LIII Simpósio Brasileiro de Pesquisa Operacional
João Pessoa - PB, 3 a 5 de novembro de 2021

Uso de Técnicas Multicritério para Escolha e Contratação de Provedores de Nuvens Seguros*

Ademir Cardoso da Silva
Universidade do Estado de Mato Grosso - UNEMAT
Av. Tancredo Neves, 1095, Bairro Cavalhada III, Cáceres - MT - Brazil
ademir.cardoso@unemat.br

Antonio Augusto de Aragão Rocha
Universidade Federal Fluminese - UFF
Rua Passo da Pátria, 156, Instituto de Computação, Bairro São Domingos, Niterói - RJ - Brazil
arocha@ic.uff.br

RESUMO

A Computação em Nuvem apresenta vantagens significativas por prover escalabilidade, flexibilidade e disponibilidade sob demanda. Porém, sua adesão ainda apresenta resistência, devido: (a) Ameaças e vulnerabilidades de segurança, existentes em soluções tradicionais, potencializadas pela complexidade e heterogeneidade das configurações relacionadas à Arquitetura (ARQ), Privacidade (PRI) e Conformidade (CONF); (b) Grande quantidade de serviços oferecidos pelos provedores, tornando a escolha um processo complexo. Propomos auxiliar o cliente na escolha de provedor de nuvem seguro aplicando o Método de Decisão Multi-Critério (MCDM) chamado Processo Hierárquico Analítico (AHP), baseado nos critérios de segurança quanto a ARQ, PRI e CONF, aumentando a confiança na contratação e apoiando na construção de Acordos de Níveis de Serviço Voltados à Segurança (Sec-SLA).

PALAVRAS CHAVE. MCDM, AHP, Privacidade, Conformidade, Segurança, SLA.

Apoio à Decisão Multicritério, PO em Telecomunicações e Sistemas de Informações

ABSTRACT

Cloud Computing presents significant advantages by providing scalability, flexibility, and on-demand availability. However, its adherence still presents resistance, due to: (a) Security threats and vulnerabilities in traditional solutions are enhanced by the complexity and heterogeneity of the ARQ, Privacy (PRI) and Conformity (CONF) configurations; (b) The large number of services offered by providers make choice a complex process. We propose to assist the client in choosing a secure cloud provider by applying the Multi-Criteria Decision Making (MCDM) called Analytic Hierarchy Process (AHP) based on the security criteria for ARQ, PRI and CONF, increasing confidence in hiring and supporting the construction of Security Service Level Agreements (Sec-SLA).

KEYWORDS. MCDM, AHP. Privacy, Conformity, Security, SLA.

Apoio à Decisão Multicritério, PO em Telecomunicações e Sistemas de Informações

*This work is partially funded by FAPESP (grant 2015/24144-7).

1. Introdução

A computação em nuvem vem sendo adotada tanto como uma solução para a redução de custos em Tecnologia da Informação (TI) quanto como uma facilitadora da flexibilidade de servidores. No entanto, sua adoção requer um estudo prévio dos assuntos que tangem sua eficiência e garantias da segurança.

Visando sanar as principais preocupações referentes à confidencialidade, integridade e disponibilidade, e garantir sua qualidade, é desejável que durante o processo de implementação de um serviço em nuvem sejam estabelecidos acordos de níveis de serviço. Um desses acordos, conhecido pela sigla SLA (*Service Level Agreement*), documenta as exigências e regras de negócios do cliente, avalia todos os aspectos do serviço e firma as responsabilidades dos envolvidos. Além desse acordo, consumidores devem também considerar o Sec-SLA, referente aos níveis de segurança do serviço, os quais requerem análises específicas para cada tipo de arquitetura de hospedagem na nuvem.

Como a nuvem hospeda dezenas de milhares de serviços online, os ataques a eles visam explorar vulnerabilidades. Metade desses serviços recebem ataques de negação de serviço distribuído ou DDoS, e 94% sofrem regularmente outros tipos de ataques [Arcuri et al., 2017; Jouini e Rabai, 2016; Miao et al., 2015]. Considerando que sua frequência aumenta conforme o serviço é mais utilizado, o problema tende a crescer, uma vez que, de acordo com a *International Data Corporation* - IDC, 50% de todo o volume de dados no planeta estará na nuvem entre 2020 e 2025 [Bayard, 2017].

A partir da análise dos tipos, características e padrões de ataques [Miao et al., 2015] e as principais medidas de mitigação e solução [Gonzalez et al., 2012] a serem incluídas no Sec-SLA, o presente artigo visa minimizar os riscos de segurança na nuvem utilizando MCDM (Tomada de Decisão de Múltiplos Critérios) com AHP (Processo de Análise Hierárquica). Para isso, seu objetivo envolve responder as seguintes questões fundamentais: (i) Como os consumidores da nuvem podem ser apoiados na escolha de um provedor que garanta maior confiança na entrega dos serviços contratados? (ii) Como o grau de confiança de provedores podem ser medido?

2. Medindo a confiança na nuvem

Para realizar a medição da segurança na nuvem, nesse artigo são calculadas medidas de segurança quanto à arquitetura (ARQ), privacidade (PRI) e conformidade (CONF) associadas à taxonomia resumida, conforme modelo proposto em [Gonzalez et al., 2012]. O cálculo considera a presença de categorias e subcategorias Si, as quais dizem respeito às medidas de proteção e mitigação adotadas pelo provedor, definidas em seu Catálogo de Serviço, vide Tabela 8. Para isso, é utilizado como inspiração o trabalho de [Silva et al., 2019], o qual segue as seguintes etapas: (i) definição de responsabilidades no perímetro de segurança da nuvem entre cliente e provedor; (ii) atribuição de um valor de risco para as medidas de mitigação e solução dos principais padrões de ataques na nuvem (Si); (iii) definição de um método abstrato para apoiar os consumidores da nuvem na distribuição de peso; e, (iv) proposição de um modelo heurístico para o cálculo de confiança em provedores de nuvem.

Procuramos definir a segurança da informação como uma área do conhecimento dedicada à proteção de ativos de informação contra acesso não autorizado ou indisponibilidade. Assumiu-se que o consumidor já definiu o modelo de nuvem em relação à implantação e ao serviço. Portanto, para cada modelo de nuvem escolhido, a confiança na nuvem foi calculada pelos seguintes itens: Medidas de segurança para a arquitetura (ARQ), Privacidade (PRI) e Conformidade (CONF), associadas à taxonomia resumida, como proposto em [Gonzalez et al., 2012]. Por exemplo, [Gonzalez

et al., 2012] consideram que as medidas de segurança para ARQ estão subdivididas em três categorias: segurança de rede, interface e virtualização. Essas categorias estão relacionadas às subcategorias (Si): solução e mitigação de questões de segurança. O firewall (S2), por exemplo, corresponde a uma medida de solução e mitigação da categoria de segurança de rede.

Podemos constatar, com base na literatura, documentos produzidos por empresas e organizações que estudam com exclusividade aplicações e implementações MCDM, como é o caso da International Society on MCDM, que se trata de um método consolidado, aplicado em diversas áreas do conhecimento. Em nosso estudo pudemos comprovar sua eficácia no tocante a escolha de fornecedores de serviços de nuvem baseado em critérios de segurança. Deve-se destacar que a vantagem principal do AHP é a habilidade inerente de manipular fatores intangíveis, fatores esses determinantes para o processo de decisão.

3. Tomada de Decisão de Múltiplos Critérios e Processo de Análise Hierárquica

No contexto atual, um dos principais objetivos do MCDM é projetar ferramentas matemáticas e computacionais para selecionar a melhor alternativa dentre várias opções, com relação a critérios específicos. Dadas as dificuldades, de clientes, em escolher serviços em nuvem, diante da variedade de provedores e serviços disponíveis, o método é testado em cenários com diferentes modelos de nuvem para a identificação do que mais se adequa às especificidades de uma determinada empresa [Şener et al., 2017].

Embora existam diversos métodos MCDM difundidos e utilizados, esse trabalho utiliza o AHP, desenvolvido por Thomas L. Saaty em 1980. Sua técnica é estruturada para tomada de decisão em ambientes complexos em que diversas variáveis ou critérios são considerados para a priorização e seleção de alternativas. Permite aos decisores a quantificação numérica de seus julgamentos subjetivos, dando ampla visão da importância relativa dos fatores que estão sob análise. O resultado é obtido por meio da comparação paritária dos critérios, subcritérios e alternativas [Saaty, 1991]. O problema de decisão multicritérios é evidenciado quando há a necessidade da escolha de uma alternativa entre duas ou mais, onde o desejo é atender a múltiplos objetivos que na maior parte das vezes são conflitantes entre si. A estes objetivos estão associados variáveis ou critérios que nos possibilita avaliar cada alternativa.

A aplicação do método AHP começa pela decomposição do problema em uma hierarquia de critérios mais facilmente analisáveis e comparáveis de modo independente, Figura 1. A partir do término da construção da hierarquia lógica, os decisores avaliam sistematicamente as alternativas por meio da comparação, de duas a duas, dentro de cada um dos critérios. Essa comparação pode usar dados concretos das alternativas ou julgamentos humano como forma de informação subjacente [Saaty, 2008]. É preciso realizar um cruzamento entre critérios com alternativas e critérios com objetivo final [Briozo e Musetti, 2015].

O AHP transforma as comparações, muitas vezes empíricas, em valores numéricos que são processados e comparados. O peso de cada um dos fatores permite a avaliação de cada um dos elementos dentro da hierarquia definida. Essa capacidade de conversão de dados empíricos em modelos matemáticos é o principal diferencial do AHP com relação a outras técnicas comparativas. Após a realização de todas as comparações os pesos relativos entre os critérios avaliados é estabelecido, a probabilidade numérica de cada alternativa é calculada. Essa probabilidade é o que determina a importância da alternativa, ou seja, a possibilidade que a alternativa tem de atender a meta estabelecida. Quanto maior a probabilidade, mais a alternativa contribui para o objetivo final.

Aplicaremos o MCDM com AHP para a proposta de [Gonzalez et al., 2012], onde foi desenvolvido uma taxonomia de segurança em nuvem para solução/mitigação levando em consideração os riscos, ameaças e vulnerabilidades apresentados em referências importantes, reconhecidas mun-

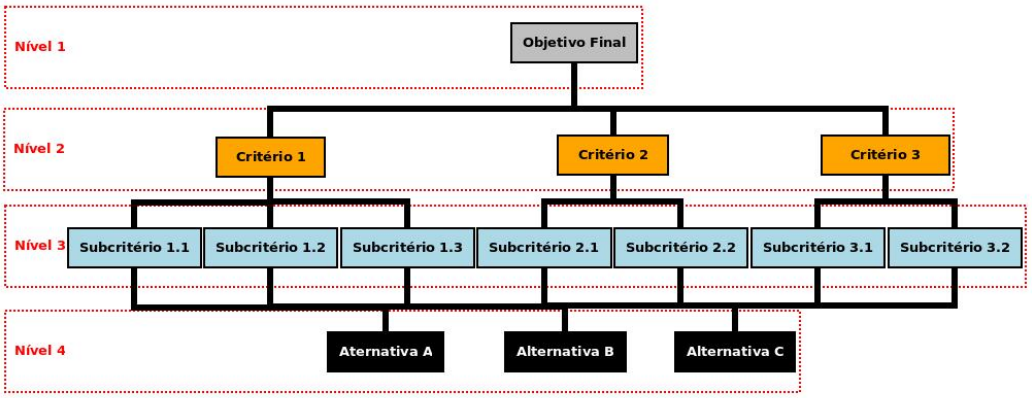


Figura 1: Representação gráfica de uma hierarquia

dialmente, utilizadas para reunir informações relevantes e organizá-las em categorias hierárquicas, com o objetivo de criar um modelo de segurança para estudar aspectos relacionados a segurança na computação em nuvem e apoiar a tomada de decisão.

Na Figura 1 visualiza-se a representação da estruturação de uma hierarquia para a resolução de um problema por meio do método AHP: tem-se no Nível 1 o "Objetivo Final"; no Nível 2, apresentam-se os "Critérios"; no Nível 3, os "Subcritérios"; e no Nível 4, as "Alternativas". Os níveis hierárquicos podem ser inseridos conforme haja necessidade, bem como a criação ou a exclusão de um determinado critério, isto garante uma certa flexibilidade na estrutura.

Definição das Alternativas: Como demonstração do método proposto neste trabalho, analisaremos a segurança para ARQ, PRI e CONF, de três das maiores potências mundiais em serviços de Nuvem [Canaltech, 2015], beseando-se em análise de dados obtidos pela **CloudHarmony** [1]. Para elas, a Amazon foi considerada a melhor empresa do setor por ter permanecido com suas plataformas fora do ar o menor tempo possível, seguida pela Google e Microsoft. Na visão das empresas, os clientes de qualquer uma das três companhias, que são o topo do ranking, trazem serviços de extrema qualidade e, pelo menos no que se refere a confiabilidade em relação à disponibilidade, que é uma característica fundamental dos provedores de nuvem, estão plenamente capacitadas para concorrer entre si pelas soluções dos usuários. Sendo assim, definimos como supostas alternativas de escolha os seguintes provedores: Amazon Web Service, Google Cloud Platform e Microsoft Azure. Estes serão submetidos a uma avaliação mais abrangente de segurança, de acordo com o conhecimento técnico do autor deste trabalho, utilizando a hierarquia de critérios elaborada em [Gonzalez et al., 2012].

A comparação entre dois elementos utilizando o AHP pode ser realizada de diferentes formas [Triantaphyllou, 2000]. No entanto, a escala de relativa importância entre duas alternativas propostas por [Saaty, 1991] é a mais amplamente utilizada Tabela 1. Atribuindo valores que variam entre 1 a 9, a escala determina a importância relativa de um critério em relação ao outro, esta comparação dá origem a uma nova tabela com os resultados, como mostra a Tabela 2. Geralmente costuma-se priorizar os números ímpares da escala de Saaty, Tabela 1, para assegurar razoável diferença entre os pontos da medição. Os números pares são adotados somente no caso de não houver um consenso natural entre os avaliadores, neste caso, será necessário atribuir um ponto intermediário como solução negociada [Saaty, 1991].

A partir da escala de Saaty é construída a matriz de julgamento, Tabela 3. Para exem-

[1] organização destinada a medir a confiabilidade de serviços de computação na nuvem utilizando informações sobre disponibilidade dos serviços oferecidos pelas empresas, levando em conta os períodos de indisponibilidade e quedas de serviço ao longo do ano.

Tabela 1: Escala fundamental de números absolutos

Importância	Definição	Explicação
1	Igual importância	As duas atividades contribuem igualmente para o objetivo.
3	Importância moderada	A experiência e o julgamento favorecem levemente uma atividade.
5	Forte importância	A experiência e o julgamento favorecem fortemente uma atividade.
7	Importância muito forte	Uma atividade é muito fortemente favorecida.
9	Absoluta importância	A evidência favorece uma atividade com alto grau de certeza.
2, 4, 6, 8	Valores intermediários	Quando se procura uma condição de compromisso entre duas definições.

plificar os cálculos do AHP na priorização de provedores de nuvem, avaliaremos a segurança dos principais servidores de nuvem sob os critérios de segurança quanto a ARQ, PRI e CONF. Na medida em que é desenvolvido faremos as devidas abordagens sobre o assunto.

Como discutido anteriormente, frisamos que o primeiro passo da construção do AHP está na determinação dos critérios que serão utilizados e cada organização desenvolve o seu conjunto de critérios de acordo com os objetivos estratégicos organizacionais. Após a definição dos critérios e hierarquia realizamos os julgamentos comparativos par a par dos critérios em relação ao Objetivo Final. Neste caso, temos o Objetivo Final no topo da hierarquia ou 1º Nível. Aplicamos o método AHP ao 2º Nível da hierarquia onde estão os critérios Arquitetura (ARQ), Privacidade (PRI) e Conformidade (CONF), como mostra a Figura 2. Visando determinar a importância relativa entre eles e seu peso para o objetivo geral.

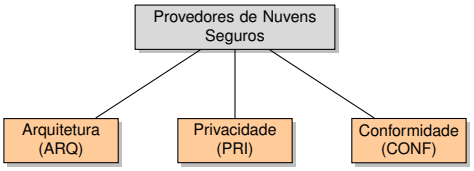


Figura 2: Hierarquia Níveis 1 e 2

Tabela 2: Julgamento paritário do nível 2

Índice de Importância									**=**	**Índice de Importância**								
Arquitetura	9	8	7	6	5	4	**3**	2	1	2	3	4	5	6	7	8	9	Privacidade
Arquitetura	9	8	7	6	**5**	4	3	2	1	2	3	4	5	6	7	8	9	Conformidade
Privacidade	9	8	7	6	5	4	3	**2**	1	2	3	4	5	6	7	8	9	Conformidade

Tabela 3: Matriz de julgamento

	Arquitetura	Privacidade	Conformidade
Arquitetura	1	3	5
Privacidade	1/3	1	2
Conformidade	1/5	1/2	1
$\sum$ **(w)**	**1,533**	**4,5**	**8**

Normalização da Matriz de Julgamento: A normalização dos valores obtidos na matriz tem por objetivo igualar todos os julgamentos a uma mesma unidade de medida. Obtém-se através da divisão de cada elemento da matriz de julgamento original pelo somatório dos julgamentos da sua respectiva coluna, Tabela 4.

Tabela 4: Normalização da Matriz de Julgamento

	Arquitetura	Privacidade	Conformidade	**AutoVetor**
Arquitetura	1 / 1,533 = 0,652	3 / 4,5 = 0,667	5 / 8 = 0,625	1,944
Privacidade	(1 / 3) / 1,533 = 0,217	1 / 4,5 = 0,222	2 / 8 = 0,25	0,689
Conformidade	(1 / 5) / 1,533 = 0,13	(1 / 2) / 4,5 = 0,111	1 / 8 = 0,125	0,366
$\sum$	**1**	**1**	**1**	**2,999**

A determinação da contribuição de cada critério para o objetivo final é calculado a partir do **Vetor de Prioridades** ou **Vetor de Eigen**. O Vetor de Eigen apresenta os pesos relativos entre

critérios e é obtido de modo aproximado[2] através da média aritmética dos valores de cada um dos critérios, conforme apresentado nas Tabelas 5 e 6. Os valores encontrados para o vetor de Eigen tem significado físico direto no AHP, pois determina a participação ou o peso daquele critério em relação ao objetivo geral.

Tabela 5: AutoVetor Normalizado

AutoVetor	**AutoVetor Normalizado**
1,944	1,944 / 2,999 = 0,648
0,689	0,689 / 2,999 = 0,230
0,366	0,366 / 2,999 = 0,122
2,999	**1**

Tabela 6: Vetor de Prioridades

Alternativas	**Cálculo da Média**	**AutoVetor Normalizado (T)**	**AutoVetor (%)**
Arquitetura	(0,652 + 0,667 + 0,625) / 3	0,648	64.80%
Privacidade	(0,217 + 0,222 + 0,25) / 3	0,230	23.00%
Conformidade	(0,13 + 0,111 + 0,125) / 3	0,122	12.20%
$\sum$		**1**	**100%**

O próximo passo é verificar a inconsistência dos dados, a fim de verificar se os tomadores de decisão foram consistentes nas suas opiniões para a tomada de decisão.

Cálculo do AutoValor Máximo: Para realizar o cálculo do autovalor máximo faz-se a multiplicação da matriz original pela matriz do AutoVetor Máximo.

Matriz julgamento inicial x AutoVetor Máximo

$$\begin{bmatrix} 1 & 3 & 5 \\ 1/3 & 1 & 2 \\ 1/5 & 1/2 & 1 \end{bmatrix} \times \begin{bmatrix} 0,648 \\ 0,230 \\ 0,122 \end{bmatrix} \rightarrow \begin{bmatrix} 1*(0,648)+3*(0,230)+5*(0,122) \\ 1/3*(0,648)+1*(0,230)+2*(0,122) \\ 1/5*(0,648)+1/2*(0,230)+1*(0,122) \end{bmatrix} = \begin{bmatrix} 1,948 \\ 0,690 \\ 0,367 \end{bmatrix}$$

$\sum = 1,948 + 0,690 + 0,367$

$\sum = 3,005$ **(AutoValor Max ou λmax)**

Cálculo do Índice de Consistência (**CI** = *Consistency Index*): Este índice mede a consistência das comparações. Aconselha-se que fique abaixo de 0,10.

$CI = \frac{\lambda max - n}{(n-1)}$ Onde: $CI = (\lambda max - n)/(n-1)$

$CI = (3,005–3)/(3-1)$

$CI = 0,005/2$

$CI = 0,003$

Cálculo da Razão de Consistência (**CR** = *Consistency Ratio*):

Por fim, calcula-se a Razão de Consistência – CR, do julgamento do avaliador. Este cálculo também considera um erro aleatório, que está relacionado com a ordem da matriz, dado pelo Índice de Consistência Aleatória (**RI** = *Random Consistency Index*) [Saaty, 1991]. Recomenda-se que o julgamento do avaliador seja refeito caso o resultado do cálculo seja maior que 0,10. Para se Calcular o CR, utiliza-se a Equação: $CR = \frac{CI}{RI}$ Onde: $CR = CI/RI$

$CR = 0,003/0,58$

$CR = 0,004$

A Tabela 7 apresenta o Índice de Consistência Aleatória para matrizes de ordem 1 a 10.

[2]O cálculo exato do vetor de Eigen é determinado apenas em casos específicos. A maioria dos casos práticos utiliza essa aproximação visando simplificar o processo de cálculo, uma vez que a diferença entre o valor real e o valor aproximado é inferir a 10% [Kostlan, 1991]

Tabela 7: Índice de Consistência Aleatória

Ordem da Matriz	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Fonte: Adaptado de [Saaty, 1991]

De forma análoga todos os subcritérios da hierarquia deverão ser submetidos aos mesmos tipos de julgamentos e cálculos até que seja apresentado os pesos de cada critério e também o resultado com a classificação de todos os servidores.

No caso, os próximos passos seriam realizar os procedimentos sucessivamente para os subcritérios dos critérios Arquitetura, Privacidade e Conformidade, respectivamente, como pode ser observado na Figura 3. Depois, o método AHP, deverá ser aplicado aos Subcritérios da Arquitetura (ARQ): Segurança de Rede, Interface e Virtualização. De igual forma aos Subcritérios do critério Privacidade (PRI): Segurança de Dados e Aspectos Jurídicos e finalmente aos Subcritérios de Privacidade (PRI): Serviços e Provedores.

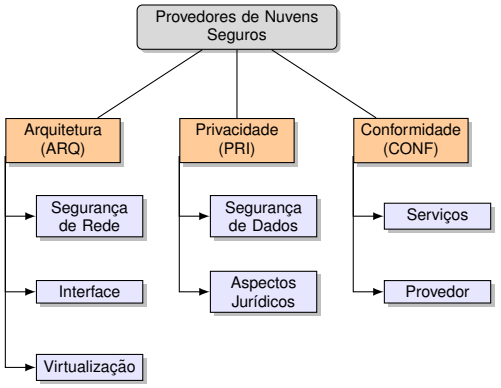


Figura 3: Hierarquia Níveis 1, 2 e 3
Fonte: Adaptado de [Gonzalez et al., 2012]

Também realizamos a aplicação do método AHP nos níveis inferiores (ramificações da hierarquia), bem como nas alternativas. O resultado dos pesos pode ser visto na Figura 4. De acordo com a Figura 5 podemos observar o ranqueamento dos provedores de serviços de nuvem, lembrando que os julgamentos realizados pelo autor se baseiam em experiências, diagnósticos e análises feitas observando divulgações de especialistas na internet, obras da literatura, manuais técnicos etc. a fim de nos permitir potencial técnico suficiente nos capacitando a realizar avaliações dos provedores na entrega de determinados serviços na nuvem. Nosso foco principal é avaliar a segurança de serviços oferecidos por provedores de nuvem e apresentar uma metodologia consistente capaz de auxiliar futuros clientes da nuvem na escolha de um provedor que inspire confiança. Sendo assim, baseado na aplicação do método proposto, chegamos a um ranqueamento final, onde o provedor da Google ficou com 38% de peso ao considerar os critérios de segurança analisados neste trabalho, o Amazon em segundo com 37,2% seguido pela Microsof. Os resultados foram obtidos utilizando o sistema AHP Online System [Goepel, 2018].

4. Estudo de Caso e análise (Cenário: Nuvem Pública SaaS)

Nesta seção é apresentado o estudo de caso, a partir da definição de um modelo abstrato, que nos permite conhecer, dentre um determinado número de provedores de nuvem, o mais confiável.

Catálogo de Serviço: O Catálogo de Serviço é um instrumento que permite fornecer uma fonte única e organizada de todos os serviços oferecidos pelos provedores na nuvem. O gerenciamento de SLA prevê a função do Catálogo de Serviços como base na implantação da gestão de

Decision Hierarchy

Level 0	Level 1	Level 2	Level 3	Glb Prio.	Amazon Web Service (AWS)	Google Cloud Platform	Microsoft Azure
Seleção de Provedor Seguro AHP	Arquitetura 0.648 AHP	Segurança de Rede 0.571 AHP	Transferência de Dados 0.137	5.1%	0.648	0.230	0.122
			Firewall 0.625	23.2%	0.571	0.286	0.143
			Configurações 0.238	8.8%	0.126	0.458	0.416
		Interface 0.143 AHP	API 0.342	3.2%	0.163	0.297	0.540
			Interface Administrativa 0.364	3.4%	0.111	0.222	0.667
			Interface do Usuário 0.204	1.9%	0.122	0.230	0.648
			Autenticações 0.090	0.8%	0.309	0.582	0.109
		Virtualização 0.286 AHP	Isolamento 0.393	7.3%	0.458	0.416	0.126
			Vulnerabilidades do Hypervision 0.086	1.6%	0.222	0.667	0.111
			Vazamento de Dados 0.340	6.3%	0.109	0.582	0.309
			Identificação de VM 0.086	1.6%	0.109	0.582	0.309
			Ataques Cross-VM 0.095	1.8%	0.109	0.582	0.309
	Privacidade 0.230 AHP	Segurança de Dados 0.750 AHP	Criptografia 0.308	5.3%	0.443	0.387	0.169
			Redundância 0.615	10.6%	0.286	0.571	0.143
			Eliminação de Dados 0.077	1.3%	0.416	0.126	0.458
		Aspectos Jurídicos 0.250 AHP	Localização dos Dados 0.130	0.7%	0.540	0.297	0.163
			Pesquisas e Conhecimento 0.138	0.8%	0.333	0.333	0.333
			Controle de Riscos 0.732	4.2%	0.309	0.582	0.109
	Conformidade 0.122 AHP	Serviços 0.750 AHP	SLA 0.187	1.7%	0.230	0.122	0.648
			Falhas ou Desastres 0.715	6.5%	0.571	0.286	0.143
			Auditoria 0.098	0.9%	0.458	0.416	0.126
		Provedor 0.250 AHP	Controle de Dados 0.300	0.9%	0.625	0.238	0.137
			Controle de Segurança 0.100	0.3%	0.216	0.103	0.682
			Bloqueio dos Dados (Lock-in) 0.600	1.8%	0.216	0.103	0.682
OK. Submit for group eval or alternative eval. Alternatives				1.0	37.2%	38.2%	24.6%

Figura 4: Resultado da aplicação do método AHP para todos os critérios

	Category	Priority	Rank
1	Amazon Web Service (AWS)	37.2%	2
2	Google Cloud Platform	38.2%	1
3	Microsoft Azure	24.6%	3

Figura 5: Ranqueamento dos provedores mais seguros

serviços de TI. Trata-se do detalhamento dos serviços ofertados pelo provedor em que se delimita o que pertence e o que não pertence ao escopo, bem como os elementos que compõem aquela entrega: tempo de atendimento, custo do serviço, cliente e a entidade responsável pela manutenção do serviço, entre outros. O conteúdo do Catálogo de Serviços pode variar de acordo com os requisitos da organização consumidora.

Faremos uma avaliação do Cenário hipotético criado para uma Nuvem Pública SaaS, provedores, categorias e subcategorias (Si) apresentadas das medidas de prevenção a ataques oferecidos, onde clientes de distintas necessidades de modelos de nuvem buscam o provedor de nuvem que forneça o maior grau de confiança. Os julgamentos no método AHP, cuja finalidade é apoiar o consumidor na escolha do provedor mais confiável para os serviços oferecidos em ARQ, PRI e CONF, foi realizado a partir do conhecimento técnico do autor deste trabalho, de acordo com o método apresentado na Seção 3.

O método AHP apresentado neste trabalho não será aplicado para os Subcritérios (Si):

Tabela 8: Catálogos de Serviço

MÉTRICAS	CATEGORIA	SUBCATEGORIA (Si)	A	B	C	D
Arquitetura (ARQ)	Segurança de Rede	S1 – Transferência de Dados	√		√	
		S2 – Firewall	√	√	√	√
		S3 – Configurações	√	√	√	
	Interface	S4 – API		√	√	
		S5 – Interface Administrativa	√	√	√	√
		S6 – Interface do Usuário	√	√		
		S7 – Autenticação	√	√	√	√
	Virtualização	S8 – Isolamento	√	√	√	√
		S9 – Vulnerabilidades do Hypervisor	√	√	√	
		S10 – Vazamento de Dados		√	√	
		S11 – Identificação de VM	√	√	√	√
		S12 – Ataques Cross-VM	√			
Privacidade (PRI)	Segurança de Dados	S13 – Criptografia	√	√	√	√
		S14 – Redundância	√	√	√	√
		S15 – Eliminação de Dados	√			√
	Aspectos Jurídicos	S16 – Localização dos Dados		√	√	
		S17 – Legislação/E-discovery		√	√	
		S18 – Controle de Riscos		√	√	
Conformidade (CONF)	Serviços	S19 – SLA	√	√	√	√
		S20 – Falhas ou Desastres	√	√	√	
		S21 – Auditoria			√	

ARQ: S2 - Firewall, S5 - Interface Administrativa, S7 - Autenticação, S8 - Isolamento e S11 - Identificação da VM; **PRI**: S13 - Criptografia, S14 - Redundância; e **CONF**: S19 - SLA. Isto se dá pelo fato de estarem presentes em todos os provedores hipotéticos criados (A, B, C e D), ou seja, o julgamento pelo método AHP, bem como o peso das subcategorias de segurança, não irá interferir no resultado final para a escolha de um provedor em detrimento de outro, conforme Tabela 8.

Cenário - Nuvem Pública SaaS: Considera-se neste cenário que uma organização consumidora necessite de um provedor para utilizar uma aplicação de correio eletrônico em uma nuvem pública, definindo como prioridades: disponibilidade a todos os funcionários da organização a um menor custo de hospedagem. Visto que a arquitetura deverá ser compartilhada com outros consumidores para atender ao menor custo de hospedagem, além de garantir uma maior disponibilidade, [Silva et al., 2019] relaciona os métodos mais importantes para este cenário. Por se tratar de uma aplicação que necessita de alta disponibilidade, a subcategoria "SLA" (que inclui garantias de maiores taxas de transferência de pacotes na rede, menor atraso e perdas) foi definida em nosso julgamento como a mais prioritária, ou seja, com maior importância em relação aos subcritérios comparados, sendo a ela atribuído o peso de 25%.

A aplicação a ser hospedada, correio eletrônico web, tem por finalidade ser utilizada por todos os funcionários da empresa como ferramenta de envio e recebimento de mensagens, homologada e autorizada pela mesma. Com isso, as próximas Si definidas como prioritárias foram: "Criptografia" (para proteger as informações sensíveis transmitidas) e "Redundância" (que define regras de armazenamento, preservação e destruição das bases de dados que compõem esta aplicação), ambas avaliadas com valor de importância igual a 11,7% cada, sendo consideradas a segunda mais importante, uma vez que a empresa busca uma hospedagem de menor custo. Buscando garantir a entrada e saída segura de dados pela internet, para este cenário o "Firewall" foi considerado com 7,7% de importância, terceiro na ordem de prioridade.

Posteriormente, as próximas quatro Si escolhidas como prioritárias foram: "Eliminação de Dados", 4,2%, "Autenticação", 3,3%, "Interface Administrativa", 3,3% e "Interface do Usuário",

3,3%, todas possuem uma forte relação de dependência com as duas Si, "Criptografia" e "Redundância", a estas quatro Si foram atribuídos peso ou valor de importância muito relevantes em relação às demais, sendo consideradas quarta e quintas Si mais prioritária em relação às vinte e uma relacionadas no Catálogo de Serviço.

Por fim, as Si "Transferência de Dados" e "Isolamento", também importantes por permitir enviar/receber mensagens e manter as bases destas mensagens eletrônicas em uma Nuvem Pública, com hardware e rede compartilhados. Definiu-se pesos menores em relação às demais Si por serem configurações que apresentam maior risco apenas na fase de implantação desta aplicação em Nuvem.

É importante ressaltar que aplicamos o julgamento do método AHP a todas as 21 Subcategoria de Si, porém os que representam maior peso para este Cenário são os 10 Si, considerados mais importantes para a Nuvem Pública SaaS por [Silva et al., 2019]. O ponto de vista que consideramos para dizer se um provedor é ou não mais satisfatório que o outro se deve ao peso, obtido por meio da aplicação do método AHP, e prestação do serviço pelo provedor em seu Catálogo de Serviços, Tabela 8. A partir da Tabela 9, que define as responsabilidades dos provedores, verificamos quais são as responsabilidades do provedor de uma nuvem Nuvem Pública - NP.

Tabela 9: Responsabilidades do Provedor

Modelo/Categoria	Segurança de Rede	Interface	Virtualização	Segurança de Dados	Aspectos Jurídicos	Serviços
NPL						
NPT	√	√	√	√	√	√
NCL						
NCT	√	√	√	√	√	√
NP	√	√	√	√	√	√
SaaS	√	√	√	√	√	√
PaaS	√		√		√	√
IaaS	√		√		√	√

Analisando o Catálogo de Serviços, Tabela 8, as Responsabilidades do Provedor de Nuvem, Tabela 9 e o peso atribuído às 10 Si consideradas mais importantes para a Nuvem Pública SaaS, chegamos aos resultados dos julgamentos apresentados na Figura 6.

Considerando o Cenário hipotético criado e o grau de importância do subcritério para este cenário, realizamos os julgamentos dos provedores pelo método AHP utilizando a escala de Saaty, conforme Tabela 1. O provedor que oferecer o maior número de Si em seu Catálogo de Serviço receberá valor 9, extrema importância em relação ao outro que não oferecer e no caso dos dois ofertarem ou não o serviço, a ambos será atribuído o valor 1, igual importância. Como os subcritérios: S2, S5, S7, S8, S11, S13, S14 e S19 estão presentes em todos os provedores hipotéticos criados A, B, C e D as suas comparações não influenciaram na confiança do provedor ou em sua escolha. As análises dos serviços foram realizadas pela existência ou não no Catálogo de Serviços e não de forma qualitativa. A maior parte destes serviços são considerados extremamente importante para o cenário criado.

De acordo com o Catálogo de Serviço, da Tabela 8, os provedores A e C oferecem o serviço S1 - Transferência de Dados, diferentemente dos provedores B e D. Sendo assim realizamos os julgamentos paritários considerando o grau de importância. De forma análoga, fizemos o julgamento de todos os Si em relação aos serviços prestados pelos provedores A, B, C e D, conforme consta no Catálogo de Serviços, como mostrado na Tabela 8.

5. Considerações finais

Comparando o método proposto neste trabalho, aplicação do método AHP para classificação e escolha de provedor confiável, com o método proposto por [Silva et al., 2019], que calcula a confiança dos provedores, podemos afirmar que apesar de obterem resultados semelhantes, utilizam métodos totalmente diferentes, entretanto, os resultados alcançados satisfazem os requisitos

Alternatives

No	Node	Criterion	Glb Priorities	Compare	A	B	C	D
1.	Arquitetura (ARQ)	S1 - Transferência de Dados	1.4%	AHP	0.450	0.050	0.450	0.050
2.		S2 - Firewall	7.7%	AHP	0.250	0.250	0.250	0.250
3.		S3 - Configurações	1.7%	AHP	0.321	0.321	0.321	0.036
4.		S4 - API	2.1%	AHP	0.050	0.450	0.450	0.050
5.		S5 - Interface Administrativa	3.3%	AHP	0.250	0.250	0.250	0.250
6.		S6 - Interface do Usuário	3.3%	AHP	0.450	0.450	0.050	0.050
7.		S7 - Autenticação	3.3%	AHP	0.250	0.250	0.250	0.250
8.		S8 - Isolamento	1.6%	AHP	0.250	0.250	0.250	0.250
9.		S9 - Vulnerabilidades do Hypervision	2.2%	AHP	0.321	0.321	0.321	0.036
10.		S10 - Vazamento de Dados	2.2%	AHP	0.050	0.450	0.450	0.050
11.		S11 - Identificação de VM	2.2%	AHP	0.250	0.250	0.250	0.250
12.		S12 - Ataques Cross-VM	2.2%	AHP	0.750	0.083	0.083	0.083
13.	Privacidade (PRI)	S13 - Criptografia	11.7%	AHP	0.250	0.250	0.250	0.250
14.		S14 - Redundância	11.7%	AHP	0.250	0.250	0.250	0.250
15.		S15 - Eliminação de Dados	4.2%	AHP	0.450	0.050	0.050	0.450
16.		S16 - Localização dos Dados	1.9%	AHP	0.050	0.450	0.450	0.050
17.		S17 - Pesquisa e Conhecimento	1.9%	AHP	0.050	0.450	0.450	0.050
18.		S18 - Controle de Riscos	1.9%	AHP	0.050	0.450	0.450	0.050
19.	Conformidade (CONF)	S19 - SLA	25%	AHP	0.250	0.250	0.250	0.250
20.		S20 - Falhas e Desastres	2.3%	AHP	0.321	0.321	0.321	0.036
21.		S21 - Auditoria	5.9%	AHP	0.083	0.083	0.750	0.083
				Total weight of alternatives:	0.253	0.256	0.288	0.202

All evaluations are completed.

Figura 6: NPSaaS - Resultado dos Julgamentos

	Category	Priority	Rank
1	A	25.3%	3
2	B	25.6%	2
3	C	28.8%	1
4	D	20.2%	4

Figura 7: NPSaaS - Ranqueamento

levantados nas duas propostas, uma vez que contribuem para o aumento da confiança do cliente possibilitando a escolha de provedores seguros, definição das responsabilidades e perímetro para a percepção da importância do SLA/Sec-SLA. Ao analisarem o mesmo Cenário de nuvem obtiveram a mesma sequência no ranqueamento dos provedores, quando classificados do mais confiável ao menos confiável.

Inspiramos nossa proposta na taxonomia apresentada por [Gonzalez et al., 2012] e primamos por mante-la na íntegra, por ser considerada de grande importância para a segurança em nuvens computacionais, também no intuito de manter uma padronização, já que foram identificados e classificados os principais problemas de segurança e soluções em Computação em Nuvem, a partir de publicações e referências de diferentes segmentos do setor **acadêmico** (documentos de conferências e revistas publicadas e instituídas pelo IEEE, ACM, Springer, Webscience e Scipress), **organizações** (CSA, NIST, ENISA, Gartner Group, KVM.org, OpenGrid, OpenStack, OpenNebula etc.) e **empresas** (ERICSSON, IBM, Xerox, Cisco, VMWare, Xen, Citrix, EMC, Microsoft e Salesforce).

Referências

Arcuri, M. C., Brogi, M., e Gandolfi, G. (2017). Cyber risk: a big challenge in developed and emerging markets. In *Identity Theft: Breakthroughs in Research and Practice*, p. 292–307. IGI Global.

Bayard, O. (2017). Por que a inovação armazenamento em nuvem faz tanto sucesso. https://tekideia.com/a-inovacao-armazenamento-em-nuvem-e-porque-o-sucesso/. Acessado em 18-08-2018.

Briozo, R. A. e Musetti, M. A. (2015). Método multicritério de tomada de decisão: aplicação ao caso da localização espacial de uma unidade de pronto atendimento–upa 24 h. *Gestão E Produção*, 22(4):805–819.

Canaltech, R. (2015). Amazon lidera lista de serviços cloud mais confiáveis. URL https://canaltech.com.br/computacao-na-nuvem/Amazon-lidera-lista-de-servicos-cloud-mais-confiaveis/.

Goepel, K. D. (2018). Implementation of an online software tool for the analytic hierarchy process (ahp-os). *International Journal of the Analytic Hierarchy Process*, 10(3).

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., e Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1):11.

Jouini, M. e Rabai, L. B. A. (2016). Threats classification: State of the art. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, p. 368–392. IGI Global.

Kostlan, E. (1991). Statistical complexity of dominant eigenvector calculation. *Journal of Complexity*, 7(4):371–379.

Miao, R., Potharaju, R., Yu, M., e Jain, N. (2015). The dark menace: Characterizing network-based attacks in the cloud. In *Proceedings of the 2015 Internet Measurement Conference*, p. 169–182. ACM.

Saaty, T. L. (1991). Método de análise hierárquica. *São Paulo: Makron*.

Saaty, T. L. (2008). Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process. *RACSAM-Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas*, 102(2):251–318.

Şener, U., Gökalp, E., e Eren, P. E. (2017). Cloudss: A decision support system for cloud service selection. In *International Conference on the Economics of Grids, Clouds, Systems, and Services*, p. 249–261. Springer.

Silva, A., Silva, K., Rocha, A., e Queiroz, F. (2019). Calculating the trust of providers through the construction weighted sec-sla. *Future Generation Computer Systems*.

Triantaphyllou, E. (2000). Multi-criteria decision making methods. In *Multi-criteria decision making methods: A comparative study*, p. 5–21. Springer.