Confiança na Nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço

Alternative Title:Trust in the Cloud from the Sec- SLA construction in various models as deployment and service

Kátia C. A. Silva
IC/UFF
Niterói - RJ - Brasil
katiasilva@ic.uff.br

Antonio A. A. Rocha
IC/UFF
Niterói - RJ - Brasil
arocha@ic.uff.br

Flávio Q. Guimarães
DCTIM da Marinha do Brasil
Rio de Janeiro - RJ - Brasil
queiroz@dctim.mar.mil.br

RESUMO

Um dos requisitos fundamentais para a consolidação da computação em nuvem, como solução robusta e confiável, é a segurança. As organizações que buscam adotar a nuvem como solução devem estar cientes que esta tecnologia herda todas as vulnerabilidades de segurança existentes em soluções tradicionais, aliadas à complexidade e heterogeneidade de suas configurações quanto à arquitetura, à privacidade e à conformidade deste novo modelo computacional. Ao impor práticas de gestão uniformes aos provedores quanto ao controle de segurança, com políticas de privacidade acordadas com seus clientes definidos em Acordo de Nível de Serviço de Segurança (*Security Service Level Agreements*), ou simplesmente *Sec-SLA*, espera-se que a nuvem seja capaz de melhorar seu controle e segurança, bem como obter respostas eficientes a incidentes. Propõe-se neste trabalho, um modelo para calcular a confiança de provedores a partir de medidas de solução e mitigação a incidentes de segurança oferecidas em seus catálogos de serviço.

Palavras-Chave

Nuvem, Confiança, *Sec-SLA*, *SLA*.

ABSTRACT

One of the fundamental requirements for cloud computing consolidation for a robust and reliable solution is security. Organizations looking to adopt the cloud as a solution should be aware that this technology brings all the problems that exist within the information security combined with the complexity and heterogeneity of your settings to provide confidentiality, integrity and system availability. To impose uniform management practices for providers and the security control, with privacy policies agreed with its customers defined in Security Service Level Agreement (Security Service Level Agreements), or simply *Sec-SLA*, it is expected that the cloud be able to improve your control and security and achieve efficient incident response. It is proposed in this paper a model to calculate the trust providers from solution and mitigation measures to security incidents offered in their service catalogs.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
SBSI 2016, May 17th-20th, 2016, Florianópolis, Santa Catarina, Brazil
Copyright SBC 2016.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection (D.4.6, K.4.2)

General Terms

Trust, Security, Risk

Keywords

Cloud, Trust, *Sec-SLA*, *SLA*.

1. INTRODUÇÃO

A adoção da computação em nuvem é vista como uma oportunidade para a redução dos investimentos em Tecnologia da Informação (*TI*), possibilitando maior flexibilidade na demanda por serviços e redução dos custos. No entanto, uma organização ao tomar a decisão de aderir a essa tecnologia deve considerar, além de seus benefícios, uma série de desafios de segurança a serem analisados e atribuídos a todos os envolvidos no modelo escolhido (tanto consumidores como provedores de serviços). A falta de definição quanto às questões de segurança e suas responsabilidades podem trazer reflexos negativos tanto para as organizações consumidoras dos serviços oferecidos pelos provedores da nuvem quanto para os usuários finais que fazem uso destes serviços.

O processo de contratação de um serviço de nuvem passa pelo estabelecimento de um Acordo de Nível de Serviço (*Service Level Agreement*), ou simplesmente *SLA*, com o provedor escolhido baseado nas demandas e regras de negócio do consumidor. O *SLA* trata-se de um contrato que formaliza as garantias que o provedor de serviço oferece em relação aos serviços contratados, a forma como estes níveis de serviço serão medidos, reportados e melhorados continuamente. O consumidor, ao analisar e estabelecer um *SLA* na nuvem, deve considerar e tratar não apenas os serviços tradicionais como, por exemplo, taxa de transferência de dados da rede, perda de pacotes ou atraso, mas também níveis de segurança com seus respectivos graus de complexidade. Estes níveis de segurança são conhecidos como *Sec-SLA*.

Em sistemas hospedados em centro de dados tradicionais, a preocupação com estes níveis de segurança a serem implementados se restringe a vulnerabilidades de acessibilidade, virtualização e aplicações web, como o *Structured*

Query Language (SQL) injection e *cross-site scripting* descritos em [11], além de questões de acesso físico, privacidade e controle de dados providenciando acesso às instalações e recursos para funcionários internos ou terceirizados. Porém, em se tratando de uma hospedagem na nuvem e de acordo com os modelos de implantação e de serviço, questões relacionadas com gestão de identidade e credenciais, verificação de dados, adulteração, integridade, confidencialidade, perda e roubo de dados, localização dos dados, autenticação do dispositivo monitorado ou qualquer outra forma de incidente de segurança devem ser analisadas de forma diferenciada para cada arquitetura.

De acordo com Subashini, S. et al.[21], à medida que o provedor da nuvem cuida apenas da parte inferior da arquitetura de segurança, os consumidores se tornam mais responsáveis por executar e gerir os recursos de segurança. No entanto, existe uma deficiência em *SLAs* estabelecidos na nuvem pela ausência de definição de responsabilidade entre consumidores e provedores nos níveis de *Sec-SLA*. Os provedores de nuvem geralmente afirmam que eles não são responsáveis pelos impactos de falhas de segurança, ou seja, por modificações não autorizadas, divulgações de dados ou interrupções de serviço causadas por atividades maliciosas. Frequentemente, os contratos de serviços são explícitos sobre a responsabilidade de riscos de segurança serem dos consumidores. Em alguns casos, os provedores prometem envidar seus melhores esforços para proteger os dados dos consumidores. Porém, todos os provedores pesquisados por Mell, P. et al.[15] assumem que a responsabilidade pela segurança em caso de violação de dados, perda de dados, ou interrupções de serviço é do consumidor, limitando-se a remediar com créditos de serviço, por incumprimento de "promessas" de disponibilidade.

Em [6] foi realizado um estudo denominado "Levantamento e análise de segurança de *SLAs* na Europa" que reforça esta deficiência em *SLA* na nuvem, não definindo responsabilidades quanto ao monitoramento e respostas a incidentes de segurança. A falta de definição de responsabilidades quanto aos níveis de *Sec-SLA* referentes à manutenção de segurança no armazenamento e transferência de dados na nuvem, tornam-se riscos que reduzem a confiança de consumidores nos serviços oferecidos pelos provedores. Já em [19] Pang, Y. et al. realizaram um estudo classificando os riscos na computação em nuvem referente a problemas de tecnologia, confiança, privacidade, integridade dos dados e falta de padronização.

O principal desafio deste trabalho é buscar respostas que minimizem os riscos na nuvem a partir das seguintes questões fundamentais: i) Como apoiar consumidores da nuvem na escolha do provedor que garanta uma maior confiança nos serviços a serem contratados? e ii) Como medir este grau de confiança? Destacam-se como principais contribuições:
1. A definição das responsabilidades de consumidores e provedores quanto ao controle e visibilidade de seus recursos a partir do modelo de nuvem e seu respectivo perímetro de segurança; e
2. A proposta de um modelo heurístico de cálculo da confiança em provedores com base em medidas de segurança referentes à arquitetura, privacidade e conformidade dos serviços oferecidos, considerando um valor de risco para cada medida de mitigação e solução dos principias padrões de ataques em sistemas computacionais.

O restante deste artigo está organizado da seguinte forma: Na Seção 2, enumera-se trabalhos relacionados à segurança e confiança na nuvem. Na Seção 3 apresenta-se um estudo sobre confiança na nuvem com base em medidas de mitigação e solução dos principais padrões de ataque nos sistemas de informação. A Seção 4 descreve a proposta desenvolvida neste trabalho para o cálculo da confiança no provedor de nuvem. Na Seção 5 buscou-se realizar uma análise comparativa de possíveis *Sec-SLA* a serem oferecidos por provedores e avaliados por consumidores. A validação do modelo abstrato do cálculo de confiança na nuvem é apresentada na Seção 6. Finalmente, na Seção 7, são expressas as considerações finais e trabalhos futuros.

2. TRABALHOS RELACIONADOS

Expõe-se nesta seção os trabalhos anteriores relevantes referentes à obtenção de confiança na nuvem. Os trabalhos em [5, 20, 21] fazem um estudo sobre a operacionalização, negociação e definição de *SLA*. Os trabalhos [13, 14] buscam medir a confiança utilizando simulação a partir de métricas de desempenho ou um repositório de *feedbacks* dos usuários para alguns modelos específicos como *Infrastructure as a Service* (*IaaS*) ou *Software as a Service* (*SaaS*). No entanto, não foram encontrados trabalhos que calculem a confiança e nem padronizem o *SLA* para segurança em nuvens nos seus diversos modelos.

O trabalho [21] afirma que os requisitos de *SLA* na nuvem variam de acordo com o modelo de serviço e implantação. Os autores em [12] ressaltam que a confiança na computação em nuvem está mais relacionada com a prevenção de uma violação de confiança do que com a garantia de compensação quando ocorrer a violação. Logo, o modelo de confiança de computação em nuvem deverá se concentrar mais na prevenção do insucesso do que na compensação de pós-fracasso. O trabalho [5] propõe uma arquitetura para criação, controle e monitoramento de *Sec-SLA*, onde define a construção de *Sec-SLA* em fases extraindo parâmetros das políticas de segurança dos próprios clientes. Porém, ressaltam a dificuldade em medir a segurança, além de deixarem claro que o modelo proposto é independente de qualquer tecnologia específica ou paradigma, como a nuvem computacional, podendo ser adaptado em trabalhos futuros. Parâmetros de políticas de segurança também são extraídos da legislação [7], de recomendações de segurança na nuvem [4, 22] e organizações como *National Institute of Standards and Technology (NIST)* [2] e *European Union Agency for Network and Information Security (ENISA)* [10].

Em [20] os autores apresentam uma arquitetura para monitoramento de segurança baseada em *Sec-SLA* para serviços *SaaS*, utilizam uma base de vulnerabilidades e atribuem aos níveis de segurança medidos, valores no intervalo de [0,4] que correspondem respectivamente a: Zero, Baixo, Médio, Alto e Crítico. No trabalho [14] a confiança na nuvem é calculada utilizando um repositório de reputação e *feedback* de usuários anteriores. Porém, cabe ressaltar que a nuvem oferece diversos serviços nos seus distintos modelos e esta reputação não é calculada considerando estas formas diferenciadas de hospedar ou consumir recursos na nuvem. Em [13] a confiança é medida por métricas de disponibilidade, integridade, eficiência e confidencialidade através do simulador *CloudSim*, considerando nas simulações apenas falhas de rede, e, não falhas ou indisponibilidades devido a incidentes de segurança que são as de maior risco para o conteúdo confiado à nuvem.

O trabalho [8] apresentou uma taxonomia onde 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, organizações e empresas. Inspirado na taxonomia apresentada em [8] o presente trabalho busca medir a confiança na nuvem, levando em consideração as falhas e os riscos quanto a violação de segurança em algumas das categorias/subcategorias confiadas ao provedor com base em padrões de ataques e suas medidas de mitigação e solução [3]. Com isso, este estudo tem como objetivo estabelecer níveis de segurança, com seus respectivos graus de complexidade, baseados nas políticas de segurança e regras de negócio do consumidor, diferentemente dos trabalhos [13, 14], que apenas estabeleceram o *SLA* que atenda as necessidades de capacidade como taxa de transferência de dados, perda de pacotes ou atraso da rede.

3. MEDINDO A CONFIANÇA NA NUVEM

Neste trabalho, buscou-se definir a segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Admitise que o modelo de nuvem quanto à implantação e quanto ao serviço encontra-se previamente definido pelo consumidor. Logo, para cada modelo de nuvem escolhido, a confiança na nuvem será calculada por medidas de segurança quanto à arquitetura (ARQ), à privacidade (PRI) e à conformidade ($CONF$), associadas à taxonomia resumida na Tabela 1, conforme proposto em [8], considerando a presença ou ausência de suas categorias e subcategorias S_i, onde i é o número de referência da subcategoria. Para exemplificar, Gonzalez et al. [8] considera que as medidas de segurança quanto a ARQ são subdivididas nas categorias de segurança de rede, interface e virtualização, as quais estão relacionadas com subcategorias S_i de solução e mitigação das questões de segurança. Como exemplo destas subcategorias temos o *firewall* (S_2) que corresponde a uma medida de solução e mitigação da categoria segurança de rede.

Tabela 1: Métricas de *ARQ*, *PRI* e *CONF*.

Métricas	Categoria	Subcategoria (Si)
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 Hypervision
		S10 - Vazamento de Dados
		S11 - Identificação de VM
		S12 - Ataques Cross-VM
Privacidade (PRI)	Segurança dos Dados	S13 - Criptografia
		S14 - Redundância
		S15 - Eliminação de Dados
	Aspectos jurídicos	S16 - Localização dos Dados
		S17 - Pesquisas e conhecimento
		S18 - Controle de Riscos
Conformidade (CONF)	Serviços	S19 - SLA
		S20 - Falhas ou Desastres
		S21 - Auditoria

3.1 Responsabilidades - Tipo de Nuvem quanto a Implantação e Serviço

Badger, L. em [2] considera que um sistema de computação em nuvem poderá ser implantado em uma infraestrutura local das organizações consumidoras (privada ou comunitária), compartilhada remotamente (pública) ou com alguns recursos locais e outros compartilhados remotamente (híbrida). Podemos então, definir os seguintes modelos de nuvem quanto à implantação: Nuvem Privada Local (NPL), Nuvem Privada Terceirizada (NPT), Nuvem Comunitária Local (NCL), Nuvem Comunitária Terceirizada (NCT), Nuvem Pública (NP) e Nuvem Híbrida (NH).

Além disso, a nuvem poderá fornecer acesso a softwares de aplicação, *Software as a Service (SaaS)*, a ambientes de desenvolvimento, *Plataform as a Service (PaaS)*, ou a recursos computacionais básicos como processamento e armazenamento, *Infrastructure as a Service (IaaS)*. A escolha do modelo de nuvem quanto à implantação e serviço deverá ser feita pela avaliação e definição de responsabilidades de controle e visibilidade dos recursos de computação. É definido como perímetro de segurança [9] um conjunto de políticas de segurança física e programáveis de forma a obter níveis de proteção em uma fronteira conceitual contra atividades remotas maliciosas. Para padronização do perímetro de segurança, utilizou-se a seguinte nomenclatura:

- Consumidor da Nuvem: indivíduo ou organização, podendo ser este consumidor uma nuvem que utiliza serviços de outras nuvens;
- Cliente: qualquer estação ou aplicação que acessa a nuvem por meio de uma conexão de rede em busca de um serviço ou aplicação oferecido pelo consumidor e hospedado na nuvem;
- Provedor da Nuvem: uma organização que oferece serviços em nuvem;
- Controle: capacidade de executar ações, com alta confiança, autorizar o que e quem poderá acessar os dados e sistemas do consumidor; e
- Visibilidade: capacidade de monitorar como os dados e sistemas do consumidor estão sendo acessados por outros, com alta confiança.

Contudo, para cada modelo de nuvem escolhido pelo consumidor, o controle e visibilidade de seus dados e sistemas dependerão da localização, posse e capacidade de configurar mecanismos de acesso e proteção de recursos utilizados pelo mesmo. A partir das definições de responsabilidades quanto ao controle e visibilidade do perímetro de segurança nos tipos de nuvem definidos em [9], associou-se na Tabela 2 a obrigatoriedade dos provedores quanto às categorias que compõe as medidas de segurança quanto à arquitetura, privacidade e conformidade na nuvem.

Tabela 2: Responsabilidades do Provedor.

Modelo \ Categoria	Segurança de Rede	Interface	Virtualização	Segurança dos Dados	Aspectos Jurídicos	Serviços
NPL						
NPT	✓	✓	✓	✓	✓	✓
NCL						
NCT	✓	✓	✓	✓	✓	✓
NP	✓	✓	✓	✓	✓	✓
SaaS	✓	✓	✓	✓	✓	✓
PaaS	✓		✓		✓	✓
IaaS	✓		✓		✓	✓

3.2 Definição do grau de importância das métricas de segurança

Foi analisado nesta seção o grau de importância de todos os itens de segurança quanto à arquitetura, à privacidade e à conformidade a comporem o *Sec-SLA*. Como referência, utilizou-se a base de padrões de ataque *Common Attack Pattern Enumeration and Classification (CAPEC)*, elaborada pela comunidade de segurança cibernética. Esta base é atualizada e disponibilizada pelo Departamento de Segurança

Interna dos EUA como parte da *Software Assurance (SWA)*, iniciativa estratégica do Escritório de Segurança Cibernética e Comunicações (*CS&C*) desde 2007. A base *CAPEC* enumera e classifica os principais domínios e mecanismos de ataques associados a 463 padrões de ataques, com medidas para mitigação e solução. Além disso, a probabilidade e os impactos na confidencialidade, na integridade e na disponibilidade, sendo esses atributos avaliados como: muito alto, alto, médio e baixo.

Em [20] foram obtidas faixas de valores para itens de *Sec-SLA* presentes na base de vulnerabilidades *National Vulnerability Database (NVD)* do *Common Vulnerability Scoring System (CVSS)*, levando em consideração apenas o impacto pela severidade da vulnerabilidade. Propõe-se neste trabalho, avaliar além do impacto na severidade, a probabilidade desses ataques, obtida pela *CAPEC* por um histórico de ocorrências, que juntos definirão o grau de risco a ser minimizado ou eliminado a partir das subcategorias S_i de mitigação e solução.

3.2.1 Considerações sobre as avaliações

As avaliações tiveram como base o Guia de Avaliação de Riscos [17], que orienta a construção de uma matriz de risco baseada na probabilidade de ocorrência e no impacto das ameaças. Embora a base original do Guia de Avaliação de Riscos [17] apresentar três níveis (alto, médio e baixo), esta avaliação foi adaptada para uma matriz 4 x 4, visto que a base *CAPEC* considera quatro níveis para a probabilidade das ameaças (muito alta, alta, média e baixa) e quatro níveis para a severidade (muito alta, alta, média e baixa), representados na Tabela 3. Logo, os possíveis níveis de risco na matriz proposta compreendem também os níveis: muito alto, alto, médio e baixo.

Para cada um dos possíveis níveis, definiu-se, então, as respectivas Faixas de Probabilidade de ocorrência das ameaças que serão *a posteriori* associadas às subcategorias S_i. Essa faixa será denotada por $FP_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$. Assim, temos: $FP_{muito\ alta} = (0.75, 1.0]$; $FP_{alta} = (0.5, 0.75]$; $FP_{média} = (0.25, 0.5]$ e $FP_{baixa} = (0, 0.25]$. De forma análoga, definiu-se as diferentes Faixas de Severidade a serem associadas às subcategorias S_i baseadas na severidade da ameaça de cada uma delas. Elas são denotadas por $FS_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$. Logo, considera-se: $FS_{muito\ alta} = (75, 100]$; $FS_{alta} = (50, 75]$; $FS_{média} = (25, 50]$ e $FS_{baixa} = (0, 25]$.

A partir de $FP_{nível}$ e $FS_{nível}$, é possível obter o que foi definido como os diferentes níveis de Faixas de Risco (denotadas por $FR_{nível}$, onde também $nível \in \{muito\ alta, alta, média, baixa\}$). Para isso, foram multiplicados os valores extremos de cada um dos níveis das Faixas de Probabilidade por todos os valores extremos das Faixas de Severidade. Tem-se, então: $FR_{muito\ alta} = (56.25, 100]$; $FR_{alta} = (25, 56.25]$; $FR_{média} = (6.25, 25]$ e $FR_{baixa} = (0, 6.25]$.

Tabela 3: Faixa de Risco.

Severidade\ Probabilidade	Muito Alta (0.75,1]	Alta (0.5,0.75]	Média (0.25,0.5]	Baixa (0,0.25]
Muito Alta (75,100]	100,00	75,00	50,00	25,00
Alta (50,75]	75,00	56,25	37,50	18,75
Média (25,50]	50,00	37,50	25,00	12,50
Baixa (0,25]	25,00	18,75	12,50	6,25

Essas escalas de risco serão associadas às medidas de mitigação e soluções (S_i subcategorias) a serem utilizadas no cálculo da confiança. Vale notar que para auxiliar em explicações futuras, atribuiu-se diferentes cores a cada uma das faixas de probabilidade, severidade e risco, sendo: muito alta (vermelha), alta (laranja), média(verde) e baixa(azul).

3.2.2 Extração de Dados e Avaliações das Subcategorias quanto ao risco

Da base *CAPEC* foram extraídos atributos necessários, juntamente com suas medidas de "mitigação e solução", que neste trabalho estão associadas às subcategorias S_i, conforme o exemplo:
Padrão de Ataque CAPEC-236 *"Catching exception throw / signal from privileged block":*

Este padrão de ataque trata de códigos sem proteção contra acessos não autorizados, possibilitando alterações maliciosas. Como medida de prevenção, sugerem no texto configurações correspondentes às subcategorias: S_3 (configurações), S_4 (API), S_5 (Interface Administrativa), S_6 (Interface do Usuário) e S_7 (Autenticação).

Após a preparação dos dados, que consiste na exclusão dos atributos irrelevantes para a análise, manteve-se na base de dados os seguintes campos: Identificador do Ataque, Identificador SoluçãoMitigação, Severidade (muito alta, alta, média e baixa), e Probabilidade (muito alta, alta, média e baixa). Realizou-se um agrupamento simples para caracterizar as subcategorias (presentes no atributo Identificador SoluçãoMitigação) de acordo com a densidade que as mesmas aparecem nas tuplas com valores do atributo Severidade: muito alta, alta, média e baixa. A partir do resultado obtido, notou-se que uma mesma subcategoria S_i está presente em mais de um nível de faixa de severidade. A fim de associar uma subcategoria a apenas uma delas, analisou-se a frequência com que cada subcategoria S_i aparece em cada uma das faixas, associando-a à faixa em que a subcategoria aparece com com maior frequência (denotada por $fs(S_i)$ na Tabela 4. Como exemplo, considere a subcategoria *Firewall* (S_2) que aparace com maior frequência (9, 58%) na $FS_{muito\ alta}$ destacada na cor "vermelha" definida para este nível de faixa.

Tabela 4: Frequências quanto à Severidade e Probabilidade.

frequencia de severidade fs(Si)										frequencia de probabilidade fp(Si)									
Si	muito alta	%	alta	%	média	%	baixa	%	Total	Si	muito alta	%	alta	%	média	%	baixa	%	Total
1	2	1,20	9	2,72	2	3,28	0	0,00	13	1	1	1,67	4	1,13	5	3,62	3	5,77	13
2	16	9,58	26	7,85	4	6,56	0	0,00	46	2	6	11,67	27	8,19	8	5,80	4	7,69	45
3	27	16,17	56	16,92	12	19,67	2	18,18	97	3	9	15,00	59	17,80	20	15,22	7	17,31	95
4	22	13,17	46	13,90	10	16,39	3	27,27	81	4	6	11,67	49	14,69	18	13,77	5	9,62	78
5	26	15,57	58	17,52	8	13,11	3	27,27	95	5	8	13,33	59	17,51	23	18,12	6	11,54	96
6	27	16,17	62	18,73	9	14,75	3	27,27	101	6	8	13,33	63	18,93	23	18,84	6	13,46	100
7	22	13,17	32	9,67	7	11,48	0	0,00	62	7	6	11,67	37	11,02	15	11,59	3	5,77	61
8	2	1,20	2	0,60	0	0,00	0	0,00	4	8	2	3,33	2	0,56	1	0,72	1	1,92	6
9	1	0,60	0	0,00	0	0,00	0	0,00	0	9	0	0,00	1	0,28	0	0,00	0	0,00	1
10	2	1,20	2	0,60	0	0,00	0	0,00	4	10	0	0,00	3	0,85	0	0,00	1	1,92	4
11	0	0,00	3	0,91	0	0,00	0	0,00	3	11	1	1,67	1	0,28	0	0,00	0	0,00	2
12	1	0,60	0	0,00	0	0,00	0	0,00	1	12	0	0,00	0	0,00	0	0,00	2	3,85	2
13	5	2,99	8	2,42	5	8,20	0	0,00	18	13	2	3,33	9	2,82	5	3,62	6	11,54	22
14	0	0,00	2	0,60	0	0,00	0	0,00	2	14	0	0,00	0	0,00	2	1,45	0	0,00	2
15	1	0,60	3	0,91	0	0,00	0	0,00	4	15	0	0,00	2	0,56	2	1,45	0	0,00	4
16	0	0,00	3	0,91	0	0,00	0	0,00	3	16	1	1,67	1	0,28	1	0,72	0	0,00	3
17	0	0,00	3	0,91	0	0,00	0	0,00	3	17	1	1,67	1	0,28	1	0,72	0	0,00	3
18	0	0,00	3	0,91	0	0,00	0	0,00	3	18	1	1,67	1	0,28	1	0,72	0	0,00	3
19	1	0,60	0	0,00	0	0,00	0	0,00	1	19	1	1,67	0	0,00	0	0,00	0	0,00	1
20	3	1,80	4	1,21	2	3,28	0	0,00	9	20	1	1,67	3	0,85	3	2,17	3	5,77	10
21	9	5,39	9	2,72	2	3,28	0	0,00	20	21	3	5,00	12	3,67	2	1,45	2	3,85	19
	167		331		61		11		570		57		334		130		49		570

Logo, as subcategorias estarão distribuídas e representadas em relação a $FS_{nível}$ do Padrão de Ataque como: $FS_{muito\ alta} = \{S_2, S_7, S_8, S_9, S_{10}, S_{12}, S_{19}, S_{21}\}$; $FS_{alta} = \{S_{11}, S_{14}, S_{15}, S_{16}, S_{17}, S_{18}\}$; $FS_{média} = \{S_1, S_3, S_{13}, S_{20}\}$ e $FS_{baixa} = \{S_4, S_5 \text{ e } S_6\}$.

Da mesma forma, realizou-se um agrupamento simples

para caracterizar as subcategorias (presentes no atributo Identificador SoluçãoMitigação) de acordo com a densidade que as mesmas aparecem nas tuplas com valores do atributo Probabilidade: muito alta, alta, média e baixa. Assim como ocorrido no atributo Severidade, notou-se que uma mesma subcategoria S_i está presente em mais de uma faixa de probabilidade referente ao atributo Probabilidade. A fim de associar uma subcategoria S_i a apenas um nível de faixa de probabilidade (muito alta, alta, média e baixa) verificou-se a frequência com que cada subcategoria S_i aparece nestes níveis, considerando o número total de subcategorias presentes em cada faixa de probabilidade e associou àquela em que aparece com maior frequência (denotada por $fp(S_i)$, conforme a Tabela 4).

Logo, as subcategorias foram distribuídas e representadas em relação a $FP_{nível}$ do Padrão de Ataque como: $FP_{muito\ alta} = \{S_2, S_7, S_8, S_{11}, S_{16}, S_{17}, S_{18}, S_{19}\}$; $FP_{alta} = \{S_3, S_4, S_6, S_9\}$; $FP_{média} = \{S_5, S_{14}, S_{15}\}$ e $FP_{baixa} = \{S_1, S_{10}, S_{12}, S_{13}, S_{20}, S_{21}\}$.

A partir dos dados obtidos na Tabela 4 pôde-se preencher a Tabela 5, subcategorias associadas à faixa de risco correspondente. Note que, por exemplo, as subcategorias S_{11}, S_{16}, S_{17} e S_{18} encontram-se classificadas como $FS_{alta} = (50, 75]$ e $FP_{muito\ alta} = (0.75, 1.0]$, resultando em uma faixa de risco com o intervalo $(56.25, 100]$ e consequentemente sendo classificadas no nível muito alto (vermelha).

Tabela 5: Subcategorias associadas à faixa de risco.

Severidade \Probabilidade	muito alta	alta	média	baixa
muito alta	2, 7, 8, 19	9		10, 12, 21
alta	11, 16, 17, 18		14, 15	
média		3		
baixa		4, 6		1, 5, 13, 20

4. PROPOSTA PARA CÁLCULO DA CONFIANÇA NA NUVEM

Esta seção descreve a proposta desenvolvida nesta trabalho para o cálculo da confiança. O modelo proposto atribui a cada subcategoria S_i um valor único de risco $r(S_i)$ a ser calculado a partir de valores únicos da severidade $s(S_i)$ e probabilidade $p(S_i)$, obtidos de acordo com as faixas de severidade e de probabilidade, conforme Tabela 4.

A maior frequência quanto à severidade $fs(S_i)$ relacionada à uma subcategoria S_i determina a faixa de severidade a qual está associada na Tabela 4. Esta faixa de severidade ($FS_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$) é dada por:
$FS_{nível} = (s^{min}_{nível}, s^{max}_{nível})$, onde:
$s^{min}_{nível}$ = valor mínimo de $FS_{nível}$
$s^{max}_{nível}$ = valor máximo de $FS_{nível}$

Considerando $s(S_i)$ como a severidade relacionada à subcategoria S_i, tem-se:

$$s(S_i) = [(s^{max}_{nível} - s^{min}_{nível}) * \frac{fs(S_i)}{100}] + s^{min}_{nível}$$

Da mesma forma, a maior frequência quanto à probabilidade $fp(S_i)$ relacionada à uma subcategoria S_i determina a faixa de probabilidade a qual está associada na Tabela 4. Esta faixa de probabilidade ($FP_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$) é dada por:
$FP_{nível} = (p^{min}_{nível}, p^{max}_{nível})$, onde:
$p^{min}_{nível}$ = valor mínimo de $FP_{nível}$
$p^{max}_{nível}$ = valor máximo de $FP_{nível}$.

Considerando $p(S_i)$ como a probabilidade relacionada à subcategoria S_i, tem-se:

$$p(S_i) = [(p^{max}_{nível} - p^{min}_{nível}) * \frac{fp(S_i)}{100}] + p^{min}_{nível}$$

Uma vez que o risco $r(S_i)$ é dado por $r(S_i) = s(S_i) * p(S_i)$ tem-se:

$$r(S_i) = \{[(s^{max}_{nível} - s^{min}_{nível}) * \frac{fs(S_i)}{100}] + s^{min}_{nível}\} * \{[(p^{max}_{nível} - p^{min}_{nível}) * \frac{fp(S_i)}{100}] + p^{min}_{nível}\}$$

Este valor encontrado deverá estar na faixa de risco a que esta subcategoria está associada na Tabela 5.
Como exemplo, calcula-se o valor da subcategoria S_2 (*Firewall*): O maior valor de $fs(S_2)$ na Tabela 4 é $9,58\%$ e pertence a $FS_{muito\ alta} = (75, 100]$. Então,

$$s(S_2) = [(100 - 75) * \frac{9,58}{100}] + 75 = 77,395$$

Da mesma forma, de acordo com a Tabela 4, o maior valor de $fp(S_2)$ é $11,66\%$ e pertence a $FP_{muito\ alta} = (0, 75, 1]$. Então,

$$p(S_2) = [(1 - 0,75) * \frac{11,66}{100}] + 0,75 = 0,779$$

Logo, o risco $r(S_2) = s(S_2) * p(S_2) = 60,302$ e encontra-se na faixa $(56,25$ a $100]$, muito alta.

Na Tabela 6 apresenta-se o valor único de risco $r(S_i)$ atribuído a cada subcategoria S_i.

Tabela 6: Valores atribuídos quanto ao risco associado.

Nível	FR	Si	fs(Si) %	FS	s(Si)	fp(Si) %	FP	p(Si)	r(Si)
muito alta	56,25-100	S2	9,58	75-100	77,4	11,66	0,75 - 1	0,78	60,3
		S7	13,17		78,29	11,66		0,78	61
		S8	1,19		75,3	3,33		0,76	57,1
		S9	0,59		75,15	0,28		0,75	56,4
		S11	0,9		75,23	1,66		0,75	56,7
		S16	0,9		75,23	1,66		0,75	56,7
		S17	0,9		75,23	1,66		0,75	56,7
		S18	0,9		75,23	1,66		0,75	56,7
		S19	0,59		75,15	1,66		0,75	56,7
alta	25-56,25	S3	19,67	50-75	54,92	17,79	0,5 - 0,75	0,54	29,9
		S14	0,6		50,15	1,44		0,5	25,3
		S15	0,9		50,23	1,44		0,5	25,3
média	6,25-25	S4	27,27	25-50	31,82	14,68	0,25 - 0,5	0,29	9,12
		S6	27,27		31,82	18,92		0,3	9,46
		S10	1,19		25,3	1,92		0,25	6,45
		S12	0,59		25,15	3,84		0,26	6,53
		S21	5,38		26,35	3,84		0,26	6,84
baixa	0-6,25	S1	3,27	0-25	0,82	5,76	0 - 0,25	0,01	0,01
		S5	27,27		6,82	18,11		0,05	0,31
		S13	8,19		2,05	11,53		0,03	0,06
		S20	3,27		0,82	5,76		0,01	0,01

A partir desta forma de avaliação das subcategorias e da obrigatoriedade das categorias que as englobam, de acordo com o perímetro de segurança de cada modelo, é possível medir a Confiança do Provedor da Nuvem, baseado no compromisso e inclusão das mesmas em *Sec-SLA*. Vale lembrar que quanto maior o risco a ser evitado pelas subcategorias S_i presentes nos *Sec-SLA* dos provedores maior será o valor de confiança deste provedor.

Dados as medidas de segurança ARQ, PRI e $CONF$, calcula-se a confiança (C) considerando:

I - A distribuição de peso (w_k) a ser definida pelo consumidor e proporcional a seu objetivo quanto a ARQ, PRI e $CONF$:
$C = (w_1 * ARQ) + (w_2 * PRI) + (w_3 * CONF)$, onde:
$\sum_{k=1}^{3} w_k = 1$, para $k \in \mathbb{N}$ e $0 \leq w_k \leq 1$

II - As subcategorias S_i presentes em ARQ, PRI e $CONF$ oferecidas pelo provedor:
$ARQ = \sum_{i=1}^{12} r(Si)$, $i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
$PRI = \sum_{i=13}^{18} r(S_i)$, $i \in \{13, 14, 15, 16, 17, 18\}$
$CONF = \sum_{i=19}^{21} r(S_i)$, $i \in \{19, 20, 21\}$

Logo, a confiança C é dada por:
$C = (w_1 * \sum_{i=1}^{12} r(Si)) + (w_2 * \sum_{i=13}^{18} r(Si)) + (w_3 * \sum_{i=19}^{21} r(Si))$, $i \in \mathbb{N}$.

A partir deste modelo heurístico, obtém-se a resposta da primeira questão fundamental "Como apoiar os consumidores da nuvem na escolha do provedor que garanta uma maior confiança nos serviços a serem contratados?"

5. ESTUDO DE CASOS E ANÁLISE

O estudo de casos a partir da definição de um modelo abstrato permite calcular a confiança para modelos distintos de nuvem, com base nas medidas de prevenção a riscos listadas na base *CA-PEC* oferecidas pelos provedores em seus Catálogos de Serviço, diferentemente da avaliação de desempenho provada por [13, 14].

5.1 ESTUDO DE CASOS

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 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. Foram avaliados três cenários hipotéticos, onde clientes com distintas necessidades de modelos de nuvem buscam o provedor de nuvem que forneça o maior grau de confiança. Na Tabela 7, são apresentadas as categorias e subcategorias das medidas de prevenção a ataques oferecidas por provedores de nuvem hipotéticos A, B, C e D em seus catálogos de serviço.

Tabela 7: Catálogos de Serviço.

Categoria	Subcategoria(Si)	A	B	C	D	r(Si)
Segurança de Rede	S1 - Transferência de Dados	✔		✔		0,01
	S2 - Firewall	✔	✔	✔	✔	60,30
	S3 - Configurações	✔	✔	✔		29,90
Interface	S4 - API		✔	✔		9,12
	S5 - Interface Administrativa	✔	✔	✔	✔	0,30
	S6 - Interface do Usuário	✔	✔			9,45
	S7 - Autenticação	✔	✔	✔	✔	61,00
Virtualização	S8 - Isolamento	✔	✔	✔	✔	57,09
	S9 - Vulnerabilidades do Hypervision	✔	✔			56,41
	S10 - Vazamento de Dados		✔	✔		6,44
	S11 - Identificação de VM	✔	✔	✔	✔	56,73
	S12 - Ataques Cross-VM	✔				6,52
Segurança dos Dados	S13 - Criptografia	✔	✔	✔	✔	0,05
	S14 - Redundância	✔	✔	✔	✔	25,25
	S15 - Eliminação de Dados	✔			✔	25,29
Aspectos jurídicos	S16 - Localização dos Dados		✔	✔		56,73
	S17 - Pesquisas e conhecimento		✔	✔		56,73
	S18 - Controle de Riscos		✔	✔		56,73
Serviços	S19 - SLA	✔	✔	✔	✔	56,67
	S20 - Falhas ou Desastres	✔	✔	✔		0,01
	S21 - Auditoria			✔		6,83

5.1.1 Cenário 1 - 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. Atribuiu-se, como exemplo, os seguintes pesos aos atributos de confiança proporcionais ao objetivo do consumidor: $w_1 = 0,3, w_2 = 0,3$ e $w_3 = 0,4$, visto que a arquitetura deverá ser compartilhada com outros consumidores para atender ao menor custo de hospedagem, além de garantir uma maior disponibilidade. A partir das responsabilidades definidas na Tabela 2 (Seção 3.1) verifica-se que o provedor de uma Nuvem Pública (NP) é responsável por todas as subcategorias presentes na Tabela 7. Calculou-se o valor de confiança C de cada provedor para este cenário:
$C = 0,3 * ARQ + 0,3 * PRI + 0,4 * CONF$
Sendo, então, os resultados:
$C_A = 139,16$; $C_B = 185,34$; $C_C = 168,31$ e $C_D = 108,47$.
Logo, o provedor com maior confiança para este cenário será o B.

5.1.2 Cenário 2 - Nuvem Privada Terceirizada

Considera-se neste cenário que o consumidor necessite de um provedor para criar uma Nuvem Privada Terceirizada (NPT), definindo como prioridade a maior segurança dos dados. Como exemplo, atribuiu-se os pesos aos atributos de confiança proporcionais ao objetivo do consumidor: $w_1 = 0,8$, $w_2 = 0,1$ e $w_3 = 0,1$ visto que a escolha é por uma arquitetura privada.

Da mesma forma que o cenário anterior, o provedor de uma nuvem NPT é responsável por todas as subcategorias presentes na Tabela 7. O valor de confiança de cada provedor para este cenário será calculado como:
$C = 0,8 * ARQ + 0,1 * PRI + 0,1 * CONF$
Sendo, então, os resultados:
$C_A = 280,89$; $C_B = 302,60$; $C_C = 250,61$ e $C_D = 199,06$.
Logo, o provedor com maior confiança para este cenário será o B.

5.1.3 Cenário 3 - Nuvem Pública PaaS

Considera-se neste cenário que o consumidor necessite de um provedor para criar uma Nuvem Pública *PaaS* (*NP PaaS*), definindo como prioridades a segurança na plataforma de desenvolvimento e a privacidade dos dados. Como exemplo, atribuiu-se os pesos aos atributos de confiança proporcionais ao objetivo do consumidor: $w_1 = 0,4$, $w_2 = 0,4$ e $w_3 = 0,2$. De forma diferente dos cenários anteriores, a partir das responsabilidades definidas na Tabela 2 (Seção 3.1) verificou-se que o provedor é responsável pelas seguintes subcategorias presentes na Tabela 7: $S_1, S_2, S_3, S_8, S_9, S_{10}, S_{11}, S_{12}, S_{16}, S_{17}, S_{18}, S_{19}, S_{20}$ e S_{21}.

Assim, calcula-se o valor de confiança de cada provedor para este cenário como:
$C = 0,4 * ARQ + 0,4 * PRI + 0,2 * CONF$
Sendo, então, os resultados:
$C_A = 118,12$; $C_B = 163,59$; $C_C = 164,96$ e $C_D = 80,98$.
Logo, o provedor com maior confiança para este cenário será o C.

5.2 Análise dos Resultados

Avaliando-se os resultados obtidos e descritos no cálculo da confiança, percebe-se que através da utilização de um valor único associado a cada subcategoria, calculado com base na faixa de severidade e probabilidade que está associada na Tabela 4, foram obtidos resultados mais precisos do que utilizando um valor correspondente por faixa de risco, como proposto em [20]. A partir desta análise, é respondida a segunda questão fundamental "Como medir este grau de confiança?".

O principal aspecto a ser destacado a partir dos três Cenários é que para cada modelo de nuvem (implantação e serviço) associado às políticas de segurança do consumidor quanto à arquitetura, privacidade e conformidade será necessário um padrão de *Sec-SLA* que melhor atenda o consumidor. Analisando apenas a reputação proposta em [14] e métricas de desempenho de *QoS* em [13] não é possível obter esta diferenciação e padronização de *Sec-SLA*. A análise sobre a eficiência do modelo heurístico proposto para o cálculo da confiança na Seção 4 é apresentada na próxima seção, comparando os resultados obtidos nos cenários hipotéticos aos resultados obtidos na implementação dos mesmos em experimentos reais.

6. EXPERIMENTOS EM AMBIENTE REAL

Ao analisar a Tabela 2 na Seção 3.1, que define a responsabilidade de consumidores e provedores nos diversos modelos de nuvem quanto a implantação e serviço, nota-se semelhanças que reduzem os possíveis ambientes a serem validados no cálculo de confiança. São elas:

1. Os modelos de implantação de nuvens *NPL* e *NCL* serão de total responsabilidade do consumidor;
2. Os demais modelos de implantação de nuvens *NPT* e *NCT*, *NP* e *NH* irão variar somente de acordo com o modelo quanto ao serviço escolhido:
   (a) Os modelos *SaaS* serão de total responsabilidade do Provedor; e
   (b) Os modelos *PaaS* e *IaaS* terão responsabilidade distintas, onde as subcategorias $S_1, S_2, S_3, S_8, S_9, S_{10}, S_{11},$

$S_{12}, S_{16}, S_{17}, S_{18}, S_{19}, S_{20}$ e S_{21} serão de responsabilidade do provedor e as demais serão de total responsabilidade do consumidor.

A partir destas semelhanças e buscando validar o modelo abstrato proposto para medir a confiança em provedores de nuvem, considerou-se os ambientes que se enquadraram na semelhança 2 de forma independente do tipo de modelo quanto a implantação (*NPT*, *NCT*, *NP* ou *NH*), variando apenas o tipo de modelo quanto ao serviço (*SaaS*, *PaaS* e *IaaS*) que correspondem às semelhanças (a) e (b). Logo, o que irá diferenciar no cálculo da confiança na nuvem serão os pesos dados pelos consumidores hipotéticos à arquitetura (w_1), à privacidade (w_2) e à conformidade (w_3) e as subcategorias S_i que cada provedor hipotético oferece em seus catálogos de serviço. O ambiente escolhido para validação foi o Centro de Tecnologia da Informação da Marinha (*CTIM*), cabe a este Centro atuar como um provedor de nuvem a todas as Organizações Militares (*OM*) da Marinha do Brasil.

6.1 Metodologia

A validação do modelo abstrato proposto para o cálculo de confiança na nuvem foi realizada com configurações correspondentes ao catálogo de serviços de cada provedor hipotético, conforme Tabela 7 na Seção 5.1. Estas configurações correspondem a presença ou ausência de algumas subcategorias presentes na Tabela 1 na Seção 3. A Tabela 8 consiste na representação dos dados obtidos a partir da Tabela 7, conforme descrito acima, acrescida dos campos que listam as configurações dos ambientes reais que representam os Cenário 1 e 3 da Seção 5.1. Após cada configuração realizada utilizou-se ferramentas de varredura, obtendo como resultado o quantitativo de vulnerabilidades encontradas nas subcategorias S_i que compõem as medidas de segurança quanto à arquitetura, à privacidade e à conformidade. Foram considerados mais confiáveis os provedores com o menor número de vulnerabilidades, sendo o resultado comparado ao valor de confiança medido nos Cenários 1 e 3 da Seção 5.1.

É importante destacar algumas considerações sobre as configurações realizadas em cada subcategoria:

a) As subcategorias $S_2, S_5, S_7, S_8, S_{11}, S_{13}, S_{14}$ e S_{19}, por estarem presentes em todos os provedores hipotéticos, não foram avaliadas. Na Tabela 8, onde encontram-se os resultados obtidos nos ambientes de validação, o campo correspondente às configurações destas subcategorias está "OK" e destacado na cor de fundo "cinza claro";

b) As subcategorias $S_{16}, S_{17}, S_{18}, S_{20}$ e S_{21} foram consideradas "OK" caso estejam presentes no catálogo e como uma vulnerabilidade caso estejam ausentes; e

c) As demais subcategorias foram configuradas, conforme descrito na Tabela 8, varridas, analisadas pelas ferramentas *Network Mapper - Nmap* [18] e *Nessus Vulnerability Scanner* [16], para explorar vulnerabilidades de rede/segurança, e pela ferramenta *Acunetix Web Vulnerability Scanner* [1] para explorar vulnerabilidades de aplicações *web*. O número de vulnerabilidades reportados nos relatórios destas ferramentas foi acrescido aos do item anterior (b).

6.1.1 Ambientes de Validação

O servidor de Correio Eletrônico disponibilizado e utilizado por consumidores e clientes da nuvem, caracterizado como um serviço oferecido em nuvem *SaaS*, foi o ambiente escolhido para validar os modelos que se enquadram na semelhança (a) do item 2 da Seção 6, mais especificamente Cenário 1 (nuvem *NP SaaS*) da Seção 5.1. A configuração do Correio Eletrônico é realizada com base em servidores virtuais, SO *Suse Linux* com a solução *IBM Domino Lotus Notes* e demais configurações necessárias de segurança e acesso. Foram configuradas e analisadas as subcategorias: $S_1, S_3, S_4, S_6, S_9, S_{10}, S_{11}$ e S_{15}, conforme descrito na Tabela 8.

O cenário escolhido para validar os modelos que se enquadram na semelhança (b) do item 2 da Seção 6 e Cenário 3 (nuvem *NP PaaS*) da Seção 5.1 foi o Gerenciador de Conteúdo Drupal, utilizado pelos consumidores para desenvolvimento de sites dinâmicos e aplicações web. Foram configuradas e analisadas as subcategorias: S_1, S_3, S_9, S_{10} e S_{12}, visto que as subcategorias S_4, S_5, S_6 e S_{15} são de responsabilidade do Consumidor da *NP PaaS*, destacadas com a cor de fundo "cinza escuro"' na Tabela 8.

6.1.2 Coleta de Dados

Como resultado das varreduras de segurança, foram encontradas vulnerabilidades na nuvem *SaaS* e *PaaS*, tais como: falhas na sincronização de dados, ausência de criptografia na rede e aplicação, políticas de senhas fracas, ambientes passíveis a ataques *CSRF*, *DoS* e *SQL Injection*, ausência de limpeza de status e dispositivo, compartilhamento de recursos como banco de dados no Drupal, protocolos inseguros, portas abertas (*FTP*), módulos e *patch* desatualizados entre outras. O quantitativo de vulnerabilidades encontradas nas métricas *ARQ*, *PRI* e *CONF* na *NP SaaS* (Correio *Lotus Notes*) e nuvem *NP* (Drupal) encontra-se descrito por subcategoria S_i na Tabela 8 e representado graficamente na Figura 1.

Tabela 8: Configurações e Vulnerabilidades.

Si	A	B	C	D	Conf. Correio Lotus Notes(SaaS)	A	B	C	D	Conf. Drupal(PaaS)
S1	✔	1	✔	1	HTTPS(443)	✔	7	✔	7	HTTPS / Desab_FTP / BD_Não_Compartilhado
S2	✔	✔	✔	✔	OK	✔	✔	✔	✔	OK
S3	✔	✔	✔	1	VPN(IPSEC)/Criptografia SSL	✔	✔	✔	4	Módulos Atualizados/Criptografia SSL
	0	1	0	2	Nr Vulnerabilidades	0	7	0	11	Nr Vulnerabilidades
S4	1	✔	✔	1	Versão Atualizada (corrige Ataque CSFR)		✔	✔		Não se aplica - Responsabilidade do Consumidor
S5	✔	✔	✔	✔	OK	✔	✔	✔	✔	
S6	✔	✔	3	8	Política de Senha Forte/Criptografia ID	✔	✔			
S7	✔	✔	✔	✔	OK	✔	✔	✔	✔	
	1	0	3	9	Nr Vulnerabilidades					
S8	✔	✔	✔	✔	OK	✔	✔	✔	✔	OK
S9	✔	✔	1	1	OK	✔	✔	1	1	OK
S10	1	✔	✔	1	OK	1	✔	✔	1	OK
S11	✔	✔	✔	✔	OK	✔	✔	✔	✔	OK
S12	✔	1	1	1	OK	✔	1	1	1	OK
	1	1	2	3	Nr Vulnerabilidades	1	1	2	3	Nr Vulnerabilidades
S13	✔	✔	✔	✔	OK	✔	✔	✔	✔	Não se aplica - Responsabilidade do Consumidor
S14	✔	✔	✔	✔	OK	✔	✔	✔	✔	
S15	✔	1	1	✔	Limpeza Remota/Status do Dispositivo	✔			✔	
	0	1	1	0	Nr Vulnerabilidades					
S16	1	✔	✔	1	OK	1	✔	✔	1	OK
S17	1	✔	✔	1	OK	1	✔	✔	1	OK
S18	1	✔	✔	1	OK	1	✔	✔	1	OK
	3	0	0	3	Nr Vulnerabilidades	3	0	0	3	Nr Vulnerabilidades
S19	✔	✔	✔	✔	OK	✔	✔	✔	✔	OK
S20	✔	✔	✔	1	Backup/Contingência	✔	✔	✔	1	Backup/Contingência
S21	1	1	✔	1	OK	1	1	✔	1	OK
	1	1	0	2	Nr Vulnerabilidades	1	1	0	2	Nr Vulnerabilidades

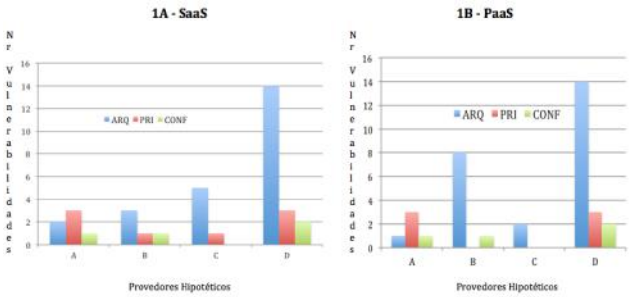

Figura 1: Vulnerabilidades dos Provedores.

6.2 Análise dos Resultados Obtidos

A partir da Figura 1, que representa graficamente o somatório das vulnerabilidades encontradas nas subcategorias S_i dos provedores hipotéticos (Tabela 8), observou-se que considerando apenas os pesos dados pelo consumidor (w_1, w_2 e w_3) às medidas de *ARQ*, *PRI* e *CONF*, o quantitativo de vulnerabilidades encontrado permite validar o modelo abstrato de cálculo de confiança proposto. Pôde-se verificar que a ordem dos provedores do mais confiável ao menos confiável permaneceu a mesma nos Gráficos *SaaS* (B, C, A e D) representado pela Figura 1A e *PaaS* (C, B, A e D) representado pela Figura 1B comparado aos Cenários correspondentes 1 e 3 da Seção 5.1.

Percebe-se ainda que o provedor D, em ambos os ambientes (Figura 1A e 1B), apresentou um alto número de vulnerabilidades quanto à *ARQ*, o que reforça a validação do modelo proposto para o cálculo de confiança, visto que em todos os Cenários da Seção 5.1 o seu valor de confiança foi bem abaixo dos demais provedores. Na Tabela 8 verifica-se que configurações passíveis a ataques como compartilhamento de recursos, ausência de criptografia, políticas de senhas fracas, vulnerabilidades no *hypervision* entre outras, estão presentes no provedor D.

Por outro lado os provedores B e C apresentaram zero vulnerabilidade em *PRI* na Figura 1B. Apesar do peso w_3 ser maior que w_1 e w_2 no ambiente correspondente à Figura 1A e o número de vulnerabilidade de *CONF* ser zero no provedor C, o provedor B se torna o mais confiável por apresentar quase a metade das vulnerabilidades em *ARQ* comparado a C. De acordo com a Tabela 7 da Seção 5.1, as subcategorias S_i presentes em *ARQ* são as de maior valor de risco obtidos na base *CAPEC* quanto a medidas de mitigação/solução de padrões de ataques [3], o que comparado ao Cenário 1 da Seção 5.1 também reforça a validação do modelo proposto.

7. CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

A perda de controle aliada à falta de visibilidade de sistemas movidos para a nuvem são questões fundamentais que, por muitas vezes, impedem os consumidores a adotarem a computação em nuvem ou, caso adotem, de obterem vantagens quanto a custo e desempenho dos recursos oferecidos. Este trabalho propôs um modelo abstrato que permite que os consumidores avaliem provedores de nuvem quanto à arquitetura, à privacidade e à conformidade a partir de suas políticas de segurança e modelo de nuvem a ser contratado. O modelo baseia-se na construção de *Sec-SLA* com medidas de mitigação/solução obtidas em bases de padrões de ataque em sistemas de informação [3]. O *Sec-SLA* é um documento formal que define de forma quantitativa os níveis de serviço a serem entregues pelos provedores. Com isso, o *Sec-SLA* lida com "o que" e não com o "como". Contudo, através do valor atribuído às métricas de segurança (arquitetura, privacidade e conformidade), obtidos neste trabalho, o "como" pode ser melhor definido, compreendido e implementado. Sabe-se que garantir 100% de segurança em qualquer sistema de computação é uma tarefa muito difícil, até mesmo em sistemas dedicados e privados. No entanto, espera-se que com a definição de responsabilidades e *Sec-SLA* bem acordados, é possível obter modelos capazes de oferecer uma maior confiança aos consumidores em ambientes de computação em nuvem. As próximas etapas deste trabalho incluem o desenvolvimento de um método abstrato para apoiar os consumidores na definição dos pesos a serem atribuídos a ARQ, PRI e CONF, utilizados no cálculo da confiança.

Referências

[1] ACUNETIX. Acunetix web vulnerability scanner - acunetix, 2012. "http://www.acunetix.com/vulnerability-scanner/.

[2] L. Badger. Cloud computing synopsis and recommendations. nist special publication 800-146, 2012. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.3178&rep=rep1&type=pdf.

[3] CAPEC. Common attack pattern enumeration and classification - capec, 2014. http://capec.mitre.org/data/definitions/3000.html.

[4] S. N. Chauhan. An approach to measure security of cloud hosted. *IEEE International Conference on Cloud Computing in Emerging Markets(CCEM)*, pages 1–6, 2013.

[5] S. D. Chaves, C. Westphall, and F. Lamin. Sla perspective in security management for cloud computing. *Sixth International Conference Networking and Services*, pages 212–217, 2010.

[6] ENISA. Survey and analysis of security parameters in cloud slas across the european public sector, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

[7] A. Gehani. Accountable clouds. *IEEE International Conference on Technologies for Homeland Security (HST)*, pages 403–407, 2013.

[8] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, and M. Pourzandi. A quantitative analysis of current security concerns and solutionsfor cloud computing. *IEEE 3rd International Conference on Cloud Computing Technology and Science*, pages 231–238, 2011.

[9] T. Grance and W. Jansen. Guidelines on security and privacy in public cloud computing. nist sp-800-144, 2011. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[10] G. Hogben and M. Dekker. Procure secure: A guide to monitoring of security service levels in cloud contracts.tecnical report, european network and information security agency (enisa). Technical report, 2012. https://www.enisa.europa.eu/media/press-releases/procure-secure-enisa2019s-new-guide-for-monitoring-cloud-computing-contracts.

[11] A. Kiezun, P. J. Guo, K. Jayaraman, and M. D. Ernst. Automatic creation of sql injection and cross-site scripting attacks. *In 30th International Conference on Software Engineering (ICSE)*, 2009.

[12] L. K. R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and S. B. Lee. Trustcloud: A framework for accountability and trust in cloud computing. hp technical reporthpl-2011-38. Technical report, 2011. http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[13] D. P. Manuel. *A trust model of cloud computing based on Quality of Service*. Annals of Operations Research, 2013.

[14] D. P. Manuel, A. I. M. Barr, and T. S. Selvi. A novel trust management system for cloud computing - iaas providers. 79:3–22, 2011.

[15] P. Mell and T. Grance. The nist definition of cloud computing. nist sp-800-145, 2011. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

[16] NESSUS. Tenable nessus vulnerability scanner - nessus, 2007. "http://www.software.com.br/p/tenable-nessus-vulnerability-scanner?gclid=CN7d2Jj3pMoCFQ8HkQodG6cKxQ.

[17] NIST. Guide for conducting risk assessments.2012.nist sp-800-30, rev.1, 2012. "http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[18] NMAP. Network mapper - nmap, 1997. "https://nmap.org/.

[19] Y. Pang, Y. Song, J. Kang, and J. K. Yun. Risk assessment and classification of focusing sla requirement in cloud computing. *International Journal of Security and Its Applications*, 2013.

[20] C. A. Silva and P. L. Geus. Arquitetura de monitoramento para security-sla em nuvem computacional do tipo saas. *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 310–313, 2014.

[21] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 1(34):1–11, 2011.

[22] J. Zhengwei. A meta-synthesis approach for cloud service provider selection based on secsla. *International Conference on Computational and Information Sciences (ICCIS)*, pages 1356–1360, 2013.