12 de Julho de 2016

UNIVERSIDADE FEDERAL FLUMINENSE

KÁTIA CRISTINA ALTOMARE SILVA

CONFIANÇA NA NUVEM A PARTIR DA CONSTRUÇÃO DE SEC-SLA NOS DIVERSOS MODELOS QUANTO À IMPLANTAÇÃO E SERVIÇO

NITERÓI

2016

UNIVERSIDADE FEDERAL FLUMINENSE

KÁTIA CRISTINA ALTOMARE SILVA

CONFIANÇA NA NUVEM A PARTIR DA CONSTRUÇÃO DE SEC-SLA NOS DIVERSOS MODELOS QUANTO À IMPLANTAÇÃO E SERVIÇO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos.

Orientador:
ANTONIO A. A. ROCHA

NITERÓI

2016

KÁTIA CRISTINA ALTOMARE SILVA

CONFIANÇA NA NUVEM A PARTIR DA CONSTRUÇÃO DE SEC-SLA NOS DIVERSOS MODELOS QUANTO À IMPLANTAÇÃO E SERVIÇO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos.

Aprovada em JUNHO de 2016.

BANCA EXAMINADORA

Prof. ANTONIO A. A. ROCHA - Orientador, UFF

Prof. JOSÉ VITERBO FILHO, UFF

Prof. RONALDO MOREIRA SALLES, IME

Niterói

2016

À Luciana Pereira Kamel, pelo incentivo, apoio, amor, compreensão nos momentos difíceis, e, principalmente, por sua inteligência intelectual e emocional que sempre procuro me espelhar.

Agradecimentos

À Deus, por me conceder o término de mais uma etapa.

À Maria de Lourdes Campos Silva, mãe e meu amor eterno, pelo incentivo e exemplo de vida que me inspirou, em vida e após, a não desistir de alcançar os objetivos.

À Marinha do Brasil, que confiou em minha capacidade de concluir esta Pós-Graduação estando presente em todos os meus passos nessa jornada. Em especial ao Capitão-de-Mar-e-Guerra (EN) Antônio Carlos da Costa Pereira, exemplo de liderança e humanidade, que foi o responsável por todo o êxito no meu processo de seleção para o Mestrado.

Aos meus orientadores, Prof. Antonio Augusto (Guto) de A. Rocha (UFF) e Capitão-de-Corveta Flávio Q. Guimarães (DCTIM) que me aceitaram e me acolheram como orientanda, norteando minhas pesquisas e contribuindo significativamente com o sucesso deste trabalho.

Aos Professores da UFF, pelos conhecimentos transmitidos, à Coordenadoria da Pós-Graduação, Secretaria e demais servidores do Instituto de Computação da Universidade Federal Fluminense – IC/UFF pelo apoio institucional e pelas facilidades oferecidas.

Aos membros da banca examinadora, pelas observações e sugestões que contribuíram e enriqueceram este trabalho.

Aos amigos que fiz durante estes dois anos, pelas nossas trocas de conhecimento e companheirismo ao longo dos semestres.

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.

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

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

TI	:	Tecnologia da Informação;
SLA	:	Service Level Agreement;
Sec-SLA	:	Security Service Level Agreement;
CAPEC	:	Common Attack Pattern Enumeration and Classification;
SaaS	:	Software as a Service;
PaaS	:	Plataform as a Service;
IaaS	:	Infrastructure as a Service;
DoS	:	Denial of Service;
NIST	:	National Institute of Standards and Technology;
ENISA	:	European Union Agency for Network and Information Security;
SLO	:	Service Level Objectives;
NVD	:	National Vulnerability Database;
QoS	:	Quality of Service;

Conteúdo

Capítulo 1

Introdução

O conceito de Computação em Nuvem tem como princípio básico a possibilidade de utilizar, em qualquer lugar e independente de plataforma, diversas e variadas aplicações, por meio da internet, como se as mesmas estivessem instaladas em ambientes locais, tais como servidores, computadores e quaisquer outros dispositivos de comunicação online. A Computação em Nuvem, assim como os Sistemas Distribuídos, caracteriza-se por ser um conjunto de unidades de processamento independentes, que, por meio da troca de comunicação e gerenciamento de sincronização, pode processar uma aplicação em diferentes localidades, de forma transparente para o usuário. Desta forma, para o consumidor da nuvem e usuário final da aplicação, todas as tarefas de desenvolvimento, armazenamento, manutenção, atualização, backup, escalonamento, entre outras, que requerem um nível de gerenciamento por profissionais mais qualificados em diversas áreas da Tecnologia da Informação (TI), deixam de ser de suas responsabilidades e passam a ser dos provedores a serem contratados. Logo, não é mais necessário, por exemplo, para algumas empresas, a aquisição de supercomputadores ou investirem na criação e manutenção de seus próprios centro de dados privados ou comunitários, pois todo poder de processamento e armazenamento dos dados passa a ser confiado à nuvem. Cabe à organização consumidora e usuária final da aplicação apenas acessar, por meio de seus dispositivos, através da internet, os recursos oferecidos pelos provedores.

Como exemplo desta nova tecnologia tem-se o Google Docs[1], o qual permite que usuários criem e editem textos, planilhas, apresentações de slides, além de armazenarem arquivos, entre outras funções, através da internet. A principal vantagem para estes usuários é ter todas estas funcionalidades disponíveis, sem a necessidade de instalarem e se

[1] https://www.google.com/docs/about/.

preocuparem com a aquisição de licenças de programas, tais como Microsoft Office[2] ou OpenOffice.org[3], para suas próprias máquinas locais. Com isso, para utilizar a aplicação disponibilizada pela nuvem, é necessário que o usuário apenas abra o navegador de internet e acesse o endereço do Google Docs para iniciar suas atividades nesta aplicação, independente do sistema operacional ou dispositivo utilizado para este fim. A única preocupação do usuário é utilizar um navegador de internet compatível para esta aplicação.

A partir das definições acima, pode-se entender que a adoção da Computação em Nuvem é uma oportunidade para a redução dos investimentos em Tecnologia da Informação (*TI*), possibilitando maior flexibilidade na demanda por serviços e redução dos custos. Assim, as organizações que necessitam criar e gerenciar quantidades maciças de dados, com maior poder de processamento para garantir seu alto desempenho, podem manter recursos financeiros e aumentar sua capacidade de investimento em seus negócios, deixando para terceiros a administração dos ativos de tecnologia, bem como o investimento em *hardware*, *software* e equipe técnica especializada. Com isso, a Computação em Nuvem, como um novo modelo de operações emergentes, promete entregar recursos de computação ilimitados e elásticos sob demanda como um utilitário.

1.1 Motivação

Apesar de todos os benefícios oferecidos pela Computação em Nuvem, uma organização ao tomar a decisão de aderir a esta tecnologia deve considerar uma série de desafios de segurança a serem analisados e atribuídos a todos os envolvidos (tanto consumidores como provedores de serviços), de acordo com o modelo escolhido. 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,

[2]https://products.office.com/pt-BR/.
[3]https://www.openoffice.org/pt-br/.

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 [25], 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.[24], 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.[18] 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 [9] 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.

Devido a falta de definição de responsabilidades e deficiências relatadas anteriormente, este trabalho tem como motivação suprir a falta de padronização de Sec-SLA na nuvem que busquem garantir mais a prevenção do insucesso do que a compensação do pós-fracasso.

1.2 Objetivos

Dados as deficiências e necessidades citadas na Seção 1.1, este trabalho tem como objetivo propor uma padronização de responsabilidades considerando os perímetros de segurança da nuvem e as principais medidas de "mitigação e solução" referentes aos padrões de ataques enumerados por uma base de vulnerabilidades, a serem incluídas nos *Sec-SLAs*. A partir desta padronização de responsabilidades e medidas, é possível medir e classificar a confiabilidade do provedor quanto a seus serviços oferecidos.

1.3 Desafios e Contribuições

A segurança na Nuvem Computacional tem como objetivo minimizar e evitar falhas em suas configurações que levem a riscos quanto à integridade, à confidencialidade e à disponibilidade de seus serviços e aplicações confiadas. A fim de garantir uma maior segurança, 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?

Para alcançar o objetivo de minimizar os riscos na nuvem, 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;

2. A proposta de um modelo heurístico de cálculo da confiança em provedores. Esta proposta é baseada em uma taxonomia onde foram identificados e classificados os

principais problemas de segurança e soluções em Computação em Nuvem. Atribuiu-se um valor de risco para cada medida de mitigação e solução dos principias padrões de ataques em sistemas computacionais que correspondem aos problemas de segurança na nuvem ; e

3. A proposta de um método abstrato para apoiar os consumidores da nuvem na distribuição dos pesos dados às métricas de segurança presentes na taxonomia utilizada. Estes pesos são necessários para o cálculo da confiança da nuvem computacional.

1.4 Organização

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

Capítulo 2

Fundamentação Teórica e Trabalhos Relacionados

Os autores em [18] definem "A computação em nuvem é um modelo para habilitar o acesso por rede ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços". Para um melhor entendimento da nuvem computacional e sobre propostas que apoiem a confiar nesta tecnologia, faz-se necessário destacar suas características essenciais, a diversidade de modelos possíveis de serem contratados, os principais riscos que inibem a sua adoção e, por fim, um levantamento dos principais trabalhos relacionados.

2.1 Fundamentação Teórica

O modelo da Nuvem Computacional é composto de cinco características essenciais, três modelos de serviço, e quatro modelos de implantação, como apresentado na Figura 2.1.

2.1.1 Características Essenciais

A identificação das características essenciais da nuvem computacional é fundamental para entender as vantagens que esta solução traz em relação às soluções tradicionais. As características dos sistemas de Computação em Nuvem são [18]:

CE1 Auto-serviço sob demanda: O consumidor pode configurar seus recursos de computação, como tempo de processamento e armazenamento em rede, automaticamente,

conforme necessário, sem necessitar intervenção humana dos provedores de serviços;

CE2 Amplo acesso por rede: Os recursos estão disponíveis através da rede e são acessados através de mecanismos padronizados que permitem o uso por clientes em dispositivos simples ou complexos em diversas plataformas (como *smartphones*, *tablets*, *laptops* ou *desktops*);

CE3 Agrupamento de recursos: Os recursos de computação do provedor são agrupados para atender a múltiplos consumidores em modalidade multi-inquilinos, com recursos físicos e virtuais diferentes dinamicamente atribuídos e reatribuídos conforme a demanda dos consumidores. Há uma certa independência de localização geográfica, uma vez que o consumidor em geral não controla ou conhece a localização exata dos recursos fornecidos (como armazenamento, processamento, memória e comunicação de rede), mas pode ser capaz de especificar a localização em um nível de abstração mais alto (como país, estado ou *datacenter*);

CE4 Elasticidade rápida: Os recursos podem ser provisionados e liberados elasticamente, em alguns casos automaticamente, para rapidamente aumentar ou diminuir de acordo com a demanda. Para o consumidor, os recursos disponíveis para provisionamento muitas vezes parecem ser ilimitados e podem ser alocados em qualquer quantidade e a qualquer tempo; e

CE5 Serviço mensurado: Os sistemas na nuvem automaticamente controlam e otimizam o uso dos recursos através de medições em um nível de abstração apropriado para o tipo de serviço (como armazenamento, processamento, comunicação de rede e contas de usuário ativas). A utilização de recursos pode ser monitorada, controlada e informada, gerando transparência tanto para o fornecedor como para o consumidor do serviço utilizado.

2.1.2 Tipos de Nuvem quanto a modelos de Serviços e Implantação

É importante que o consumidor, de acordo com a necessidade das aplicações a serem implementadas e utilizadas na nuvem, escolha o modelo que melhor atenda as suas regras de negócio. Por exemplo, certas organizações consumidoras podem não desejar que todos os usuários possam acessar e utilizar determinados recursos no seu ambiente de Computação em Nuvem. Com isso, a restrição ou abertura do acesso deverá ser configurada de

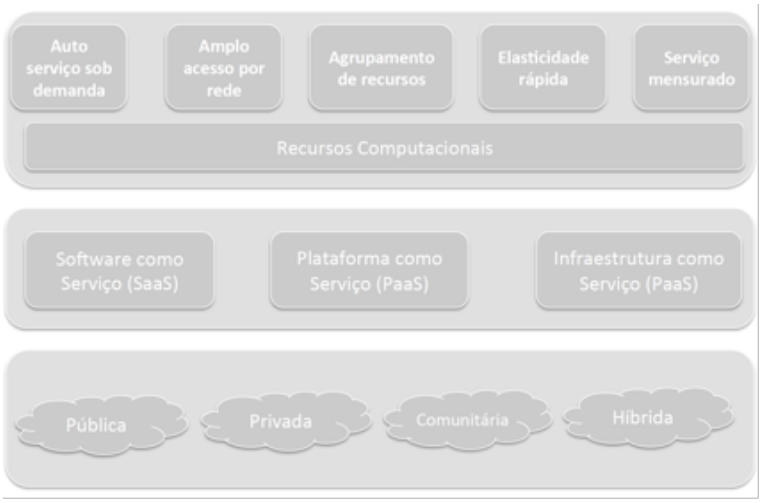

Figura 2.1: Características essenciais da nuvem e seus modelos quanto à implantação e serviço.

acordo com tipo de informação e nível de visão desejado. Além disso, a nuvem oferece seus recursos (infraestrutura, plataforma e software) na forma de serviços a serem contratados. Logo, cabe à organização consumidora escolher os modelos quanto à implantação e serviço a serem contratados. A classificação dos modelos quanto à implantação e serviço é ilustrada, nas camadas correspondentes a estes serviços, na Figura 2.2. Os principais modelos de nuvem são:

1. Quanto à Implantação:

   (a) Nuvem Privada (NPr): São constituídas por uma infraestrutura de nuvem que é implementada apenas para uma única organização, quer seja gerida internamente ou alojada por terceiros a nível externo. Estas requerem um nível significativo de envolvimento, tanto dos departamentos de gestão como de *TI*, no sentido de virtualizar o ambiente de negócio, o que significa também avaliar como os recursos existentes podem ser reatribuídos na nuvem. As nuvens privadas proporcionam o ambiente para soluções de segurança avançada, elevada disponibilidade ou tolerantes a falhas, que não são possíveis numa nuvem pública. Todavia, como se trata na realidade de soluções "autônomas" por direito próprio, a criação de uma nuvem privada implica ainda um investimento significativo, não podendo, por isso, proporcionar as economias de curto prazo características da nuvem pública.

   (b) Nuvem Comunitária (NC): A infraestrutura na nuvem é provisionada para uso exclusivo por uma determinada comunidade de consumidores de organizações que têm interesses em comum (de missão, requisitos de segurança, políticas,

observância de regulamentações). A sua propriedade, gerenciamento e operação podem ser de uma ou mais organizações da comunidade, de terceiros ou de uma combinação mista, e pode estar dentro ou fora das instalações das organizações participantes.

(c) Nuvem Pública (*NP*): Os serviços, as aplicações e o armazenamento são disponibilizados aos utilizadores através da Internet "como um serviço" – normalmente através de um modelo de pagamento conforme utilização. Apesar de nuvens públicas serem atrativas para muitas organizações, dado que reduzem a complexidade e os prazos de execução, porque a arquitetura subjacente é fixa, existe menos possibilidade personalização no que diz respeito a segurança e desempenho.

(d) Nuvem Híbrida (*NH*): Pode ser constituída por serviços em nuvem privada (interna) e serviços em nuvem pública (externa) ou quaisquer outras combinações de nuvens públicas, privadas e comunitárias. O normal é que as organizações executem uma aplicação sobretudo na nuvem privada, mas utilizem a nuvem pública para lidar com picos de utilização. Regras e políticas personalizadas regem as áreas como a segurança e a estrutura subjacente, sendo as tarefas atribuídas a nuvens internas ou externas conforme necessário.

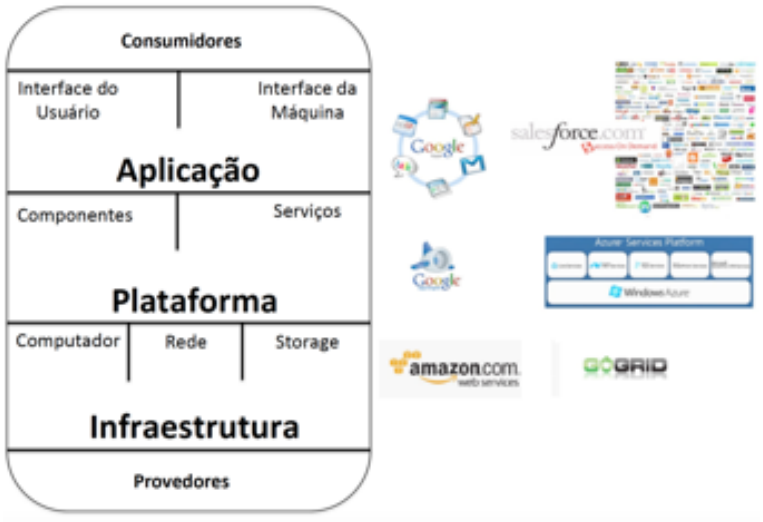

Figura 2.2: Camadas de serviços na nuvem e algumas soluções disponíveis.

2. Quanto ao Serviço:

(a) *Cloud Software as a Service (SaaS)*: Este modelo oferece software de aplicações, tais como processadores de texto através da rede, correio eletrônico entre outras, como exemplo temos o Google App.

(b) *Cloud Platform as a Service (PaaS)*: *PaaS* oferece uma série de ferramentas de sistema e desenvolvimento que vêm instaladas em recursos virtualizados, como exemplo temos o *Google Engine* e *Salesforce*. Tais serviços em nuvem podem ser utilizados para apoiar vídeo sob demanda (*VoD*) que tem como característica uma grande exigência quanto a restrições de qualidade de serviço (*QoS*).

(c) *Cloud Infrastructure as a Service (IaaS)*: O modelo *IaaS* oferece recursos, como máquinas ou processadores virtuais e espaço de armazenamento, permitindo que o usuário selecione a melhor forma como estes recursos serão utilizados, como exemplo temos a *Amazon*, Azure e *GoGrid*.

2.1.3 Riscos na Computação em Nuvem

A contratação de um modelo de nuvem mal dimensionado e configurado pelo provedor pode representar ameaças de segurança da informação para as organizações consumidoras e usuários finais. Além disso, os provedores de nuvem podem ser afetados por ataques maliciosos e falhas de infraestrutura como, por exemplo, falta de energia. Como exemplo, podem ocorrer falhas nos servidores de nome de domínio Internet, afetando diretamente as operações da nuvem e impedindo até mesmo o acesso às nuvens. Em maio de 2009, o *Google* foi alvo de um ataque sério de negação de serviço (*denial of service*), conhecido como *DoS*, que derrubou serviços como *Gmail* e *Google News* por vários dias. Outro exemplo ocorreu em 29 de junho de 2012, quando uma tempestade na costa leste dos Estados Unidos tirou algumas instalações da *Amazon* com base em Virgínia e afetou as empresas que utilizam sistemas exclusivamente nesta região. *Instagram*, um serviço de compartilhamento de fotos, declarou ser uma das vítimas desta paralisação [7].

Pang, Y. et al.[25] realizaram um estudo classificando os riscos na Computação em Nuvem referentes à: Tecnologia, Confiança, Privacidade, Integridade dos Dados e Falta de Padronização. Destaca-se neste trabalho alguns destes riscos que estão relacionados com as características essenciais da nuvem citadas na Seção 2.1.1. São eles:

R1 Multialocação: a falta de proteção de dados dos usuários contra o acesso não autorizado de outros usuários executando processos nos mesmos servidores físicos é um grande risco. Com o uso generalizado de Computação em Nuvem e considerando o fato de que dados importantes dos usuários podem estar sendo armazenados, esse é um risco que influencia e por muitas vezes inibe organizações a adotarem a nuvem como solução;

R2 Localização de Recursos: o fato de nem sempre ser informado aos consumidores exatamente onde os recursos para os serviços prestados estão localizados, pode ser um problema. Devido a leis de conformidade e privacidade de dados em vários países, localidade de dados é de extrema importância em muitas arquiteturas corporativas;

R3 Autenticação e confiança das informações armazenadas e transferidas: por muitas vezes, dados críticos estão localizados na infraestrutura do provedor da nuvem, com isso, dados podem ser alterados sem o consentimento do proprietário. Os dados alterados que forem recuperados e processados pelo proprietário poderão comprometer a tomadas de decisões críticas. Logo, autenticidade dos dados, neste caso, é muito importante e deverá ser garantida. Porém, não existem normas comuns para garantir a integridade dos dados; e

R4 Confidencialidade: Na maioria das arquiteturas da nuvem, a maior parte da infraestrutura de *TI* e armazenamento de dados estão localizados fora dos limites físicos das organizações, sendo distribuídos nos diversos Centro de Dados dos provedores. Com isso, destaca-se duas consequências importantes:

a Os consumidores têm um controle limitado sobre a infraestrutura de *TI*, portanto, os consumidores devem estabelecer mecanismo que imponham a aplicação de suas políticas de segurança para garantir a confidencialidade e integridade dos dados;e

b Os provedores da nuvem, por muitas vezes têm privilégios excessivos, permitindo-lhes amplo controle e capacidade de modificar os dados dos consumidores.

Tabela 2.1: Características essenciais e riscos.

Características \Riscos	**R1**	**R2**	**R3**	**R4**
CE1	X	X		
CE2	X	X		X
CE3	X	X	X	X
CE4	X	X		
CE5			X	X

A partir da Tabela 2.1, verifica-se que existe uma correlação entre as características essenciais e alguns riscos referentes à Computação em Nuvem, tais como:

- A característica auto-serviço sob demanda (CE1), ao permitir que consumidores configurem recursos sem necessitar de intervenção dos provedores de serviços, está sujeita a riscos como compartilhar dados em servidores físicos mal protegidos (Multi-alocação R1) ou armazenar dados em locais onde a política de privacidade não atenda suas regras de negócio (Localização de Recursos R2);

- O amplo acesso (CE2) a partir de qualquer dispositivo (como smartphones, tablets, laptops ou desktops), também está sujeito a riscos no armazenamento e processamento de dados sem proteção (R1) ou em locais que contrariem a políticas de privacidade (R2);

- É possível observar que características tais como escalabilidade (CE3) e elasticidade (CE4), que atraem consumidores devido a facilidade de implantação e economia quanto a investimentos, por vezes tornam-se riscos devido a falta de transparência quanto a autenticação (R3), autorização (R1), localização (R2) e controle dos dados (R4); e

- Finalmente, a transparência no monitoramento dos recursos utilizados (CE5), ao permitir que consumidores e provedores controlem e otimizem o armazenamento, processamento, comunicação de rede, por vezes podem ferir regras de autenticação (R3) e confidencialidade (R4) de informações mais sigilosas.

2.2 Trabalhos Relacionados

Expõe-se nesta seção os trabalhos anteriores relevantes referentes à obtenção de confiança na nuvem. Os trabalhos em [6, 23, 24] fazem um estudo sobre a operacionalização, negociação e definição de *SLA*. Os trabalhos [16, 17] 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 *SLAs* para segurança em nuvens nos seus diversos modelos.

O trabalho [24] afirma que os requisitos de *SLA* na nuvem variam de acordo com o modelo de serviço e implantação. Os autores em [14] 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 [6] 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 Computação em Nuvem, podendo ser adaptado em trabalhos futuros. Parâmetros de políticas de segu-

rança também são extraídos da legislação [10], de recomendações de segurança na nuvem [5, 26] e organizações como *National Institute of Standards and Technology (NIST)* [3] e *European Union Agency for Network and Information Security (ENISA)* [13].

Em [23] 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 [17] 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 [16] 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.

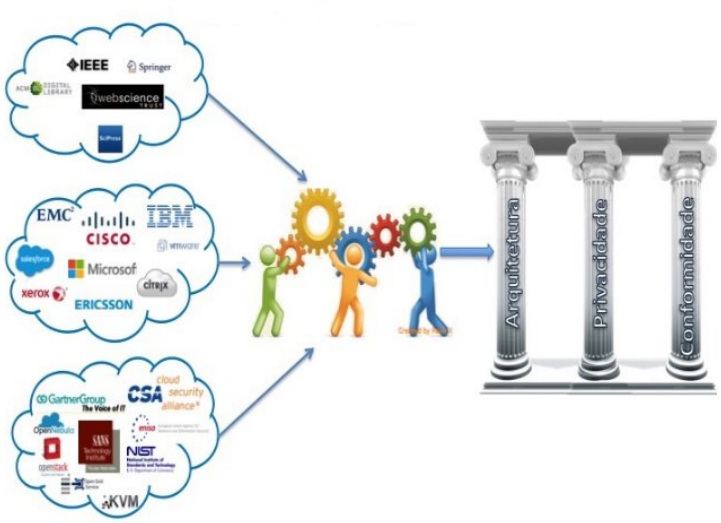

Figura 2.3: Taxonomia proposta por Gonzales et al.[11]

O trabalho [11] 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 (documentos de conferências e revistas publicadas e instituídas pelo *IEEE*, *ACM*, *Springer*, *Webscience*, e *Scipress*), organizações (relatórios, *white papers* e reportagens do *SANS Institute*, *CSA*, *NIST*, *ENISA*, *Gartner Group*, *KVM.org*, *OpenGrid*, *OpenStack* e *OpenNebula*) e empresas (*white papers*, manuais, reportagens e conteúdos da web provenientes da *ERICSSON*, *IBM*, *Xerox*, *Cisco*, *VMWare*, *Xen*, *Citrix*, *EMC*, *Microsoft* e *Salesforce*), conforme Figura

2.3.

Inspirado na taxonomia apresentada em [11] 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 [4].

Qualidade de Serviço na Nuvem proposta por Silva et al.

Os autores em [23] classificam os serviços prestados em *TI*, quanto a qualidade, como:

a Mensuráveis: em que é possível medir com precisão a disponibilidade, capacidade, custo, latência, tempo de provisionamento e escalabilidade; e

b Não mensuráveis: onde não é possível medir métricas como interoperabilidade, modificabilidade e segurança.

Assim como no presente trabalho, a métrica não mensurável explorada em [23] de maior importância para a garantia da confiança na nuvem foi a segurança. Visando a melhoria da segurança na nuvem, Silva et al [23] apresentaram uma arquitetura para monitoramento de segurança, baseada em *Security-SLA*, para os serviços de uma nuvem *SaaS*. O sistema de monitoramento proposto para o cenário *SaaS* baseia-se em uma hierarquia de métricas de segurança para a infraestrutura do serviço contratado utilizando uma escala de valores para tratar o problema de como aferir a segurança (qualidade não mensurável). A solução de monitoramento proposta teve como objetivo acompanhar o cumprimento de acordos de *Security-SLA* para nuvem *SaaS*. Nesta solução, cada cláusula do acordo denominada Objetivo de Nível de Serviço (*Service Level Objectives*), ou simplesmente *SLO*, está associada a uma métrica de segurança que assume valores no intervalo de [0-4] para tratar os valores não mensuráveis ou intangíveis do ambiente de nuvem computacional. Este intervalo representa no monitoramento os níveis de segurança medidos: Crítico, Alto, Médio, Baixo, Zero. O resultando ao final do processo gera um Índice de Segurança denominado *Sec-Ind*.

O processo de monitoramento depende do tipo de serviço que está sendo contratado, onde as ameaças e vulnerabilidades são identificadas para este perfil de serviço, sendo calculado em seguida o risco através do impacto das operações executadas sobre o serviço usando como referência a base de vulnerabilidades (*National Vulnerability Database*), ou simplesmente *NVD*, do *Common Vulnerability Scoring System (CVSS)*. A base de vulne-

rabilidades *NVD* se caracteriza por apoiar na correção de vulnerabilidades tendo como base o cálculo da severidade das vulnerabilidades descobertas nos sistemas de informação. Analisando os valores dos Sec-Ind é determinado o grau de confiabilidade dos valores coletados pelas métricas de segurança.

No presente trabalho, apresenta-se duas propostas para o cálculo da confiança na nuvem, também baseadas em faixas de valores, porém utilizando uma base de vulnerabilidade (*CAPEC*) [4] que considera, além do impacto da severidade utilizado pela base *NVD*, o impacto da probabilidade das vulnerabilidades e ameaças para a obtenção do risco associado.

A partir das definições da Nuvem Computacional presentes na Seção 2.1 e trabalhos relacionados na Seção 2.2 que procuram medir a confiança, a partir da métrica de segurança (não mensurável), neste estudo são estabelecidos níveis de segurança, com seus respectivos graus de complexidade, baseados nas políticas de segurança e regras de negócio do consumidor, diferentemente dos trabalhos [16, 17], que apenas estabeleceram o SLA que atenda as necessidades de capacidade como taxa de transferência de dados, perda de pacotes ou atraso da rede.

Capítulo 3

Medindo a Confiança na Nuvem

Nos capítulos anteriores enumerou-se características, modelos, riscos e deficiências quanto a falta de padronizações que possam garantir uma maior confiabilidade na nuvem. No entanto, falta discutir o que leva as organizações consumidoras a não confiarem nesta nova tecnologia.

O valor da informação e o público a que se destina é o que motiva a necessidade da maioria das preocupações que impedem a adesão à nuvem computacional. Na nuvem poderão existir informações ostensivas a todos e outras extremamente sigilosas destinadas a poucos. Nem toda a informação possui o mesmo valor e este valor vai depender de quem terá acesso, dentro ou fora da organização, e que saiba fazer uso da mesma. Dentro da organização pode-se considerar os três diferentes níveis de tomada de decisão: operacional, tático e estratégico. Normalmente os dados pontuais do nível operacional serão agrupados, filtrados e analisados como informação do nível tático e que irão evoluir para o conhecimento e aporte à tomada de decisões no nível estratégico [22]. Contudo, a ênfase em processos horizontais com mais decisões sendo delegadas àqueles mais voltados ao nível operacional e tático da organização levou a uma necessidade maior de comprometimento de todas as partes da organização, da mesma forma ocorrerá com sistemas confiados a nuvem. Seja como for, toda a cadeia de transformação por que passa a informação é responsável por ela. Todos são responsáveis tanto pela informação como pelo uso que fazem dela. Contudo, a informação, como qualquer outro ativo da organização e da nuvem, deve ter um responsável, um proprietário, conforme expresso na *NBR ISO/IEC 27002:2013* [1].

Por tudo é necessário que as políticas de controle de acesso e prevenção a incidentes sejam bem definidas e estejam estabelecidas nos *SLAs*. Conflitos entre as políticas de segurança e as operações de manutenção contínua e de emergência que zelem pela conti-

nuidade do negócio não devem ser ignorados. As políticas de segurança não podem ser incompatíveis com a garantia da disponibilização do serviço. Como exemplo podemos citar sistemas de missão crítica operacionais, como sistemas militares e de saúde, que exigem políticas de segurança mais restritas e devem cumprir um conjunto de controles de segurança implementados nestas políticas. O objetivo principal destas políticas é proteger dados sigilosos e garantir a funcionalidade dos sistemas que fazem uso destes dados. Considera-se um sistema militar que controle a movimentação de viaturas em áreas de conflito e que este sistema esteja implantado em uma arquitetura de Nuvem Privada Terceirizada (NPT). Por se tratar de uma Nuvem Privada (NPr), onde não se tem o compartilhamento de recursos com outros consumidores da nuvem, este sistema parece ser imune a violações e roubo de informações. Porém, através do serviço de inteligência desta organização militar, foi descoberto que estas informações foram acessadas por pessoas não autorizadas. Como pode ter ocorrido esta falha? Como descobrir? A resposta poderá ser pelas informações de monitoramento. E surgem outras questões, como:

1. Quem é o responsável pelo monitoramento?
2. As configurações e exigências de seguranças acordadas no SLA foram implantadas pelo responsável?
3. Existem logs que possam ser analisados? Logs são registros, normalmente armazenados em arquivos $ASCII$ ou texto simples, capazes de armazenar o que se passa com sistemas computacionais e serviços de rede. A correlação de logs de eventos, segurança e auditoria são fundamentais para que se possa reconstruir o que efetivamente ocorreu com um sistema computacional no passado.
4. Existe a possibilidade desses registros de log serem alterados?

Como mencionado anteriormente, os serviços de nuvem exigem uma confiança entre o cliente e o provedor a partir de uma definição prévia de responsabilidades, mas como estabelecer esta confiança? Como escolher o provedor que melhor atenda as necessidades do consumidor?

As próximas seções e demais capítulos compõem a proposta deste trabalho que tem como objetivo principal evitar e minimizar questões como as citadas acima.

3.1 Taxonomia - Principais problemas da Computação em 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. Admiti-se 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 métricas de segurança quanto à arquitetura (ARQ), à privacidade (PRI) e à conformidade ($CONF$), associadas à taxonomia resumida na Tabela 3.1, criada a partir das Figuras 2,3 e 4 presentes na proposta de [11], 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. [11] considera que as métricas de segurança quanto à 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 métrica de solução e mitigação da categoria segurança de rede.

Tabela 3.1: 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 de Dados	S13 - Criptografia
		S14 - Redundância
		S15 - Eliminação de Dados
	Aspectos Jurídicos	S16 - Localização dos Dados
		S17 - Pesquisa e Conhecimento
		S18 - Controle de Riscos
Conformidade (CONF)	Serviços	S19 - SLA
		S20 - Falhas e Desastres
		S21 - Auditoria

Desta forma, buscando garantir a segurança nos serviços ofertados e obter a confiança de seus futuros consumidores, as seguintes categorias e subcategorias S_i devem ser oferecidas pelo provedor:

1. Categorias de Arquitetura (ARQ):

(a) Segurança de Rede: O provedor da nuvem deverá garantir aos consumidores a capacidade de mover dados e serviços da organização para a nuvem, trazer os dados novamente para dentro da organização quando necessário ou mover para outro provedor. O consumidor deverá realizar uma análise profunda dos níveis, ferramentas e técnicas de segurança disponibilizados pelos provedores, tais como: *firewall*, mecanismos de *VPN*, soluções *IDS/IPS*, protocolos seguros como *SSH*, *IPSEc* e suas implementações.

(b) Interface: Os provedores disponibilizam um conjunto de interfaces para gerenciar e interagir com os serviços oferecidos (provisionamento, gerenciamento, orquestração, monitoramento etc.). Logo, a segurança e a disponibilidade de alguns serviços da nuvem dependem da segurança destas *APIs*. Medidas como autenticação, controle de acesso, cifragem e monitoramento são fundamentais para a garantia da segurança. As interfaces devem ser protegidas contra tentativas acidentais ou maliciosas de violação de políticas de segurança. O modelo de segurança das interfaces disponibilizadas pelo provedor deve ser cuidadosamente analisado e avaliado, garantindo que mecanismos consistentes de autenticação e controle de acesso estejam implementados. A implantação de mecanismos de autenticação robustos e esquemas de delegação de direitos confiáveis são fundamentais para o gerenciamento de identidades e para a prestação de serviços em nuvens.

(c) Virtualização: A virtualização é uma tecnologia amplamente utilizada pela nuvem, tem como característica abstrair o hardware, intermediando o acesso de várias aplicações aos mesmos recursos físicos como processador e memória. O provedor deverá garantir ao consumidor ou inquilino de máquinas físicas compartilhadas uma multi alocação segura por meio de isolamento (impedindo a captura de dados de outras *VMs*) entre *VMs* alocadas sobre uma mesma plataforma física (co-residente), monitoramento de vulnerabilidades em nível de hipervisor e aplicar medidas preventivas a ataques *Cross-VM* (impedindo a obtenção de dados por vias não autorizadas).

2. Categorias de Privacidade (*PRI*):

(a) Segurança dos Dados: Os provedores precisam prover a proteção das informações sensíveis sob seu controle contra acesso não-autorizado a partir da criptografia dos dados e discos (*hash*) garantindo a integridades dos dados confiados à nuvem. Além disso, é necessário a definição de regras para armazenamento,

backup, recuperação de desastres, preservação e destruição, após o uso, de mídias contendo estes dados.

(b) Aspectos Jurídicos: O provedor é responsável pelas informações pessoais e dados sob o seu controle, devendo garantir que os mesmos estejam em conformidade com as legislações onde encontram-se localizados fisicamente, associados a políticas e requisitos internos da organização ou consumidor da nuvem. A legislação sobre privacidade pode limitar a capacidade dos provedores em transferir alguns tipos de informações para outros países, visto que alguns mecanismos que garantam a integridade dos mesmo podem ser proibidos na legislação de privacidade onde estão localizados fisicamente. Devem existir termos sobre responsabilidade de uso considerando políticas e restrições legais relativas à privacidade, com sanções legais em caso do mau uso.

3. Categoria de Conformidade (*CONF*):

(a) Serviços: O provedor deverá possibilitar ao consumidor a definição de todas as garantias quanto a desempenho, disponibilidade e tempo de recuperação a todos os tipos de incidentes que possam afetar o seu negócio. A capacidade de auditar também deverá ser explícita quanto a liberação de logs para fins de investigação.

3.2 Responsabilidades - Tipo de Nuvem quanto à Implantação e Serviço

Badger, L. em [3] 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 a 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 [12] um conjunto de políticas de segurança física e programáveis de forma a obter níveis de proteção em uma fronteira conceitual contra atividades remotas maliciosas, ilustrado na Figura 3.1.

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.

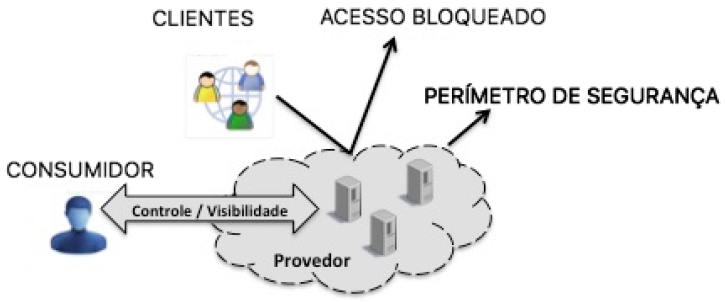

Figura 3.1: Perímetro de Segurança.

Com isso, considera-se que o nível de controle e visibilidade que o consumidor possui e delega à nuvem (confiança) é definido pelos diversos modelos na nuvem e seus respectivos perímetros de segurança, apresentados a seguir.

3.2.1 Nuvem quanto à implantação

- Nuvem Privada Local (*NPL*): O perímetro de segurança e suas configurações e medidas de controle e visibilidade serão de responsabilidade do consumidor da *NPL*.
- Nuvem Privada Terceirizada (*NPT*): A segurança e o processamento de dados da nuvem dependem da capacidade, disponibilidade e segurança dos perímetros que abrangem a área de controle do consumidor e provedor. Estes perímetros deverão

ser unidos por uma comunicação segura e protegida. A fim de evitar a confluência dos recursos de uma nuvem privada com outros recursos do consumidor que estão fora da nuvem, o provedor assume a responsabilidade da proteção da comunicação entre os perímetros.

- Nuvem Comunitária Local (*NCL*): Assim como no modelo *NPL*, serão de responsabilidade do consumidor o perímetro de segurança, suas configurações, medidas de controle e visibilidade. Inclui-se também as ligações ou comunicações seguras com as demais organizações membros da comunidade.

- Nuvem Comunitária Terceirizada (*NCT*): As medidas de controle e visibilidade são as mesmas do modelo *NPT*. O que diferencia é que o provedor deverá aplicar uma comunicação segura com políticas de compartilhamento entre as organizações membros da comunidade.

- Nuvem Pública (*NP*): O perímetro de segurança dos recursos consumidos bem como suas configurações, medidas de controle e visibilidade serão de responsabilidade do provedor da *NP*. Os consumidores possuem controle e visibilidade limitados pelos provedores, detalhes de operações e implementações são geralmente consideradas proprietárias e não divulgadas aos consumidores.

- Nuvem Híbrida (*NH*): Conforme definido no Capítulo 1, uma nuvem *NH* pode ser composta por duas ou mais nuvens privadas, comunitárias ou públicas. Além disso, há variações significativas em relação a ser local ou terceirizada. Devido a inúmeras configurações possíveis não iremos enumerá-las neste trabalho.

3.2.2 Nuvem quanto ao serviço

- *Infrastructure as a Service (IaaS)*: O consumidor tem o controle sobre o sistema operacional, armazenamento, aplicativos implantados e, possivelmente, controle limitado de componentes de rede selecionados.

- *Plataform as a Service (PaaS)*: O consumidor não gerencia ou controla a infraestrutura subjacente da nuvem, incluindo rede, servidores, sistemas operacionais, ou de armazenamento, mas tem controle sobre os aplicativos implementados e possivelmente das configurações de hospedagem plataformas oferecidas pelo ambiente na nuvem.

- *Software as a Service (SaaS)*: O consumidor não gerencia ou controla a infraestrutura subjacente da nuvem, incluindo rede, servidores, sistemas operacionais, armazenamento, ou mesmo aplicações, sendo limitado a definições de configuração aplicativo específico oferecido pela nuvem.

Tabela 3.2: Responsabilidades do Provedor.

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

A partir das definições de responsabilidades quanto ao controle e visibilidade do perímetro de segurança nos tipos de nuvem definidos em [12], associou-se na Tabela 3.2 a obrigatoriedade dos provedores quanto às categorias que compõe as métricas de segurança quanto à arquitetura, à privacidade e à conformidade na nuvem.

3.3 Definição do grau de importância das métricas de segurança

Nesta seção foi analisado 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 [23] 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.

3.3.1 Considerações sobre as avaliações

As avaliações tiveram como base o Guia de Avaliação de Riscos [20], 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 [20] 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 3.3. 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 $FP_{\acute{n}ivel}$, onde $\acute{n}ivel \in \{muito\ alta, alta, média, baixa\}$. 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 nas severidades ameaça de cada uma delas. Elas são denotadas por $FS_{\acute{n}ivel}$, onde $\acute{n}ivel \in \{muito\ alta, alta, média, baixa\}$. Logo, consideramos:

- $FS_{muito\ alta} = (75, 100]$;
- $FS_{alta} = (50, 75]$;
- $FS_{média} = (25, 50]$ e
- $FS_{baixa} = (0, 25]$.

A partir de $FP_{nível}$ e $FS_{nível}$, é possível obter o que definimos como os diferentes níveis de Faixas de Risco (denotada por $FR_{nível}$, onde também $nível \in \{muito\ alta, alta, média, baixa\}$). Para isso, multiplicamos os valores extremos de cada um dos níveis das Faixas de Probabilidade por todos os valores extremos das Faixas de Severidade. Temos, então:

- $FR_{muito\ alta} = (56.25, 100]$;
- $FR_{alta} = (25, 56.25]$;
- $FR_{média} = (6.25, 25]$ e
- $FR_{baixa} = (0, 6.25]$.

Essas escalas de risco são associadas às medidas de mitigação e soluções (S_i subcategorias) 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).

Tabela 3.3: Faixas 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

3.3.2 Extração de Dados e Avaliações das Subcategorias quanto ao risco

A base *CAPEC* possui vinte e quatro atributos, são eles : *IDAttack, Name, Typical Severity, Description, Attack Prerequisites, Typical Likelihood of Exploit, Methods of Attack, Examples-Instances, Attacker Skill or Knowledge Required, Probing Techniques, Indicators-Warnings of Attack, Solutions and Mitigations, Attack Motivation-Consequences, Context Description, Injection Vector, Payload, Activation Zone, Payload Activation Impact, CIA Impact, Related Weaknesses, Relevant Security Requeriments, Relevant Security Principles, Related Guidelines e References*. A base foi extraída em formato *XML* e convertida no formato *CSV*. Após a conversão, esta base foi preparada a partir da limpeza de atributos desnecessários, com suas medidas de "mitigação e solução" incluídas, conforme

exemplo a seguir: 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 acesso 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 quatro atributos, são eles: Identificador do Ataque(*IDAttack*), Identificador SoluçãoMitigação(*Solutions and Mitigations*), Severidade (*Typical Severity*)(muito alta, alta, média e baixa) e Probabilidade (*Typical Likelihood of Exploit*)(muito alta, alta, média e baixa). Realizou-se um agrupamento simples, utilizando a ferramenta de Mineração de Dados Weka [1], 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 3.4).

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.

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} e S_{21};
- FS_{alta} : S_{11}, S_{14}, S_{15}, S_{16}, S_{17} e S_{18};
- $FS_{média}$: S_1, S_3, S_{13} e S_{20};
- FS_{baixa} : S_4, S_5 e S_6.

Da mesma forma, realizou-se um agrupamento simples para caracterizar as subcatego-

[1] http://www.cs.waikato.ac.nz/ml/weka/.

Tabela 3.4: Frequências quanto à Severidade.

Si	muito alta	%	alta	%	média	%	baixa	%	Total
S1	2	1,20	9	2,72	2	3,28	0	0,00	13
S2	16	9,58	26	7,85	4	6,56	0	0,00	46
S3	27	16,17	56	16,92	12	19,67	2	18,18	97
S4	22	13,17	46	13,90	10	16,39	3	27,27	81
S5	26	15,57	58	17,52	8	13,11	3	27,27	95
S6	27	16,17	62	18,73	9	14,75	3	27,27	101
S7	22	13,17	32	9,67	7	11,48	0	0,00	62
S8	2	1,20	2	0,60	0	0,00	0	0,00	4
S9	1	0,60	0	0,00	0	0,00	0	0,00	0
S10	2	1,20	2	0,60	0	0,00	0	0,00	4
S11	0	0,00	3	0,91	0	0,00	0	0,00	3
S12	1	0,60	0	0,00	0	0,00	0	0,00	1
S13	5	2,99	8	2,42	5	8,20	0	0,00	18
S14	0	0,00	2	0,60	0	0,00	0	0,00	2
S15	1	0,60	3	0,91	0	0,00	0	0,00	4
S16	0	0,00	3	0,91	0	0,00	0	0,00	3
S17	0	0,00	3	0,91	0	0,00	0	0,00	3
S18	0	0,00	3	0,91	0	0,00	0	0,00	3
S19	1	0,60	0	0,00	0	0,00	0	0,00	1
S20	3	1,80	4	1,21	2	3,28	0	0,00	9
S21	9	5,39	9	2,72	2	3,28	0	0,00	20
	167		**331**		**61**		**11**		**570**

rias (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 nestas 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 3.5).

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} e S_{19};
- FP_{alta} : S_3, S_4, S_6 e S_9;
- $FP_{média}$: S_5, S_{14} e S_{15};
- FP_{baixa} : S_1, S_{10}, S_{12}, S_{13}, S_{20} e S_{21}.

A partir dos dados obtidos nas Tabelas 3.4 e 3.5 pôde-se preencher a Tabela 3.6, subcategorias associadas à Faixa de Risco correspondente, definida na Tabela 3.3.

Tabela 3.5: Frequências quanto à Probabilidade.

Si	muito alta	%	alta	%	média	%	baixa	%	Total
S1	1	1,67	4	1,13	5	3,62	3	5,77	13
S2	6	11,67	27	8,19	8	5,80	4	7,69	45
S3	9	15,00	59	17,80	20	15,22	7	17,31	95
S4	6	11,67	49	14,69	18	13,77	5	9,62	78
S5	8	13,33	59	17,51	23	18,12	6	11,54	96
S6	8	13,33	63	18,93	23	18,84	6	13,46	100
S7	6	11,67	37	11,02	15	11,59	3	5,77	61
S8	2	3,33	2	0,56	1	0,72	1	1,92	6
S9	0	0,00	1	0,28	0	0,00	0	0,00	1
S10	0	0,00	3	0,85	0	0,00	1	1,92	4
S11	1	1,67	1	0,28	0	0,00	0	0,00	2
S12	0	0,00	0	0,00	0	0,00	2	3,85	2
S13	2	3,33	9	2,82	5	3,62	6	11,54	22
S14	0	0,00	0	0,00	2	1,45	0	0,00	2
S15	0	0,00	2	0,56	2	1,45	0	0,00	4
S16	1	1,67	1	0,28	1	0,72	0	0,00	3
S17	1	1,67	1	0,28	1	0,72	0	0,00	3
S18	1	1,67	1	0,28	1	0,72	0	0,00	3
S19	1	1,67	0	0,00	0	0,00	0	0,00	1
S20	1	1,67	3	0,85	3	2,17	3	5,77	10
S21	3	5,00	12	3,67	2	1,45	2	3,85	19
	57		**334**		**130**		**49**		**570**

Tabela 3.6: Subcategorias associadas à 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]	2, 7, 8 e 19	9		10, 12 e 21
Alta (50,75]	11, 16, 17 e 18		14 e 15	
Média (25,50]		3		
Baixa (0,25]		4 e 6		1, 5, 13 e 20

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).

Neste Capítulo, a partir do conceito de perímetro de segurança na nuvem para os seus diversos modelos quanto à implantação e serviço, definiu-se as responsabilidades de consumidores e provedores quanto ao controle e visibilidade de seus recursos. Pode-se ainda mensurar, a partir de uma base de vulnerabilidades ($CAPEC$) o grau de importância das principais medidas de mitigação e solução a serem garantidas por seus responsáveis, a fim de minimizar os riscos na Nuvem Computacional.

Capítulo 4

Propostas para Cálculo de Confiança na Nuvem

Esta capítulo descreve duas propostas desenvolvidas neste trabalho para o cálculo da confiança na nuvem, sendo a primeira baseada no trabalho de Silva et al. [23], conforme citado na Seção 2.2. Além disso, buscou-se definir a importância ou a distribuição de peso às métricas de segurança quanto à Arquitetura, à Privacidade e à Conformidade, utilizadas para o cálculo da confiança em ambas as propostas. Para isso se fez necessário um estudo dos conceitos de mensuração da importância de atributos, bem como uma revisão das principais abordagens e metodologias utilizadas nos trabalhos já realizados nas áreas de planejamento, gestão e medição da qualidade de serviço.

4.1 Primeira Proposta - Valor Faixa

A primeira proposta atribui a cada subcategoria S_i um valor de risco correspondente à Faixa de Risco ($FR_{nível}$), obtida pela Faixa de Severidade ($FS_{nível}$) e Faixa de Probabilidade ($FP_{nível}$), a que pertence na Tabela 3.6. Este valor de risco é denominado Valor Faixa $fx(S_i)$, o qual será igual a :

- 1 se $S_i \in \{FR_{baixa}\}$;
- 2 se $S_i \in \{FR_{média}\}$;
- 3 se $S_i \in \{FR_{alta}\}$ e
- 4 se $S_i \in \{FR_{muito\ alta}\}$.

Como exemplo, será atribuído à subcategoria S_5 (Interface Administrativa) o $fx(S_5) = 1$ por pertencer a FR_{baixa}. No entanto, será atribuído a S_7 (Autenticação) o $fx(S_7) = 4$ por pertencer a $FR_{muito\ alta}$. Esta proposta é semelhante a de Silva et. al [23], descrita na Seção 2.2, que calcula o risco a partir de uma base de vulnerabilidades *NVD*, atribuindo a cada métrica um valor na faixa de $[0, 4]$ correspondente a níveis de segurança medidos como: Crítico, Alto, Médio, Baixo, Zero. Como descrito na Seção 2.2, o que diferencia as duas propostas é a base de vulnerabilidades em sistemas de informação utilizada para definir a faixa de valores do risco associado a cada vulnerabilidade. A base *NVD*, utilizada em [23], considera apenas o impacto da severidade, enquanto que a base *CAPEC*, utilizada nas duas propostas do presente trabalho, considera além do impacto da severidade, a probabilidade destas vulnerabilidades. A base *CAPEC* define o impacto da probabilidade das vulnerabilidades a partir de um histórico de ocorrências, baseado em publicações e referências de diferentes segmentos do sertor acadêmico, organizações e empresas.

4.2 Segunda Proposta - Valor Único

A segunda proposta atribui a cada subcategoria S_i um valor único de risco denominado Valor Único $r(S_i)$ a ser calculado a partir de valores únicos da severidade $s(S_i)$ e probabilidade $p(S_i)$. Valores estes obtidos de acordo com as faixas de severidade e de probabilidade, conforme Tabelas 3.4 e 3.5.

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 3.4. A faixa de severidade de uma subcategoria S_i, denominada $FS_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$, é dada por:

$$FS_{nível} = (s_{min}, s_{max}), \text{ onde:}$$
$$s^{min}_{nível} = \text{valor mínimo de } FS_{nível}.$$
$$s^{max}_{nível} = \text{valor máximo de } FS_{nível}.$$

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

$$\mathrm{s}(\mathrm{S}_i) = [(s^{max}_{nível} - s^{min}_{nível}) * \frac{fs(S_i)}{100}] + s^{min}_{nível}. \quad (4.1)$$

Onde: $fs(S_i)$ = frequência quanto à severidade relacionada à subcategoria $s(S_i)$.

.

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 3.5. A faixa de probabilidade de uma subcategoria S_i, denominada $FP_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$, é dada por:

$$FP_{nível} = (p_{min}, p_{max}), \text{ onde:}$$
$$p^{min}_{nível} = \text{valor mínimo de } FP_{nível}.$$
$$p^{max}_{nível} = \text{valor máximo de } FP_{nível}.$$

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

$$\mathrm{p}(\mathrm{S}_i) = [(p^{max}_{nível} - p^{min}_{nível}) * \frac{fp(S_i)}{100}] + p^{min}_{nível}. \quad (4.2)$$

Onde: $fp(S_i)$ = frequência quanto à probabilidade relacionada à subcategoria $s(S_i)$.

Uma vez que o risco $r(S_i)$ é dado por:

$$\mathrm{r}(\mathrm{S}_i) = s(S_i) * p(S_i). \quad (4.3)$$

tem-se:

$$\mathrm{r(S}_i) = \{[(s^{max}_{nível} - s^{min}_{nível}) * \frac{fs(S_i)}{100}] + s^{min}_{nível}\} * [(p^{max}_{nível} - p^{min}_{nível}) * \frac{fp(S_i)}{100}] + p^{min}_{nível}\}. \quad (4.4)$$

Este valor encontrado deverá estar na faixa de risco a que esta subcategoria está associada na Tabela 3.6.

Tabela 4.1: Valores atribuídos quanto ao risco associado.

Nível	FR	Si	fS(Si) %	FS	s(Si)	fP(Si) %	FP	p(Si)	r(Si)
muito alto	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	56,41
		S11	0,9		75,23	1,66		0,75	56,73
		S16	0,9		75,23	1,66		0,75	56,73
		S17	0,9		75,23	1,66		0,75	56,73
		S18	0,9		75,23	1,66		0,75	56,73
		S19	0,59		75,15	1,66		0,75	56,67
alto	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	25,26
		S15	0,9		50,23	1,44		0,5	25,29
médio	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
baixo	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

Como exemplo, calcula-se o valor da subcategoria S_2 (Firewall):

O maior valor de $fs(S_2)$ na Tabela 3.4 é $9,58\%$. Além disso, $fs(S_2)$ pertence à $FS = (75, 100)$ (muito alta), onde $s^{max}_{nível} = 100$ e $s^{min}_{nível} = 75$.

Substituindo estes valores à Equação 4.1, tem-se:

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

Da mesma forma, de acordo com a Tabela 3.5, o maior valor de $fp(S_2)$ é $11,66\%$. Além disso, $fs(S_2)$ pertence à $FP = (0.75, 1)$ (muito alta), onde $p^{max}_{nível} = 1$ e $p^{min}_{nível} = 0.75$.

Substituindo estes valores à Equação 4.2, tem-se:

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

Logo, substituindo os valores encontrados de $s(S_2)$ e $p(S_2)$ na Equação 4.3, obtem-se o risco

$$r(S_2) = s(S_2) * p(S_2) = 77,395 * 0,779 = 60,302,$$

que encontra-se na faixa $(56.25, 100]$, muito alta.

Na Tabela 4.1 apresenta-se o valor único de risco $r(S_i)$ atribuído a cada subcategoria S_i.

4.3 Distribuição de pesos à *ARQ*, à *PRI* e à *CONF*

Nesta seção são apresentados métodos para apoiar os consumidores da nuvem na distribuição dos pesos w_1, w_2 e w_3, que correspondem, respectivamente, às métricas de segurança quanto à Arquitetura (ARQ), à Privacidade (PRI) e à Conformidade ($CONF$), necessárias para o cálculo da confiança da nuvem computacional.

Malhotra em [15] evidencia uma técnica, denominada "Escalonamento por comparação por pares", que consiste em apresentar aos clientes (entrevistados) dois objetos para que escolham um entre eles, de acordo com algum critério. A técnica requer que todos os emparelhamentos possíveis entre os objetos, tomados dois a dois, sejam realizados, isto é, para n objetos analisados, deverão ser realizadas $n * (n - 1)/2$ comparações. A forma de analisar os dados é somar, para todos os respondentes, o número de vezes em que um objeto é preterido por outro e então dividir esta soma pelo número de respondentes, multiplicando o resultado por 100. Algumas desvantagens dessa técnica são a possibilidade de a ordem de apresentação tornar os resultados tendenciosos e a ocorrência de violações da suposição da transitividade de preferência.

Outra técnica amplamente utilizada em pesquisa de marketing, acordo Malhotra [15], é a escala "*Likert*". Esta técnica exige que os entrevistados indiquem o grau de concordância ou discordância com cada uma de uma série de afirmações sobre objetos de estímulo. A análise pode ser feita item por item, analisando o perfil, ou então calculando um escore total para cada respondente somando-se todos os itens [15]. Uma importante premissa desse método é que cada uma das afirmações meça algum aspecto de um mesmo fator comum. Caso contrário, os itens não poderão ser somados. Assim, a escala resultante

é unidimensional. Segundo Malhotra em [15], a escala *Likert* possui diversas vantagens, entre elas a facilidade de construção e aplicação, como também o entendimento por parte dos entrevistados. Como desvantagem, o autor destaca que a escala *Likert* exige maior tempo para ser concluída do que outras escalas de classificação por itens, visto que os respondentes precisam ler cada uma das afirmações.

A fim de evitar as desvantagens apresentadas nas técnicas de "Escalonamento por comparação por pares" e "*Likert*", Carvalho et al. [8] propuseram um método em termos dos atributos individuais, também obtidos por meio de um questionário em pesquisa de campo, para medir a qualidade de serviços postais no Brasil. O questionário consiste em 39 atributos que correspondem aos serviços prestados pelas agências postais (próprias) da Empresa Brasileira de Correios e Telégrafos (*ECT*) e pelas agências postais franqueadas. Para evitar a complexidade e dificuldade na ordenação dos itens, foi proposto que o respondente ordenasse apenas um subconjunto de seis atributos, relativamente pequeno em relação aos 39, e partir dessa operação parcial para obter uma ordenação completa dos atributos. A justificativa para esta metodologia reside na literatura sobre escolha entre produtos, segundo a qual um consumidor avalia apenas um grupo reduzido de marcas, entre duas a oito no máximo, em uma determinada compra. No entanto, para uma situação de pesquisa por meio de questionário de autopreenchimento, os autores sugeriram que seis atributos seriam um valor ideal.

Adaptando esta metodologia a este trabalho, considera-se:

- As 21 subcategorias S_i das métricas de segurança, presentes na Tabela 3.1, correspondem aos 39 serviços prestados em [8]. Sabe-se que dessas 21 subcategorias, 12 pertencem à *ARQ*, 6 à *PRI* e 3 à *CONF*.
- A fim de manter a proporcionalidade quanto ao número de subcategorias existentes em *ARQ*, *PRI* e *CONF*, o subconjunto de subcategorias que correspondem aos 6 produtos mais importantes em [8] é definido pela junção de 6 subcategorias de *ARQ*, 3 de *PRI* e 1 de *CONF*. Totalizando 10 subcategorias escolhidas como mais importantes pelo consumidor.

Assim como em [8], o método proposto é dividido em duas fases, onde:

- 1ª Fase: Semelhantemente à abordagem proposta por Carvalho et al. [8], os respondentes, que neste trabalho são os consumidores da nuvem, são solicitados a enumerar, por ordem decrescente de importância, 10 subcategorias S_i da Tabela

3.1. Dentre estas 10 subcategorias, é obrigatório incluir 6 subcategorias de *ARQ*, 3 de *PRI* e 1 de *CONF*, a fim de formar a lista prévia contendo todos os atributos a serem analisados. Este procedimento se refere à capacidade limitada de indivíduos em processar informações, lidar com complexidade e perseguir objetivos racionais. Segundo este conceito, as pessoas não conseguem analisar ou enumerar todo o contingente de informações que surge para elas durante uma transação. Uma forma de lidar com este conceito é partir do pressuposto de que as pessoas, perante um grande número de informações, tendem a limitar sua análise a apenas alguns aspectos considerados principais para a tomada de decisão. Como objetivos deste passo buscou-se encontrar, dentro de todas as subcategorias S_i, as consideradas como mais importantes (medida ordinal qualitativa). Adicionalmente procurou-se reduzir o tempo necessário para enumerar as subcategorias e, assim, não levar os consumidores à fadiga ou ao aborrecimento.

- 2ª Fase: Os consumidores são solicitados a atribuir notas ou valores de importância, variando de 1 a 100, às subcategorias escolhidas na primeira fase, segundo um processo comparativo com a subcategoria escolhida em primeiro lugar, o qual, por definição, recebe nota 100. Depois, as notas atribuídas a cada uma das subcategorias são somadas, totalizando a pontuação de cada medida de segurança hierarquicamente superior (*ARQ*, *PRI* e *CONF*). Por fim, calcula-se a média ponderada, considerando os valores das S_i, de *ARQ*, *PRI* e *CONF*, resultando no valor de importância w_1, w_2 e w_3 que correspondem, respectivamente, à *ARQ*, à *PRI* e à *CONF*. Assim, esta segunda fase passa a apresentar os objetivos de incluir uma medida quantitativa das diferenças de postos; facilitar a atribuição de notas ou valores, evitando utilizar o escalonamento de soma constante e finalmente incluir um ponto de referência (a subcategoria escolhida como mais importante), procurando melhorar a discriminação das mesmas.

  Pode-se enumerar as seguintes vantagens do método proposto para o presente trabalho:

  1. Não é necessário pedir aos consumidores que dêem diretamente uma nota ou valor de importância à w_1, à w_2 e à w_3, separadamente;
  2. Não se inferem os pesos refletindo a importância das subcategorias, na verdade, o valor inferido, a partir das subcategorias escolhidas para comporem o subconjunto das 10 mais importantes, refletem a importância das métricas de segurança *ARQ*, *PRI* e *CONF*; e

3. Não é necessário pedir que o consumidor ordene (em ordem de importância) todas as 21 subcategorias presentes na Tabela 3.1.

Como exemplo, supõe-se que um consumidor deseja contratar um modelo de Nuvem Pública *SaaS* (*NPSaaS*) para disponibilizar a seus usuários um catálogo de objetos pertencentes a colecionadores, definindo como prioridade uma maior disponibilidade a um menor custo. Cabe ressaltar que não se faz necessário nesta aplicação qualquer forma de autenticação ou criptografia devido à ostensividade da mesma. Supõe-se ainda que, após aplicar o método proposto, foi obtida a Tabela 4.2 representando as 10 subcategorias S_i (6 subcategorias de *ARQ*, 3 de *PRI* e 1 de *CONF*) escolhidas como as de maior prioridade, em ordem decrescente, com suas respectivas notas ou valores atribuídos.

Tabela 4.2: Valores atribuídos às 10 S_i mais importantes.

Medida de Segurança	**Ordenação da Si (+ a - importante)**	**Valor V(Si)**
Conformidade (CONF)	S19 - SLA	100
Arquitetura (ARQ)	S2 - Firewall	35
Privacidade (PRI)	S18 - Controle de Riscos	35
Privacidade (PRI)	S14 - Redundância	35
Arquitetura (ARQ)	S3 - Configurações	15
Arquitetura (ARQ)	S5 - Interface Administrativa	15
Arquitetura (ARQ)	S6 - Interface do Usuário	15
Arquitetura (ARQ)	S4 - API	10
Privacidade (PRI)	S16 - Localização de Dados	5
Arquitetura (ARQ)	S7 - Autenticação	5

A partir da ordenação e distribuição de valores das 10 S_i mais importantes, definidas pelo consumidor na Tabela 4.2, calcula-se a média ponderada, considerando os valores das S_i pertencentes à *ARQ*, à *PRI* e à *CONF*, resultando no valor de importância w_1, w_2 e w_3:

$$w_1 = \frac{\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)}{\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_{14})+\mathrm{V}(S_{16})+\mathrm{V}(S_{18})+\mathrm{V}(S_{19})}$$

$$w_1 = \frac{35+15+10+15+15+5}{35+15+10+15+15+5+35+5+35+100} = 0,351.$$

$$w_2 = \frac{\mathrm{V}(S_{14})+\mathrm{V}(S_{16})+\mathrm{V}(S_{18})}{\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_{14})+\mathrm{V}(S_{16})+\mathrm{V}(S_{18})+\mathrm{V}(S_{19})}$$

$$w_2 = \frac{35+5+35}{35+15+10+15+15+5+35+5+35+100} = 0,277.$$

$$w_3 = \frac{\mathrm{V}(S_{19})}{\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_{14})+\mathrm{V}(S_{16})+\mathrm{V}(S_{18})+\mathrm{V}(S_{19})}$$

$$w_3 = \frac{100}{35+15+10+15+15+5+35+5+35+100} = 0,370.$$

Logo, os pesos atribuídos à w_1, à w_2 e à w_3 serão, respectivamente: 0.351, 0.277 e 0.370.

A partir do método aplicado, é possível avaliar e distribuir os pesos dados a w_1, w_2 e w_3 tanto por uma abordagem qualitativa (primeira fase) quanto pela abordagem quantitativa (segunda fase).

4.4 Cálculo da Confiança

A partir destas duas formas 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 métricas de segurança ARQ, PRI e $CONF$, calcula-se a confiança (C) considerando:

- A distribuição de peso (w_k) a ser definida pelo consumidor e proporcional a seu objetivo quanto à ARQ, à PRI e à $CONF$, conforme Seção 4.3:

$$\mathrm{C}{=}(\mathrm{w}_1 * ARQ) + (w_2 * PRI) + (w_3 * CONF). \quad (4.5)$$

onde:

$$\sum_{k=1}^{3} w_k = 1, \text{ para } k \in \mathbb{N} \text{ e } 0 \leq w_k \leq 1. \quad (4.6)$$

- A proposta escolhida para obter o valor de risco de cada subcategoria S_i, onde:

– Caso a escolha seja pela primeira proposta, as subcategorias S_i presentes em *ARQ*, *PRI* e *CONF* oferecidas pelo provedor, conforme Seção 4.1:

$ARQ_{Faixa} = \sum_{i=1}^{12} fx(Si)$, $i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
$PRI_{Faixa} = \sum_{i=13}^{18} fx(S_i)$, $i \in \{13, 14, 15, 16, 17, 18\}$.
$CONF_{Faixa} = \sum_{i=19}^{21} fx(S_i)$, $i \in \{19, 20, 21\}$.

Logo, C é dada por:

$$\mathrm{C}_{Faixa} = (w_1 * \sum_{i=1}^{12} fx(Si)) + (w_2 * \sum_{i=13}^{18} fx(Si)) + (w_3 * \sum_{i=19}^{21} fx(Si)), \quad i \in \mathbb{N}. \quad (4.7)$$

– De forma análoga, escolhendo a segunda proposta, o valor único de risco $r(S_i)$ das subcategorias S_i presentes em *ARQ*, *PRI* e *CONF* oferecidas pelo provedor, conforme Seção 4.2:

$ARQ_{Único} = \sum_{i=1}^{12} r(Si)$, $i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
$PRI_{Único} = \sum_{i=13}^{18} r(S_i)$, $i \in \{13, 14, 15, 16, 17, 18\}$.
$CONF_{Único} = \sum_{i=19}^{21} r(S_i)$, $i \in \{19, 20, 21\}$.

Logo, C é dada por:

$$\mathrm{C}_{Único} = (w_1 * \sum_{i=1}^{12} r(Si)) + (w_2 * \sum_{i=13}^{18} r(Si)) + (w_3 * \sum_{i=19}^{21} r(Si)), \quad i \in \mathbb{N}. \quad (4.8)$$

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

Capítulo 5

Estudo de Casos e Análise

Neste capítulo é apresentado o estudo de casos, a partir da definição de um modelo abstrato, que permite calcular a confiança para modelos distintos de nuvem. O cálculo da confiança C é baseado nas medidas de prevenção a riscos listadas na base *CAPEC* oferecidas pelos provedores em seus Catálogos de Serviço, diferentemente da avaliação de desempenho provada por [16, 17].

De forma análoga, é apresentado um estudo de caso com base no trabalho de Silva et al[23], descrito na Seção 2.2, a fim de comparar a eficiência da avaliação da métrica não mensurável segurança, importante para ambos os trabalhos.

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.

Neste trabalho 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. A distribuição dos pesos w_1, w_2 e w_3 que correspondem, respectivamente, à *ARQ*, à *PRI* e à *CONF*, foi calculada e definida a partir do conhecimento técnico

da autora deste trabalho, de acordo com o método descrito na Seção 4.3. Na Tabela 5.1, 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. Encontram-se também nesta Tabela os valores de risco, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$ de cada subcategoria S_i, conforme definidos nas Seções 4.1 e 4.2. A partir destes valores de risco, calcula-se o valor de confiança $C_{Único}$ e C_{Faixa}, correspondentes a cada provedor hipotético.

Tabela 5.1: Catálogos de Serviço.

Métricas	Categoria	Subcategoria(Si)	A	B	C	D	fx(Si)	r(Si)
Arquitetura (ARQ)	Segurança de Rede	S1 - Transferência de Dados	X		X		1	0,01
		S2 - Firewall	X	X	X	X	4	60,30
		S3 - Configurações	X	X	X		3	29,90
	Interface	S4 - API		X	X		2	9,12
		S5 - Interface Administrativa	X	X	X	X	1	0,30
		S6 - Interface do Usuário	X	X			2	9,45
		S7 - Autenticação	X	X	X	X	4	61,00
	Virtualização	S8 - Isolamento	X	X	X	X	4	57,09
		S9 - Vulnerabilidades do Hypervision	X	X	X		4	56,41
		S10 - Vazamento de Dados		X	X		2	6,44
		S11 - Identificação de VM	X	X	X	X	4	56,73
		S12 - Ataques Cross-VM	X				2	6,52
Privacidade (PRI)	Segurança de Dados	S13 - Criptografia	X	X	X	X	1	0,05
		S14 - Redundância	X	X	X	X	3	25,25
		S15 - Eliminação de Dados	X			X	3	25,29
	Aspectos Jurídicos	S16 - Localização dos Dados		X	X		4	56,73
		S17 - Pesquisa e Conhecimento		X	X		4	56,73
		S18 - Controle de Riscos		X	X		4	56,73
Conformidade (CONF)	Serviços	S19 - SLA	X	X	X	X	4	56,67
		S20 - Falhas e Desastres	X	X	X		1	0,01
		S21 - Auditoria			X		2	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.

Visto que a arquitetura deverá ser compartilhada com outros consumidores para atender ao menor custo de hospedagem, além de garantir uma maior disponibilidade, os valores atribuídos às 10 S_i mais importantes para este cenário, utilizando o método proposto na Seção 4.3, encontram-se na Tabela 5.2.

Justificativa da Tabela 5.2:
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 como a mais prioritária e com valor de importância igual a 100. A aplicação a ser hospedada, correio eletrônico web, tem por finalidade ser utilizada por todos os funcionários da empresa como a ferramenta de envio e recebimento de mensagens, homologada e autorizada pela mesma. Com isso, as próximas S_i 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 30% da mais prioritária, uma vez que a empresa busca uma hospedagem de menor custo. As próximas quatro S_i escolhidas como prioritárias foram: "Eliminação de Dados", "Autenticação", "Interface Administrativa" e "Interface do Usuário", todas possuem uma forte relação de dependência com as duas S_i de prioridades anteriores, "Criptografia" e "Redundância", por isso foi atribuído a estas quatro S_i 50% do valor de importância das anteriores ou 15% da *"SLA"*, considerada a S_i mais prioritária. Por fim, as S_i "Transferência de Dados" e "Isolamento" foram escolhidas como as duas últimas prioritárias pela importância de enviar/receber mensagens e manter as bases destas mensagens eletrônicas em uma Nuvem Pública, com hardware e rede compartilhados. Definiu-se um valor de 5% em relação a mais prioritária por serem configurações que apresentam uma maior risco apenas na fase de implantação desta aplicação na Nuvem.

Tabela 5.2: Valores atribuídos às 10 S_i mais importantes da NPSaaS

Medida de Segurança	**Ordenação da Si (+ a - importante)**	**Valor V(Si)**
Conformidade (CONF)	S19 - SLA	100
Privacidade (PRI)	S13 - Criptografia	30
Privacidade (PRI)	S14 - Redundância	30
Arquitetura (ARQ)	S2 - Firewall	20
Privacidade (PRI)	S15 - Eliminação de Dados	15
Arquitetura (ARQ)	S7 - Autenticação	15
Arquitetura (ARQ)	S6 - Interface do Usuário	15
Arquitetura (ARQ)	S5 - Interface Administrativa	15
Arquitetura (ARQ)	S1 - Transferência de Dados	5
Arquitetura (ARQ)	S8 - Isolamento	5

A partir desta Tabela, calcula-se w_1, w_2 e w_3:

$$w_1 = \frac{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_8)}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_8)+\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})+\mathrm{V}(S_{19})}$$

$$w_1 = \frac{5+20+15+15+15+5}{5+20+15+15+15+5+30+30+15+100} = 0,3.$$

$$w_2 = \frac{\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_5)+\mathrm{V}(S_6)+\mathrm{V}(S_7)+\mathrm{V}(S_8)+\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})+\mathrm{V}(S_{19})}$$

$$w_2 = \frac{30+30+15}{5+20+15+15+15+5+30+30+15+100} = 0,3.$$

$$w_3 = \frac{\mathrm{V}_{(S_{19})}}{\mathrm{V}_{(S_1)}+\mathrm{V}_{(S_2)}+\mathrm{V}_{(S_5)}+\mathrm{V}_{(S_6)}+\mathrm{V}_{(S_7)}+\mathrm{V}_{(S_8)}+\mathrm{V}_{(S_{13})}+\mathrm{V}_{(S_{14})}+\mathrm{V}_{(S_{15})}+\mathrm{V}_{(S_{19})}}$$

$$w_3 = \frac{100}{5+20+15+15+15+5+30+30+15+100} = 0,4.$$

Com isso, os seguintes pesos são atribuídos: $w_1 = 0,3, w_2 = 0,3$ e $w_3 = 0,4$.

A partir das responsabilidades definidas na Tabela 3.2 (Seção 3.2) verifica-se que o provedor de uma nuvem *NP* é responsável por todas as subcategorias presentes na Tabela 5.1. Calculou-se, a partir da Equação 4.5 definida na Seção 4.4, o valor de confiança C de cada provedor para este cenário:

$$C = 0,3 * ARQ + 0,3 * PRI + 0,4 * CONF.$$

Calculando a Confiança (C) para cada provedor hipotético:

Provedor A:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (4, 10, 16, 17, 18, 21)\}$.

$ARQ_A = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (4, 10)\}$.
$PRI_A = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (16, 17, 18)\}$.
$CONF_A = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{AÚnico} = (0,01+60,3+29,9+0,3+9,45+61+57,09+56,41+56,73+6,52) = 337,71.$
$ARQ_{AFaixa} = (1+4+3+1+2+4+4+4+4+2) = 29.$

$PRI_{AÚnico} = (0,05+25,25+25,29) = 50,59.$
$PRI_{AFaixa} = (1+3+3) = 7.$

$CONF_{AÚnico} = (56,67+0,01) = 56,68.$
$CONF_{AFaixa} = (4+1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{AÚnico} = 0,3 * ARQ_{AÚnico} + 0,3 * PRI_{AÚnico} + 0,4 * CONF_{AÚnico} = 139,16.$
e
$C_{AFaixa} = 0,3 * ARQ_{AFaixa} + 0,3 * PRI_{AFaixa} + 0,4 * CONF_{AFaixa} = 12,8.$

Provedor B

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 12, 15, 21)\}$.

$ARQ_B = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 12)\}$.
$PRI_B = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.
$CONF_B = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{BÚnico} = (60,3+29,9+9,12+0,3+9,45+61+57,09+56,41+6,44+56,73) = 346,74.$
$ARQ_{BFaixa} = (4 + 3 + 2 + 1 + 2 + 4 + 4 + 4 + 2 + 4) = 30.$

$PRI_{BÚnico} = (0,05 + 25,25 + 56,73 + 56,73 + 56,73) = 195,49.$
$PRI_{BFaixa} = (1 + 3 + 4 + 4 + 4) = 16.$

$CONF_{BÚnico} = (56,67 + 0,01) = 56,68.$
$CONF_{BFaixa} = (4 + 1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{BÚnico} = 0,3 * ARQ_{BÚnico} + 0,3 * PRI_{BÚnico} + 0,4 * CONF_{BÚnico} = 185,34.$
e
$C_{BFaixa} = 0,3 * ARQ_{BFaixa} + 0,3 * PRI_{BFaixa} + 0,4 * CONF_{BFaixa} = 15,8.$

Provedor C:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (6, 12, 15)\}$.

$ARQ_C = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (6, 12)\}$.
$PRI_C = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.
$CONF_C = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N}\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{CÚnico} = (0,01+60,3+29,9+9,12+0,3+61+57,09+56,41+6,44+56,73) = 337,3.$
$ARQ_{CFaixa} = (1+4+3+2+1+4+4+4+2+4) = 29.$

$PRI_{CÚnico} = (0,05+25,25+56,73+56,73+56,73) = 195,49.$
$PRI_{CFaixa} = (1+3+4+4+4) = 16.$

$CONF_{CÚnico} = (56,67+0,01+6,83) = 63,51.$
$CONF_{CFaixa} = (4+1+2) = 7.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{CÚnico} = 0,3 * ARQ_{CÚnico} + 0,3 * PRI_{CÚnico} + 0,4 * CONF_{CÚnico} = 185,24.$
e
$C_{CFaixa} = 0,3 * ARQ_{CFaixa} + 0,3 * PRI_{CFaixa} + 0,4 * CONF_{CFaixa} = 16,3.$

Provedor D:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 6, 9, 10, 12, 16, 17, 18, 20, 21)\}$.

$ARQ_D = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 6, 9, 10, 12)\}$.
$PRI_D = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (16, 17, 18)\}$.

$CONF_D = \sum_{i=19}^{21} Si,\ \{i \in \mathbb{N} \mid i \neq (20, 21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{DÚnico} = (60,3 + 0,3 + 61 + 57,09 + 56,73) = 235,42.$
$ARQ_{DFaixa} = (4 + 1 + 4 + 4 + 4) = 17.$

$PRI_{DÚnico} = (0,05 + 25,25 + 25,29) = 50,59.$
$PRI_{DFaixa} = (1 + 3 + 3) = 7.$

$CONF_{DÚnico} = (56,67) = 56,67.$
$CONF_{DFaixa} = (4) = 4.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{DÚnico} = 0,3 * ARQ_{DÚnico} + 0,3 * PRI_{DÚnico} + 0,4 * CONF_{DÚnico} = 108,47.$
e
$C_{DFaixa} = 0,3 * ARQ_{DFaixa} + 0,3 * PRI_{DFaixa} + 0,4 * CONF_{DFaixa} = 8,8.$

Logo, considerando o valor de confiança $C_{Único}$, calculado a partir do valor de risco único $r(S_i)$ de cada subcategoria S_i, a sequência dos provedores, do mais confiável ao menos confiável, será : B, C, A e D.Porém, considerando o valor de confiança C_{Faixa}, calculado a partir do valor de risco na faixa $fx(S_i)$ de cada subcategoria S_i, a sequência dos provedores, do mais confiável ao menos confiável, será : C, B, A e D.

5.1.2 Cenário 2 - Nuvem Privada Terceirizada

Considera-se neste cenário que o consumidor necessite de um provedor para criar uma nuvem NPT, definindo como prioridade a maior segurança dos dados.

Por ser uma arquitetura privada, os valores atribuídos às S_i mais importantes para este cenário encontram-se na Tabela 5.3.

Justificativa da Tabela 5.3:
Sabe-se que a característica principal dos consumidores de Nuvem Privada é não admitir

a possibilidade de compartilhamento de hardware ou rede, principalmente em instalações terceirizadas, como neste Cenário. A S_i escolhida como a mais prioritária e atribuída com valor de importância igual a 100 foi a "Transferência de Dados", por se considerar crítico o compartilhamento e transferência destes dados na Internet. Em seguida, definiu-se como as próximas duas prioritárias: *"Firewall"* e "Autenticação", buscando garantir a entrada e saída de dados de forma segura pela *Internet*, atribuindo um valor de 95% em relação à primeira S_i. Além da segurança necessária no fluxo de dados, a interface utilizada pelos administradores e usuários finais desta nuvem também devem ter uma alta prioridade, sendo escolhidas as S_i: "Interface Administrativa" e "Interface do Usuário" com valor de importância igual a 90%. A S_i "Configurações" e "Auditoria"(que garante o cumprimento das configurações), foram as próximas escolhidas com valores de 80% e 70%, respectivamente. As duas próximas S_i necessárias e presentes, assim como a "Auditoria", na eficácia da S_i "Configurações" quanto a segurança de dados foram: "Redundância" e "Criptografia", associadas a estas um valor de importância 30%, próximo à 50% do valor das anteriores, 80% e 70%. Por fim, foi escolhida a S_i "Eliminação de Dados", definida com valor de 10%, necessária como garantia e cláusula de sigilo de dados em ambientes de Nuvem Privadas Terceirizadas, principalmente em caso de final de contrato de hospedagem na Nuvem.

Tabela 5.3: Valores atribuídos às 10 S_i mais importantes da NPT

Medida de Segurança	**Ordenação da Si (+ a - importante)**	**Valor V(Si)**
Arquitetura (ARQ)	S1 - Transferência de Dados	100
Arquitetura (ARQ)	S2 - Firewall	95
Arquitetura (ARQ)	S7 - Autenticação	95
Arquitetura (ARQ)	S4 - Interface do Usuário	90
Arquitetura (ARQ)	S5 - Interface Administrativa	90
Arquitetura (ARQ)	S3 - Configurações	80
Conformidade (CONF)	S21 - Auditoria	70
Privacidade (PRI)	S14 - Redundância	30
Privacidade (PRI)	S13 - Criptografia	30
Privacidade (PRI)	S15 - Eliminação de Dados	10

A partir desta Tabela, calcula-se w_1, w_2 e w_3:

$$w_1 = \frac{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_7)}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_7)+\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})+\mathrm{V}(S_{21})}$$

$$w_1 = \frac{100+95+80+90+90+95}{100+95+82+90+90+95+30+30+10+70} = 0,8.$$

$$w_2 = \frac{\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_7)+\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})+\mathrm{V}(S_{21})}$$

$$w_2 = \frac{30+30+10}{100+95+80+90+90+95+30+30+10+70} = 0,1.$$

$$w_3 = \frac{\mathrm{V}(S_{21})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_3)+\mathrm{V}(S_4)+\mathrm{V}(S_5)+\mathrm{V}(S_7)+\mathrm{V}(S_{13})+\mathrm{V}(S_{14})+\mathrm{V}(S_{15})+\mathrm{V}(S_{21})}$$

$$w_3 = \frac{70}{100+95+80+90+90+95+30+30+10+70} = 0,1.$$

Com isso, os seguintes pesos são atribuídos: $w_1 = 0,8, w_2 = 0,1$ e $w_3 = 0,1$.

Da mesma forma que o cenário anterior, o provedor de uma nuvem NPT é responsável por todas as subcategorias presentes na Tabela 5.1. O valor de confiança de cada provedor para este cenário será calculado, a partir da Equação 4.5 definida na Seção 4.4, como:

$$C = 0,8 * ARQ + 0,1 * PRI + 0,1 * CONF$$

Calculando a Confiança (C) para cada provedor hipotético:

Provedor A

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (4, 10, 16, 17, 18, 21)\}$.

$ARQ_A = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (4, 10)\}$.
$PRI_A = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (16, 17, 18)\}$.
$CONF_A = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{AÚnico} = (0,01+60,3+29,9+0,3+9,45+61+57,09+56,41+56,73+6,52) = 337,71.$
$ARQ_{AFaixa} = (1+4+3+1+2+4+4+4+4+2) = 29.$

$PRI_{AÚnico} = (0,05+25,25+25,29) = 50,59.$
$PRI_{AFaixa} = (1+3+3) = 7.$

$CONF_{AÚnico} = (56,67+0,01) = 56,68.$
$CONF_{AFaixa} = (4+1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{AÚnico} = 0,8 * ARQ_{AÚnico} + 0,1 * PRI_{AÚnico} + 0,1 * CONF_{AÚnico} = 280,89.$
e
$C_{AFaixa} = 0,8 * ARQ_{AFaixa} + 0,1 * PRI_{AFaixa} + 0,1 * CONF_{AFaixa} = 24,4.$

Provedor B

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 12, 15, 21)\}$.

$ARQ_B = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 12)\}$.
$PRI_B = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.
$CONF_B = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{BÚnico} = (60,3+29,9+9,12+0,3+9,45+61+57,09+56,41+6,44+56,73) = 346,74.$
$ARQ_{BFaixa} = (4 + 3 + 2 + 1 + 2 + 4 + 4 + 4 + 2 + 4) = 30.$

$PRI_{BÚnico} = (0,05 + 25,25 + 56,73 + 56,73 + 56,73) = 195,49.$
$PRI_{BFaixa} = (1 + 3 + 4 + 4 + 4) = 16.$

$CONF_{BÚnico} = (56,67 + 0,01) = 56,68.$
$CONF_{BFaixa} = (4 + 1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{BÚnico} = 0,8 * ARQ_{BÚnico} + 0,1 * PRI_{BÚnico} + 0,1 * CONF_{BÚnico} = 302,60.$
e
$C_{BFaixa} = 0,8 * ARQ_{BFaixa} + 0,1 * PRI_{BFaixa} + 0,1 * CONF_{BFaixa} = 26,1.$

Provedor C:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (6, 12, 15)\}$.

$ARQ_C = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (6, 12)\}$.
$PRI_C = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.
$CONF_C = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N}\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{CÚnico} = (0,01+60,3+29,9+9,12+0,3+61+57,09+56,41+6,44+56,73) = 337,3.$
$ARQ_{CFaixa} = (1+4+3+2+1+4+4+4+2+4) = 29.$

$PRI_{CÚnico} = (0,05+25,25+56,73+56,73+56,73) = 195,49.$
$PRI_{CFaixa} = (1+3+4+4+4) = 16.$

$CONF_{CÚnico} = (56,67+0,01+6,83) = 63,51.$
$CONF_{CFaixa} = (4+1+2) = 7.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{CÚnico} = 0,3 * ARQ_{CÚnico} + 0,3 * PRI_{CÚnico} + 0,4 * CONF_{CÚnico} = 295,74.$
e
$C_{CFaixa} = 0,3 * ARQ_{CFaixa} + 0,3 * PRI_{CFaixa} + 0,4 * CONF_{CFaixa} = 25,5.$

Provedor D:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 6, 9, 10, 12, 16, 17, 18, 20, 21)\}$.

$ARQ_D = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 6, 9, 10, 12)\}$.
$PRI_D = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (16, 17, 18)\}$.
$CONF_D = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (20, 21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{DÚnico} = (60,3 + 0,3 + 61 + 57,09 + 56,73) = 235,42.$
$ARQ_{DFaixa} = (4 + 1 + 4 + 4 + 4) = 17.$

$PRI_{DÚnico} = (0,05 + 25,25 + 25,29) = 50,59.$
$PRI_{DFaixa} = (1 + 3 + 3) = 7.$

$CONF_{DÚnico} = (56,67) = 56,67.$
$CONF_{DFaixa} = (4) = 4.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{DÚnico} = 0,3 * ARQ_{DÚnico} + 0,3 * PRI_{DÚnico} + 0,4 * CONF_{DÚnico} = 199,06.$
e
$C_{DFaixa} = 0,3 * ARQ_{DFaixa} + 0,3 * PRI_{DFaixa} + 0,4 * CONF_{DFaixa} = 14,7.$

Logo, considerando tanto o valor de confiança $C_{Único}$, calculado a partir do valor de risco único $r(S_i)$ de cada subcategoria S_i, quanto o valor de confiança C_{Faixa}, calculado a partir do valor de risco na faixa $fx(S_i)$ de cada subcategoria S_i, a sequência dos provedores, do mais confiável ao menos confiável, será : B, C, A e D

5.1.3 Cenário 3 - Nuvem Pública PaaS

Considera-se neste cenário que o consumidor necessite de um provedor para criar uma nuvem *NP PaaS*, definindo como prioridades a segurança na plataforma de desenvolvimento e a privacidade dos dados. Os valores atribuídos às S_i mais importantes para este cenário encontram-se na Tabela 5.4.

Justificativa da Tabela 5.4:
Neste cenário, a aplicação a ser hospedada em uma Nuvem Pública trata-se de uma ferramenta ou plataforma de desenvolvimento de aplicações finais. Com isso, qualquer falha ou abertura de segurança que afete a uma aplicação desenvolvida, por meio desta plataforma implantada na nuvem, poderá afetar a todas as demais desenvolvidas por outros

clientes. Logo a S_i definida como a mais prioritária e com valor igual a 100 foi a "Controle de Riscos". A fim de avaliar os riscos e buscar com maior eficiência e exatidão a definição de responsabilidades, a próxima S_i definida foi a "Auditoria", com valor de importância igual a 95% da primeira pela necessidade de ser realizada com uma frequência bem próxima a esta. As próximas quatro S_i escolhidas como prioritárias foram: "Pesquisas e Conhecimento", "Localização de Dados", "Transferências de Dados" e *"Firewall"*, sendo definidas com a mesma prioridade por serem essenciais quanto a políticas e regras que garantam a definição dos possíveis riscos a serem avaliados e contornados pelas duas primeiras S_i prioritárias, associando a estas um valor de importância 45%, próximo à 50% do valor das anteriores, 100% e 95%. As últimas S_i escolhidas foram: "Isolamento", "Ataques *Cross-VM*", "Vazamento de Dados" e "Vulnerabilidades no Hypervision", que se referem a garantias de privacidade e segurança quanto ao hardware e rede compartilhados na Nuvem Pública. Definiu-se a estas quatro S_i um valor de importância igual a 25%, visto que existe a necessidade destas quatro configurações em conjunto para a garantia da primeira S_i, "Controle de Riscos".

Tabela 5.4: Valores atribuídos às 10 S_i mais importantes da NPPaaS

Medida de Segurança	**Ordenação da Si (+ a - importante)**	**Valor V(Si)**
Privacidade (PRI)	S18 - Controle de Riscos	100
Conformidade (CONF)	S21 - Auditoria	95
Privacidade (PRI)	S17 - Pesquisas e Conhecimento	45
Privacidade (PRI)	S16 - Localização de Dados	45
Arquitetura (ARQ)	S1 - Transferência de Dados	45
Arquitetura (ARQ)	S2 - Firewall	45
Arquitetura (ARQ)	S8 - Isolamento	25
Arquitetura (ARQ)	S12 - Ataques Cross-VM	25
Arquitetura (ARQ)	S10 - Vazamento de Dados	25
Arquitetura (ARQ)	S9 - Vulnerabilidades do Hypervision	25

A partir desta Tabela, calcula-se w_1, w_2 e w_3:

$$w_1 = \frac{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_8)+\mathrm{V}(S_9)+\mathrm{V}(S_{10})+\mathrm{V}(S_{12})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_8)+\mathrm{V}(S_9)+\mathrm{V}(S_{10})+\mathrm{V}(S_{12})+\mathrm{V}(S_{16})+\mathrm{V}(S_{17})+\mathrm{V}(S_{18})+\mathrm{V}(S_{21})}$$

$$w_1 = \frac{45+45+25+25+25+25}{45+45+25+25+25+25+45+45+100+95} = 0,4.$$

$$w_2 = \frac{\mathrm{V}(S_{16})+\mathrm{V}(S_{17})+\mathrm{V}(S_{18})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_8)+\mathrm{V}(S_9)+\mathrm{V}(S_{10})+\mathrm{V}(S_{12})+\mathrm{V}(S_{16})+\mathrm{V}(S_{17})+\mathrm{V}(S_{18})+\mathrm{V}(S_{21})}$$

$$w_2 = \frac{45+45+100}{45+45+25+25+25+25+45+45+100+95} = 0,4.$$

$$w_3 = \frac{\mathrm{V}(S_{21})}{\mathrm{V}(S_1)+\mathrm{V}(S_2)+\mathrm{V}(S_8)+\mathrm{V}(S_9)+\mathrm{V}(S_{10})+\mathrm{V}(S_{12})+\mathrm{V}(S_{16})+\mathrm{V}(S_{17})+\mathrm{V}(S_{18})+\mathrm{V}(S_{21})}$$

$$w_3 = \frac{95}{45+45+25+25+25+25+45+45+100+95} = 0,2.$$

Com isso, os seguintes pesos são atribuídos: $w_1 = 0,4, w_2 = 0,4$ e $w_3 = 0,2$.

De forma diferente dos cenários anteriores, a partir das responsabilidades definidas na Tabela 3.2 (Seção 3.2) verificamos que o provedor é responsável pelas seguintes subcategorias presentes na Tabela 5.1: $S_1, S_2, S_3, S_8, S_9, S_{10}, S_{11}, S_{12}, S_{16}, S_{17}, S_{18}, S_{19}, S_{20}$ e S_{21}.

Assim, a partir da Equação 4.5 definida na Seção 4.4, calculamos o valor de confiança de cada provedor para este cenário:

$$C = 0,4 * ARQ + 0,4 * PRI + 0,2 * CONF.$$

Calculando a Confiança (C) para cada provedor hipotético:

Provedor A

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (4,5,6,7,10,13,14,15,16,17,18,21)\}$.

$ARQ_A = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (4,5,6,7,10)\}$.
$PRI_A = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (13,14,15,16,17,18)\}$.
$CONF_A = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{AÚnico} = (0,01 + 60,3 + 29,9 + 57,09 + 56,41 + 56,73 + 6,52) = 266,96.$
$ARQ_{AFaixa} = (1 + 4 + 3 + 4 + 4 + 4 + 2) = 22.$

$PRI_{AÚnico} = 0.$
$PRI_{AFaixa} = 0.$

$CONF_{AÚnico} = (56,67 + 0,01) = 56,68.$
$CONF_{AFaixa} = (4 + 1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{AÚnico} = 0,4 * ARQ_{AÚnico} + 0,4 * PRI_{AÚnico} + 0,2 * CONF_{AÚnico} = 118,12.$
e
$C_{AFaixa} = 0,4 * ARQ_{AFaixa} + 0,4 * PRI_{AFaixa} + 0,2 * CONF_{AFaixa} = 9,8.$

Provedor B

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1,4,5,6,7,12,13,14,15,21)\}$.

$ARQ_B = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1,4,5,6,7,12)\}$.
$PRI_B = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (13,14,15)\}$.
$CONF_B = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{BÚnico} = (60,3 + 29,9 + 57,09 + 56,41 + 6,44 + 56,73) = 266,87.$
$ARQ_{BFaixa} = (4 + 3 + 4 + 4 + 2 + 4) = 21.$

$PRI_{BÚnico} = (56,73 + 56,73 + 56,73) = 170,19.$
$PRI_{BFaixa} = (4 + 4 + 4) = 12.$

$CONF_{BÚnico} = (56,67 + 0,01) = 56,68.$
$CONF_{BFaixa} = (4 + 1) = 5.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{BÚnico} = 0,4 * ARQ_{BÚnico} + 0,4 * PRI_{BÚnico} + 0,2 * CONF_{BÚnico} = 186,16.$
e
$C_{BFaixa} = 0,4 * ARQ_{BFaixa} + 0,4 * PRI_{BFaixa} + 0,2 * CONF_{BFaixa} = 14,2.$

Provedor C:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (4, 5, 6, 7, 12, 13, 14, 15)\}$.

$ARQ_C = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (4, 5, 6, 7, 12)\}$.
$PRI_C = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (13, 14, 15)\}$.
$CONF_C = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N}\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{CÚnico} = (0,01 + 60,3 + 29,9 + 57,09 + 56,41 + 6,44 + 56,73) = 266,88.$
$ARQ_{CFaixa} = (1 + 4 + 3 + 4 + 4 + 2 + 4) = 22.$

$PRI_{CÚnico} = (56,73 + 56,73 + 56,73) = 170,19.$
$PRI_{CFaixa} = (4 + 4 + 4) = 12.$

$CONF_{CÚnico} = (56,67 + 0,01 + 6,83) = 63,51.$
$CONF_{CFaixa} = (4 + 1 + 2) = 7.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{CÚnico} = 0,4 * ARQ_{CÚnico} + 0,4 * PRI_{CÚnico} + 0,2 * CONF_{CÚnico} = 187,53.$
e
$C_{CFaixa} = 0,4 * ARQ_{CFaixa} + 0,4 * PRI_{CFaixa} + 0,2 * CONF_{CFaixa} = 15.$

Provedor D:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 5, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, 18, 20, 21)\}$.

$ARQ_D = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 3, 4, 5, 6, 7, 9, 10, 12)\}$.
$PRI_D = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (13, 14, 15, 16, 17, 18)\}$.

$CONF_D = \sum_{i=19}^{21} Si,\ \{i \in \mathbb{N} \mid i \neq (20, 21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{DÚnico} = (60,3 + 57,09 + 56,73) = 174,12.$
$ARQ_{DFaixa} = (4 + 4 + 4) = 12.$

$PRI_{DÚnico} = (0) = 0.$
$PRI_{DFaixa} = (0) = 0.$

$CONF_{DÚnico} = (56,67) = 56,67.$
$CONF_{DFaixa} = (4) = 4.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{DÚnico} = 0,4 * ARQ_{DÚnico} + 0,4 * PRI_{DÚnico} + 0,2 * CONF_{DÚnico} = 80,982.$
e
$C_{DFaixa} = 0,4 * ARQ_{DFaixa} + 0,4 * PRI_{DFaixa} + 0,2 * CONF_{DFaixa} = 5,6.$

Logo, considerando tanto o valor de confiança $C_{Único}$, calculado a partir do valor de risco único $r(S_i)$ de cada subcategoria S_i, quanto o valor de confiança C_{Faixa}, calculado a partir do valor de risco na faixa $fx(S_i)$ de cada subcategoria S_i, a sequência dos provedores, do mais confiável ao menos confiável, será : C, B, A e D

5.2 Estudo de Caso comparado à proposta de Silva et al.

Apesar do objetivo do presente trabalho, que consiste em calcular a confiança em provedores de nuvem com base em *Sec-SLA*, ser diferente do objetivo de Silva et al. [23], que é apresentar uma arquitetura de monitoramento de segurança de *Sec-SLA*, ambos os trabalhos buscam medir a métrica segurança, considerada não mensurável na nuvem.

A fim de avaliar e comparar a eficiência das propostas apresentadas nos dois trabalhos, utilizou-se a mesma base de vulnerabilidades *CAPEC*. Porém, a fim de medir o valor de

risco associado a cada vulnerabilidade ou subcategoria S_i, considera-se apenas o impacto na severidade da base *CAPEC*, assim como a proposta de Silva et al. [23]. Vale lembrar que a proposta de Silva et al. utiliza a base *NVD*, que considera apenas o impacto da severidade.

Com isso, a Faixa de Risco ($FR_{nível}$) é avaliada considerando apenas a Faixa de Severidade ($FS_{nível}$). Com base na Tabela 3.4 da Subseção 3.3.2, que representa a Faixa de Severidade, as subcategorias estão distribuídas e representadas em relação à Faixa de Risco $FR_{nível}$ do Padrão de Ataque como:

- $FR_{muito\ alta}$: S_2, S_7, S_8, S_9, S_{10}, S_{12}, S_{19} e S_{21};
- FR_{alta} : S_{11}, S_{14}, S_{15}, S_{16}, S_{17} e S_{18};
- $FR_{média}$: S_1, S_3, S_{13} e S_{20};
- FR_{baixa} : S_4, S_5 e S_6.

Além disso, sabe-se que :

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 3.4. Esta faixa de severidade $FS_{nível}$, onde $nível \in \{muito\ alta, alta, média, baixa\}$, é dada por:

$$FS_{nível} = (s_{min}, s_{max}), \text{ onde:}$$
$$s^{min}_{nível} = \text{valor mínimo de } FS_{nível}.$$
$$s^{max}_{nível} = \text{valor máximo de } FS_{nível}.$$

Portanto, considerando $s(S_i)$ como a severidade relacionada à subcategoria S_i, o Valor Único $r(S_i)$ de risco, calculado a partir apenas da Equação 4.1 definida na Seção 4.2 e não considerando a probabilidade $p(S_i)$, é dado por:

$$\mathrm{r(S}_i) = s(S_i) = [(s^{max}_{nível} - s^{min}_{nível}) * \frac{fs(S_i)}{100}] + s^{min}_{nível}. \quad (5.1)$$

Na Tabela 5.5 encontra-se o Valor Único de risco $\mathrm{r}(S_i)$ atribuído a cada subcategoria S_i.

Tabela 5.5: Valores atribuídos ao risco considerando a proposta de Silva et al.

Nível	Si	fs(Si) %	FS	FR	s(Si)	r(Si)
Muito Alta	S2	9,58	75-100	75-100	77,395	77,395
	S7	13,17			78,2925	78,2925
	S8	1,2			75,3	75,3
	S9	0,6			75,15	75,15
	S10	1,2			75,3	75,3
	S12	0,6			75,15	75,15
	S19	0,6			75,15	75,15
	S21	5,39			76,3475	76,3475
Alta	S11	0,91	50-75	50-75	50,2275	50,2275
	S14	0,6			50,15	50,15
	S15	0,91			50,2275	50,2275
	S16	0,91			50,2275	50,2275
	S17	0,91			50,2275	50,2275
	S18	0,91			50,2275	50,2275
Média	S1	3,28	25-50	25-50	25,82	25,82
	S3	19,67			29,9175	29,9175
	S13	8,2			27,05	27,05
	S20	3,28			25,82	25,82
Baixa	S4	27,27	0-25	0-25	6,8175	6,8175
	S5	27,27			6,8175	6,8175
	S6	27,27			6,8175	6,8175

Tabela 5.6: Catálogos de Serviço segundo a proposta de Silva et al.

Métricas	Categoria	Subcategoria(Si)	A	B	C	D	fx(Si)	r(Si)
Arquitetura (ARQ)	Segurança de Rede	S1 - Transferência de Dados	X		X		2	25,82
		S2 - Firewall	X	X	X	X	4	77,4
		S3 - Configurações	X	X	X		2	29,92
	Interface	S4 - API		X	X		1	6,81
		S5 - Interface Administrativa	X	X	X	X	1	6,81
		S6 - Interface do Usuário	X	X			1	6,81
		S7 - Autenticação	X	X	X	X	4	78,29
	Virtualização	S8 - Isolamento	X	X	X	X	4	75,3
		S9 - Vulnerabilidades do Hypervision	X	X	X		4	75,15
		S10 - Vazamento de Dados		X	X		4	75,3
		S11 - Identificação de VM	X	X	X	X	3	50,23
		S12 - Ataques Cross-VM	X				4	75,15
Privacidade (PRI)	Segurança de Dados	S13 - Criptografia	X	X	X	X	2	27,05
		S14 - Redundância	X	X	X	X	3	50,15
		S15 - Eliminação de Dados	X			X	3	50,23
	Aspectos Jurídicos	S16 - Localização dos Dados		X	X		3	50,23
		S17 - Pesquisa e Conhecimento		X	X		3	50,23
		S18 - Controle de Riscos		X	X		3	50,23
Conformidade (CONF)	Serviços	S19 - SLA	X	X	X	X	4	75,15
		S20 - Falhas e Desastres	X	X	X		2	25,82
		S21 - Auditoria			X		4	76,35

5.2.1 Cenário 1 - Nuvem Pública SaaS aplicado a proposta de Silva et al.

Considera-se o mesmo cenário apresentado na Subseção 5.1.1 de uma Nuvem Pública *SaaS*, porém, a partir da proposta de Silva et al. [23]. Desta forma, os novos valores de risco na faixa fx(S_i) e único r(S_i), definidos na Seção 5.2, estão presentes na Tabela 5.6 que corresponde aos catálogos de serviço dos provedores hipotéticos A, B, C e D.

Calculou-se, a partir da Equação 4.5 definida na Seção 4.4, o valor de confiança C de

cada provedor para este cenário:

$$C = 0,3 * ARQ + 0,3 * PRI + 0,4 * CONF.$$

Calculando a Confiança (C) para cada provedor hipotético:

Provedor A:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (4, 10, 16, 17, 18, 21)\}$.

$ARQ_A = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (4, 10)\}$.
$PRI_A = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (16, 17, 18)\}$.
$CONF_A = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{AÚnico} = (25,82+77,4+29,92+6,81+6,81+78,29+75,3+75,15+50,23+75,15) = 500,88$.
$ARQ_{AFaixa} = (2 + 4 + 2 + 1 + 1 + 4 + 4 + 4 + 3 + 4) = 29$.

$PRI_{AÚnico} = (27,05 + 50,15 + 50,23) = 127,43$.
$PRI_{AFaixa} = (2 + 3 + 3) = 8$.

$CONF_{AÚnico} = (75,15 + 25,82) = 100,97$.
$CONF_{AFaixa} = (4 + 2) = 6$.

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{AÚnico} = 0,3 * ARQ_{AÚnico} + 0,3 * PRI_{AÚnico} + 0,4 * CONF_{AÚnico} = 228,88$.
e
$C_{AFaixa} = 0,3 * ARQ_{AFaixa} + 0,3 * PRI_{AFaixa} + 0,4 * CONF_{AFaixa} = 13,5$.

Provedor B

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1, 12, 15, 21)\}$.

$ARQ_B = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (1, 12)\}$.
$PRI_B = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.
$CONF_B = \sum_{i=19}^{21} Si$, $\{i \in \mathbb{N} \mid i \neq (21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{BÚnico} = (77,4+29,92+6,81+6,81+6,81+78,29+75,3+75,15+75,3+50,23) = 482,02$.
$ARQ_{BFaixa} = (4+2+1+1+1+4+4+4+4+3) = 28$.

$PRI_{BÚnico} = (27,05+50,15+50,23+50,23+50,23) = 227,89$.
$PRI_{BFaixa} = (2+3+3+3+3) = 14$.

$CONF_{BÚnico} = (75,15+25,82) = 100,97$.
$CONF_{BFaixa} = (4+2) = 6$.

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{BÚnico} = 0,3 * ARQ_{BÚnico} + 0,3 * PRI_{BÚnico} + 0,4 * CONF_{BÚnico} = 253,37$.
e
$C_{BFaixa} = 0,3 * ARQ_{BFaixa} + 0,3 * PRI_{BFaixa} + 0,4 * CONF_{BFaixa} = 15$.

Provedor C:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (6, 12, 15)\}$.

$ARQ_C = \sum_{i=1}^{12} Si$, $\{i \in \mathbb{N} \mid i \neq (6, 12)\}$.
$PRI_C = \sum_{i=13}^{18} Si$, $\{i \in \mathbb{N} \mid i \neq (15)\}$.

$CONF_C = \sum_{i=19}^{21} Si,\ \{i \in \mathbb{N}\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{CÚnico} = (25,82+77,4+29,92+6,81+6,81+78,29+75,3+75,15+75,3+50,23) = 501,03$.
$ARQ_{CFaixa} = (2+4+2+1+1+4+4+4+4+3) = 29$.

$PRI_{CÚnico} = (27,05+50,15+50,23+50,23+50,23) = 227,89$.
$PRI_{CFaixa} = (2+3+3+3+3) = 14$.

$CONF_{CÚnico} = (75,15+25,82+76,35) = 177,32$.
$CONF_{CFaixa} = (4+2+4) = 10$.

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{CÚnico} = 0,3 * ARQ_{CÚnico} + 0,3 * PRI_{CÚnico} + 0,4 * CONF_{CÚnico} = 289,599$.
e
$C_{CFaixa} = 0,3 * ARQ_{CFaixa} + 0,3 * PRI_{CFaixa} + 0,4 * CONF_{CFaixa} = 16,9$.

Provedor D:

Conforme Tabela 5.1 e Tabela 3.2 da Seção 3.2, estão presentes no Catálogo de Serviços as subcategorias S_i, $1 \leq i \leq 21$ e $\{i \in \mathbb{N} \mid i \neq (1,3,4,6,9,10,12,16,17,18,20,21)\}$.

$ARQ_D = \sum_{i=1}^{12} Si,\ \{i \in \mathbb{N} \mid i \neq (1,3,4,6,9,10,12)\}$.
$PRI_D = \sum_{i=13}^{18} Si,\ \{i \in \mathbb{N} \mid i \neq (16,17,18)\}$.
$CONF_D = \sum_{i=19}^{21} Si,\ \{i \in \mathbb{N} \mid i \neq (20,21)\}$.

De acordo com os valores de risco definidos para cada subcategoria S_i, Valor Faixa $fx(S_i)$ e Valor Único $r(S_i)$, dispostos na Tabela 5.1, tem-se:

$ARQ_{DÚnico} = (77,4+6,81+78,29+75,3+50,23) = 288,03$.

$ARQ_{DFaixa} = (4 + 1 + 4 + 4 + 3) = 16.$

$PRI_{DÚnico} = (27,05 + 50,15 + 50,23) = 127,43.$
$PRI_{DFaixa} = (2 + 3 + 3) = 8.$

$CONF_{DÚnico} = (75,15) = 75,15.$
$CONF_{DFaixa} = (4) = 4.$

Substituindo os valores encontrados nas Equações 4.8 e 4.7, calcula-se os valores de Confiança $C_{Único}$ e C_{Faixa}:

$C_{DÚnico} = 0,3 * ARQ_{DÚnico} + 0,3 * PRI_{DÚnico} + 0,4 * CONF_{DÚnico} = 154,69.$
e
$C_{DFaixa} = 0,3 * ARQ_{DFaixa} + 0,3 * PRI_{DFaixa} + 0,4 * CONF_{DFaixa} = 8,8.$

Logo, considerando o valor de confiança $C_{Único}$, calculado a partir do valor de risco único $r(S_i)$ de cada subcategoria S_i, a sequência dos provedores, do mais confiável ao menos confiável será : C, B, A e D. Diferentemente do resultado obtido na Subseção 5.1.1, onde o maior valor de confiança $C_{Único}$ é atribuído a B. Porém, considerando o valor de confiança C_{Faixa}, calculado a partir do valor de risco na faixa $fx(S_i)$ de cada subcategoria S_i, o provedor de maior confiança para ambos os cenários é o provedor C.

5.3 Análise dos Resultados

Comparando os resultados apresentados nas Seções 5.1 e 5.2, ambos considerando o mesmo cenário de uma Nuvem Pública SaaS, observou-se que provedores distintos foram classificados como o mais confiável, utilizando o valor único associado a cada subcategoria $r(Si)$. No Cenário 1 da Subseção 5.1.1, que utiliza a proposta deste trabalho para o cálculo da Confiança, o provedor com o maior valor de Confiança $C_{Único}$ foi o provedor B. Diferentemente, o mesmo Cenário 1, aplicado à proposta de Silva et al. [23], obteve como resultado de maior valor de Confiança $C_{Único}$ o provedor C. Porém, utilizando o valor de risco correspondente por faixa de risco $fx(Si)$, os resultados apresentados nas Seções 5.1 e 5.2 quanto ao provedor mais confiável (C_{Faixa}) foram os mesmos, o provedor C.

Intuitivamente, percebe-se que a diferença principal no cálculo da Confiança (C) de um provedor não é somente o fato de considerar um valor de risco único ($C_{Único}$), como

na Subseção 4.2, ou um valor associado a uma faixa de risco, como na Subseção 4.1 e 2.2(C_{Faixa}), propostas respectivamente do presente trabalho e de Silva et al. [23]. O que diferencia, nas propostas de ambos os trabalhos, é o fato do presente trabalho considerar na avaliação de risco associado a cada subcategoria S_i o impacto da severidade e da probabilidade. O que não ocorre no trabalho de Silva et al. [23], pois considera somente o impacto da severidade na avaliação de risco. Cabe ressaltar que todos os cenários foram avaliados a partir da mesma base de vulnerabilidades *CAPEC*.

A análise sobre qual forma de avaliação do risco associado é a mais eficiente, utilizando o impacto da severidade e da probabilidade ou somente o impacto da severidade, encontra-se no próximo capítulo, visto que a constatação sobre a eficiência somente ser possível comparando os resultados obtidos nos cenários hipotéticos aos resultados obtidos nos experimentos em ambiente real. Porém, a análise sobre considerar o valor de risco único $r(Si)$ ou por faixa de risco $fx(Si)$ associado a cada subcategoria S_i é feita a seguir.

Avaliando os resultados obtidos e descritos no cálculo da confiança ($C_{Único}$ e C_{Faixa}), como exemplo, no Cenário 1 da Subseção 5.1.1, observa-se que o provedor C, com valor $C_{CFaixa} = 16,3$, foi considerado mais confiável em relação ao provedor B, com valor de $C_{BFaixa} = 15,8$. Porém, o mesmo não ocorreu, e por pouca diferença, considerando o valor $C_{CÚnico} = 185,24$ encontrado para o provedor C e o valor $C_{BÚnico} = 185,34$ encontrado para o provedor B. Portanto, sendo o provedor B, a partir do cálculo de confiança $C_{Único}$, o provedor considerado como o mais confiável.

Analisando a diferença entre os valores de confiança do provedor mais confiável ao menos confiável, considerando o valor de risco único $r(Si)$ e por faixa de risco $fx(Si)$, pôde-se notar que a diferença entre as duas formas de calcular a Confiança C ($C_{Único}$ e C_{Faixa}) tornam uma avaliação mais precisa do que a outra. Observa-se que a diferença percentual entre o valor de confiança calculado para os provedores B e C, considerando o valor único $r(Si)$ foi de $0,05\%$ ($C_{BÚnico} = 185,34$ e $C_{CÚnico} = 185,24$). Porém, considerando o valor correspondente por faixa de risco $fx(Si)$, a diferença entre valor de confiança calculado para os provedores B e C passa a ser de $3,06\%$ ($C_{BFaixa} = 15,8$ e $C_{CFaixa} = 16,3$), com uma diferença de $3,11\%$ entre as duas formas de avaliar a confiança ($C_{Único}$ e C_{Faixa}).

Da mesma forma, avaliando a diferença entre os valores de confiança dos provedores B e A, considerando o valor único $r(Si)$, foi de aproximadamente 25% ($C_{BÚnico} = 185,34$ e $C_{AÚnico} = 139,16$). Porém, considerando o valor correspondente por faixa de risco $fx(Si)$, a diferença entre valor de confiança calculado para os provedores B e A passa a ser de

19% ($C_{BFaixa} = 15,8$ e $C_{AFaixa} = 12,8$), agora com uma diferença de 6% entre as duas formas de avaliar.

Avaliando a diferença mais extrema, entre os provedores B (maior confiança) e D (menor confiança), considerando o valor único $r(Si)$, foi de aproximadamente $58,5\%$ ($C_{BÚnico} = 185,34$ e $C_{DÚnico} = 108,47$). Porém, considerando o valor correspondente por faixa de risco $fx(Si)$, a diferença entre valor de confiança calculado para os provedores B e D passa a ser de 42% ($C_{BFaixa} = 15,8$ e $C_{DFaixa} = 9,2$), com uma diferença bem maior, de $16,5\%$ entre as duas formas de avaliar ($C_{Único}$ e C_{Faixa}). Com isso, nota-se que através da utilização de um valor único associado a cada subcategoria $r(Si)$, calculado com base na faixa de severidade e probabilidade que está associada nas Tabelas 3.3 e 3.4, foram obtidos resultados mais precisos do que utilizando um valor correspondente por faixa de risco $fx(Si)$.

Intuitivamente, essa maior precisão se deve pelo intervalo de valores possíveis do valor de risco associado a cada subcategoria S_i ser de $[1, 4]$, na primeira proposta (Seção 4.1), enquanto que, na segunda proposta (Seção 4.2), ser de $[0, 100]$. Logo, utilizando a segunda proposta é possível obter, de forma mais precisa, o quão mais confiável um provedor é dos demais avaliados, em relação à primeira proposta. A partir desta análise, respondemos 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, à privacidade e à conformidade será necessário um padrão de *Sec-SLA* que melhor atenda o consumidor. Analisando apenas a reputação proposta em [17] e métricas de desempenho de *QoS* em [16] não é possível obter esta diferenciação e padronização de *Sec-SLA*.

Capítulo 6

Experimentos em Ambiente Real

Ao analisar a Tabela 3.2 na Seção 3.2, que define a responsabilidade de consumidores e provedores nos diversos modelos de nuvem quanto à 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 à 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), obtidos a partir do modelo proposto na Seção 4.3, além das 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 neste trabalho para o cálculo de confiança na nuvem foi realizada com configurações correspondentes ao catálogo de serviços de cada provedor hipotético, conforme Tabela 5.1 da Seção 5.1. Estas configurações correspondem a presença ou ausência de algumas subcategorias presentes na Tabela 3.1 da Seção 3.1. A Tabela 6.1 consiste na representação dos dados obtidos a partir da Tabela 5.1, 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 métricas de segurança quanto à arquitetura, à privacidade e à conformidade. O cálculo do número de vulnerabilidades de cada provedor hipotético ($NrVulnerabilidades_{Provedor}$) é feito conforme equação a seguir:

$$\text{NrVulnerabilidades}_{Provedor} = (w_1 * ARQ_{NrVulnerabilidades}) + (w_2 * PRI_{NrVulnerabilidades}) + (w_3 * CONF_{NrVulnerabilidades}). \quad (6.1)$$

onde:

$$\sum_{k=1}^{3} w_k = 1, \text{ para } k \in \mathbb{N} \text{ e } 0 \leq w_k \leq 1. \quad (6.2)$$

e o número de vulnerabilidades quanto à ARQ, à PRI e à $CONF$, obtidos a partir da Tabela 6.1, será :

$ARQ_{NrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ i \in \{1,2,3,4,5,6,7,8,9,10,11,12\}.$
$PRI_{NrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ i \in \{13,14,15,16,17,18\}.$
$CONF_{NrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ i \in \{19,20,21\}.$

Foram considerados mais confiáveis os provedores que, considerando o número de vulne-

rabilidades presentes na Tabela 6.1 e substituindo os mesmos na Equação 6.1, obtiveram o menor valor de $NrVulnerabilidades_{Provedor}$. Em seguida, comparou-se os resultados obtidos ao valor de confiança medido nos Cenários 1 e 3 da Seção 5.1. Além desta validação, foi analisada a eficiência de como medir a métrica segurança, comparando o valor de $NrVulnerabilidades_{Provedor}$, encontrado a partir das vulnerabilidades presentes na Tabela 6.1 e Equação 6.1, aos resultados obtidos no Cenário 1 da Seção 5.2. Cabe lembrar que este cenário considera apenas o impacto da severidade da base *CAPEC*, conforme Tabela 5.6.

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 6.1, 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 6.1, varridas, analisadas pelas ferramentas *Network Mapper - Nmap* [21] e *Nessus Vulnerability Scanner* [19], para explorar vulnerabilidades de rede/segurança, e pela ferramenta *Acunetix Web Vulnerability Scanner* [2] para explorar vulnerabilidades de aplicações *web*. O número de vulnerabilidades reportados nos relatórios destas ferramentas foi acrescido aos do item (b).

6.1.1 Ambientes de Validação

O servidor de Correio Eletrônico é 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), mais especificamente Cenário 1 (nuvem *NP SaaS*) das Seções 5.1 e 5.2. A configuração do Correio Eletrônico é realizada com base em servidores virtuais, SO *Suse Linux* com a solução *IBM Domino Lotus Notes*[1] 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 6.1.

[1]https://www-01.ibm.com/software/br/lotus/products/notes/.

Tabela 6.1: Configurações e Vulnerabilidades.

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

O cenário escolhido para validar os modelos que se enquadram na semelhança (b) e Cenário 3 (nuvem *NP PaaS*) da Seção 5.1 foi o Gerenciador de Conteúdo Drupal[2], 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 6.1.

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 nuvem *NP SaaS* (Correio *Lotus Notes*) encontra-se descrito por subcategoria S_i na Tabela 6.1 e representado graficamente na Figura 6.1. Da mesma forma, o quantitativo de vulnerabilidades encontradas nas métricas *ARQ*, *PRI* e *CONF* na nuvem *NP* (Drupal) encontra-se descrito por subcategoria S_i na Tabela 6.1 e representado graficamente na Figura 6.2.

Aplicando os dados obtidos no Cenário 1 da Subseção 5.1.1, onde foram atribuídos os

[2]https://www.drupal.org.

pesos $w_1 = 0,3, w_2 = 0,3$ e $w_3 = 0,4$, além de definidas as responsabilidades a partir da Tabela 3.2 (Seção 3.2), calculou-se o $NrVulnerabilidades_{Provedor}$ considerando a Equação 6.1 e Tabela 6.1:

$NrVulnerabilidades_{Provedor} = (0,3 * ARQ_{NrVulnerabilidades}) + (0,3 * PRI_{NrVulnerabilidades}) + (0,4 * CONF_{NrVulnerabilidades})$.

Calculando o $NrVulnerabilidades_{Provedor}$ para cada provedor hipotético:

Provedor A:

$ARQ_{ANrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.
$PRI_{ANrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.
$CONF_{ANrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{ANrVulnerabilidades} = (0 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 1 + 0 + 0) = 2$.
$PRI_{ANrVulnerabilidades} = (0 + 0 + 0 + 1 + 1 + 1) = 3$.
$CONF_{ANrVulnerabilidades} = (0 + 0 + 1) = 1$.

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_A$:

$NrVulnerabilidades_A = 0,3 * ARQ_{ANrVulnerabilidades} + 0,3 * PRI_{ANrVulnerabilidades} + 0,4 * CONF_{ANrVulnerabilidades} = 1,9$.

Provedor B

$ARQ_{BNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.
$PRI_{BNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.
$CONF_{BNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si), \{i \in \mathbb{N}\}$.

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{BNrVulnerabilidades} = (1+0+0+0+0+0+0+0+0+0+0+1) = 2.$
$PRI_{BNrVulnerabilidades} = (0+0+1+0+0+0) = 1.$
$CONF_{BNrVulnerabilidades} = (0+0+1) = 1.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_B$:

$NrVulnerabilidades_B = 0,3 * ARQ_{BNrVulnerabilidades} + 0,3 * PRI_{BNrVulnerabilidades} + 0,4 *$
$CONF_{BNrVulnerabilidades} = 1,3.$

Provedor C:

$ARQ_{CNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$
$PRI_{CNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$
$CONF_{CNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{CNrVulnerabilidades} = (0+0+0+0+0+3+0+0+0+0+0+1) = 4.$
$PRI_{CNrVulnerabilidades} = (0+0+1+0+0+0) = 1.$
$CONF_{CNrVulnerabilidades} = (0+0+0) = 0.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_C$:

$NrVulnerabilidades_C = 0,3 * ARQ_{CNrVulnerabilidades} + 0,3 * PRI_{CNrVulnerabilidades} + 0,4 *$
$CONF_{CNrVulnerabilidades} = 1,5.$

Provedor D:

$ARQ_{DNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$
$PRI_{DNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$
$CONF_{DNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{DNrVulnerabilidades} = (1+0+1+1+0+8+0+0+1+1+0+1) = 14.$
$PRI_{DNrVulnerabilidades} = (0+0+0+1+1+1) = 3.$
$CONF_{DNrVulnerabilidades} = (0+1+1) = 2.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_D$:

$NrVulnerabilidades_D = 0,3 * ARQ_{DNrVulnerabilidades} + 0,3 * PRI_{DNrVulnerabilidades} + 0,4 * CONF_{DNrVulnerabilidades} = 5,9.$

Logo, considerando o número de vulnerabilidades presentes em cada provedor, calculado a partir da Equação 6.1 e Tabela 6.1, a sequência dos provedores, do mais confiável ao menos confiável, será : B, C, A e D.

De forma análoga, aplicando os dados obtidos no Cenário 3 da Subseção 5.1.3, onde foram atribuídos os pesos $w_1 = 0,4, w_2 = 0,4$ e $w_3 = 0,2$, além de definidas as responsabilidades a partir da Tabela 3.2 (Seção 3.2), calculou-se o $NrVulnerabilidades_{Provedor}$ considerando a Equação 6.1 e Tabela 6.1:

$NrVulnerabilidades_{Provedor} = (0,4 * ARQ_{NrVulnerabilidades}) + (0,4 * PRI_{NrVulnerabilidades}) + (0,2 * CONF_{NrVulnerabilidades})$.

Calculando $NrVulnerabilidades_{Provedor}$ para cada provedor hipotético:

Provedor A:

$ARQ_{ANrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (4,5,6,7)\}.$
$PRI_{ANrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (13,14,15)\}.$
$CONF_{ANrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{ANrVulnerabilidades} = (0+0+0+0+0+7+0+0) = 7.$
$PRI_{ANrVulnerabilidades} = (1+1+1) = 3.$
$CONF_{ANrVulnerabilidades} = (0+0+1) = 1.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_A$:

$NrVulnerabilidades_A = 0,4 * ARQ_{ANrVulnerabilidades} + 0,4 * PRI_{ANrVulnerabilidades} + 0,2 * CONF_{ANrVulnerabilidades} = 4,2.$

Provedor B

$ARQ_{BNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (4,5,6,7)\}.$
$PRI_{BNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (13,14,15)\}.$
$CONF_{BNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{BNrVulnerabilidades} = (7 + 0 + 0 + 0 + 0 + 0 + 0 + 1) = 8.$
$PRI_{BNrVulnerabilidades} = (0 + 0 + 0) = 0.$
$CONF_{BNrVulnerabilidades} = (0 + 0 + 1) = 1.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_B$:

$NrVulnerabilidades_B = 0,4 * ARQ_{BNrVulnerabilidades} + 0,4 * PRI_{BNrVulnerabilidades} + 0,2 * CONF_{BNrVulnerabilidades} = 3,4.$

Provedor C:

$ARQ_{CNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (4,5,6,7)\}.$
$PRI_{CNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (13,14,15)\}.$
$CONF_{CNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{CNrVulnerabilidades} = (0 + 0 + 0 + 0 + 0 + 0 + 0 + 1) = 1.$
$PRI_{CNrVulnerabilidades} = (0 + 0 + 0) = 0.$
$CONF_{CNrVulnerabilidades} = (0 + 0 + 0) = 0.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_C$:

$NrVulnerabilidades_C = 0,4 * ARQ_{CNrVulnerabilidades} + 0,4 * PRI_{CNrVulnerabilidades} + 0,2 * CONF_{CNrVulnerabilidades} = 0,4.$

Provedor D:

$ARQ_{DNrVulnerabilidades} = \sum_{i=1}^{12} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (4,5,6,7)\}.$
$PRI_{DNrVulnerabilidades} = \sum_{i=13}^{18} NrVulnerabilidades(Si),\ \{i \in \mathbb{N} \mid i \neq (13,14,15)\}.$
$CONF_{DNrVulnerabilidades} = \sum_{i=19}^{21} NrVulnerabilidades(Si),\ \{i \in \mathbb{N}\}.$

De acordo com o número de vulnerabilidades presentes na Tabela 6.1 para cada subcategoria S_i, tem-se:

$ARQ_{DNrVulnerabilidades} = (7 + 0 + 4 + 0 + 1 + 1 + 0 + 1) = 14.$
$PRI_{DNrVulnerabilidades} = (1 + 1 + 1) = 3.$
$CONF_{DNrVulnerabilidades} = (0 + 1 + 1) = 2.$

Substituindo os valores encontrados na Equação 6.1, calcula-se o valor do $NrVulnerabilidades_D$:

$NrVulnerabilidades_D = 0,4 * ARQ_{DNrVulnerabilidades} + 0,4 * PRI_{DNrVulnerabilidades} + 0,2 * CONF_{DNrVulnerabilidades} = 7,2.$

Logo, considerando o número de vulnerabilidades presentes em cada provedor, calculado a partir da Equação 6.1 e Tabela 6.1, a sequência dos provedores, do mais confiável ao menos confiável, será : C, B, A e D.

6.2 Análise dos Resultados Obtidos

A partir das Figuras 6.1 e 6.2, que representam graficamente o somatório das vulnerabilidades encontradas nas subcategorias S_i dos provedores hipotéticos (Tabela 6.1) nos cenários de nuvem *NP SaaS* e *NP PaaS*, 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

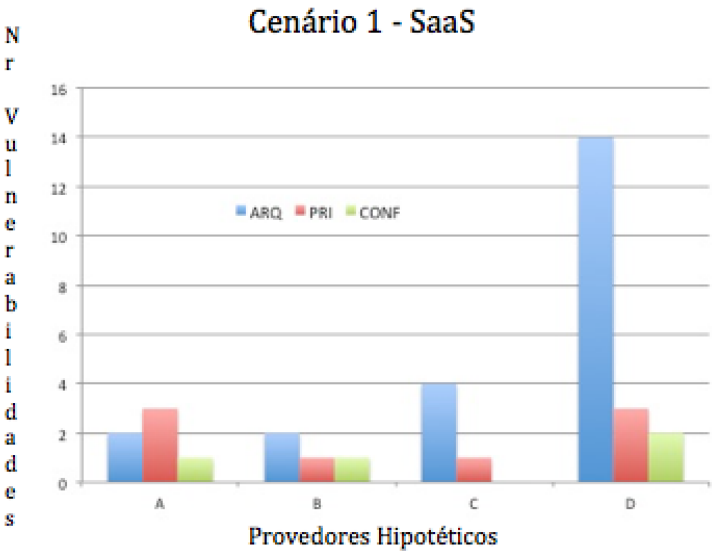

Figura 6.1: Número de vulnerabilidades encontradas nos provedores hipotéticos referente ao Cenário 1.

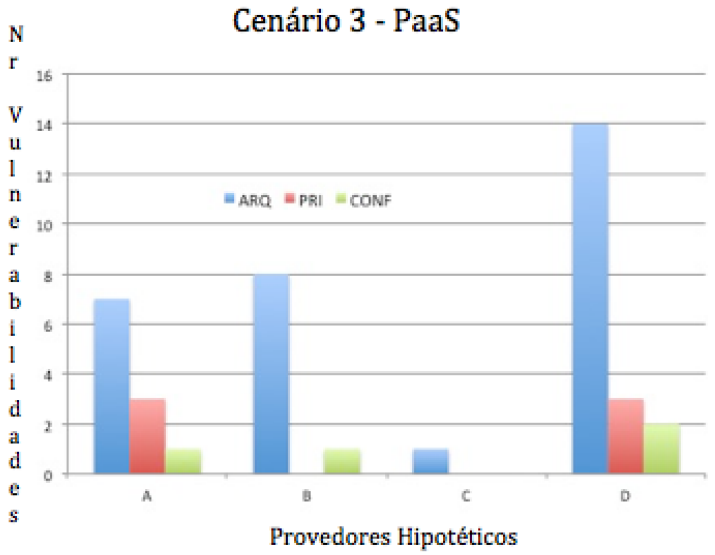

Figura 6.2: Número de vulnerabilidades encontradas nos provedores hipotéticos referente ao Cenário 3.

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 no gráfico Cenário 1 - *SaaS* (B, C, A e D), representado pela Figura 6.1. Assim como no gráfico Cenário 3 - *PaaS* (C, B, A e D), representado pela Figura 6.2, comparado aos resultados obtidos nos Cenários correspondentes 1 e 3 da Seção 5.1.

Percebe-se ainda que o provedor D, em ambos os ambientes (Figuras 6.1 e 6.2), 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 6.1 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 6.2. Além disso, apesar do peso w_3 ser maior que w_1 e w_2 no ambiente correspondente à Figura 6.1 e o número de vulnerabilidade de *CONF* ser zero no provedor C, o provedor B se torna o mais confiável por apresentar a metade das vulnerabilidades em *ARQ* presentes em C. De acordo com a Tabela 5.1 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 [4], o que comparado ao Cenário 1 da Seção 5.1 também reforça a validação do modelo proposto.

Nota-se ainda que o resultado contraditório do valor de confiança encontrado no Cenário 1 da Seção 5.1, onde utilizando a primeira proposta o provedor C foi o mais confiável e utilizando a segunda proposta o provedor B foi o mais confiável, é resolvido definitivamente nos resultados obtidos nesta seção. Sendo o provedor B o mais confiável de acordo com o resultado do experimento real na Subseção 6.1.2. Com isso, pôde-se afirmar que utilizando a segunda proposta, onde calcula-se a confiança na nuvem a partir de um valor único de risco, obtém-se, de forma correta e mais precisa, o quão mais confiável um provedor é dos demais avaliados, em relação à primeira proposta. O que reforça a análise realizada na Seção 5.3.

Além disso, considerando o resultado obtido na Subseção 5.2.1, referente a proposta de Silva et al., a sequência do provedor mais confiável ao menos confiável seria C, B, A e D. Porém, a partir do resultado obtido no experimento em ambiente real (Correio Eletrônico que corresponde ao Cenário 1 - *NP SaaS*) presente na Tabela 6.1 e representado

graficamente na Figura 6.2, a sequência do provedor mais confiável ao menos confiável é B, C, A e D. Conforme descrito na Seção 5.3, o que diferencia a proposta deste trabalho à Silva et al. [23] é o fato do presente trabalho considerar na avaliação de risco associada a cada subcategoria S_i o impacto da severidade e da probabilidade. O que não ocorre no trabalho de Silva et al. [23], pois considera somente o impacto da severidade na avaliação de risco. Portanto, percebe-se que utilizando a proposta de Silva et al. a métrica não mensurável segurança não é medida corretamente.

Capítulo 7

Considerações Finais e Trabalhos Futuros

A perda de controle aliada a 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.

A fim de apoiar consumidores da nuvem na escolha de provedores mais confiáveis, a partir da segurança garantida pelos mesmos, este trabalho propôs um modelo abstrato que permite que estes 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 [4]. Como exemplo de uma possível aplicacão deste trabalho, destaca-se a adoção da nuvem pelo Comitê Olímpico Internacional (*COI*), onde todos os sistemas das Olimpíadas e Paraolimpíadas de 2016 encontram-se na nuvem. Porém, o modelo escolhido foi de uma nuvem 100% privada e dedicada. Com isso, percebe-se que a opção foi garantir uma maior segurança, apesar de um maior custo. A dúvida é: Seria mesmo necessário tal investimento? Ou bastaria apenas contratar, temporariamente, um provedor com garantias de segurança e desempenho, bem acordadas, que atenderia às necessidades do evento? Como resposta a esta pergunta, sugere-se que o responsável por contratar a nuvem que atenda às necessidades do *COI* siga o modelo proposto neste trabalho e busque o provedor que lhe garanta uma maior confiança.

Destacam-se como principais contribuições:

- 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;

- A proposta de um modelo heurístico de cálculo da confiança em provedores com base em medidas de segurança referentes à arquitetura, à privacidade e à conformidade dos serviços oferecidos, considerando um valor de risco único para cada medida de mitigação e solução dos principias padrões de ataques em sistemas computacionais;

- A proposta de um método abstrato para apoiar os consumidores da nuvem na distribuição dos pesos dados às métricas de segurança quanto à Arquitetura (ARQ), à Privacidade (PRI) e à Conformidade ($CONF$). Estes pesos são necessários para o cálculo da confiança da nuvem computacional e não devem ser atribuídos de forma arbitrária;

- O emprego do estudo de caso como método de pesquisa científica, permitiu questionar a eficácia do modelo heurístico proposto para o cálculo de confiança na nuvem. Sabe-se que o estudo de caso é geralmente organizado em torno de um pequeno número de questões. Com isso, buscando cobrir todos os possíveis cenários e permitir a melhor compreensão sobre um conjunto ainda maior de casos, aplicou-se as semelhanças presentes no Capítulo 6 quanto a responsabilidade de provedores e consumidores a dois ambientes presentes da Marinha que correspondem a dois dos cenários do Estudo de Casos. A partir da análise dos resultados obtidos nesses ambientes, foram validados os possíveis cenários, incluindo os presentes no Estudo de Casos, que cobriram todos os modelos da nuvem.

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.

Devido a atualização anual dos padrões de ataque da base CAPEC, se faz necessário a atualização com a mesma periodicidade dos valores de risco único associados às medidas de mitigação/solução obtidas nesta base [4].

As próximas direções deste estudo se encaminham no sentido dos trabalhos de Silva et

al.[23], pois no futuro, a ideia é padronizar e construir uma ferramenta de monitoramento dos Sec-SLA para os diversos modelos da Nuvem Computacional quanto à implantação e serviço. Além disso, pretende-se avaliar a sensibilidade da escolha do provedor mais confiável, analisando os possíveis pesos atribuídos às métricas de segurança quanto à Arquitetura (ARQ), à Privacidade (PRI) e à Conformidade ($CONF$) a serem definidos pelo consumidor a partir do método proposto neste trabalho.

Referências

[1] ABNT. Tecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. abnt - associação brasileira de normas técnicas, 2013. http://http://www.abntcatalogo.com.br/norma.aspx?ID=306582.

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

[3] Badger, L. 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.

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

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

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

[7] Dan, M. Computação em nuvem: Vulnerabilidades na nuvem. technet magazine., 2013. http://http://www.cdn.ueg.br/source/trindade/conteudoN/3637/Computao_em_nuvem__Vulnerabilidades_em_nuvem___TechNet_Magazine.pdf.

[8] de Carvalho, A. F.; LEITE, F. V. Atribute importance in service quality: an empirical test of the pbz conjecture in brazil. international journal of service industry management. 487–504.

[9] 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.

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

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

[12] Grance, T.; Jansen, W. 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.

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

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

[15] Malhotra, K. N. *Pesquisa de Marketing: uma orientação aplicada.* Bookman, 2001.

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

[17] Manuel, D. P.; Barr, A. I. M.; Selvi, T. S. A novel trust management system for cloud computing - iaas providers. 3–22.

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

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

[20] 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.

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

[22] Rud; OLivia; Parr. *Data Mining Cookbook: Modeling Data for Marketing, Risk, and Customer Relationship Management.* Wiley Computer Publishing, 2001.

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

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

[25] Y., P.; Y., S.; J., K.; K, Y. J. Risk assessment and classification of focusing sla requirement in cloud computing. *International Journal of Security and Its Applications* (2013).

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