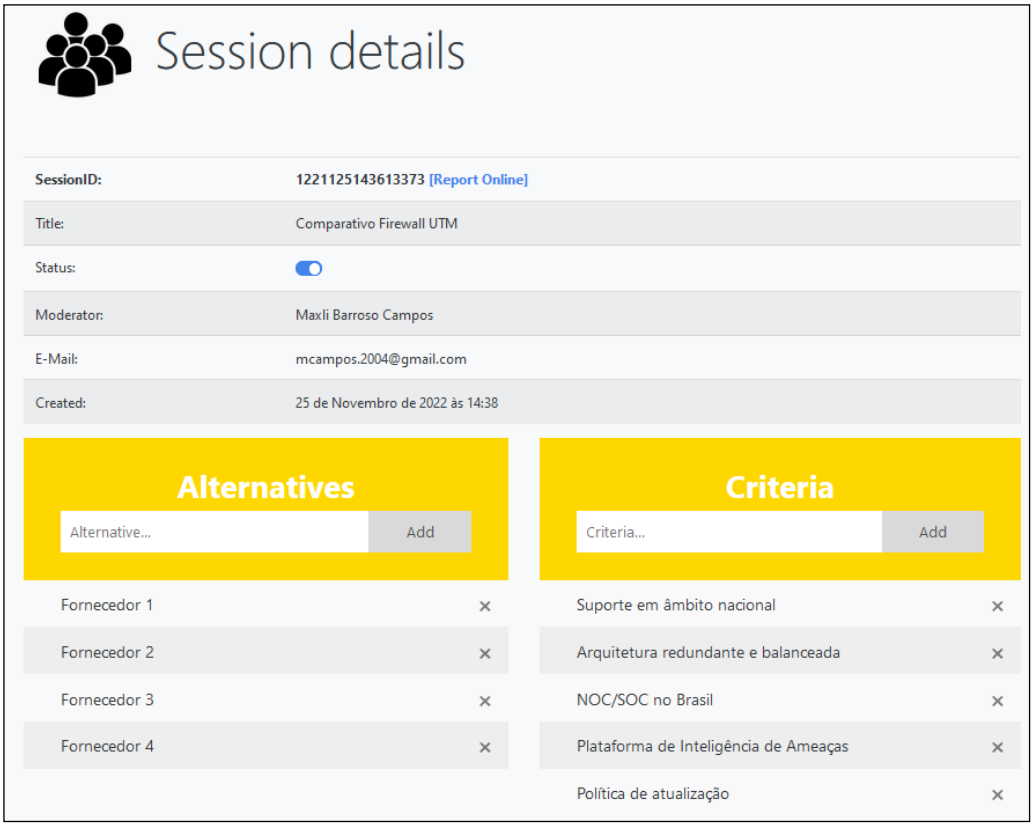
Levando em consideração a necessidade de se manter uma boa relação entre o cliente e o fornecedor e que a atividade de pré-venda ser tão importante quanto a relação contratual e o pós-venda, as empresas que não retornaram a proposta também foram descartadas.

Sendo assim, foi implantado na plataforma SAPEVO-M um total de 4 (quatro) empresas como amostras consideradas no estudo de caso, que por uma questão inerente à segurança da informação não foram citadas, na medida em que uma das primeiras fases de um ataque cibernético bem-sucedido consiste justamente em identificar os ativos de informação das empresas.

Logo, a proposta do trabalho consiste em orientar o processo de aquisição para APF por meio de contratação direta, seja por dispensa de licitação ou inexigibilidade, mantendo justamente o sigilo da compra, ficando condicionado uma consulta ao pesquisador, que a seu critério irá disponibilizar o nome das empresas que foram foco desta pesquisa.

A plataforma SADEMON permite que um usuário moderador insira facilmente as alternativas e critérios, e libere uma chave com um ID para que os decisores avaliem as alternativas e critérios, conforme Figura 5:

FIGURA 5: Página com os detalhes da sessão e as variáveis de decisão multicritério



Fonte: Elaborado pelo autor

Após receber o ID da sessão, cada decisor participante deve acessar a plataforma e indicar, dentro de sua análise, sua indicação de preferência com relação ao conjunto de comparações paritárias entre critérios e alternativas, conforme apresentado na Figura 6.

FIGURA 6: Página de definição de preferências (Sofware SADEMON)

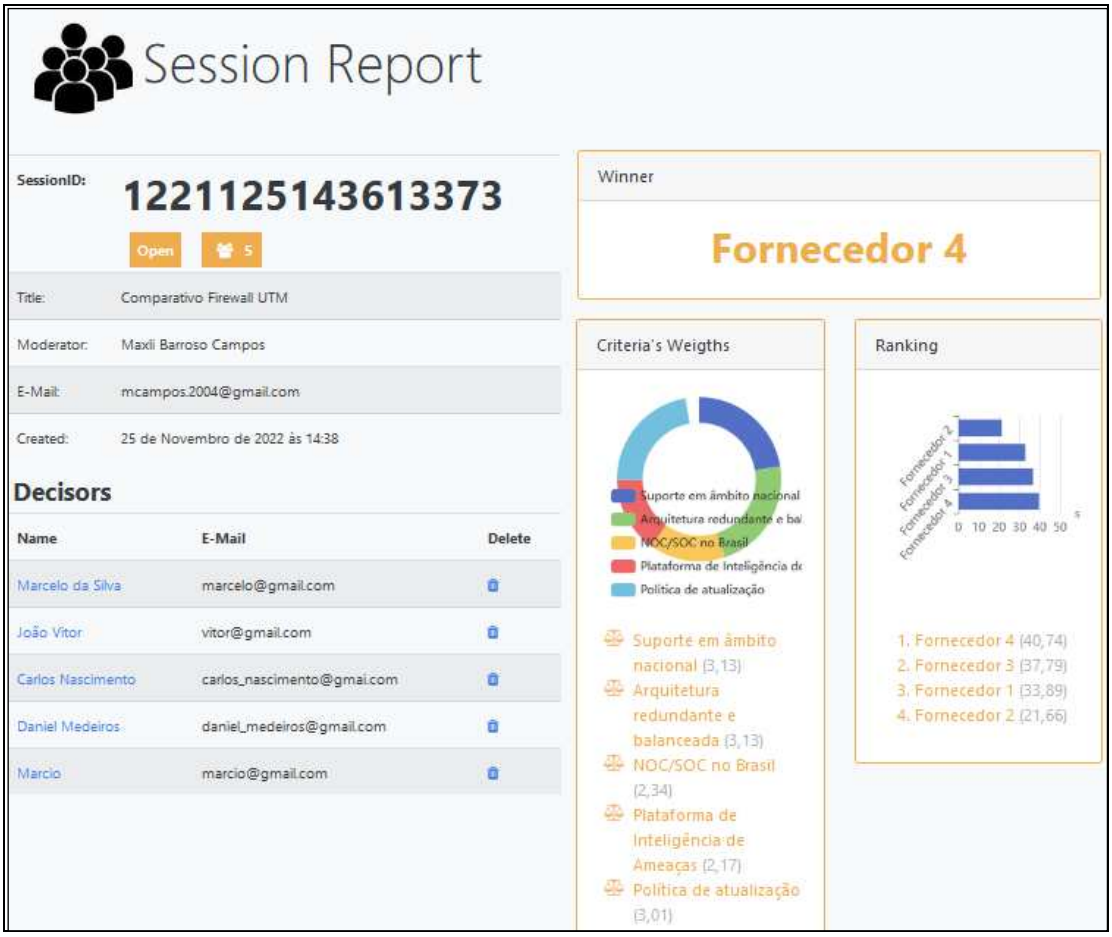
Fonte: Elaborado pelo autor

Finalizada o processo de participação do grupo de decisores, a sessão é finalizada e as indicações de preferências são agregadas, gerando os respectivos resultados das preferências dos decisores, de modo local, e de forma global, expressando assim a opinião do grupo de modo transparente. A Figura 7 apresenta o resultado global, após a interação de todos os decisores.

O relatório indica os resultados da interação e a decisão tomada pelo grupo, formado por 5 (cinco) profissionais da área de segurança da informação da APF, que em última instância também são responsáveis por conduzir processos de aquisição. Toda a documentação recebida pelo pesquisador, sendo a proposta comercial, com o detalhamento dos critérios indicados e atendidos pelas empresas, assim como o *datasheet* da solução foram encaminhados aos respondentes.

Essa interação teve como objetivo demonstrar a viabilidade da utilização do método de ordenação SAPEVO-M no apoio à tomada de decisão sem a necessidade de concordância prévia entre os decisores sobre os pesos de cada critério. Bem como a facilidade de sua aplicabilidade trazida pela interação através da plataforma SADEMON.

FIGURA 7: Relatório final com o resultado global do levantamento



Fonte: Elaborado pelo autor

6. DISCUSSÃO DOS RESULTADOS

O resultado apresentado na Figura 7 consolida as preferências dos decisores de forma global e consensual. Quanto aos critérios, foi identificado que os aspectos de suporte em âmbito nacional e arquitetura redundante e balanceada acabaram sendo das mais importantes no apoio à tomada de decisão, apresentando ambas a maior pontuação de 3,13.

O segundo critério foi a política de atualização com 3,01, seguida pelo critério possuir NOC/SOC no Brasil com 2,34 e por último o critério do fornecedor possuir uma plataforma de inteligência de ameaças com 2,17.

Os resultados acabam demonstrando que os decisores possuem grande preocupação com aspectos de resiliência da solução implementada. Logo, fica claro que toda e qualquer solução na área cibernética deve privilegiar uma arquitetura redundante e balanceada, sendo capaz de manter seu funcionamento em casos de falhas ou ataques cibernéticos, mantendo um tráfego seguro por meios alternativos, evitando casos de indisponibilidade.

E nos casos de crise, de uma eventual indisponibilidade, o fornecedor deve disponibilizar suporte técnico especializado em um regime de atendimento alinhado às necessidades do órgão.

Em relação a prioridade das alternativas, o Fornecedor 4 mostrou-se o mais favorável com uma pontuação relativamente mais alta que a segunda alternativa, que ficou com o Fornecedor 3.

Este resultado acaba tendo relação direta com a preocupação dada pelo Fornecedor 4 em submeter para o pesquisador um material completo acerca de sua solução, que atende não só a parte dos requisitos técnicos, mas ao indicar que possui no Brasil um NOC/SOC próprio em território nacional e relatórios de *threat intelligence* de atividades suspeitas no espaço cibernético brasileiro acaba se tornando um grande diferencial frente as outras soluções.

Tal aspecto por si só acaba estabelecendo uma diferença muito grande entre as soluções, na medida em que boa parte das soluções disponibilizadas no mercado brasileiro compilam informações de *threat intelligence* de atividades suspeitas na internet do mercado americano ou europeu.

Complementando a análise, fica claro que a alternativa de possível contratação com o Fornecedor 2 mostrou-se a menos favorável na avaliação global e apresentando baixas pontuações nas avaliações individuais, podendo concluir que a alternativa não apresentaria relevância em nenhum dos cenários. Este resultado, em contrapartida, reflete um pouco a falta de cuidado do fornecedor em se preocupar em encaminhar materiais que comprovassem a sua capacidade de atender aos requisitos técnicos mínimos estabelecidos neste trabalho.

No final de todo o processo e buscando apoiar futuras aquisições e contratações de soluções de um Firewall UTM, os gestores de segurança da informação da APF poderiam indicar para suas equipes técnicas que tanto o Fornecedor 4, Fornecedor 3 e o Fornecedor 1 seriam soluções passíveis de compor um processo de licitação, dado que a diferença na pontuação de ambos foi baixa, nesta ordem de prioridade.

7. CONSIDERAÇÕES FINAIS

O presente estudo de caso empregou um modelo computacional destinado ao apoio à decisão em cenários complexos com múltiplos decisores, por meio do software SADEMON, que foi implementado empregando o método SAPEVO-M, construído sob a abordagem multicritério de apoio à decisão.

A plataforma SADEMON foi empregada na interação e integração de 5 (cinco) TD que atuam na área de segurança da informação e possibilitou que cada um, de maneira independente,

pudesse agregar sua visão quanto a melhor solução de Firewall UTM atualmente disponível no mercado brasileiro e aderente aos requisitos estratégicos mínimos indicados no trabalho.

Após a interação, os TD relataram que a ferramenta se apresentou como um importante instrumento para auxílio a tomada de decisão para problemas que a primeira vista parecem complexos, possibilitando a estruturação de critérios ou preferências, assim como apresentação de resultados de forma clara.

Pode-se concluir então que por meio da implementação do modelo em um estudo de caso real foi possível demonstrar uma tomada de decisão baseada na avaliação da melhor solução de segurança da informação Firewall UTM, por meio da agregação das preferências compiladas em um resultado global, expondo as alternativas mais favoráveis dentro de um conjunto de múltiplos critérios.

Adicionalmente, serve como um importante instrumento para apoiar a estratégia de uma possível contratação de equipamentos de segurança da informação, na medida em que o Brasil ainda não conta com uma norma padronização estabelecendo requisitos mínimos para apoiar processos de contratação de equipamentos de proteção cibernética.

REFERÊNCIAS

BRASIL. Presidência da República. **Lei nº 9.649, de 27 de maior de 1998**. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Brasília, DF, 1998. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9649cons.htm> . Acesso: 19/01/2023.

BRASIL. Presidência da República. **Medida Provisória nº 2.216-37, de 31 de agosto de 2001.** Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Brasília, DF, 2001. Disponível em: < https://www.planalto.gov.br/ccivil_03/mpv/2216-37.htm > . Acesso: 19/01/2023.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação (PNSI). 2018. **Decreto no 9.637**. Brasília, DF, 2018.Disponível em: < https://dou.vlex.com.br/vid/decreto-n-9-637-751750029#:~:text=Fica%20institu%C3%ADda%20a%20Pol%C3%ADtica%20Nacional,da%20informa%C3%A7%C3%A3o%20a%20n%C3%ADvel%20nacional.> . Acesso: 19/01/2023.

BRASIL. Instrução Normativa nº 1, de 4 de abril de 2019. IN SGD/ME nº 1, de 2019, **DOU**, Brasília-DF, p. 54 – 70, abril 2019b. Disponível em: <https://www.governodigital.gov.br/ documentos-earquivos/INSTRUCAO%20NORMATIVA%20No%201-%20DE%204%20DE %20ABRIL%20DE%202019.pdf/at_download/file>. Acesso em: 04.11.2022.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa – Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2020. Disponível em: < https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa>. Acesso: Acesso: 19/01/2023.

BROWN, T. **Design thinking: Uma metodologia para decretar o fim das velhas ideias**. Rio de Janeiro: Elsevier, 2010.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. ed. Kindle. Rio de Janeiro: Brasport, 2015.

CTIR GOV. **Estatística e levantamento de incidentes**. Disponivel em: < https://www.gov.br/ctir/pt-br/ assuntos/ ctir-gov-em-numeros/incidentes>. Acesso em 04.11.2022.

DE ALMEIDA, Adiel Teixeira; GEIGER, Martin J.; COSTA MORAIS, Danielle. Challenges in multicriteria decision methods. **IMA Journal of Management Mathematics**, 29:247-252, 2018. Disponível em: <https://academic.oup.com/imaman/article-abstract/29/3/247/4951675?login=false>. Acesso: 19/01/2023.

GARTNER Inc. **Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans: Organizations Can Reduce Risk by Implementing a Security Control Framework**. Press Release, newsroom, julho 2021. STAMFORD, Connecticut. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we> . Acesso: 19/01/2023.

GOMES, L. F. A. M.; MURY, A. R.; GOMES, C. F. S. **Multicriteria ranking with ordinal data. Systems Analysis Modelling Simulation**, v. 27, n. 2–3, p. 139–145, 1997. Disponível em: < https://www.researchgate.net/profile/Carlos-Francisco-Gomes/publication/257132839_Multicriteria_Ranking_with_Ordinal_Data/links/53f8c14f0cf27925e2e0d12f/Multicriteria-Ranking-with-Ordinal-Data.pdf> . Acesso: 19/01/2023.

GOMES, C. F. S.; SANTOS, M.; TEIXEIRA, L. F. H. S. B.; SANSEVERINO, A. M.; BARCELOS, M. R. S. SAPEVO-M a group multicriteria ordinal ranking method. **Pesquisa Operacional**, v. 40, p. 1–20, 2020. Disponível em:< https://www.scielo.br/j/pope/a/xHJsxR6NYtjvQqdDzj7NTJK/abstract/?lang=en>. Acesso: 19/01/2023.

GONÇALVES, Elisa Pereira. **Conversas sobre iniciação à Pesquisa Científica**. 4. ed. Campinas, SP: Alínea, 2007. p 96. Disponível em: <http://bds.unb.br/handle/123456789/373>. Acesso: 19/01/2023.

MCKENZIE, Timothy M. **Is cyber deterrence possible?** Alabama: Air University Press, Air Force Research Institute, 2017. Disponível em: <https://apps.dtic.mil/sti/pdfs/AD1122446.pdf>. Acesso: 19/01/2023.

MOFARRAH, Abdullah; HUSAIN, Tahir, HAWBOLDT, Kelly; VEITCH, Brian. Decision-making tool for produced water management. In: **Produced water**. Springer, New York, NY, 2011. p. 573-586.

MOREIRA, Miguel Ângelo Lellis; DOS SANTOS, Marcos; GOMES, Carlos Francisco Simões. **SADEMON: uma plataforma computacional web para o método SAPEVO-M**. Disponível em: <https://www.researchgate.net/profile/Marcos-Santos-85/publication/358425911_SADEMON_uma_plataforma_computacional_web_para_o_metodo_SAPEVO-

M/links/62023aca04acd5476f6e9886/SADEMON-uma-plataforma-computacional-web-para-o-metodo-SAPEVO-M.pdf>. Acesso: 19/01/2023.

SMITH, Zhanna Malekos; LOSTRI, Eugenia; LEWIS, James A. The Hidden Costs of Cybercrime. **MCAFFE. 2020**. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>. Acesso em: 10.04.2022.

TEN, Chee-Wooi, MANIMARAM, Govindarasu; LIU, Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. **IEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans**, 40(4), 853–865, 2010. Disponível em: <https://ieeexplore.ieee.org/abstract/document/5477189>. Acesso em: 10.09.2022.

Anexo "A"
Levantamento para apoio à Aquisição Firewall UTM

Nome do Fabricante: _____

Responsável pelo preenchimento: _____

Contato do responsável pelo preenchimento: _____

Tempo que levou para responder o levantamento: _____

Item	Descrição	Atende	Observações
1	Throughput 3Gbps Throughput (UDP) 40 Gbps IPS Throughput de 10Gbps VPN Throughput (IPSEC/SSL) de 8Gbps Webfilter Throughput (HTTP/HTTPS SSL Inspection) de 10/3Gbps Mínimo de 8 (oito) portas		
2	Suporte Técnico – remoto 14 horas x 6 dias, por 36 meses		
3	Solução de Gerenciamento Centralizado de Firewall		
4	Suporte on-site em todas as regiões do Brasil		
5	Suporte on-site na área do RJ/SP/BSB		
6	Permite arquitetura redundante e balanceada		
7	Possui plataforma de Inteligência de Ameaças		
8	Possui NOC/SOC na América do Sul		
9	Possui rotina de atualização da solução		
10	Possui rotina de atualização de patches		
11	Valor da Caixa stand-alone		
12	Valor das Caixas em sistema de balanceamento e redundância		

Observações:

1) Solicito, por favor, que encaminhe juntamente com o levantamento materiais para consulta e indicações de site para confirmação das informações.
2) Em se tratando de uma pesquisa acadêmica, a resposta é oportuna se for encaminhada em um prazo de até 2 (duas) semanas do recebimento deste formulário.