MARCO ANTONIO TORREZ ROJAS

GERENCIAMENTO DE ACORDO DE NÍVEL DE SERVIÇO DE SEGURANÇA PARA COMPUTAÇÃO EM NUVEM

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Doutor em Ciências.

São Paulo
2016

MARCO ANTONIO TORREZ ROJAS

GERENCIAMENTO DE ACORDO DE NÍVEL DE SERVIÇO DE SEGURANÇA PARA COMPUTAÇÃO EM NUVEM

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Doutor em Ciências.

Área de Concentração:
Engenharia da Computação

Orientador:
Tereza Cristina Melo de Brito Carvalho

São Paulo
2016

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Rojas, Marco Antonio Torrez
Gerenciamento de Acordo de Nível de Serviço de Segurança para Computação em Nuvem / M. A. T. Rojas -- versão corr. -- São Paulo, 2016.
169 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1.Segurança 2.SLA 3.Computação em Nuvem I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

AGRADECIMENTOS

À minha orientadora, Professora Tereza Cristina Melo de Brito de Carvalho, pela orientação e pelas oportunidades que propiciaram meu crescimento científico, profissional e humano.

À minha esposa Giselle Rizzatti por todo o suporte prestado, pelo seu apoio, carinho e compreensão durante esta etapa importante da minha vida. Esta é uma conquista conjunta.

À meus pais, Justiniano e Cristina, e minhas irmãs, Marianela, Rita e Carmen que sempre apoiaram e incentivaram as minhas decisões durante as diversas jornadas da minha vida. E também a minha gratidão a minha família Catarinense (João, Eli Ana e Carlos) por todo o apoio prestado.

Ao Professor Wilson Ruggiero, pelo incentivo durante o desenvolvimento deste trabalho. E em seu nome agradecer aos demais professores do PCS (Departamento de Engenharia da Computação e Sistemas Digitais) que contribuíram para a minha formação.

Ao Professor Marcos Antonio Simplicio Junior, pelas discussões e sugestões no âmbito do desenvolvimento deste trabalho, e outros.

Aos meus colegas de pós-graduação, do LARC (Laboratório de Arquitetura e Redes de Computadores), em especial: Fernando Redígolo, Charles, Rony, Cristina, Nelson, Fernando Sbampato, Karen, Akio, Rosangela, Schwarz, Weslley, Penteado, Dino, Ewerton, Bruno Medeiros, Thiago, Ákio, Cleber, Edivaldo e Lúcio. Do LASSU (Laboratório de Sustentabilidade), em especial: Bruno Bastos, Ana, Carlos, Marcelo, Guilherme, Camila, Gabriela, Viviane e Vivian. Pelo apoio, amizade e discussões científicas durante este período de convivência.

À Ericsson Centro de Inovações do Brasil, pelo suporte financeiro e apoio científico durante os projetos de pesquisa realizados. Meus agradecimentos em especial a Catalin Meirosu, Mats Näslund, Kazi Ullah Walli e Abu Shohel Ahmed pelas contribuições nos projetos que estivemos envolvidos relacionados a segurança. Também a minha gratidão a Eduardo Oliva e Maria Valéria Marquezini pelo suporte prestado.

À FDTE (Fundação para o Desenvolvimento Tecnológico da Engenharia) pelo suporte financeiro e organizacional durante os projetos em que estive envolvido. Agradecimento especial à Edilaine e equipe pelo suporte durante as atividades de gerenciamento dos contratos e prestação de contas.

À Secretaria do PCS pelo suporte prestado durante este período de convivência. Agradecimento especial a Lea e equipe.

De forma geral, minha gratidão a todas as pessoas que estiveram presentes durante este período e possibilitaram que a USP/POLI/PCS estivesse operacional suportando as nossas atividades do dia a dia.

In Pursuit of Simplicity

E.W.Dijkstra

RESUMO

O paradigma de computação em nuvem, por meio de seus modelos de serviço e implantação, apresenta para os provedores de serviço e consumidores benefícios e desafios. Um dos principais desafios apontados pela área de computação em nuvem é com relação à segurança da informação, especificamente a questão de conformidade com relação a contratos firmados entre o provedor e o consumidor. O acordo de nível de serviço (SLA) é um destes contratos, no qual são estabelecidos requisitos para a entrega e operação do serviço contratado pelo consumidor, bem como penalidades em caso de não atendimento a requisitos estabelecidos no contrato. Comumente, em um SLA definido entre provedor de serviço e consumidor as necessidades de disponibilidade e desempenho com relação ao serviço contratado são especificados, o que não ocorre com relação às necessidades de segurança. A necessidade de especificação de requisitos de segurança em um SLA, em especial confidencialidade e integridade, para o contexto de computação em nuvem, bem como arquiteturas de computação que tratem de requisitos de segurança em um SLA e efetuem o gerenciamento destes requisitos durante o ciclo de vida do SLA, encontram-se em evolução, se comparado aos requisitos de disponibilidade. Considerando a demanda crescente de incorporação de SLA de Segurança nos contratos de serviços de computação em nuvem, este trabalho tem como objetivo propor e avaliar um arcabouço de gerenciamento de serviços de computação em nuvem para o modelo de infraestrutura como serviço (IaaS), tendo como base requisitos de segurança especificados em um SLA, em especial os requisitos de confidencialidade e integridade. O gerenciamento proposto pelo arcabouço contempla as etapas do ciclo de vida de um SLA, que compreende as fases de: i) definir e especificar o SLA; ii) gerenciar e implantar o SLA; iii) executar e gerenciar o SLA e iv) finalizar o SLA. A validação do arcabouço proposto é realizada por meio da sua aplicação em um cenário de uso, onde será verificado o atendimento aos requisitos de segurança definidos e especificados no SLA. Para assegurar que o arcabouço proposto é seguro, bem como a sua integração com o ambiente de computação em nuvem é realizada análise de ameaças do arcabouço, e ações de mitigação apresentadas. Ao final, mostra-se que o arcabouço de gerenciamento proposto cumpre com os objetivos e requisitos propostos.

Palavras-chave: Computação em Nuvem. Acordo de Nível de Serviço. SLA. Segurança. SLA de Segurança. Gerenciamento de SLA de Segurança.

ABSTRACT

The cloud computing paradigm given its service and deployment models presents several benefits and challenges. One of the main challenges is related to information security, in particular, the compliance contracts between consumers and service provider. Service Level Agreements (SLAs) are contracts in which requirements about service operation and delivery as well as penalties in case of non-compliance of these requirements are defined. A SLA is usually defined in terms of availability and performance requirements, and data security requirements are normally not specified in details as these requirements. The need for security requirements specified in an SLA, especially confidentiality and integrity to the cloud computing paradigm, as well computing architectures to deal with SLA security requirements and management of cloud services based on SLA security requirements in an automated manner during its entire lifecycle are still in evolution, compared to availability requirements. In order to deal with these ineeds, this work aims to propose and evaluate a framework to orchestrate the management of cloud services for the infrastructure as a service (IaaS) based on SLA security requirements, specifically the confidentiality and integrity requirements. The management proposed by the framework comprehend the steps of the SLA lifecycle: i) SLA specification and definition; ii) SLA deployment and management; iii) SLA execute and monitoring; and iv) SLA termination. The validation of proposed framework is performed by its application in a usage scenario, checking the compliance with defined security requirements and specified in the SLA. To ensure the security of proposed framework and its cloud computing environment integration, a threat modeling is performed and mitigation actions are presented. At last, it is shown that the proposed management framework meets the specified framework requirements.

Keywords: Cloud Computing. Service Level Agreement. SLA. Security. Security SLA. Security SLA Management.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

ACM *Association of Computing Machinery*

API *Application Program Interface*

CIA *Confidentialilty, Integrity and Availability*

CPNI *Centre for the Protection of National Infrastructure*

CSA *Cloud Security Alliance*

CSA STAR *CSA Security, Trust Assurance Registry*

CSCC *Cloud Standard Customer Council*

CSMIC *Cloud Services Measurement Initiative Consortium*

DMTF *Distributed Management Task Force*

DSS *Defense Security Service*

ENISA *European Network and Information Security Agency*

GQM *Global-Question-Metric*

IBM *International Business Machines*

IaaS Infraestrutura como Serviço

IEEE *Institute of Electrical and Electronic Engineers*

IPSec *Internet Protocol Security*

ISACA *Information Systems Audit and Control Association*

ITU-T *International Telecommunication Union*

KPIs *Key Performance Indicators*

KQIs *Key Quality Indicators*

LARC Laboratório de Arquitetura e Redes de Computadores

MV Máquina Virtual

NIST *National Institute of Standards and Technology*

PCI DSS *Payment Card Industry Data Security Standard*

QoP *Quality of Protection*

QoS *Quality of Service*

QTP *Quantitative Policy Trees*

REM *Reference Evaluation Methodology*

SDN *Software-Defined Networking*

SLA Acordo de Nível de Serviço

SLA *Security Level Agreement*

SPI Software, Plataforma e Infraestrutura

STAR *Security, Trust & Assurance Registry*

STRIDE *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*

TI Tecnologia da Informação

TIC Tecnologia da Informação e Comunicação

TMF *TeleManagement Forum*

TPM *Trust Platform Module*

SSL *Secure Socket Layer*

TSL *Transport Socket Layer*

VEP *Virtual Execution Platform*

VMM Monitor de Máquina Virtual

1 INTRODUÇÃO

A computação em nuvem é um paradigma de computação que permite a entrega de serviços sob demanda por parte do provedor, tendo como base uma infraestrutura compartilhada e distribuída de Tecnologia da Informação (TI). A forma que esta entrega é realizada está relacionada aos modelos de serviço ofertados, que por sua vez auxiliam na definição de responsabilidades por parte do provedor e consumidor. As responsabilidades e papéis estão vinculados ao modelo de implantação da nuvem, representando os tipos de nuvens que podem ser adotados para provimento do serviço mais adequado às necessidades do consumidor.

O paradigma de computação em nuvem apresenta diversos benefícios para o consumidor (MELL; GRANCE, 2011), dentre eles flexibilidade, redução de custos e rápida entrega do serviço, e tais benefícios são responsáveis pela adesão crescente a este paradigma, como observado na pesquisa realizada pela Aberdeen Group com foco na Europa e América do Norte (CSAPLAR, 2013). Diretamente relacionado com sua adoção e benefícios, as necessidades de segurança são identificadas, podendo a responsabilidade pela segurança dos dados ou informação variar de acordo com o modelo de serviço/implantação de computação em nuvem. A segurança neste paradigma de computação é um dos principais desafios para a sua adoção, pois o consumidor almeja ter no mínimo equivalência da segurança provida pela nuvem com a sua experiência de operação em ambiente local (BOUCHENAK, 2013). Este desejo de equivalência de segurança e os desafios nativos de segurança do ambiente de computação em nuvem são objeto de pesquisa por parte da comunidade acadêmica e científica, e divulgado

pelos provedores de serviço e organizações de padronização.

Gonzalez (2012), classifica os problemas de segurança no contexto de computação em nuvem em sete categorias, identificando os problemas mais representativos com relação a segurança, seguindo critérios de agrupamento e eliminação de redundâncias nos documentos analisados. Além disso, são apresentados de forma individual os problemas e as soluções que compõem as categorias classificadas. Dentro dos problemas apresentados, a questão relativa à forma de se governar e gerenciar a nuvem tem destaque, desta forma a atenção aos processos organizacionais de segurança da informação fazem-se necessários. Dentre estes processos tem-se o acordo de nível de serviço (SLA) que personifica a visão compartilhada de gerenciamento apresentada pelo paradigma de computação em nuvem, ou seja, que a responsabilidade pela segurança é definida e acordada por ambos, e dependendo do modelo e serviço de nuvem selecionado este compartilhamento afeta os níveis operacionais. Com relação às soluções pesquisadas, as que tratam a questão da definição e tratamento de necessidades de SLA foram verificadas. Nesta verificação, é possível constatar que esta área necessita maior aprofundamento de pesquisa por parte da comunidade acadêmica e científica, sendo almejada pelo mercado consumidor e provedores. Esta mesma necessidade é apontada por Bouchenak (2013) com relação a adoção de requisitos de segurança da informação no contexto de SLA, identificado por SLA de segurança.

Diante destas informações a pesquisa nas questão de SLA e SLA de segurança foi efetuada. Esta pesquisa tem por objetivo identificar o cenário atual dos problemas e soluções pertinentes a aplicação de SLA de segurança no contexto de computação em nuvem, com base na visão da comunidade acadêmica e científica, bem como a necessidade apontadas pelo mercado e órgãos de padronização. Finalmente apresenta um arcabouço proposta de solução para um problema identificado, bem como a sua avaliação.

1.1 Motivação e Descrição do Problema

O SLA define a relação entre o provedor e o consumidor considerando o serviço de computação em nuvem contratado, e define as condições de gerenciamento do serviço tendo como base métricas quantitativas e qualitativas. Este acordo entre as partes envolvidas, provedor e consumidor, trata de requisitos de disponibilidade, desempenho, conformidade, segurança, privacidade e outros. O gerenciamento do serviço contratado é efetuado durante as etapas do ciclo de vida, ou seja, durante as etapas que compreendem o processo pelo qual o serviço passa, tendo como início a definição dos requisitos e finalizando na desativação do serviço, onde cada etapa do ciclo contém necessidades específicas que precisam ser tratadas.

As principais necessidades abordadas pelo SLA estão relacionadas com desempenho, disponibilidade e qualidade de serviço (QoS, *Quality of Service*) oferecidos pelo ambiente de computação em nuvem, o que reflete a necessidade mínima de equivalência desejada pelo consumidor. Por outro lado, aspectos de segurança e monitoração dos requisitos de segurança são deixados em segundo plano. Esta ausência de especificação de requisitos de segurança e monitoração em SLA ajudam a corroborar com o fato da falta de especificação de serviços de segurança representar um problema para a adoção do modelo de computação em nuvem.

A necessidade de definição e tratamento de requisitos de segurança em SLA para o contexto de computação em nuvem encontram-se em evolução (GARCIA, 2011), bem como arquiteturas de computação em nuvem que tratam requisitos de SLA (BOUCHENAK, 2013), e que realizem a gestão desse ambiente com base em métricas de segurança quantitativas e não qualitativas (LUNA, 2012a). Dentre os requisitos fundamentais da tríade de segurança, composta pela confidencialidade, integridade e disponibilidade (CIA, *Confidentiality, Integrity and Availability*), o requisito disponibilidade e sua monitoração é comumente abordado no SLA (ITU-T-FG, 2012), no entanto, requi-

sitos de confidencialidade e integridade usualmente estão em segundo plano (DEKKER; HOGBEN, 2011)(LUNA; LANGENBERG; SURI, 2012b). Diante destas necessidades apontadas, o presente trabalho apresenta um arcabouço para gerenciamento de serviços de computação em nuvem de infraestrutura com base em acordo de nível de serviço de segurança durante as etapas do seu ciclo de vida.

1.2 Objetivos do Trabalho

Este trabalho tem como objetivo geral propor e validar um arcabouço de gerenciamento de serviços de computação em nuvem para o modelo de Infraestrutura como Serviço (IaaS), que atenda requisitos de segurança especificados em um SLA, em especial os requisitos de confidencialidade e integridade. Para a gerência dos serviços de computação em nuvem, como por exemplo: máquinas virtuais, armazenamento e rede.; o arcabouço deve contemplar as etapas do ciclo de vida de um SLA no seu processo de gerenciamento. Os objetivos específicos deste trabalho são:

- Analisar a aplicação de SLA no contexto de computação em nuvem, seu ciclo de vida, taxonomias existentes, principais problemas e soluções que são abordados em um SLA;
- Identificar os problemas e necessidades que envolvem a aplicação de premissas de segurança em um SLA relacionadas à computação em nuvem;
- Analisar as principais publicações científica-acadêmicas que tratam de soluções para os problemas relacionados a aplicação de requisitos de segurança definidos em um SLA para o ambiente de computação em nuvem;
- Projetar mecanismos que suportem as etapas do ciclo de vida do arcabouço de entrega dos serviços de computação em nuvem, tendo como base os requisitos de segurança (confidencialidade e integridade) definidos em um SLA;

- Projetar a integração dos mecanismos do arcabouço necessários para atender as etapas do ciclos de vida do SLA, pois, o gerenciamento do serviços comumente envolve a utilização de mais de um serviço, e por consequência mais de um mecanismos de segurança; e

- Avaliar o arcabouço proposto a partir de sua aplicação em cenários de uso, verificando o atendimento aos requisitos definidos na sua concepção.

Para atender aos objetivos geral e específicos propostos faz-se necessário a aplicação de um método científico, o qual é composto por etapas. A Subseção 1.3 apresenta o método empregado.

1.3 Método

Para dar suporte ao desenvolvimento desta pesquisa, o método hipotético-dedutivo será adotado, que consiste em encontrar um problema ou lacuna no conhecimento científico, definição de hipóteses de solução e respectiva avaliação das hipóteses formuladas (PRODANOV; FREITAS, 2013). A lacuna ou problema é identificado por meio de pesquisa em referências científicas, a solução é proposta e avaliada por meio de cenários de uso e verificação sobre o cumprimento de requisitos.

Para efetuar um mapeamento das referências relacionadas, a abordagem proposta pela revisão sistemática (SAMPAIO; MANCINI, 2007) foi adotada nesta tese. As seguintes etapas do método foram aplicadas:

- Identificação das bases de dados consultadas: Na pesquisa realizada foram consultadas as seguintes bases de dados eletrônicas de publicações científicas do, IEEE (*Institute of Electrical and Electronic Engineers*), ACM (*Association of Computing Machinery*), Springer, WebScience e SciPress. Padronizações e boas práticas de orgãos, tais como: NIST (*National Institute of Standards and Tech-*

nology), ENISA (*European Network and Information Security Agency*), CPNI (*Centre for the Protection of National Infrastructure*), CSA (*Cloud Security Alliance*), DTMF (*Distributed Management Task Force*), CSCC (*Cloud Standard Customer Council*), ITU-T (*International Telecommunication Union*) e ISACA (*Information Systems Audit and Control Association*). Publicações das principais organizações do setor que atuam na área de computação em nuvem, tais como: IBM (*International Business Machines*), Microsoft, Accenture e Amazon, dentre outras;

- Palavras-chave de consulta: Na pesquisa as seguintes palavra-chave foram adotadas: *cloud* (computação em nuvem), *security* (segurança), *Service Level Agreement* (acordo de nível de serviço) e SLA;

- Estratégia de busca: Para a busca não se limitar aos artigos escritos em inglês, as palavras-chave em português também foram empregadas. A busca efetuou-se a partir de consulta aos sítios das bases identificadas, e também, a partir do buscador do Google;

- Revisão e seleção dos artigos: Durante a seleção dos artigos para estudo, a avaliação dos títulos e dos resumos (*abstracts*) foi realizada, caso a avaliação do resumo não seja suficiente, foi realizada a leitura completa do artigo, objetivando não excluir um artigo importante da revisão sistemática. Nesta etapa foram identificadas trezentas e setenta e uma (371) referências; e

- Análise crítica dos artigos selecionados: Consiste em analisar os artigos identificados que envolvem a especificação de requisitos de segurança em SLA no contexto de computação em nuvem. Foram identificados oito (8) artigos nesta etapa e analisados qualitativamente, possibilitando identificar os principais problemas que envolvem a questão de tratar requisitos de segurança em SLA para o contexto de computação em nuvem.

1.4 Organização do Trabalho

O presente trabalho está organizado em capítulos e seções com o objetivo de apresentar uma visão da área de forma geral, seguida por um detalhamento dos tópicos abordados pela pesquisa e culminando na proposta de pesquisa. O trabalho está organizado em sete capítulos principais após o capítulo introdutório, sendo eles:

- O Capítulo 2 é constituído pelo estudo dos principais problemas e soluções de segurança relacionados aos modelos de computação em nuvem. Informações sobre definição e conceitos básicos de Computação em Nuvem encontram-se no Apêndice A;

- O Capítulo 3 apresenta a definição de acordo de nível de serviço (SLA), análise do ciclo de vida e taxonomias de SLA propostas para o contexto de computação em nuvem. O capítulo é finalizado com a identificação de problemas e soluções abordadas em um SLA dentro do contexto de computação em nuvem;

- O Capítulo 4 contém o estudo e a identificação das necessidades apontadas por parte do consumidor e do provedor com relação à aplicação de requisitos de segurança em SLA. Além disso, apresenta um estudo dos principais trabalhos de pesquisa que apresentam propostas de soluções para os problemas relacionados à questão de SLA de segurança;

- O Capítulo 5 apresenta o arcabouço proposto para a gerencia de serviços de computação em nuvem com base em requisitos de segurança definidos no SLA. Também apresenta a descrição geral e detalhada do arcabouço, que inclui o processo de integração com a nuvem e como o gerenciamento do SLA é realizado. Além disso, é introduzida a abordagem defesa em profundidade modelada em árvore, que tem por objetivo efetuar o mapeamento dos mecanismos de segurança fornecidos pelo provedor da nuvem e seu fluxo de execução, e com base

nestes efetuar a definição do SLA de segurança, bem como o processo de gerenciamento destes mecanismo de segurança em conjunto com os serviços da nuvem;

- O Capítulo 6 contempla a avaliação do arcabouço proposto, com base em cenários de uso e considerações sobre o cumprimento de requisitos. Além disso, uma análise das ameaças de segurança do arcabouço e sua integração com a nuvem é efetuada. Com o objetivo de identificar o impacto destas ameças para o ambiente de nuvem e para o próprio arcabouço; e

- O Capítulo 7 apresenta as considerações finais e contribuições alcançadas neste trabalho, bem como, publicações efetuadas durante o período do programa de doutorado e proposta de trabalhos futuros.

2 SEGURANÇA EM COMPUTAÇÃO EM NUVEM

A computação em nuvem, além dos benefícios, apresenta também, desafios à sua adoção, tanto para provedores como para consumidores. Informações sobre definição e conceitos básicos de Computação em Nuvem encontram-se no Apêndice A. Um dos principais desafios deste modelo de computação está relacionado à segurança da informação, que consiste de mecanismos, regulamentações e processos para proteger a informação das ameaças e vulnerabilidades apresentadas por este paradigma. Este capítulo apresenta estes desafios no contexto da computação em nuvem.

2.1 Segurança em Nuvens Computacionais

As necessidades de segurança encontram-se definidas nos modelos de serviço e implantação, bem como a responsabilidade atribuída aos atores do processo, ou seja, os consumidores e os provedores de serviços. A Figura 1 ilustra a responsabilidade compartilhada em relação à segurança dos serviços executados na nuvem com base nos modelos de serviços propostos pelo NIST (MELL; GRANCE, 2011).

Analisando a Figura 1, pode-se notar que a responsabilidade com relação à segurança é compartilhada por parte do consumidor e provedor, variando o nível de responsabilidade de acordo com o modelo de serviço adotado e o recurso oferecido. Neste cenário, é importante identificar os principais problemas e desafios de segurança dentro do contexto de computação em nuvem, uma vez que a gestão da segurança é uma obrigação compartilhada entre provedor e consumidor.

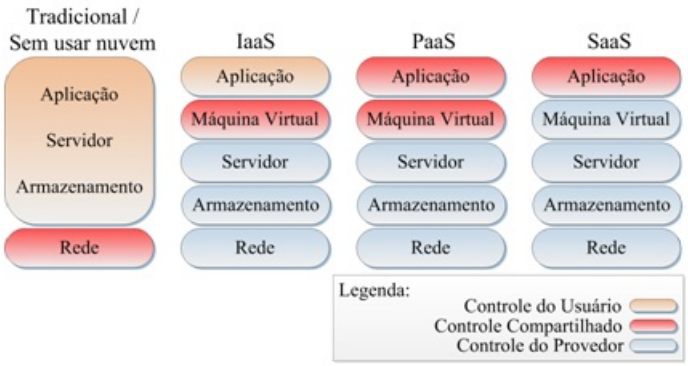

Figura 1: Responsabilidade de segurança no modelo de serviços do NIST.
Fonte: (GONZALEZ, 2013)

2.1.1 Problemas de Segurança

Na pesquisa realizada em Venters e Whitley (2012), com consumidores e provedores de serviço de computação em nuvem, foram identificados seis desejos com relação aos serviços de computação em nuvem: equivalência de segurança (i), equivalência de disponibilidade (ii), equivalência de latência (iii), oferta de serviços diversificados (iv), abstração da complexidade administrativa da infraestrutura do ambiente (v) e escalabilidade de serviços (vi). Com relação a (i), o desejo é receber serviços que são no mínimo equivalentes com relação à segurança vivenciada quando está se operando em ambiente local. Isto reflete o sentimento de insegurança por parte das organizações com relação à confiabilidade dos dados processados e armazenados pelo modelo de computação em nuvem.

As preocupações com segurança são alvo de pesquisa por parte da academia, provedores de soluções e organizações de padronização, objetivando apresentar soluções adequadas para os problemas apontados. Os principais problemas de segurança apontados por estas pesquisas foram agrupados em sete categorias em Gonzalez et al. (2012), com o objetivo de facilitar o seu entendimento e posterior estudo, sendo elas:

- **Segurança de rede:** Problemas de segurança associados à rede de comunicação de dados, elementos de processamento e armazenamento da nuvem. Como exemplos de problemas desta categoria, podem-se mencionar: transferência de

dados, *firewalls* e configurações de segurança para o ambiente;

- **Interface:** Problemas relacionados às interfaces oferecidas pelos serviços para interação com a nuvem por parte dos usuários, administradores e elementos programáveis. Como exemplos de problemas desta categoria, podem-se citar: API *(Application Program Interface)*, administração do ambiente de nuvem, acesso do usuário final e mecanismos de autenticação e autorização para acesso à nuvem;

- **Segurança de dados:** Problemas de proteção dos dados no ambiente em nuvem com relação à confidencialidade, integridade e disponibilidade (CIA) . Estes serviços são considerados fundamentais no contexto da segurança da informação (BISHOP, 2002). Como exemplos de problemas desta categoria, podem-se citar: criptografia de dados, redundância de recursos e atenção especial ao processo de descarte dos dados. O processo de descarte visa garantir que os dados não possam ser recuperados após seu uso;

- **Virtualização:** Problemas relacionados com técnicas de virtualização empregadas pela nuvem para poder compartilhar e administrar os recursos físicos da infraestrutura. Como exemplos de problemas desta categoria, podem-se mencionar: Isolamento de recursos, vulnerabilidades do *hypervisor*[1], vazamento de dados do ambiente compartilhado, autenticação e autorização entre máquina virtuais do ambiente e ataques entre máquinas virtuais;

- **Governança:** Problemas relacionados à perda do controle administrativo e de segurança causados pela utilização das soluções baseadas em nuvem. Como exemplos de problemas desta categoria, podem-se relacionar: controle dos dados em ambiente de nuvem, controle dos níveis de segurança em ambiente de nuvem e dependência em relação ao serviços de nuvem (*lock-in*);

[1] *Hypervisor* ou Monitor de Máquina Virtual (VMM), é uma camada de software responsável por fornecer ao sistema operacional visitante o suporte a abstração da máquina virtual.

- **Conformidade:** Requisitos de conformidade a serem atendidos pelos serviços, bem como disponibilidade, transparência e auditoria. Como exemplos de problemas desta categoria, podem-se citar: acordo de nível de serviço, disponibilidade do ambiente e serviço de nuvem, possibilitar auditoria de segurança e conformidade de serviços e usuários; e

- **Questões legais:** Aspectos relacionados a requisitos legais a serem considerados pela nuvem. Como exemplos de problemas desta categoria, podem-se mencionar: aspectos relacionados à localização geográfica dos dados, possibilidade de análise forense mantendo confidencialidade, privilégios de administrador do provedor da nuvem e legislações.

A Figura 2 ilustra as sete categorias agrupadas, bem como a participação percentual de cada categoria nos problemas de segurança em computação (GONZALEZ, 2012). Este agrupamento em categorias possibilita um entendimento dos principais problemas encontrados e sua comparação com relação a outras categorias, assim podendo identificar quais são os mais representativos percentualmente.

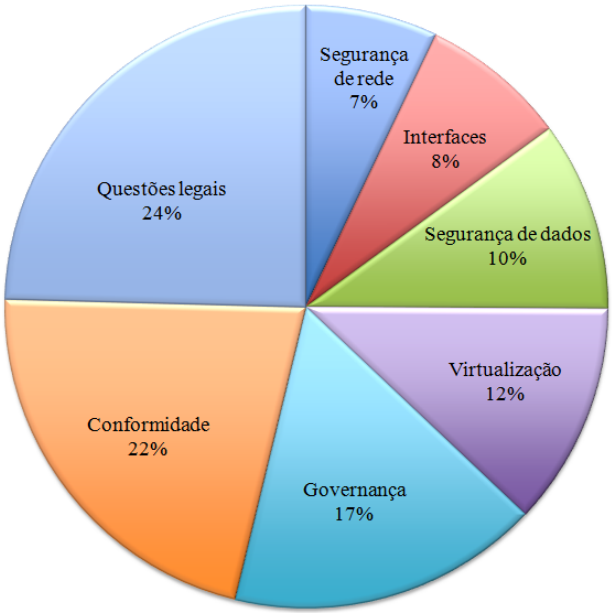

Figura 2: Problemas de segurança em computação em nuvem agrupadas em categorias. Fonte: (GONZALEZ, 2012)

Efetuando análise da Figura 2, pode-se notar que os problemas relativos a ques-

tões legais lideram o ranking, seguidos pelos problemas de conformidade. Estas duas categorias representam 46% dos problemas levantados, pois, abordam os aspectos desejados pelo consumidor com relação à segurança. Um dos principais aspectos desejados pelo consumidor é a questão de equivalência de segurança, ou seja, o consumidor deseja ter o mesmo nível de experiência de computação em seu ambiente local no ambiente de computação em nuvem. A Figura 3 ilustra o levantamento aprofundado dos problemas de segurança apresentados em Gonzalez (GONZALEZ, 2012), no contexto de computação em nuvem.

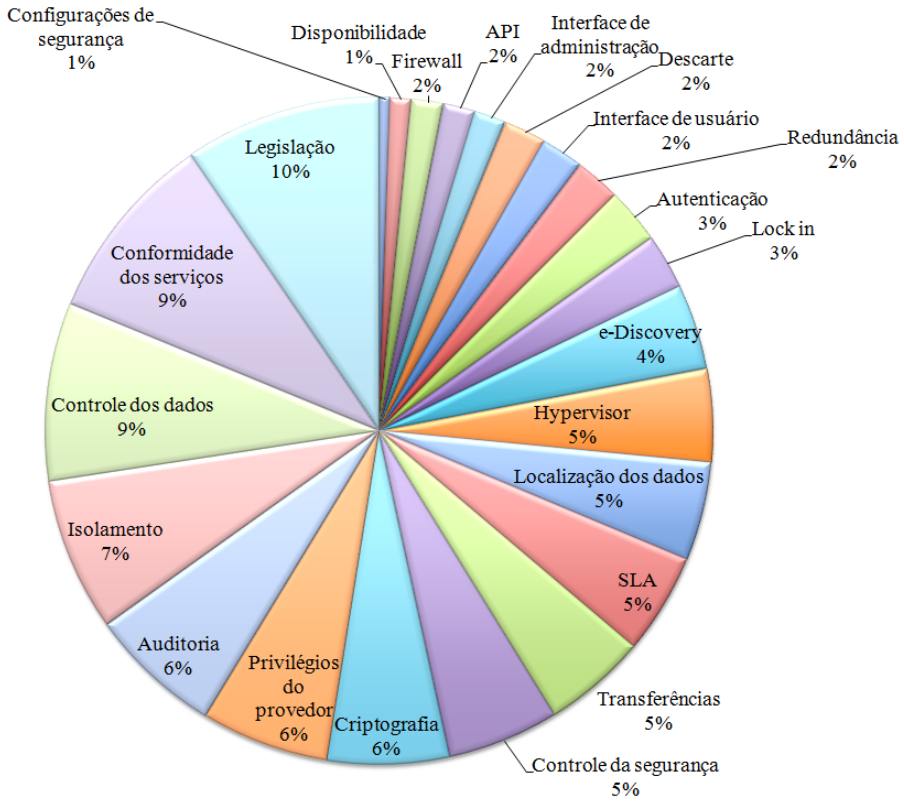

Figura 3: Problemas de segurança em computação em nuvem.
Fonte: (GONZALEZ, 2012)

Efetuando análise da Figura 3, nota-se que os problemas relativos à segurança levantados estão em um maior nível de detalhamento, auxiliando no processo de identificação dos principais problemas de forma individual e a sua participação percentual no total. Basicamente os problemas podem ser divididos e classificados em três faixas percentuais: abaixo de 3%, os problemas que representam uma baixa preocupação, entre 4% e 6%, os problemas que representam uma preocupação média e acima de 7%,

os problemas que representam uma preocupação alta. Esta divisão e classificação não apresenta relação com o risco que o problema representa no contexto de computação em nuvem.

Dentre os problemas de segurança apresentados pela Figura 3, é concentrada a atenção ao problema de SLA com 5% de participação, que segundo a divisão e a classificação propostas se encontra na faixa média de preocupações em computação em nuvem. O SLA contém a definição de responsabilidades por parte do consumidor e do provedor de serviço com relação ao modelo de serviço e implantação adotado. Desta forma, é importante entender detalhadamente quais necessidades devem ser englobadas na definição destas responsabilidades. O levantamento de soluções busca trazer uma visão do nível de desenvolvimento das soluções de segurança.

2.1.2 Soluções de Segurança

No levantamento efetuado em Gonzalez et. al. (2012), também foi dada atenção às soluções de segurança propostas pela academia e pelo mercado para os problemas de computação em nuvem apresentados. A Figura 4 ilustra este levantamento das soluções propostas.

Analisando a Figura 4, pode-se notar que o problema relativo à questão de SLA contém apenas 7% das soluções encontradas durante o levantamento detalhado de soluções. Apesar do percentual ser intermediário dentro da amostra, sua representatividade nas soluções é significativa, ocupando a quinta posição em conjunto com a solução para o problema de privilégios de administrador do provedor da nuvem.

Por meio da comparação quantitativa entre os problemas de segurança e as soluções de segurança apresentados, com foco em SLA, é possível inferir que a mesma não possui uma grande base de conhecimento tanto para problemas como para soluções. Desta forma a área de SLA necessita de maior atenção para que seus problemas sejam tratados adequadamente, por parte da academia e do mercado.

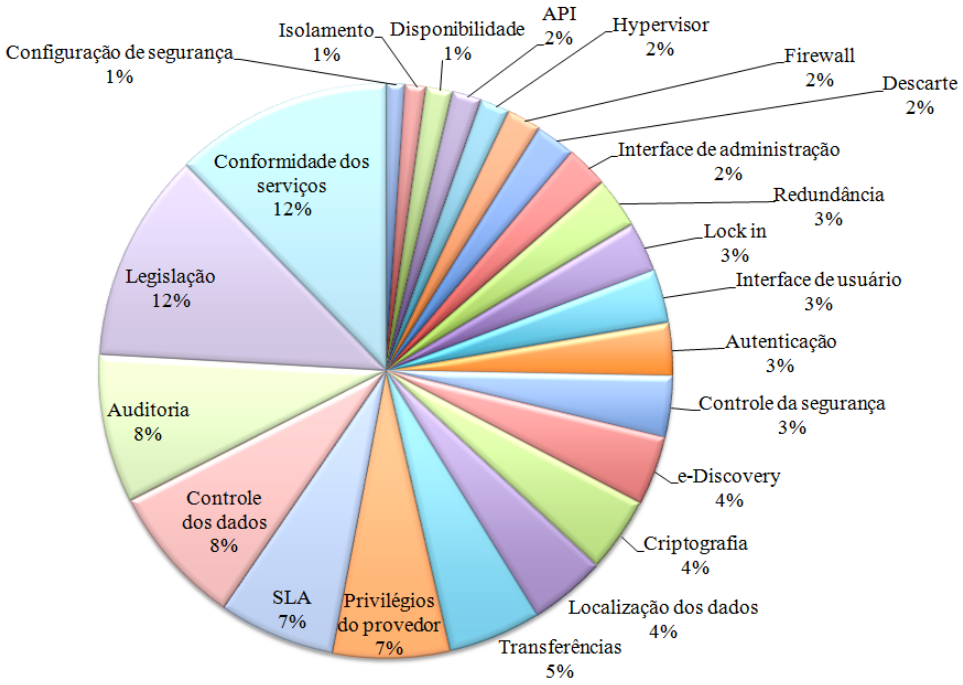

Figura 4: Soluções de segurança em computação em nuvem.
Fonte: (GONZALEZ, 2012)

2.2 Considerações do Capítulo

Neste capítulo foi realizado uma introdução às principais características do modelo de computação em nuvem, apresentando a sua definição e os modelos de serviço e implantação definidos pelo NIST. Por meio destes modelos, é possível verificar que a computação em nuvem apresenta uma visão compartilhada de responsabilidades em relação à administração dos recursos de infraestrutura providos.

Em seguida, discutiu-se aspectos relacionados à segurança, nos quais é possível identificar necessidades de segurança apresentadas pelo modelo compartilhado de serviços e implantação. Na sequência, apresentaram-se os principais problemas de segurança e as propostas de soluções pesquisados pela comunidade acadêmica e mercado para o contexto de computação em nuvem, o que possibilitou um entendimento quantitativo da representatividade dos problemas e soluções dentro do contexto.

Por fim, é focado no problema de SLA, devido à sua representação percentual como problema de segurança e, também, à representação percentual de soluções pro-

postas para este problema. Verificou-se que estas quantidades percentuais são próximas, significando que sua necessidade é proporcional à quantidade de soluções apresentadas, mas este fato não representa que a área está consolidada com relação a este tema, e também não permite conhecer em maiores detalhes a dimensão deste problema.

Diante desta necessidade de entendimento detalhado de SLA dentro do contexto de computação em nuvem, no Capítulo 3 (Acordo de Nível de Serviço) será realizada uma análise detalhada deste problema levantado. Este estudo compreende os principais problemas e soluções que envolvem o SLA de segurança para computação em nuvem, além de uma análise dos principais trabalhos sobre o tema e sua relação com o ciclo de vida de um SLA.

3 ACORDO DE NÍVEL DE SERVIÇO

A computação em nuvem oferece e entrega serviços gerenciados ao consumidor. Para garantir que estes serviços atendam aos objetivos da organização, é necessário definir um acordo de nível de serviço entre consumidor e provedor do serviço. Para a definição de um SLA é necessário compreender quais são necessidades e requisitos de serviços que devem ser atendidos.

Para realizar um estudo detalhado acerca de SLA para computação em nuvem, foi empregada o método de revisão sistemática da literatura (SAMPAIO; MANCINI, 2007). A revisão foi composta por trezentas e setenta e uma referências da academia (publicações do IEEE, ACM, Springer, WebScience e SciPress), organizações de pesquisa (SANS Institute, CSA, NIST, ENISA, ISACA, ITU-T, DMTF e TMF) e mercado (*white papers*, manuais e conteúdo digital de empresas como IBM, Microsoft, Accenture e Amazon).

Este capítulo apresenta o aprofundamento deste estudo, iniciando pela definição de acordo de nível de serviço, ciclo de vida, levantamento de taxonomias de SLA existentes e proposta de uma taxonomia baseando-se nos problemas levantados. Por fim, discutem-se e analisam-se os principais problemas e soluções apontados, tomando-se por base a taxonomia proposta nesta pesquisa. As seções e subseções apresentam os resultados desta pesquisa.

3.1 Definições de SLA

Diversas definições de SLA foram encontradas durante o processo de revisão sistemática, a Tabela 1 apresenta uma compilação destas definições dentro do contexto de computação em nuvem. Estas definições foram elaboradas por organizações de padronização com reputação internacional e, neste trabalho, busca-se elucidar o seu entendimento para adoção pelo próprio trabalho.

Tabela 1: Definições de SLA

Definição	Autor
Um acordo entre o provedor de serviço e cliente documentando quantitativamente o nível de serviço acordado.	CSMIC (UNIVERSITY, 2011)
SLA é um contrato entre provedor e consumidor, que especifica as necessidades do consumidor e o compromisso do provedor com estas necessidades. Tipicamente um SLA inclui os seguintes itens, tempo ativo, privacidade, segurança e procedimentos de *backup*.	NIST (MELL; GRANCE, 2011)
SLA representa o entendimento entre o consumidor e o provedor da nuvem sobre o nível de serviço acordado a ser entregue, e, em caso de falhas do provedor na entrega do serviço no nível acordado, a compensação que deve ser oferecida ao consumidor.	NIST (JANSEN; GRANCE, 2011)
Um acordo de serviço abreviado indicando as promessas técnicas de desempenho feitas pelo provedor, incluindo soluções para as falhas de desempenho. Um SLA é composto de três partes: A primeira parte contém um conjunto de promessas feitas para os assinantes; a segunda um conjunto de promessas explícitas não feitas para os assinantes, ou seja, limitações, e a terceira um conjunto de obrigações que os assinantes devem aceitar.	ITU-T (ITU-T-FG, 2012)
Um acordo de nível de serviço é um elemento formal vinculado a um contrato comercial negociado entre duas organizações, o provedor de serviços e o consumidor. Documenta o entendimento comum entre as partes sobre aspectos do produto, papéis e responsabilidades. SLAs podem incluir diversos aspectos sobre o produto, como requisitos de desempenho, atendimento ao usuário, bilhetagem, provisionamento de serviços, etc.	TMF (DAMM, 2012)
SLA representa o contrato entre o usuário e provedor da nuvem e visa orientar a maneira em que métricas de servidor/rede/armazenamento, bem como de *middleware*/aplicações são coletadas e apresentadas. É importante considerar o mapeamento de Indicadores-Chave de qualidade (KQIs,*Key Quality Indicators*) orientados para o consumidor à infraestrutura, plataforma e Indicadores-Chave de Desempenho (KPIs, *Key Performance Indicators*) relacionado a métricas de software.	DTMF e TMF (DMTF, 2013)
SLAs são documentos formais, acordados por ambas as partes (consumidor e provedor), que definem um conjunto de objetivos de níveis de serviço. Estes objetivos podem abordar a disponibilidade, desempenho, segurança, conformidade e privacidade.	CSCC (BAUDOIN, 2013)

Fonte: elaborada pelo autor.

Conforme observado na Tabela 1, o SLA define a relação entre o provedor e o consumidor do serviço de computação em nuvem, estabelecendo o nível de serviço contratado, métricas quantitativas e qualitativas de gerenciamento do serviço, bem como critérios de indenização para o cliente em caso de não cumprimento do contrato. Este acordo pode incluir requisitos de disponibilidade, desempenho, segurança, conformidade, privacidade e outros requisitos que foram acordados entre ambas as partes. Esta interação entre o provedor e o consumidor para tratar do SLA é composta de diversas fases, estas fases compreendem o ciclo de vida do SLA.

3.2 Ciclo de Vida

As fases do ciclo de vida do SLA compreendem etapas que são necessárias para que o SLA seja concretizado por parte do consumidor e do provedor do serviço e os objetivos definidos sejam atendidos. Estas fases permitem entender as necessidades específicas a serem abordadas em cada etapa.

Na literatura, foram encontrados vinte e uma propostas de ciclo de vida de SLA dentro do contexto de computação em nuvem. Estas referências encontram-se listadas na Tabela 2.

Tabela 2: Relação de Referências com Propostas de Ciclo de Vida

Referência	Autor	Referência	Autor
1	(SINTON, 2002)	12	(ZHANG; WU; CHEUNG, 2013)
2	(ITU-T-FG, 2012)	13	(KLINGERT; SCHULZE; BUNSE, 2011)
3	(RAK; CUOMO; VILLANO, 2013)	14	(FANIYI; BAHSOON, 2012)
4	(SU, 2012)	15	(SUN; SINGH; HUSSAIN, 2012)
5	(MAVROGEORGI, 2012)	16	(BOUCHENAK, 2013)
6	(FREITAS; PARLAVANTZAS; PAZAT, 2011)	17	(THEILMAN, 2010)
7	(TORKSHAVAN; HAGHIGHI, 2012)	18	(JRAD; TAO; STREIT, 2012)
8	(KIRKHAM, 2012)	19	(AIB; DAHEB, 2010)
9	(ABDULLAH; TALIB, 2012)	20	(BIANCO; LEWIS; MERSON, 2008)
10	(DING; ZHAO, 2012)	21	(MYERSON, 2013)
11	(DASTJERDI; BUYYA, 2012)		

Fonte: elaborada pelo autor.

A Tabela 3 apresenta em sua primeira coluna uma consolidação de todas as fases propostas nas referências, cada fase proposta pela referência se encontra assinalada, podendo ter mais de uma ou não. A sequência numérica apresentada na Tabela 2 tem relação direta com a sequência em que as referências foram citadas.

Tabela 3: Fases do ciclo de vida do SLA

	Referências																				
Fases do SLA	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**
Desenvolvimento do produto/serviço	★	★										★	★						★		
Especificação inicial				★																	
Especificação de modelo do serviço									★												
Publicação/descoberta do serviço									★				★								
Definição de parâmetros e preços das ofertas e requisições										★											
Projeto e desenvolvimento																	★				
Oferta do serviço																	★				
Localizar provedor de serviço															★			★			
Definir SLA							★								★			★			★
Desenvolvimento do serviço e template do SLA																				★	
Negociação / venda do serviço	★	★	★		★	★	★		★	★	★		★	★			★		★	★	★
Implementação do serviço	★	★					★												★		
Entrega do serviço								★					★	★		★					★
Fase de estabelecimento do serviço								★		★	★				★			★			
Otimização do recurso selecionado									★												
Empacotamento do serviço												★									
Distribuição do serviço												★									
Provisionamento do serviço													★				★				
Preparação do ambiente																				★	
Ativação do serviço				★																	
Execução do serviço	★	★		★				★				★	★						★	★	
Avaliação e correção de ações				★									★								
Monitoração do serviço			★	★			★		★	★				★	★			★			★
Relatar atividades e ocorrências														★							
Operações do serviço																	★				
Avaliação do serviço	★	★							★											★	
Gerenciamento do serviço					★					★		★									★
Aplicar especificações			★		★		★														
Encerrar o serviço																★	★			★	
Finalizar o serviço						★				★	★		★	★	★			★			★
Desativar o serviço		★										★									
Terminar o SLA				★																	
Terminar e bilhetar o serviço									★										★		
Aplicar sanções															★			★			
Total de fases	5	6	3	6	3	2	5	3	7	6	3	6	8	5	6	2	6	6	5	6	6

Fonte: elaborada pelo autor.

Com base na Tabela 3, é verificada a existência de propostas com uma quantidade variável de fases, de duas a oito fases. Analisando as fases em comum apresentadas pelas referências citas é possível agrupa-las em função de sua descrição para a fase proposta. Consolidando estas fases, propõe-se, então, uma nova taxonomia para o ciclo de vida do SLA. A Figura 5 ilustra a proposta deste novo ciclo de vida que contém quatro fases.

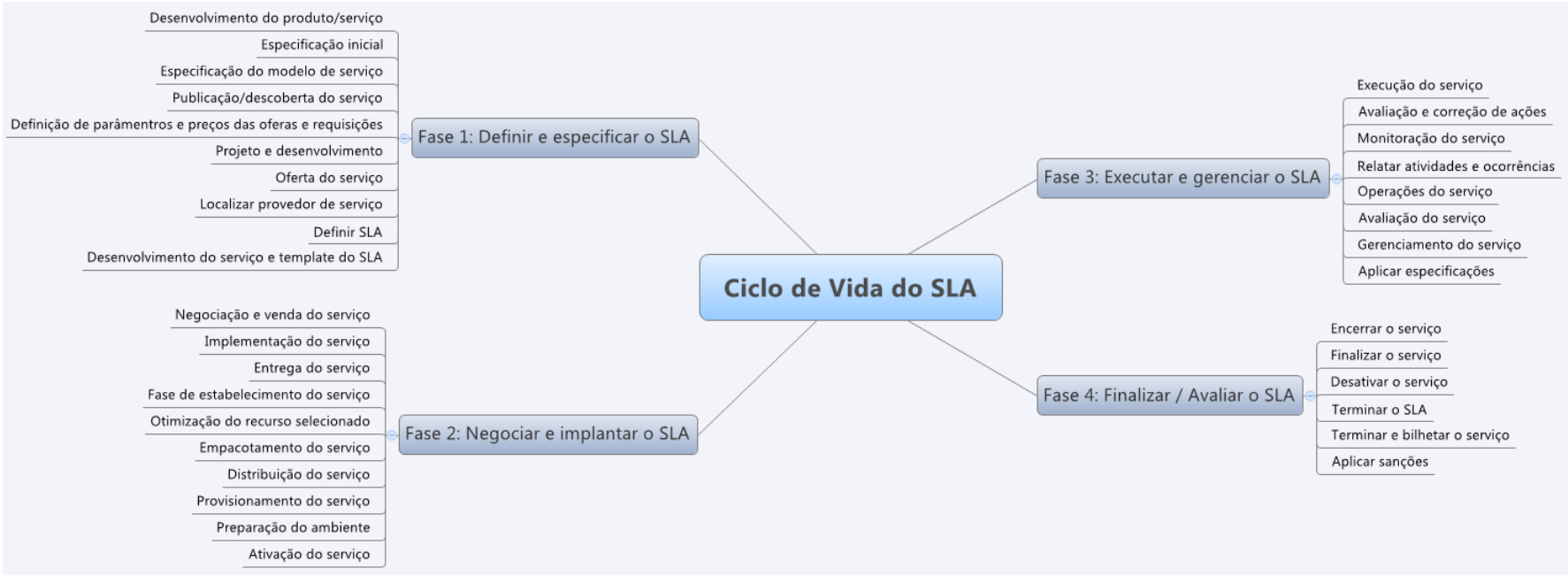

Figura 5: Proposta de ciclo de vida do SLA.
Fonte: elaborada pelo autor.

As fases do ciclo de vida do SLA apresentadas na Figura 5 são descritas como:

- **Fase 1 - Definir e especificar o SLA:** Nesta fase, é realizada a especificação dos requisitos que contemplam o SLA, identificando as necessidades do consumidor e as características do modelo de serviço adotado e suportado pelo provedor, bem como aspectos legais. Esta etapa é abordada em profundidade no documento apresentado pelo TM Forum (DAMM, 2012);

- **Fase 2 - Negociar e implantar o SLA:** Nesta fase, são negociadas, entre o provedor do serviço e o consumidor, as condições financeiras e os níveis aceitáveis de atendimento das necessidades do consumidor. Além disso, são definidas sanções para ambas as partes em caso de não atendimento de alguma cláusula definida, bem como a periodicidade e o conteúdo dos relatórios a serem entregues pelo provedor do serviço. Em seguida, é necessário provisionar e configurar o ambiente a ser fornecido ao consumidor atendendo aos requisitos especificados no SLA;

- **Fase 3 - Executar e gerenciar o SLA:** Nesta fase, é efetuada a operacionalização do serviço que está ativo e sendo executado, atendendo os requisitos especificados no SLA. Simultaneamente à execução, são realizados: a monitoração em tempo real da instância em execução, o gerenciamento dos requisitos a serem atendidos, a emissão de relatórios de controle, a aplicação de política de uso, ações corretivas a serem tomadas, as ações reativas e serem adotadas e o controle de violações;

- **Fase 4 - Finalizar e bilhetar o SLA:** Nesta fase, é tratado o encerramento do serviço em função do fim do contrato ou violação do mesmo. A desativação da instância é realizada, além da liberação dos recursos alocados e da revogação dos acessos do consumidor. Também são tratados assuntos relacionados à bilhetagem dos recursos consumidos e emissão das faturas de cobrança. Em caso

de penalidades em função do não atendimento de algum requisito por parte do provedor, o mesmo pode ser revertido em desconto para o consumidor ou ser oferecido outro mecanismo de compensação.

A dinâmica do processo que contempla as quatro fases do ciclo de vida é ilustrada pela Figura 6. Esta dinâmica consiste na interação entre as fases e a condição de retomada de cada uma delas.

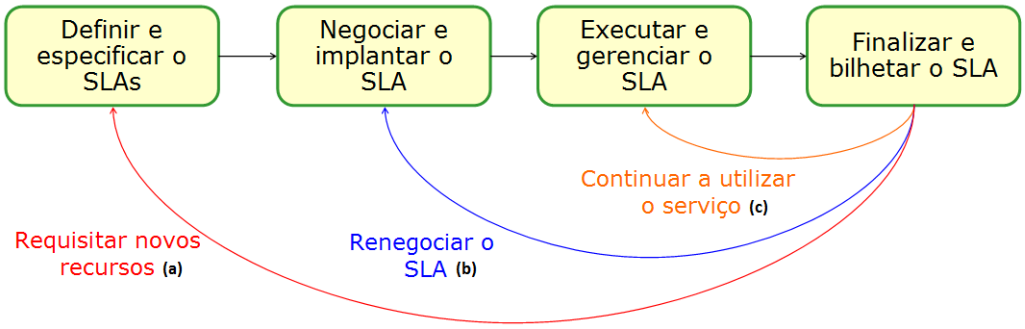

Figura 6: Dinâmica do ciclo de vida do SLA proposto.
Fonte: elaborada pelo autor.

A partir da Figura 6, é possível verificar que, ao se chegar à fase final do processo, podem ocorrer três ações distintas em caso de necessidade de manter a utilização do serviço. Estas fases são:

- **Ação (a)** - Necessidade de novos recursos ou redefinição dos requisitos relacionados ao modelo adotado ou aspectos legais;
- **Ação (b)** - Renegociar o SLA em função da necessidade de mudança de nível de atendimento, custo ou recursos utilizados;
- **Ação (c)** - Continuar a utilizar o serviço, executando novamente o processo sem a necessidade de alterar a definição ou a especificação do SLA corrente.

O entendimento das fases que compreendem o ciclo de vida do SLA por parte do consumidor e do provedor auxiliam no processo de elaboração de um SLA e no

entendimento das necessidades relacionadas especificamente a cada fase. As necessidades estão relacionadas em uma taxonomia, com o objetivo de apresentar quais são as categorias que necessitam ser levadas em consideração em um SLA.

3.3 Análise de Soluções e Problemas Abordados em SLAs

Visando compreender o atual cenário dos problemas e soluções relacionados a SLA no contexto de computação em nuvem, bem como identificar o seu impacto, o levantamento quantitativo a partir das referências pesquisadas foi efetuado. Este levantamento tem como base as necessidades apontadas pela taxonomia de SLA proposta, e consiste em identificar os principais problemas e soluções apontadas para a questão de SLA com foco em computação em nuvem. Além disso, este levantamento também identificou o modelo de serviço e implantação relacionado, com base na visão dos grupos de interesse citados. O levantamento e a análise destes problemas e soluções também foi efetuado utilizando o método de revisão sistemática.

3.3.1 Problemas de SLA

O levantamento efetuado em relação aos problemas que podem compor um SLA de computação em nuvem podem ser observados na Figura 7. Os problemas apontados refletem as necessidades que devem ser abordadas em um SLA, orientando o consumidor e o provedor de serviço durante a definição e a especificação de um SLA.

Na Figura 7, verifica-se que os três principais problemas apontados são: desempenho, disponibilidade e QoS, que refletem a preocupação em manter o nível de serviço necessário para o negócio. Ocupando a quarta posição na relação dos problemas levantados, está a questão de segurança; em quinto, a monitoração, que também está relacionada com a manutenção do nível de serviço. Desta forma, pode-se concluir que dos cinco principais problemas levantados, quatro estão relacionados com o nível de

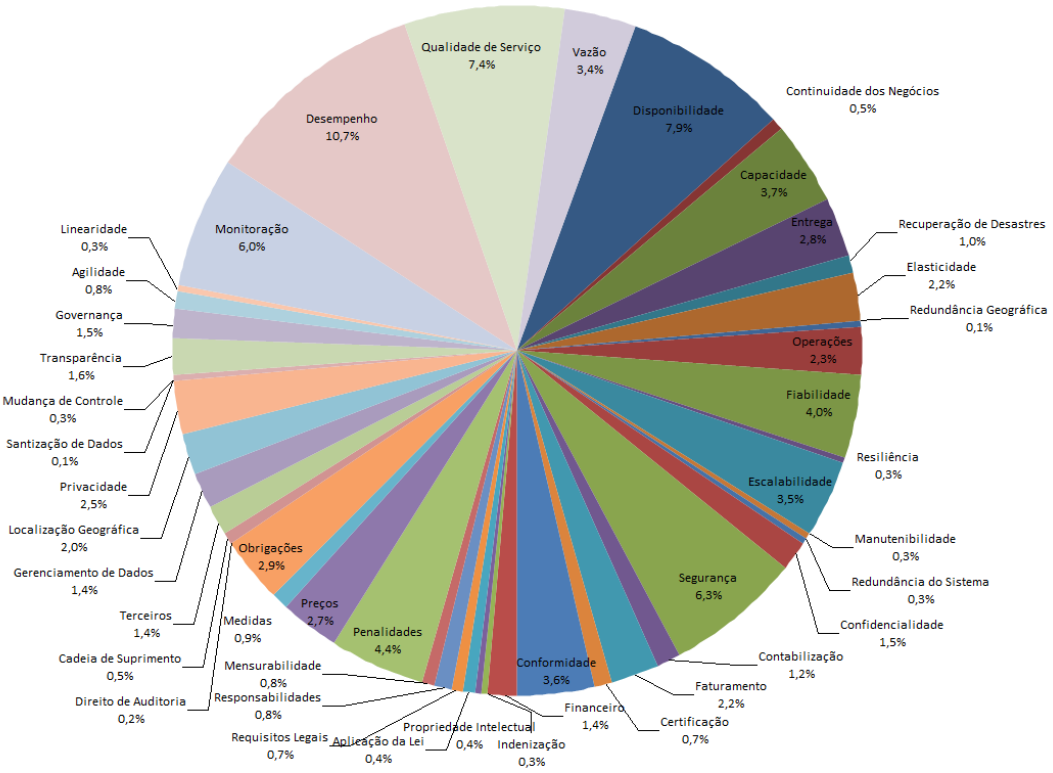

Figura 7: Problemas de SLA em computação em nuvem.
Fonte: elaborada pelo autor.

serviço e um com os aspectos de segurança, evidenciando que a segurança é deixada para segundo plano em detrimento de desempenho e disponibilidade.

Este levantamento reflete a intensidade com que as preocupações aparecem considerando o ponto de vista da academia, do mercado e das organizações de padronização. Esta relação serve como guia para que o consumidor possa estar atento às necessidades a serem verificadas na negociação de um SLA com um provedor de serviço. Agrupando as preocupações levantadas de acordo com os dados apresentados da Figura 7, a partir das categorias da taxonomia proposta, obtém-se o gráfico observado na Figura 8.

Na Figura 8, verifica-se que o principal problema a ser abordando pelo SLA é a segurança, com 37%, seguido de desempenho com 29%, conformidade com 25%, gerenciamento de dados com 6% e governança com 3%. Segurança, desempenho e conformidade dominam os problemas que devem ser abordados na elaboração de um SLA, sendo que a segurança ocupa o primeiro lugar em função de incluir a disponibi-

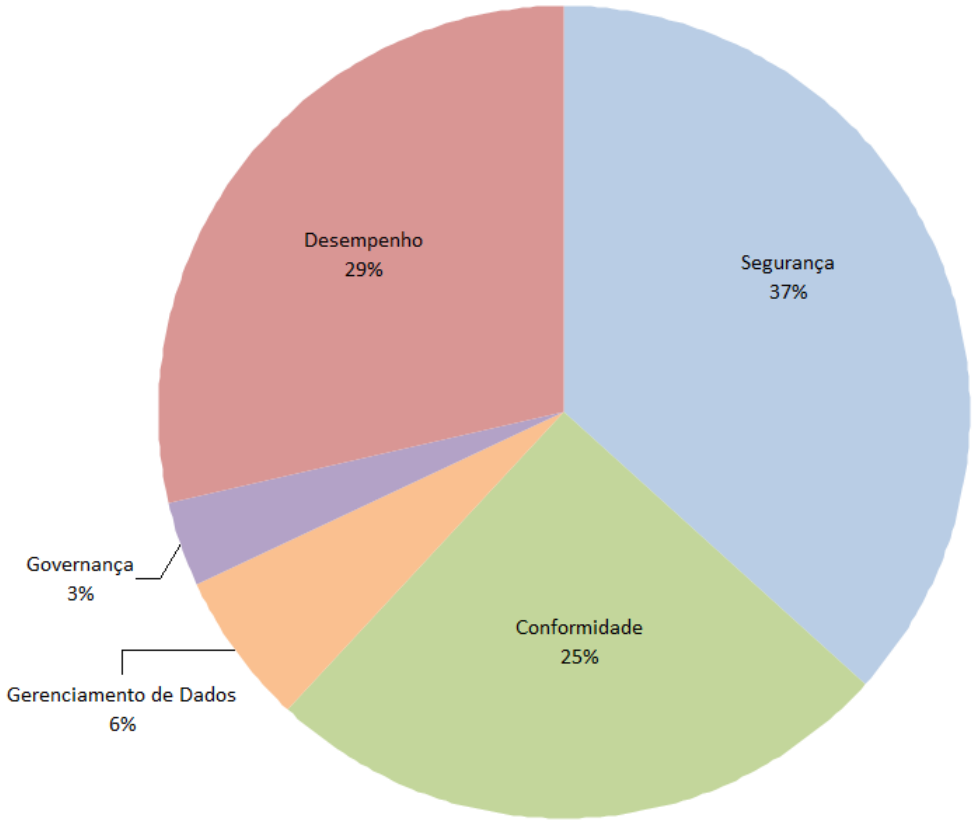

Figura 8: Problemas de SLA agrupados.
Fonte: elaborada pelo autor.

lidade em sua categoria.

No levantamento efetuado é identificada a relação entre os problemas abordados pelo SLA e os modelos de serviço e implantação. A Figura 9 apresenta esta relação, que consiste em mapear a qual modelo de serviço ou implantação o problema se refere.

Na Figura 9, verifica-se que, a grande maioria não especificou que modelo de implantação e serviço está relacionado ao problema a ser tratado pelo SLA. Relacionando os modelos de implantação e os problemas de SLA apontados, verifica-se que a nuvem privada é a primeira a apresentar esta preocupação com relação ao tratamento do SLA, seguida da nuvem seguida comunitária, nuvem pública e nuvem híbrida. Efetuando o relacionamento dos modelos de serviços e os problemas de SLA apontados, verifica-se que a IaaS é o modelo que apresenta mais preocupação com relação a questão de SLA, seguida pelo modelos SaaS e PaaS.

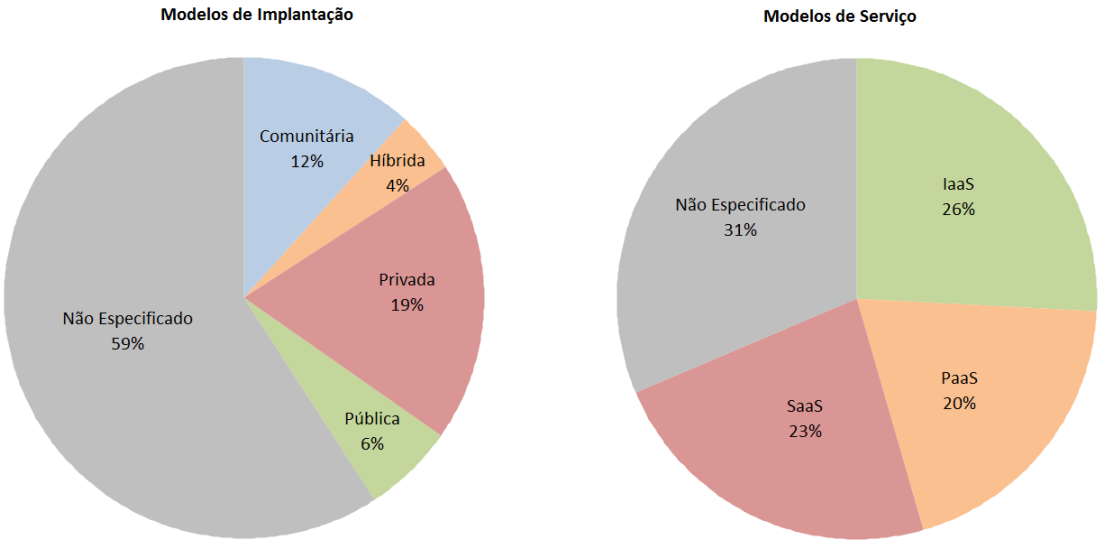

Figura 9: Relação entre os problemas de SLA e modelos de serviço e implantação.
Fonte: elaborada pelo autor.

Deste modo, os principais problemas que devem ser abordados pelo SLA estão relacionados principalmente com o modelo de implantação de nuvem privada e o modelo de serviço IaaS. Isto reflete de forma direta a responsabilidade com relação à segurança dos serviços executados na nuvem para estes modelos de implantação e serviço.

3.3.2 Soluções de SLA

Uma vez elencados os principais problemas que devem ser abordados pelo SLA, baseando-se nas mesmas referências, é realizado o levantamento das soluções. Neste contexto, soluções estão relacionadas com indicações de ações que devem ser realizadas para solucionar o problema, não necessariamente é uma solução pronta. Os resultados deste levantamento são apresentados na Figura 10.

Na Figura 10, verifica-se que, das cinco principais soluções levantadas, quatro correspondem aos principais problemas levantados. Sendo que nas três primeiras posições de soluções não houve mudança e são ocupadas por desempenho, disponibilidade e qualidade de serviço, o elemento que ingressou nesta lista é a fiabilidade (relacionado à confiabilidade) ocupando a quinta posição e a monitoração a quarta posição. A

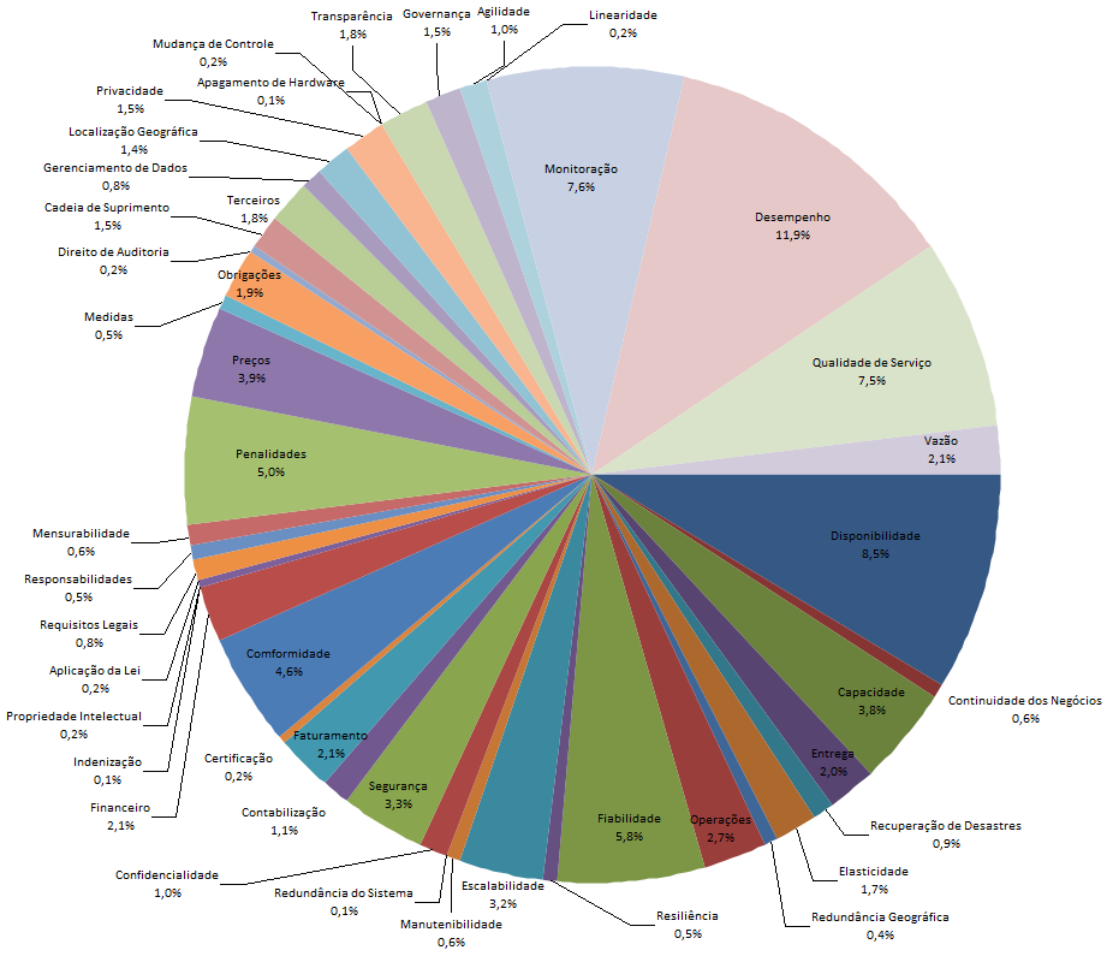

Figura 10: Soluções de SLA em computação em nuvem.
Fonte: elaborada pelo autor.

segurança ocupa a quarta posição em problemas e ocupa a oitava posição em soluções; esta diferença representa que a busca por soluções para os problemas de segurança não tem a mesma intensidade de pesquisa que os outros problemas reportados.

As soluções apontadas no levantamento refletem a intensidade com que tais soluções estão sendo abordadas pela academia e pelo mercado. Neste caso, não foi identificada contribuição das organizações de padronização, já que estas buscam desenvolver guias com recomendações, melhores práticas e padrões, e não buscam apresentar soluções.

Levando em consideração as cinco principais soluções apontadas, verifica-se que a continuidade das operações mantendo a qualidade de nível de serviço é a principal

motivação junto com a confiança do provedor de serviços. Agrupando as soluções levantadas em categorias da taxonomia proposta (GONZALEZ, 2012), obtém-se o gráfico observado na Figura 11.

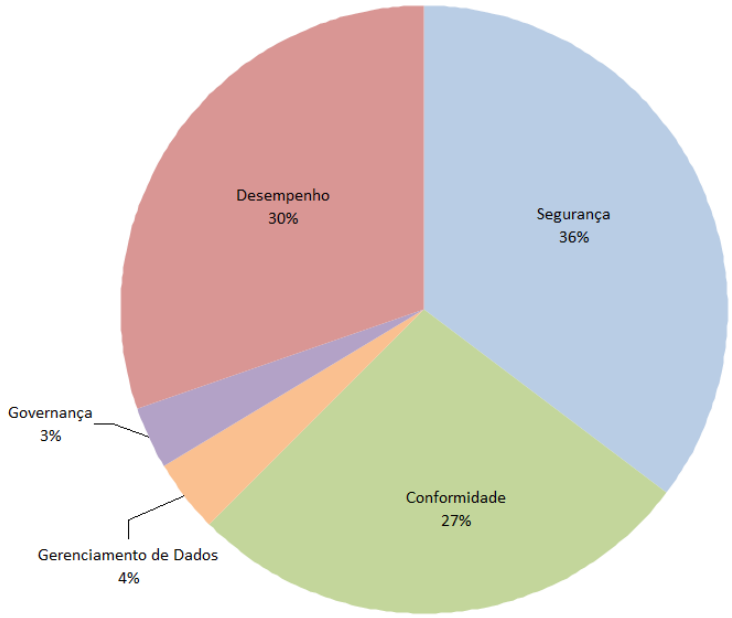

Figura 11: Soluções de SLA agrupados
Fonte: elaborada pelo autor.

Na Figura 11, é possível analisar que as três principais soluções apontadas pelo levantamento de soluções correspondem aos principais problemas detectados no levantamento de problemas. Isso reflete um alinhamento entre as necessidades levantadas e o desenvolvimento de soluções propostas pela academia e pelo mercado.

Dentro do levantamento de soluções efetuado, foi identificada a relação entre as soluções abordadas para SLA e os modelos de serviço e implantação. A Figura 12 ilustra esta relação, que consiste em mapear a que modelo de serviço ou implantação a solução está se referindo.

Na Figura 12, verifica-se que, no levantamento de soluções efetuado, a grande maioria não especificou quais modelos de implantação (60%) e serviço (30%) estão relacionados à solução proposta. Comparando com o levantamento efetuado dos modelos com relação aos problemas, não houveram mudanças na relação de soluções proposta para os modelos de implantação e, também, para os modelos de serviço.

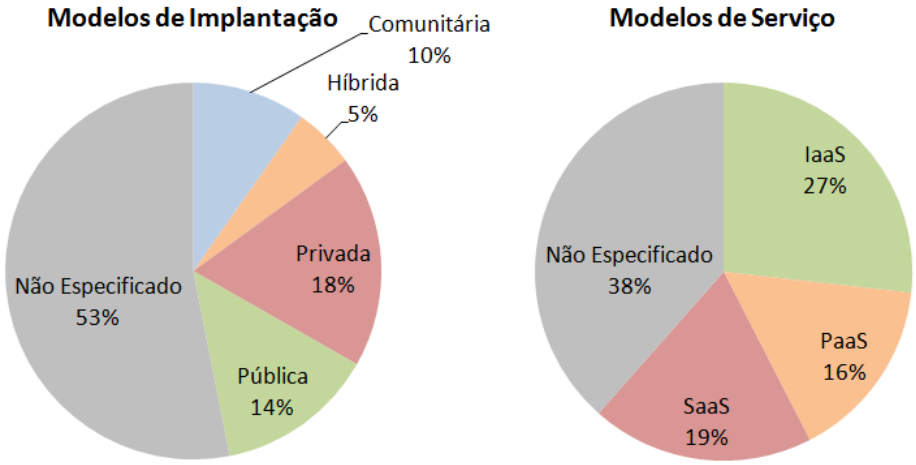

Figura 12: Relação entre as soluções de SLA e modelos de serviço e implantação
Fonte: elaborada pelo autor.

Analisando os problemas levantados para os modelos de implantação e serviço com as soluções propostas, verifica-se que a relação de propostas de soluções está proporcional aos problemas apontados, o que representa um alinhamento entre as necessidades apresentadas e as soluções propostas tendo como base a visão da academia e do mercado.

3.3.3 Comparação entre Problemas e Soluções

Com o objetivo de comparar os resultados dos levantamentos efetuados para problemas e soluções dentro do contexto de SLA em computação em nuvem, a Figura 13 foi elaborada. Os valores nos eixos correspondem a quantidade de citações para uma determinada categoria. Com relação aos tons (ou cores), adotou-se que: em tom mais claro (azul na versão colorida) estão as citações de soluções; enquanto em tom levemente mais escuro (vermelho na versão colorida) estão as citações de problemas. Em tom escuro (roxo na versão colorida) estão as áreas onde ocorre sobreposição.

Baseando-se na Figura 13, é possível analisar a relação entre problemas e soluções, identificando-se duas classes de relação. A primeira identifica que a quantidade de citações para problemas é maior do que a de soluções, sinalizando que existe campo para a pesquisa de solução para o referido problema. Como exemplo, é possível ci-

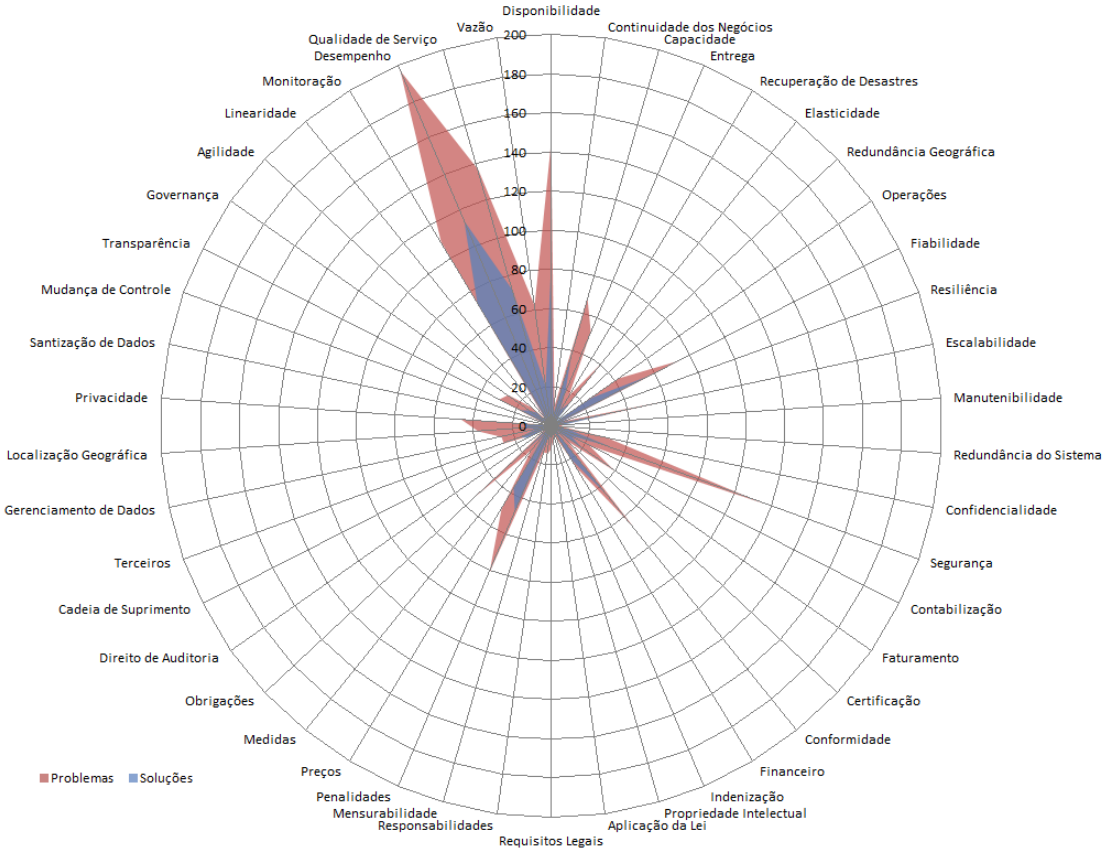

Figura 13: Comparação entre soluções e problemas de SLA.
Fonte: elaborada pelo autor.

tar as seguintes categorias: desempenho, fiabilidade, disponibilidade, conformidade, penalidades, entre outras. A segunda classe identifica que existem poucas soluções em relação ao número de problemas apresentados, evidenciando-se os problemas; esta evidência identifica que é uma área com demanda para a pesquisa de soluções para o referido problema. Por exemplo, recuperação de desastres, elasticidade, faturamento, obrigações, terceiros, gerenciamento de dados, localização geográfica e privacidade. A Figura 14 ilustra esta relação entre problemas e soluções agrupando-as de acordo com a taxonomia proposta.

A Figura 14 ilustra que para todos os grupos propostos, o número de problemas relatados é superior ao número de soluções apresentadas. Além disso, existem categorias de problemas e soluções para as quais foi identificada a existência de mais pesquisa abordando este tema, como por exemplo, desempenho, segurança e conformidade. Os

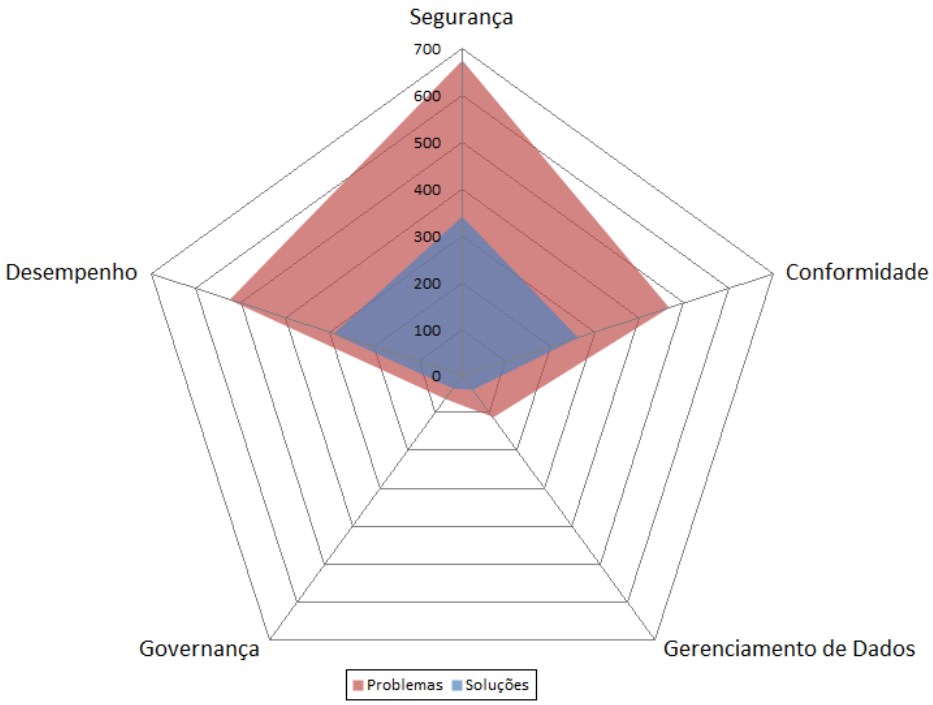

Figura 14: Comparação entre soluções e problemas de SLA agrupados.
Fonte: elaborada pelo autor.

problemas e soluções das categorias de governança e gerenciamento de dados apresentam menor volume de pesquisa em relação à categoria de segurança, desempenho e conformidade. Neste sentido, os principais problemas apontados são segurança, desempenho e conformidade; já com relação às soluções, as principais categorias podem ser considerados a **segurança, conformidade e desempenho**. Por fim, constata-se que existe **grande oportunidade para pesquisa com relação a SLA** nestas categorias.

3.4 Taxonomias de SLA

No levantamento efetuado dos problemas que devem ser abordados pelo SLA dentro do contexto de computação em nuvem, segundo a academia, organizações de padronização e mercado, foram encontradas quarenta e seis necessidades. Estas necessidades constituem o vocabulário de termos e de definições a serem tratados na definição e na especificação de um SLA. O entendimento e o conhecimento destas necessidades tem por finalidade facilitar a comunicação entre o consumidor e o provedor.

Com o objetivo de classificar estas necessidades em categorias e proporcionar uma visão mais clara dos elementos-chave que podem ser definidos em um SLA, foi efetuado um levantamento de propostas de taxonomia de SLA. Neste levantamento, foram encontradas somente duas propostas, uma elaborada pelo NIST (BADGER, 2011), e outra pelo ITU-T (*International Telecommunication Union*) (ITU-T-FG, 2012) que propõe uma taxonomia para SLA.

3.4.1 Taxonomia de SLA Proposta pelo NIST

O NIST identificou que o SLA relacionado à computação em nuvem é uma importante lacuna para sua adoção, necessitando maior investigação. Em abril de 2011, um subgrupo do NIST foi formado para efetuar este levantamento (BADGER, 2011). Este levantamento constatou a existência de disparidades e ambiguidades em relação à definição de SLA por parte dos provedores de serviços.

Para fins de uniformização de vocabulário, terminologia e elementos-chave, bem como de criação de um guia que possa mapear estes requisitos, foi elaborada uma taxonomia para SLA de computação em nuvem. A taxonomia proposta pelo NIST pode ser observada na Figura 15.

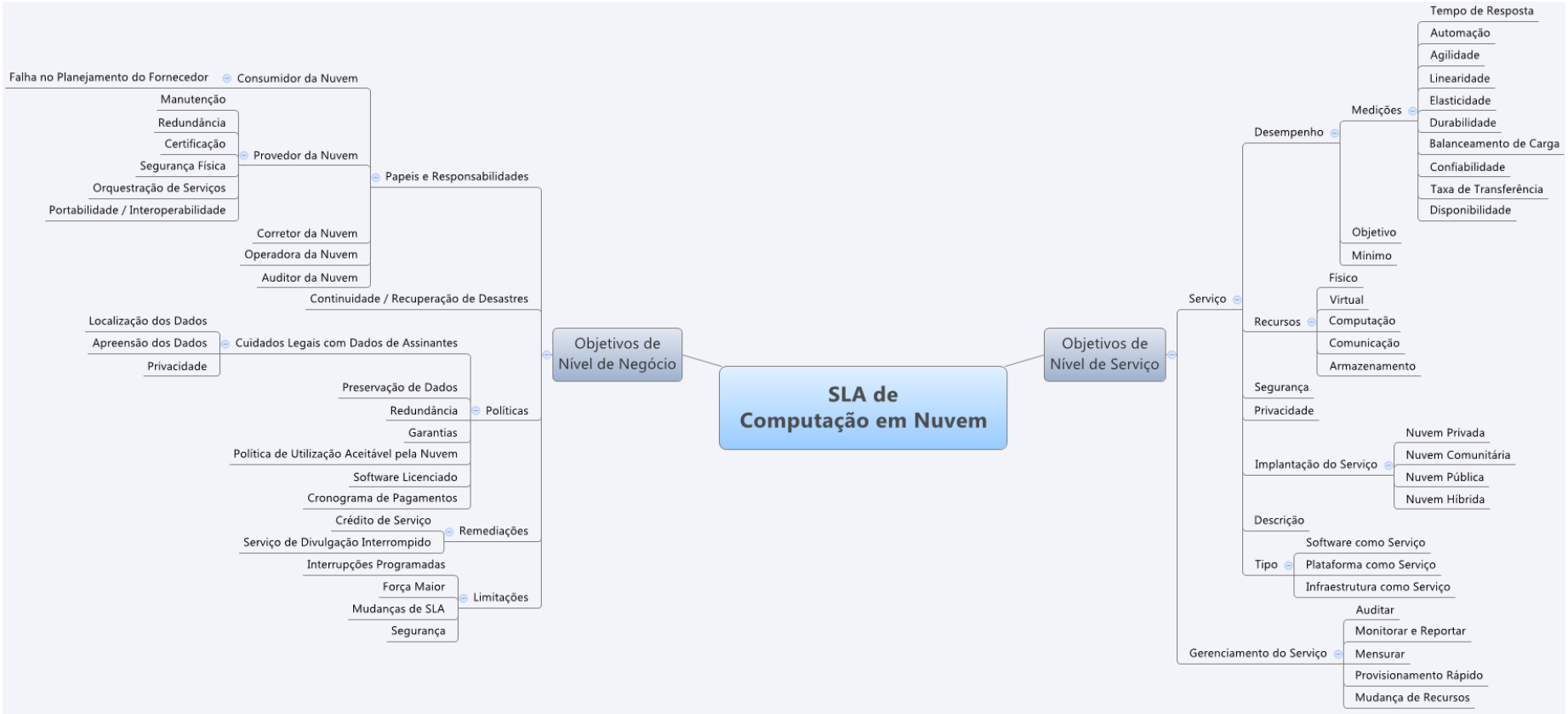

Figura 15: Taxonomia do NIST de SLA em computação em nuvem.
Fonte: adaptada de (BADGER, 2011).

Na Figura 15, é possível constatar que a proposta do NIST apresenta uma divisão das necessidades de SLA em objetivos de nível de negócio e de serviço, bem como uma divisão dos requisitos que exigem métricas. Além disso, faz a categorização de requisitos e apresenta categorias relacionadas. Analisando a proposta de taxonomia de SLA do NIST, avalia-se que a mesma não é adequada para a classificação das necessidades encontradas pelo levantamento de problemas e soluções, pois a divisão em dois níveis (negócio e serviço) não possibilita uma visão das categorias com maior impacto. Se a divisão for efetuada levando em consideração o segundo nível (Serviço), é possível agrupar, mas estas não refletem a real necessidade da categoria. Por exemplo, a categoria Medições (Tempo de Resposta) contém necessidades de desempenho, contém necessidades de segurança (Disponibibilidade) e operacional (Automação). Verifica-se que apresenta necessidades de várias categorias, o que compromete o seu agrupamento em categorias e posterior análise.

3.4.2 Taxonomia de SLA Proposta pelo ITU-T

O ITU-T (ITU-T-FG, 2012) apresenta uma relação de recursos que devem ser considerados pelo consumidor e pelo provedor de serviço para a elaboração de um SLA de infraestrutura de computação em nuvem, bem como a sua descrição. Também apresenta uma classificação das métricas de SLA em categorias; esta classificação encontra-se ilustrada na Figura 16.

Na Figura 16, considera-se esta classificação como uma taxonomia de SLA constituída de oito categorias. As métricas apresentadas podem ser divididas em quantitativas e qualitativas. Como exemplo de métrica quantitativa, pode-se citar o tempo de resposta e como exemplo de métrica qualitativa, pode-se citar a certificação. Analisando a proposta de taxonomia de SLA do ITU-T, verifica-se que a mesma apresenta uma classificação mais alinhada às categorias levantadas, mas é insuficiente para contemplar as quarenta e seis necessidades apontadas no levantamento dos problemas que

Figura 16: Taxonomia do ITU-T de SLA em computação em nuvem.
Fonte: adaptada de (ITU-T-FG, 2012).

devem ser abordados pelo SLA no contexto de computação em nuvem. Além disso, apresentar categorias que podem ser agrupadas em função de sua descrição, como por exemplo, manutenibilidade, que pode ser enquadrada em disponibilidade. Neste caso a manutenibilidade tem por objetivo corroborar com a disponibilidade do ambiente, desta forma sendo um item de disponibilidade.

3.4.3 Proposta de Taxonomia de SLA

Para contemplar as quarenta e seis necessidades de SLA apontadas (Subseção 3.3.1), uma proposta de taxonomia que englobe estas necessidades faz-se necessária, de forma a representar as necessidades apontadas pela academia, organizações de padronização e mercado. Para elaborar tal taxonomia é necessário a classificar as necessidades levantadas e sua respectiva descrição em categorias. Esta classificação em categorias é efetuada levando-se em consideração os documentos do CSA (*Cloud Security Alliance*) (BRUNETTE; MOGULL, 2009), ENISA (CATTEDDU; HOGBEN, 2009), NIST (MELL; GRANCE, 2011) e ITU-T (ITU-T-FG, 2012), bem com as taxonomias apresentadas, pois, são documentos relacionados à taxonomia proposta que aborda as questões de SLA e segurança. A Figura 17 ilustra a proposta de taxonomia de SLA dentro do contexto de computação em nuvem.

Justifica-se que tais documentos sejam serem levados em consideração na proposta de taxonomia pelo fato de serem relacionados ao aspecto que a taxonomia deseja abordar quanto a SLA: segurança.

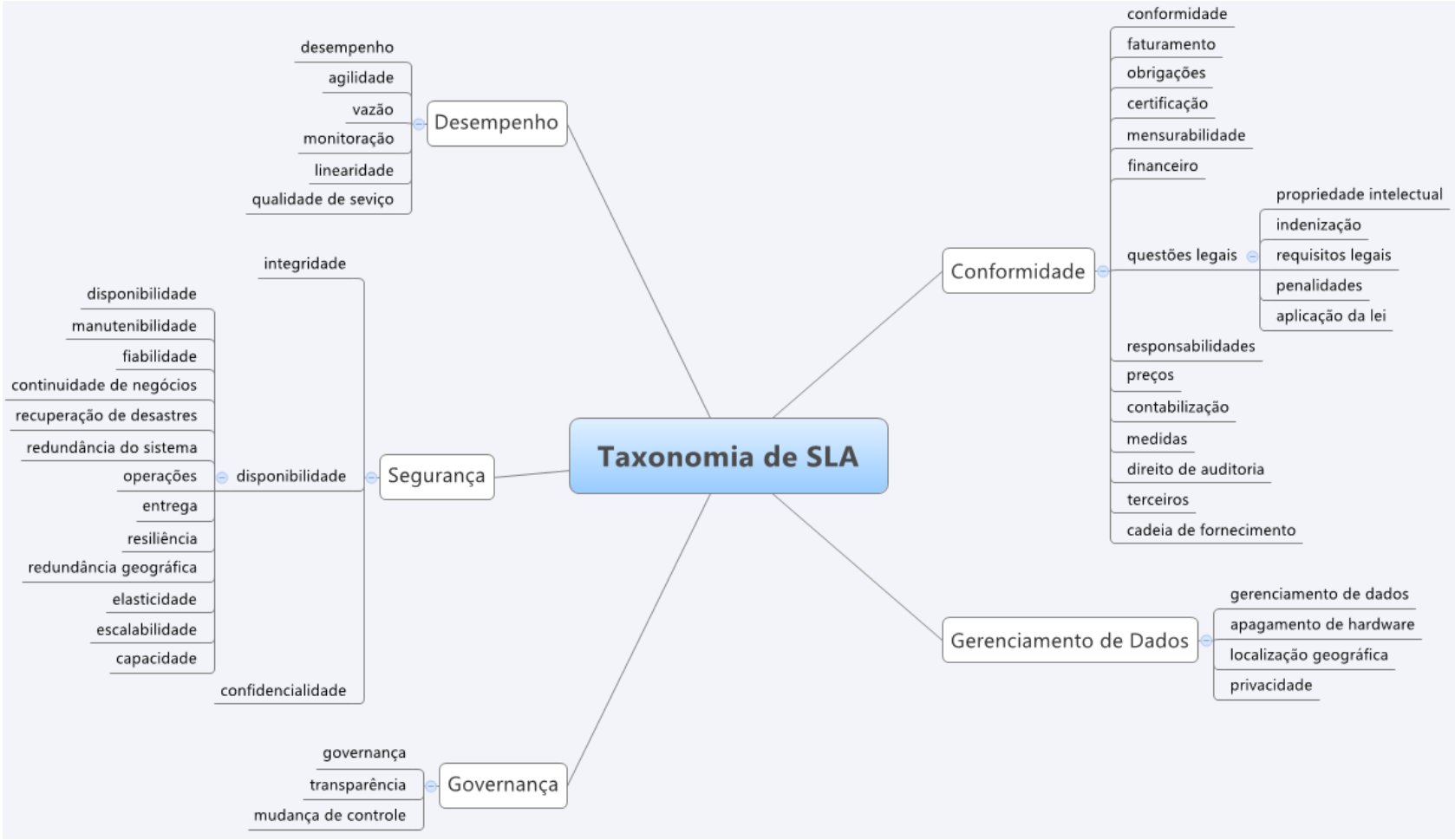

Figura 17: Proposta de taxonomia de SLA em computação em nuvem.
Fonte: elaborada pelo autor.

Com base na Figura 17, verifica-se que a classificação em categorias gerou uma taxonomia de SLA constituída de cinco categorias: desempenho, governança, gerenciamento de dados, segurança e conformidade, sendo que as duas últimas apresentam dois níveis. A categoria de conformidade contém, como segundo nível, as questões legais e a categoria de segurança contém, como segundo nível a confiabilidade. A taxonomia apresentada auxilia no processo de especificação de um SLA, em relação a:

- Conhecimento do vocabulário empregado na especificação de um SLA;
- Conjunto de assuntos que devem ser levados em consideração durante a especificação de um SLA;
- Premência de entendimento pelo provedor e consumidor sobre as necessidades que devem ser abordadas em um SLA;
- Necessidade de uma equipe multidisciplinar para tratar da especificação do SLA, devido à complexidade dos assuntos levantados; e
- Diminuição do risco para ambas as partes do que concerne à da operação negociada.

Assim, a taxonomia proposta representa uma consolidação das taxonomias existentes, complementada pelas necessidades de requisitos de SLA apontadas. Também apresentado uma consolidação das categorias.

3.5 Considerações do Capítulo

Neste capítulo, foi apresentada uma introdução ao conceito de SLA dentro do contexto de computação em nuvem, apresentando-se uma coletânea de definições, com o objetivo de ilustrar a inexistência de uma definição consolidada sobre o tema. Também foi apresentada uma nova proposta de ciclo de vida de SLA consolidando propostas existentes.

Em seguida, é efetuada uma análise quantitativa dos problemas relacionados a SLA e respectivas soluções. Esta análise possibilita verificar de forma geral que a grande maioria dos problemas apontados se encontram com poucas propostas de solução, o que reflete a existência de oportunidades para desenvolvimento de pesquisa nestas áreas. Duas áreas destacam-se com relação à necessidade de aprofundamento de pesquisa: segurança e gerenciamento de dados. Desta forma, um aprofundamento nas soluções propostas foi efetuado, buscando compreender a necessidade de segurança para ambas as categorias, pois, gerenciamento de dados tem relação direta com a questão de segurança na manipulação dos dados. Este aprofundamento visa compreender quais são os requisitos de segurança que devem ser abordados e tratados dentro do contexto de SLA de computação em nuvem.

Por fim, foi elaborada uma nova proposta de taxonomia com base nos problemas levantados, em função da inexistência de uma taxonomia adequada e, também, para auxiliar no entendimento das categorias que estão relacionadas com estes problemas. No levantamento apresentado sobre os problemas, verifica-se que existem diversos assuntos que podem ser abordados na especificação de um SLA. Isso reflete a complexidade que o assunto representa tanto para o consumidor como para provedor de serviço. Portanto, a especificação adequada de um SLA exerce um papel importante para o negócio da empresa e consistem em mais um desafio para a adoção da computação em nuvem.

4 ACORDO DE NÍVEL DE SERVIÇO DE SEGURANÇA

A partir das informações do levantamento das soluções que abordam requisitos de segurança de SLA dentro do contexto de computação em nuvem, foi realizado um aprofundamento qualitativo sobre o tema. Este aprofundamento visa compreender os problemas que estão sendo tratados, quais as principais soluções e abordagens empregadas para tratar dos problemas levantados.

Este capítulo introduz os principais conceitos relacionados à SLA (*Security Level Agreement)* de segurança, bem como apresenta soluções existentes que lidam com requisitos de segurança especificados em um SLA para serviços oferecidos por sistemas de computação em nuvem. Neste sentido, este capítulo traz um breve histórico sobre SLA, a aplicação de SLA de segurança no contexto de computação em nuvem e soluções propostas para problemas de SLA de segurança.

4.1 Histórico

A necessidade de abordar requisitos de SLA de segurança está presente na área de TIC (Tecnologia da Informação e Comunicação), bem como nos paradigmas de computação atuais. Com o objetivo de compreender como esta necessidade evoluiu, um breve histórico é apresentado.

No trabalho de Henning (HENNING, 1999), é encontrado o primeiro estudo da literatura que discute a questão da viabilidade em expressar adequadamente requisitos

de segurança em um contexto de SLA, pois, em SLA, é pressuposto definir níveis de serviço mensuráveis. Estes serviços são mensurados de forma quantitativa e não qualitativa. O artigo também aborda a dificuldade de encontrar na literatura informações que possibilitem o desenvolvimento de um SLA de segurança, bem como a questão da ausência de serviços tangíveis e mensuráveis, e o fato dos serviços de segurança não terem sido concretamente quantificáveis, em contraste com a área de telecomunicações que possui métricas bem definidas. Henning (1999) propôs que definições de SLA de segurança devem contemplar atividades de gerenciamento operacional e administrativo, e não somente mecanismos que implementam e monitoram as políticas de segurança sobre os usuários do sistema. Esta proposta deve-se em razão da dificuldade de mensurar de forma quantitativa requisitos de segurança e por consequência efetuar a monitoração dos mecanismos de segurança que utilizam estas métricas quantitativas.

No artigo de Irvine (IRVINE; LEVIN, 2000) o conceito de segurança como uma dimensão de QoS (*Quality of Service*) aplicada a sistemas distribuídos é discutida. Com a finalidade de ilustrar esse conceito apresenta por meio de exemplos como especificar e mensurar variáveis de segurança, e como estes exemplos podem ser utilizados para melhorar a segurança e o desempenho de sistemas. O artigo é concluído estabelecendo que a segurança pode ser uma dimensão semântica significativa de QoS, ou seja, que requisitos de segurança são um tipo de QoS.

O artigo de Righi (RIGHI; PELISSARI; WESTPAHALL, 2004) aborda a relação de interdependência entre as áreas de segurança e gerenciamento de redes quando se trata do desenvolvimento de acordos de níveis de serviço orientados à segurança. O trabalho apresenta a definição e a validação de métricas voltadas para acordos de níveis de serviço de segurança, com foco principal em métricas e parâmetros que podem ser empregados nos contratos de SLA de segurança.

O artigo de Righi (RIGHI; KREUTZ; WESTPAHALL, 2006) aborda a necessidade da utilização de acordos de níveis de serviços voltados à segurança, ao qual chamou de

Sec-SLA, entre as partes envolvidas. Para atender esta necessidade identificada propõe uma arquitetura para monitoração e controle de Sec-SLA, onde este acordo pode ser fiscalizado por ambas as partes, o consumidor e provedor do serviço. Righi (2006) conclui estabelecendo que as necessidades apresentadas pela monitoração e pelo controle da Sec-SLA englobam duas grandes áreas, a segurança e gerenciamento de redes.

No artigo de Yearworth (YEARWORTH; MONAHAN; PYM, 2008) é abordado o desenvolvimento de um modelo de operação de segurança adequado ao tratamento de desempenho em função das necessidades de SLA de segurança estabelecidas para o ambiente, ou seja, garantindo que os mecanismos de segurança não impactem o desempenho contratado. Também é abordada a questão da necessidade de entendimento de todos os custos que envolvem a operação de segurança, pois, estes custos afetam a organização.

No trabalho de Monaham (MONAHAN; YEARWORTH, 2008) é constatada a necessidade apontada por usuários de tratar requisitos de segurança dentro do contexto de SLA. Esta necessidade motivou a pesquisa sobre requisitos de segurança que podem ser abordados por meio de um SLA entre provedor e consumidor. Também conclui-se que o tratamento de SLA de segurança podem prover maior visibilidade operacional dos serviços oferecidos por parte da operadora e pode ser utilizado como um diferencial competitivo.

Desta forma, pode-se verificar que a necessidade de tratar os requisitos de segurança em acordos de níveis de serviço não é uma necessidade atual, mas uma necessidade identificada dentro do contexto de sistemas distribuídos e que pressupõe a interdependência entre as áreas de gerenciamento e segurança de redes. Estes requisitos devem ser tratados com base em métricas ou níveis de serviços mensuráveis, que tem o objetivo de validar e monitorar as necessidades apontadas no SLA.

Os termos *Security* SLA (SLA de Segurança) ou Sec-SLA são comumente empregados para designar a necessidade de abordar requisitos de segurança em acordos de

níveis de serviço, bem como mecanismos de monitoração e controle destes requisitos de segurança, mas não são os únicos na literatura científica. O termo QoP *(Quality of Protection)* (JAATUN; BERNSMED; UNDHEIM, 2012) é empregado para informar que o serviço entregue pelo provedor de serviços leva em consideração um conjunto específico de requisitos de segurança, mas sua utilização é menos comum que *Security* SLA ou Sec-SLA. Com base nesta explicação de terminologias, pode-se concluir que a definição de Sec-SLA expressa a necessidade de tratar requisitos de segurança, bem como mecanismos de monitoração e controle em acordos de nível de serviço.

As necessidades de segurança em computação em nuvem em sua maioria são similares às necessidades encontradas ambientes de TI (MEEGAN, 2012; VENTERS; WHITLEY, 2012), no entanto a necessidade de inserção de requisitos e parâmetros de segurança em contratos de SLA são especificas ao contexto da computação em nuvem (BOUCHENAK, 2013; FERREIRA, 2013). Desta forma, a necessidade de se especificar requisitos de segurança em SLA para serviços de computação em nuvem é um caminho natural para consumidores e provedores de serviço.

4.2 SLA de Segurança

As métricas de SLA podem ser classificadas em categorias, estas incluem disponibilidade, desempenho, segurança (ITU-T-FG, 2012), qualidade e custo (JAATUN; BERNSMED; UNDHEIM, 2012). Dentro dos serviços básicos de segurança da tríade CIA (*Confidentialilty, Integrity and Availability*), a disponibilidade é comumente abordada em SLA de computação em nuvem, já os requisitos de integridade e confidencialidade não são abordados. A monitoração da disponibilidade também é mais desenvolvida comparada aos demais serviços de segurança (DEKKER; HOGBEN, 2011; LUNA; LANGENBERG; SURI, 2012b).

A questão de SLA de segurança tem sido abordada mais recentemente para o con-

texto de computação em nuvem (BOUCHENAK, 2013), bem como, arquiteturas de referência e tecnologias que habilitam o uso de métricas. Neste contexto, encontram-se em um estágio embrionário (GARCIA, 2011), bem como, lidar com as métricas de formas quantitativa e não qualitativa (LUNA, 2012a). Além destas questões, a representação de SLA de segurança e sua divulgação são pouco abordadas para o contexto de nuvem (MELAND, 2012; FERREIRA, 2013).

4.2.1 Práticas de Segurança

Com o objetivo de compreender como estas questões são tratadas, uma pesquisa referenciada envolvendo práticas, obrigações, recomendações, benefícios e desafios é apresentada para o contexto de SLA de segurança aplicado em ambientes de computação em nuvem. No que concerne às práticas usuais dos provedores de serviço de tratamento de requisitos de segurança definidos no SLA, conforme (MEEGAN, 2012; BAUDOIN, 2013; LUNA, 2012a), consideram-se que:

- O provedor é o único responsável por determinar a ocorrência de violações de SLA de segurança;
- O SLA é composto de termos genéricos que informam que o provedor deve proteger os dados do consumidor sem especificar o nível de proteção e como será realizada esta proteção;
- Aplica-se uma especificação genérica sobre as medições de segurança mantidas e efetuadas, acompanhadas da obrigação do consumidor de determinar e avaliar se os valores medidos são adequados segundo o SLA de segurança contratado;
- Não há obrigatoriedade de mencionar como as medições de segurança são realizadas pelo provedor;
- Há ausência de definições e obrigações para com a proteção da segurança dos dados do consumidor; e

- Não há especificação de níveis de serviço de segurança nos contratos, desta forma impedem que o usuário tome decisões relevantes sobre a segurança de seu ambiente.

4.2.2 Obrigações do Provedor de Serviço

Por meio destas práticas usuais é possível constatar que os aspectos de segurança têm sido negligenciados por parte dos provedores de serviço no que tange à especificação e monitoração dos SLAs e métricas associadas. Além disso, observa-se também o despreparo dos consumidores em lidar com este tema. Para auxiliar tanto provedores como consumidores, os provedores de serviço associados ao CSA (*Cloud Security Alliance*) (ONLINE, 2014) criaram uma base de dados pública (CSA *Security, Trust Assurance Registry*) que contém os controles de segurança adotados pelos provedores de serviço. A relação de obrigações do provedor de serviço com relação a SLA de segurança, conforme (MEEGAN, 2012; HOGBEN; DEKKER, 2012; ITU-T-FG, 2012; JAATUN; BERNSMED; UNDHEIM, 2012; PATEL; JETHAVA, 2012; SCHNJAKIN; ALNEMR; MEINEL, 2010), incluem:

- Considerar boas práticas relacionadas à segurança e privacidade. As práticas de segurança e privacidade devem estar explícitas, separadas e claramente identificada nos documentos;

- Se o provedor sofrer ataques de segurança que causem danos aos dados do usuário, é obrigação do provedor restaurar os dados de um backup;

- O provedor deve garantir, subcontratar um profissional ou fornecer informações de segurança para auxiliar o consumidor no processo de avaliação e seleção dos mecanismos de segurança apropriados. Esta opção também deve estar disponível em caso de resposta a incidentes de segurança;

- O usuário/consumidor deve ser informado como o provedor trata da confidenci-

alidade da informação, bem como as vulnerabilidades existentes e medidas de mitigação utilizadas;

- O provedor deve avaliar e reportar as vulnerabilidades de segurança, controles, serviços e mecanismos por ele empregados;
- Quando o dado é transferido para a nuvem, a responsabilidade por proteger e garantir a segurança dos dados é do provedor; e
- O provedor deve adquirir certificações relevantes referentes a padrões de segurança (por exemplo: ISO 27001, PCI DSS (*Payment Card Industry Data Security Standard*), etc.).

4.2.3 Métricas de Segurança

É possível, então, constatar a necessidade, por parte do provedor, de desenvolver um processo para tratar os aspectos relacionados à segurança. O suporte diferenciado para ao consumidor também deve ser consideração em relação a esta questão. Existem recomendações sobre medidas relacionadas a métricas de segurança, que devem ser especificadas em uma SLA, conforme discutem (KEN, 2012; MEEGAN, 2012; WHITESIDE, 2012; DEKKER; HOGBEN, 2011; ITU-T-FG, 2012; CPNI, 2010; KANDUKURI; PATURI; RAKSHIT, 2009; HENNING, 1999; LUNA; LANGENBERG; SURI, 2012b):

- O SLA deve especificar responsabilidades de segurança e, também, incluir a divulgação de vulnerabilidades de segurança por parte do provedor para os consumidores;
- Os requisitos de segurança especificados e contratados em um SLA por parte de um provedor devem ser estendidos a todos os parceiros envolvidos em alguma etapa da prestação do serviço;

- Métricas e padrões para avaliar o desempenho e a efetividade do gerenciamento da segurança da informação devem ser estabelecidos e especificados no SLA acordado;

- Políticas de privacidade de dados por parte do provedor devem ser incluídas no SLA. Como exemplos de políticas, podem-se citar: tratamento dos dados, política de retenção dos dados, tratamento do dado durante o processo de comunicação, como o dado é armazenado e utilizado;

- O direito de auditar o provedor deve ser uma cláusula do SLA, possibilitando que o consumidor possa realizar auditoria do provedor de serviço com suporte à rastreabilidade e transparência do SLA de segurança definido. Assim, o provedor deve oferecer recursos para execução da auditoria;

- O SLA deve conter definições mensuráveis de parâmetros de segurança e o consumidor deve receber relatórios sobre a avaliação de incidentes;

- Deve estar prevista compensação financeira para o caso de falhas nos serviços contratados;

- Os detalhes a respeito dos algoritmos de cifragem e políticas de controle de acesso devem estar especificados;

- O SLA pode conter parâmetros não quantitativos, como regulamentações, restrições geográficas para processamento e/ou tratamento de dados e padrões de processo de negócios (e.g., ISO 2000);

- O processo de monitoração de segurança, incluindo a coleta de evidências, deve conter como foram coletadas as evidências e quem é responsável por essa coleta;

- O SLA deve conter detalhes sobre como a segurança é mantida pelo provedor, quais os métodos empregados e como as reclamações dos consumidores são atendidas;

- As definições de segurança em SLA devem tratar as atividades de gerenciamento de segurança operacional e administrativa; e
- A inclusão de itens de segurança no SLA obrigam explicitamente as partes interessadas (*stakeholders*) a tratarem a questão de segurança.

Pelas obrigações apresentadas, verifica-se que existem diversas necessidades que devem ser tratadas dentro do contexto da definição de requisitos de segurança em SLA. As necessidades cobrem desde a definição de parâmetros a serem monitorados até a definição de penalidades em caso de falhas.

4.2.4 Benefícios

Este conjunto de obrigações reportadas representam grandes desafios para o provedor de serviço, bem como para todos os atores envolvidos. A adoção de SLA de segurança apresenta benefícios tanto para o provedor como para o consumidor, conforme indicado por (LUNA, 2012a; BOUCHENAK, 2013; JAATUN; BERNSMED; UNDHEIM, 2012; SWEET, 2012; FICCO; RAK; DI MARTINO, 2012; MELAND, 2012), e são eles:

- O uso de SLA de segurança tem o potencial para prover benefícios tangíveis para o provedor de serviço, especialmente os associados com a melhoria da administração de segurança e práticas de gerenciamento, proporcionando assim maior transparência para os usuários finais;
- Oferece orientação clara sobre compromissos explícitos de segurança, possibilitando que o provedor de serviço expresse quais são as garantias dos seus serviços de segurança e as consequências e desdobramentos no caso do não cumprimento dessas garantias;
- Permite mitigar os riscos de segurança associados a arquiteturas orientadas a

serviço e aumentar a confiança dos prestadores de serviço com relação aos mecanismos de segurança existentes e sua eficácia;

- O SLA de segurança é uma das principais áreas a serem examinadas na avaliação de risco no negócio;

- Incorporando parâmetros de segurança nos serviços requisitados pode-se melhorar a QoS dos serviços que são providos. Estes parâmetros também geram implicações nas soluções de segurança a serem implementadas para monitorar a entrega dos serviços de nuvem; e

- Permite auxiliar o paradigma de computação em nuvem a alcançar seu potencial pleno como uma alternativa dominante de terceirização, para isso, os requisitos de segurança do cliente devem ser garantidos por meio de SLA.

A adoção de parâmetros de segurança em SLA apresenta benefícios tangíveis e não tangíveis tanto para os provedores como para consumidores, conforme apresentado. Segundo o relatório da pesquisa realizada pela empresa CA Technologies[1] e Instituto Ponemon (BOUCHENAK, 2013) com 127 provedores de serviço nos EUA e Europa, mais de 80% dos participantes não acreditam que prover segurança em seu serviço será um diferencial competitivo. Na realidade, pressupõe-se que segurança é um valor assumido (embutido) no serviço prestado pelas soluções de computação em nuvem.

A questão de utilização de requisitos de segurança em SLA é um grande desafio para provedores de serviço e consumidores, conforme observado nas informações apresentadas. A academia também pactua e aponta desafios que envolvem esta questão e aponta desafios nesta área. Estes desafios consistem em comparar obrigações entre provedores de serviço (BAUDOIN, 2013), taxonomias, métricas e arquiteturas de referência conforme apontado por Garcia (GARCIA, 2011), e a necessidade de mecanismos

[1] http://www.ca.com/

de manutenção da segurança e tratamento das reclamações dos consumidores como apontado em (KANDUKURI; PATURI; RAKSHIT, 2009).

Pode-se constatar que o tratamento de SLA de segurança por parte do provedor de serviços de nuvem, bem como por parte do consumidor é um assunto em desenvolvimento e desafiador. Estes desafios não envolvem somente os aspectos técnicos, mas também cultural e financeiro no tratamento destas questões que envolvem a segurança e sua especificação em um SLA.

4.3 Trabalhos Relacionados

Por meio do levantamento quantitativo ilustrado na Figura 14, pode-se verificar que existe uma lacuna entre os problemas e as soluções de SLA de segurança atreladas ao contexto de computação em nuvem; esta lacuna representa oportunidades de pesquisa nesta área. A Figura 11 aponta que 37% das soluções de SLA estão relacionadas à segurança.

Uma análise qualitativa destes trabalhos faz-se necessária, para verificar quais problemas estão sendo tratados, quais abordagens estão sendo utilizadas e os resultados alcançados. Nesta análise, requisitos referentes ao serviço de disponibilidade não serão levados em consideração, por se tratarem de requisitos comumente tratados por parte do provedor e de conhecimento do consumidor. Além desta análise, também é apresentada a relação das soluções de segurança com o ciclo de vida do SLA proposto (Figura 5), esta relação tem como objetivo identificar em que etapa se concentram os trabalhos analisados. Apresenta-se na Tabela 4 os trabalhos relacionados em ordem cronológica, contendo: autor, ano de publicação e fase(s) do ciclo de vida ao qual o trabalho se relaciona.

Tabela 4: Trabalhos relacionados versus fases do ciclo de vida

	2011 Garcia	2011 Rank	2012 Jegou	2012a Luna	2012b Luna	2012 Silva	2012 Ulha	2013 Ferreira	2014 Taha	2015 Benedicts	2015 Luna	2016b Casola	2016a Casola	2016 Modic	2016 Trapero
Fase 1-Definir e especificar o SLA	A	B	C	D	E	F	G	H	I	J	K	L	M	O	Q
Desenvolvimento do produto/serviço															
Especificação inicial															
Especificação do modelo de serviço															
Publicação/descoberta do serviço				1											
Definição de parâmetros e preços de ofertas e requisições	1				1	2	1	3			1		2		1
Projeto e desenvolvimento															
Oferta do serviço				1	1		1				2			1	
Localizar provedor de serviço				1											
Definir SLA									1			1	2		1
Desenv. serviço/modelo do SLA															
Fase 2-Negociação e venda do serviço															
Implementação do serviço															
Entrega do serviço		1				1		2		1		1			
Fase de estabelecimento do serviço				2	2										
Otimização do recurso selecionado													1		
Empacotamento do serviço															
Distribuição do serviço															
Provisionamento do serviço		1				1						1	1		
Preparação do ambiente												1			
Ativação do serviço															
Fase 3-Executar e gerenciar o SLA															
Execução do serviço	2		1					1							
Avaliação e correção das ações	2									1					1
Monitoração do serviço	2		1					1		1		1	1		1
Relatar atividades e ocorrências			1												
Operações do serviço															
Avaliação do serviço															
Gerenciamento do serviço			1												1
Aplicar especificações															
Fase 4-Finalizar e Avaliar SLA															
Encerrar o serviço															
Finalizar o serviço															
Desativar o serviço															
Terminar o SLA															
Terminar e bilhetar o serviço															
Aplicar sanções										2					

Fonte: elaborada pelo autor.

Na tabela 4 é apresentada a relação entre os trabalhos relacionados e o desafio da fase do ciclo de vida do SLA que o mesmo trata. Verifica-se que os trabalhos podem apresentar soluções para mais de um desafio de uma fase do ciclo de vida do SLA, o que é representado por meio dos indicadores 1, 2 e 3. Estes indicadores apontam qual ou quais desafios o trabalho foi elaborado, e quais o mesmo também contribui de foram indireta; esta representação é dada pela ordem crescente do indicador. Apresenta-se, um resumo descritivo dos trabalhos considerados nesta análise, bem como a sua relação com as fases do ciclo de vida do SLA:

- **Artigo A -** ***A Security Metrics Framework for the Cloud*** **- (GARCIA, 2011).**
  Neste trabalho é apresentada uma proposta de arcabouço para a elaboração de métricas para a avaliação de segurança por parte do provedor da nuvem, levando em consideração os diferentes modelos de serviço e implantação. O arcabouço é constituído de três etapas: a) A primeira etapa consiste em desenvolver uma taxonomia que leve em consideração as ameaças e os requisitos de segurança; b) A segunda etapa consiste em desenvolver as métricas com base em métodos de avaliação e dados históricos; c) A terceira etapa consiste em desenvolver a arquitetura de referência (escalável, não-intrusiva e interoperável) além de especificar técnicas de avaliação, monitoração do ambiente de forma estática e dinâmica. A principal contribuição do trabalho é a apresentação do arcabouço para elaboração de métricas de segurança com base na experiência de equipe em projetos da Comunidade Europeia que tratam do assunto. O trabalho não apresenta resultados da aplicação da arquitetura proposta, ficando para trabalhos futuros. Este trabalho é enquadrado na Fase 1 do ciclo de vida, devido à questão de definição de parâmetros de segurança a serem abordados no SLA e, também, na Fase 3 pois as métricas definidas necessitam ser aplicadas, colocadas em execução, monitoradas e usadas para relatar ocorrências;

- **Artigo B -** ***A SLA-based interface for security management in cloud and GRID***

integrations **- (RANK; LICCARDO; AVERSA, 2011) .**

Neste trabalho é apresentada uma abordagem para o desenvolvimento de uma aplicação de computação em nuvem, tendo como base a API do projeto mOSAIC[2]. Esta aplicação utiliza parâmetros definidos no SLA para habilitar o gerenciamento de segurança do ambiente, em especial, o gerenciamento de mecanismos de autenticação e autorização. A solução proposta consiste em gerenciar os diferentes papéis dos consumidores e as diferentes políticas de segurança necessárias em três contêineres distintos. O sistema de gerenciamento define em que contêiner o consumidor será alocado em função da definição feita no seu SLA. Como prova de conceito da abordagem proposta, a mesma foi empregada no ambiente de GRID Globus GT4[3]. A principal consideração com relação ao trabalho é o fato de estar vinculada ao ambiente GRID Globus utilizado e restrito às ferramentas disponibilizadas por este ambiente. Este trabalho foi enquadrado na Fase 2 por utilizar os requisitos de segurança como parâmetro para a entrega dos serviços, bem como o provisionamento do serviço no ambiente;

- **Artigo C -** ***Managing OVF Applications Under SLA Constraints on Contrail Virtual Execution Platform*** **- (JEGOU, 2012).**

  Neste trabalho é apresentado o mecanismo VEP (*Virtual Execution Platform*) que é um componente do Contrail[4], projeto desenvolvido pela comunidade Europeia que teve por objetivo desenvolver um arcabouço para gerenciar e monitorar aplicações distribuídas em um ambiente federado de computação em nuvem, levando em consideração requisitos definidos em um SLA. Os requisitos de SLA relativos à segurança são incorporados e suportados pelo projeto; principalmente

[2]O projeto mOSAIC visa o desenvolvimento de uma plataforma de código aberto que possibilita por meio de uma API a negociação de serviços de nuvem com base nas necessidades requisitadas pela aplicação, basicamente fornece uma camada de intermediação para os serviços solicitados pela aplicação. - http://www.mosaic-cloud.eu.

[3]O GRID Globus é um conjunto de ferramentas de código aberto empregado para a construção de grades computacionais. - http://toolkit.globus.org/toolkit/

[4]É uma pilha de componentes que são projetados para integrar uma série de nuvens independentes em um ambiente de nuvem federado. A alocação dos recursos a serem empregados para execução de uma aplicação e definida por meio de uma SLA. - http://contrail-project.eu/web/guest.

os que tratam da autenticação e autorização entre os ambientes federados. A aplicação a ser instanciada no ambiente é monitorada e controlada durante todo o seu ciclo de vida, sendo que este monitoramento também é responsável pelo processo de notificações em caso de violação. A restrição do VEP está relacionada ao ambiente IaaS, já que este deve ser capaz de prover mecanismos para alocação e monitoração de recursos federados. Contudo, não está claro quais outras necessidades de segurança ou outros mecanismos do Contrail, como a questão de confidencialidade e integridade, são tratadas pelo VEP. Este trabalho foi enquadrado na Fase 3, pois engloba todas as atividades de execução do serviço, monitoração do serviço, relatar ocorrências e gerenciamento do serviço;

- **Artigo D -** ***Quantitative Assessment of Cloud Security Level Agreements - A Case Study*** **- (LUNA, 2012a).**

  Neste trabalho é apresentado um estudo de caso em que é aplicada uma avaliação quantitativa de segurança dos provedores de serviço de nuvem, para tal, a base de informações do CSA chamada STAR que contém práticas de segurança aplicadas por parte do provedor é utilizada. Com base neste estudo é apresentado um conjunto de métricas utilizadas para quantitativamente comparar SLAs de segurança no contexto de computação em nuvem. Para o desenvolvimento das métricas a abordagem REM (*Reference Evaluation Methodology*) foi empregada, devido à sua flexibilidade para modelar e avaliar políticas de segurança. Esta técnica originalmente foi proposta por Casola (CASOLA, 2005), para avaliar quantitativamente politicas de segurança e não foi empregada ao cenário de computação em nuvem, sendo necessário adaptar a mesma para que seja empregada neste cenário. As principais contribuições do trabalho são: uma proposta para aplicar métricas de segurança para comparar, referenciar e avaliar a adequação dos provedores de serviço com relação ao SLA de segurança de forma quantitativa. Outras contribuições são: a aplicação deste método para avaliar a base da

CSA STAR e verificação do posicionamento dos provedores com relação a esta questão. O método apresentado avalia, de forma geral, os mecanismos propostos e não individualmente, colocando os mecanismos em um mesmo patamar. Este trabalho foi enquadrado na Fase 1 do ciclo de vida, devido ao tratamento de métricas de segurança que podem ser empregadas para definir um SLA de segurança (publicação/descoberta de serviço, oferta de serviço e localizar provedor de serviço). Além disso, esse trabalho auxilia na avaliação da oferta de serviços do provedor e pode ser enquadrado na Fase 2, especificamente na fase de estabelecimento do serviço. Pode ser empregado pelo consumidor para auxiliar na negociação com o provedor de serviços, já que permite avaliar e comparar os serviços relacionados à segurança que estão sendo ofertados;

- **Artigo E -** ***Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees*** **- (LUNA; LANGENBERG; SURI, 2012b).**

  Neste trabalho é apresentado um método para comparar quantitativamente e qualitativamente os requisitos do SLA de segurança suportador por provedores de computação em nuvem. A abordagem utilizada para desenvolver o método consiste na aplicação de QPT (*Quantitative Policy Trees*), uma estrutura de dados em árvore que possibilita representar e raciocinar sistematicamente, sobre o SLA de segurança. O método consiste de três etapas: a) A primeira inclui o levantamento dos requisitos definidos pelos provedores de serviço com relação ao SLA de segurança; cada requisito levantado é avaliado e recebe um peso com o objetivo de representar sua importância do ponto de vista do usuário; b) Na segunda etapa, estes requisitos de SLA de segurança são mapeados em QPTs, no qual o nível principal é situado na raiz da árvore, os nós intermediários contêm categorias intermediárias e os nós folhas, contém o mecanismo de segurança ao qual o valor atribuído que pode ser quantitativo ou qualitativo; c) Na terceira etapa, são comparadas as árvores geradas para os provedores de serviço que estão sendo avalia-

das. A base do CSA STAR é utilizada para exemplificar e apresentar do método proposto. Ainda, é comentado no artigo que o sistema QUANTSaaS (*QUANTifiable Security-as-a-Service*) deve ser desenvolvido como prova de conceito. O método avalia em categorias os requisitos de segurança, o que facilita a comparação entre os provedores de serviço. O método apresenta como critério para os nós folha a atribuição por parte do consumidor de um valor que pode ser quantitativo ou qualitativo para o mecanismo de segurança empregado; a questão é que este critério é subjetivo, ou seja, é definido sem seguir alguma recomendação acadêmica ou boa prática do mercado. Esta subjetividade pode levar o método a apresentar informações imprecisas, e estas podem levar a falhas na tomada de decisão, o que não é desejado tratando-se de requisitos de segurança. Também não é recomendado que a decisão de avaliar um dos mecanismos recaia somente sobre o consumidor, já que esta é uma tarefa complexa e requer um conhecimento avançado sobre os mesmos. Este trabalho foi enquadrado na Fase 1 do ciclo de vida, pois permite avaliar a oferta do serviço relacionado à SLA de segurança entre provedores de serviço, bem como definir parâmetros para os requisitos que podem vir a compor um SLA de segurança. Também pode ser enquadrado na Fase 2, pois pode servir como base para uma negociação com o provedor de serviço, na fase de estabelecimento do serviço;

- **Artigo F -** ***A Methodology for Management of Cloud Computing using Security Criteria*** **- (SILVA; FERREIRA; GEUS, 2012).**

  Neste trabalho é desenvolvida uma proposta para avaliar a segurança de um ambiente de computação em nuvem utilizando uma hierarquia de métricas. Esta hierarquia produz um índice utilizado para calcular o índice de alocação. O índice de alocação, por sua vez, trata da alocação e do gerenciamento dos recursos entregues ao consumidor. Esta entrega é feita de acordo com as regiões relacionadas à infraestrutura física do provedor, que está relacionada com o índice de

alocação calculado. Desta forma, o compartilhamento de recursos ocorre entre os consumidores que possuem o mesmo índice e atendem aos mesmos critérios de segurança. O método aplicado para gerar a hierarquia de métricas de segurança é o GQM (*Goal-Question-Metric*), que originalmente foi desenvolvido para avaliar as falhas de *software* tratadas de forma qualitativa e subjetiva. A aplicação do processo de gerar a hierarquia de métricas possibilitou o tratamento das métricas em: métricas de grupo e sub-métricas, que são abordagens para tratar as métricas que podem ser especificadas de diversas formas e apresentam diferentes maneiras de contribuir com a métrica. Este trabalho foi enquadrado na Fase 2 devido ao seu enfoque principal que é o provisionamento do serviço e entrega do serviço em função dos requisitos de segurança. Também, pode ser enquadrado na Fase 1, pois apresenta um método para se especificar parâmetros de segurança para o ambiente e definição de SLA;

- **Artigo G -** ***Automated Security Compliance Tool for the Cloud*** **- (ULLA, 2012).** Neste trabalho é apresentada uma proposta de ferramenta automatizada para avaliação de níveis de conformidade de segurança de provedores de nuvem. Esta ferramenta possibilita ao usuário uma melhor avaliação das ofertas de serviços fornecidas pelos provedores de serviços levando-se em consideração os requisitos de segurança. Para atingir este objetivo, é realizada uma prova de conceito que contempla a integração do arcabouço do CloudAudit[5] definido pelo CSA com a solução aberta de computação em nuvem OpenStack[6]. Desta forma o consumidor pode verificar os requisitos de segurança empregados pela plataforma OpenStack, que estão em conformidade com os requisitos especificados pelo CSA, avaliando-se, assim, seu nível de conformidade. O trabalho apresenta

[5]O CloudAudit tem por objetivo fornecer uma interface e método aberto para as empresas e consumidores interessados em promover auditoria em ambiente de computação em nuvem (IaaS, PaaS e SaaS). - https://cloudsecurityalliance.org/research/cloudaudit/

[6]O OpenStack é um conjunto de projetos de software de código aberto empregados para configurar e operar a infraestrutura de computação em nuvem, e prover serviços como máquinas virtuais, armazenamento e rede para os usuários. - https://www.openstack.org/

uma solução específica para auditar as conformidades de segurança com base no CloudAudit e Openstack. Não é abordado como outras soluções de auditoria e soluções de nuvem podem ser integradas na arquitetura implementada. Este trabalho foi enquadrado na Fase 1, pois é uma abordagem para avaliar como o provedor de serviços atende aos requisitos de segurança (oferta de serviço) e também para identificar quais são os parâmetros empregados;

- **Artigo H - Uma Arquitetura para Monitoramento de Segurança baseda em Acordos de Níveis de Serviço para Nuvens de Infraestrutura - (FERREIRA, 2013).**

  Neste trabalho é apresentada uma proposta de mecanismo para monitoração de máquinas virtuais em um ambiente de nuvem de infraestrutura, tendo como base parâmetros de segurança definidos em um SLA. A abordagem empregada de *black box* e introspecção oriunda da área de Engenharia de Software é utilizada no processo de monitoração, com o objetivo de eliminar a necessidade de instalação de ferramentas na máquina virtual. A partir do mecanismo de monitoração é possível identificar ataques a maquinas virtuais. O trabalho apresenta algumas restrições com relação à integração dos sistemas de monitoração ao ambiente de gerenciamento de infraestrutura da nuvem, pois não utiliza uma interface padrão ou segue recomendações de padronização. Considerações são efetuadas em relação à ausência da definição de parâmetros de segurança para o ambiente de máquinas virtuais a ser monitorado, e também quais são estes parâmetros (métricas). Este trabalho é enquadrado principalmente na Fase 3, pois atua no processo de monitoração e execução do serviço. O mesmo também é enquadrado na Fase 2, pois durante o processo de implementação e entrega das máquinas virtuais utiliza parâmetros de segurança definidos no SLA de segurança. Também enquadra-se na Fase 1, pois apresenta uma forma de representar as políticas de segurança em acordos de nível de serviço, desta forma auxiliando no processo de

definição de parâmetros de segurança que devem compor um SLA de segurança;

- **Artigo I -** ***AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security*** **- (TAHA, 2014).**

  Neste trabalho é apresentado uma abordagem para conduzir análise quantitativa e qualitativa dos níveis de segurança providos pelo provedor da nuvem. Utilizando-se da abordagem AHP (*Analytic Hierarchy Process*) apresentam uma técnica para tomada de decisão que possibilita comparar e avaliar a segurança fornecida pelo provedor com base no SLA de segurança definido. Além disso, apresenta um método que auxilia o usuário na especificação de requisitos de segurança com base em suas necessidades. Este trabalho é enquadrado na Fase 1, pois tem seu foco na definição de requisitos de SLA de segurança, ou seja, definição do SLA;

- **Artigo J -** ***REST-based SLA Management for Cloud Applications*** **- (BENEDICTIS, 2015).**

  Neste trabalho é apresentado o projeto de serviços de gerenciamento de nuvens computacionais orientadas por SLAs, aplicando REST (*REpresentational State Transfer)* APIs. Por meio desta API a integração com as plataformas, aplicações e infraestruturas atuais de nuvem é facilitada. O gerenciamento proposto consiste na negociação do serviço, entrega do serviço, monitoração e aplicação de ações corretivas em caso de não atendimento ao SLA definido. No processo de monitoramento também é possível solicitar a mudança de SLA, caso seja possível o suporte por parte do provedor. No caso das ações corretivas as mesmas também podem ser aplicadas na forma de sanções financeiras, ou seja, o provedor fornece desconto por não atender ao SLA acordado. Este trabalho é enquadrado na Fase 2, pois engloba a entrega do serviço, e Fase 3 efetuando a monitoração e aplicação de ações corretiva. Também pode ser enquadrado na Fase 4 pois permite aplicar sanções;

- **Artigo K -** ***Quantitative Reasoning about Cloud Security Using Service Level Agreement*** **- (LUNA, 2015).**

  Neste trabalho são apresentadas duas técnicas para efetuar uma avaliação quantitativa e análise do SLA de segurança com base nos níveis de segurança fornecidos pelo provedor da nuvem. As técnicas QPT (*Quantitative Policy Trees*) e QHP (*Quantitative Hierarchical Process*) são empregadas para quantificar e agregar os níveis e segurança providos pelos diferentes elementos que compõe um SLA de segurança. Desta forma possibilita uma avaliação mais acurada quantitativamente dos níveis de segurança providos pela nuvem com base no SLA de segurança definido. Este trabalho enquadra-se na Fase 1, pois, trata explicitamente da avaliação do parâmetros definidos SLA de segurança. Também pode ser aplicado para avaliar a oferta de serviços por parte do provedor, comparando quantitativamente as ofertas dos SLAs de segurança;

- **Artigo L -** ***Per-Service Security SLA: a New Model for Security Management in Clouds*** **- (CASOLA, 2016b).**

  Neste trabalho é apresentado um arcabouço que habilita a adoção do SLA de segurança específico para cada serviço. Assim, o usuário pode especificar quais medidas do SLA de segurança oferecido pelo provedor da nuvem quer aplicar para os serviços de sua instância. Desta forma, é possível estipular um SLA de segurança distinto para cada instância requisitada pelo usuário. O arcabouço contempla a definição dos termos do SLA de segurança, gerenciamento dos recursos necessários para atender o SLA definido e monitoração da execução do SLA contratado. Este trabalho enquadra-se na Fase 1, pois, aborda o processo de definição do SLA de segurança. A Fase 2 efetuando a preparação do ambiente, provisionamento do serviço e respectiva entrega. Também enquadra-se na Fase 3, pois, efetua a monitoração do SLA de segurança especificado para a sua instância;

- **Artigo M -** ***Automatically Enforcing Security SLAs in the Cloud*** **- (CASOLA, 2016a).**

  Este trabalho apresenta um abordagem para o provisionamento ótimo dos recursos computacionais da nuvem com base em requisitos de segurança definidos em um SLA. Para tal, um arcabouço é introduzido para atender a especificação inicial e definição dos parâmetros que vão compor o SLA, aplicar o método para provisionamento do serviço e otimização dos recursos selecionados, bem como efetuar a sua monitoração continua. O foco principal do artigo é método para provisionamento de serviços com suporte do SLA de segurança. Este trabalho enquadra-se principalmente na Fase 2 pois foca no provisionamento do serviço, bem como a sua otimização. Também, enquadra-se a Fase 3 pela monitoração contínua verificando o atendimento aos requisitos definidos, e na Fase 1 por possibilitar a definição do SLA e respectivos parâmeros a serem aplicados aos recursos do ambiente da nuvem;

- **Artigo N -** ***Novel Efficient Techniques for Real-Time Cloud Security Assessment*** **- (MODIC, 2016).**

  Neste trabalho é apresentado um método chamado MIP (*Moving Intervals Process*) para avaliar quantitativamente ou qualitativamente o provedor de serviço com relação as suas ofertas de garantia de segurança. Este método possibilita a avaliação do provedor de serviço com base na qualidade global de prover recursos de segurança que atendam os requisitos definidos pelo usuário. Este trabalho enquadra-se especificamente na Fase 1 pois foca na avaliação do provedor com relação aos serviços de segurança prestados, ou seja, na oferta do serviço;

- **Artigo O -** ***A Novel Approach to Manage Cloud Security SLA Incidents*** **- (TRAPERO, 2016).**

  O trabalho apresenta uma proposta de arcabouço para monitorar e garantir que o SLA de segurança definido seja cumprido. O arcabouço contempla a represen-

tação formal do SLA de segurança, que possibilita a especificação dos requisitos de segurança que devem ser atendidos e respectivas restrições, que são utilizadas para monitorar o atendimento ao SLA definido. O processo de monitoração também efetua a ação de correções em caso de alguma violação ou não atendimento de um requisito de SLA definido. Este trabalho enquadra-se na Fase 1, pela definição formal dos parâmetros que são definidos em um SLA de segurança. Também, na Fase 3 se pois efetua o gerenciamento do serviço, realizando a monitoração de violações e aplicando ações corretivas quando necessário;

A Tabela 4 apresenta o assunto específico que o trabalho relacionado esta tratando. Com base nesta tabela obtêm-se a Tabela 5 que apresenta uma visão geral da fase ou fases do ciclo de vida de atuação dos respectivos trabalhos listados. Esta visão permite verificar quais são as fases que possuem mais pesquisa desenvolvida em termos quantitativos e também as fases que possuem menor quantidade de pesquisa desenvolvida. Os indicadores 1, 2 e 3 são utilizados para representar a fase de atuação e relevância do trabalho para a fase.

Tabela 5: Relação entre artigos e fase do ciclo de vida de SLA

Trabalho	Fase 1	Fase 2	Fase 3	Fase 4	Total
A	1		2		2
B		1			1
C			1		1
D	1	2			2
E	1	2			2
F	2	1			2
G	1				1
H	3	2	1		3
I	1				1
J		1	1	2	3
K	1				1
L	1	1	1		3
M	2	1	1		3
N	1				1
O	1		1		2
Total	12	8	7	1	28

Fonte: elaborada pelo autor.

Analisando a Tabela 5, pode-se constatar que a Fase 1 (Definir e especificar o SLA) é a fase que detêm mais trabalhos direcionados (doze trabalhos), nove trabalhos são direcionados especificamente a esta fase e três são direcionados indiretamente. Este direcionamento representa a importância desta fase com relação à questão de SLA de segurança, pois é a base sobre a qual as demais fases do processo ocorrem, ou seja, a definição de parâmetros que vão compor o SLA de segurança. A Fase 2 (Negociar e implantar o SLA) é a segunda fase com mais trabalhos relacionados (oito trabalhos), sendo que cinco são direcionados especificamente para esta fase e três indiretamente. Estes trabalhos estão principalmente relacionados ao provisionamento e entrega do serviço com base no SLA de segurança definido. A Fase 3 (Executar e gerenciar o SLA) é a terceira fase com mais trabalhos relacionados (sete trabalhos), sendo que somente seis são direcionados especificamente para esta fase e um trabalho é indiretamente. Estes trabalhos focam principalmente a monitoração e ações corretivas na gestão do SLA de segurança. Na Fase 4 (Finalizar e bilhetar o SLA) verificou-se um trabalho não relacionado diretamente, este trabalho aborda a questão de sanções em caso de não atendimento ao SLA de segurança definido. Este resultado com relação a Fase4 permite a consideração de três hipóteses: a primeira é que esta fase não atrai o interesse de pesquisadores com seus desafios; a segunda é que trata-se de uma área que já está consolidada, ou seja, bem desenvolvida; a terceira é que se trata de uma área desafiadora e que ainda não está consolidada.

Com relação à análise dos trabalhos, é possível verificar quantas fases os trabalhos foram tratados diretamente ou indiretamente. Somente o trabalho **L** tratou das três fases do ciclo de vida de forma direta, ou seja, foi desenvolvido para atender estas fases. Os trabalhos **H, J, M** trataram de três fases do ciclo de vida do SLA, de forma direta e indireta, enquanto que os trabalhos **A, D, E, F, O** trataram de duas fases do ciclo de vida. Verifica-se que os trabalhos **B, C, G, I, K, N** focaram em uma fase especifica do ciclo de vida. Também, é constatado que nenhum trabalho de forma

direta ou indireta abordou as quatro fases do ciclo de vida do SLA.

4.4 Considerações do Capítulo

Neste capítulo é realizada uma introdução ao histórico da necessidade da aplicação de requisitos de segurança em SLA em diversos contextos ligados a TIC, incluindo a área de computação em nuvem. Pode-se constatar que esta necessidade é recorrente na área de TIC e, também, acompanha os novos paradigmas, como é o caso da computação em nuvem. Para este modelo de computação em nuvem, esta necessidade está sendo apontada como fundamental, pois trata-se de mais uma ferramenta para auxiliar na gestão da entrega dos serviços de um ambiente de computação em nuvem contratados por parte dos consumidores e ofertados pelos provedores de serviços.

Em seguida, efetuou-se um levantamento de quais são as principais questões que envolvem o assunto de SLA de segurança, tanto por parte do provedor como do consumidor. Este levantamento é constituído das práticas atuais dos provedores com relação a esta necessidade, obrigações dos provedores com relação ao tratamento destes requisitos, recomendações do que deve ser especificado em um SLA e benefícios com relação a esta prática. De forma geral, foi possível constatar que a questão da especificação de requisitos de segurança em SLA é pouco aplicada por parte dos provedores e também pouco questionada por parte dos consumidores, neste caso ocasionada pela complexidade da questão ou desconhecimento. Também é verificada a existência de benefícios para o provedor do serviço e consumidor na definição de requisitos de segurança em SLA e como estes podem contribuir para a transição para o modelo computacional de nuvem.

Por fim, é realizada uma análise dos artigos que abordam soluções aos problemas pertinentes a SLA de segurança e relacionados com as fases do ciclos de vida de SLA proposto, possibilitando desta forma identificar as fases do ciclo de vida e sua relação

com pesquisa envolvida na sua respectiva fase. Com base na Figura 11, observa-se que 37% das soluções levantadas abordam a questão de segurança em SLA, que equivale a cento quarenta e quatro artigos. Efetuando uma análise dos artigos, e identificando os que apresentam contribuição específica na área de SLA de segurança, e como também apresentam de forma clara sua contribuição para esta área, obtém-se quinze artigos analisados de forma detalhada. Estes artigos representam $10,42\%$ do total de artigos levantados e, também, permitem inferir que a área de SLA de segurança está em evolução por parte da área acadêmica em função do desenvolvimento contínuos dos ultimo anos, e principalmente pelo volume de trabalho produzidos no ano de 2016. Assim, representando um campo fértil para pesquisa dada a sua grande importância para a área de TIC.

5 PROPOSTA DO ARCABOUÇO SECSLA

A necessidade apresentada pelo mercado, academia e órgãos de padronização com relação à aplicação de requisitos de segurança definidos em um SLA, para os serviços oferecidos pelos provedores de computação em nuvem, é a motivação para a proposta deste arcabouço SecSLA. Este capítulo apresenta os requisitos funcionais e não funcionais do arcabouço proposto, descreve a arquitetura do arcabouço, e o ambiente de nuvem selecionado para a implementação do protótipo do arcabouço SecSLA como prova de conceito.

5.1 Requisitos do Arcabouço

Arcabouços, que suportem requisitos de segurança definidos em um SLA para o contexto de computação em nuvem, necessitam atender requisitos com relação ao próprio arcabouço, bem como, da plataforma de computação em nuvem ao qual será integrado. Nesta seção os Requisitos Funcionais (RF) e Requisitos Não-Funcionais (RNF) desejados para o arcabouço são apresentados:

- RF1: o arcabouço deve fornecer uma interface de interação entre o consumidor e o provedor do serviço de nuvem. A interface deve possibilitar a definição dos níveis de SLA necessários para o fornecimento do serviço, bem como os mecanismos a serem empregados;
- RF2: o arcabouço deve permitir a integração com várias plataformas de compu-

tação em nuvem, não estando restrito a uma plataforma específica;

- RF3: o arcabouço deve tratar os parâmetros de entrada definidos no SLA pelo consumidor. O tratamento desses parâmetros inclui a definição dos mecanismos de segurança que são necessários para fornecer os níveis de SLA especificados;
- RF4: o arcabouço deve definir a ordem de execução dos mecanismos de segurança, atendendo o nível de SLA especificado;
- RF5: o arcabouço deve assegurar ao consumidor o atendimento dos níveis de SLA especificados;
- RF6: o arcabouço deve assegurar o gerenciamento das fases do ciclo de vida de um SLA;
- RF7: o arcabouço deve possibilitar a auditoria das operações realizadas pelo arcabouço e também da nuvem;
- RF8: o arcabouço deve prover contabilização relacionada às suas próprias operações, aos mecanismos executados, aos serviços entregues e às ações executadas na nuvem; e
- RNF1: o arcabouço deve fornecer uma interface de comunicação interna e externa transparente para interagir com qualquer tipo de interface.

Com base nos requisitos especificados, o arcabouço SecSLA foi projetado. Estes requisitos refletem a necessidade levantada com relação ao gerenciamento de SLA de segurança por parte do provedor da nuvem, suportando a fases do ciclo de vida de um SLA.

5.2 Arquitetura do Arcabouço

A arquitetura do arcabouço SecSLA, para entrega de serviços de nuvem com base em requisitos de segurança definidos por meio de um SLA é ilustrada na Figura 18. A arquitetura é constituída de dois grupos de funcionalidades: a) gerenciamento da definição de requisitos de segurança (CIA), efetuada pela Interface SecSLA integrada ao serviço Horizon do OpenStack; e b) gerenciamento do atendimento dos requisitos de segurança definidos no SLA para o ambiente de nuvem hospedeiro, efetuada pelo arcabouço SecSLA em conjunto com os serviços do OpenStack.

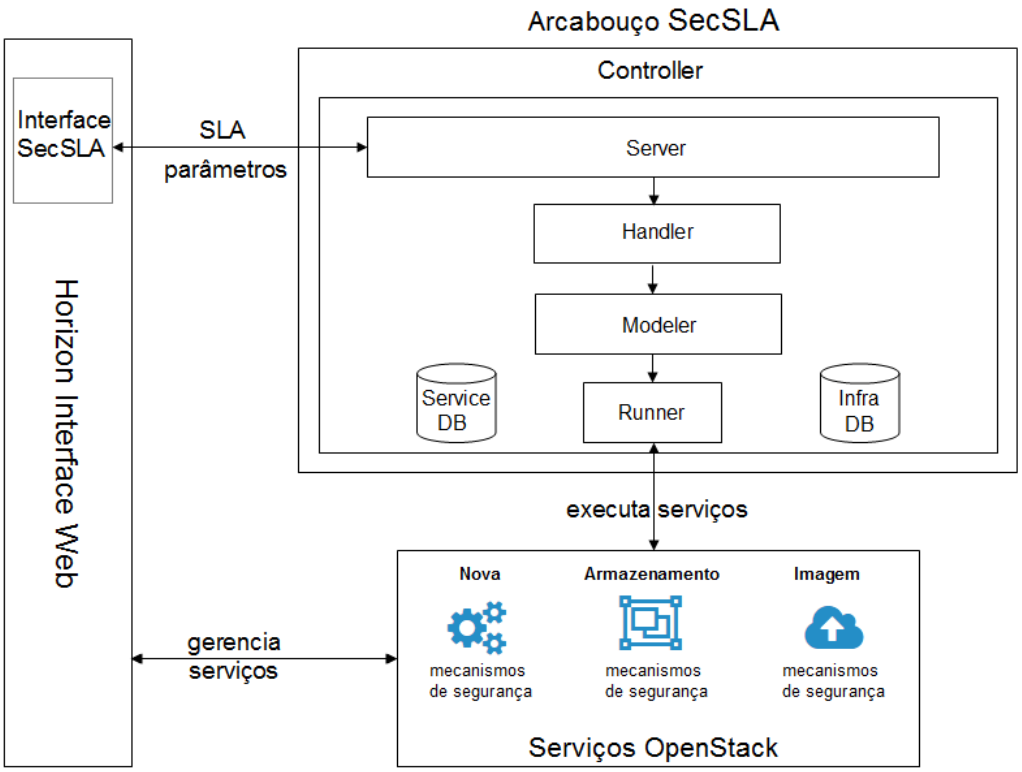

Figura 18: Arquitetura do arcabouço de SLA de segurança (SecSLA).
Fonte: elaborada pelo autor.

A Figura 18 mostra uma visão geral dos módulos do arcabouço SecSLA e a sua integração com os recursos computacionais providos pela solução de computação em nuvem, OpenStack. Também, é apresentado como os módulos estão relacionados entre si, visando facilitar o entendimento do modo de operação do arcabouço como um todo.

5.2.1 Descrição Geral do Arcabouço

Conforme ilustrado na Figura 18, o arcabouço é constituído por módulos que se inter-relacionam. Estes módulos têm suas funcionalidades bem definidas, e são:

- Controller: é responsável pelo gerenciamento e monitoração dos demais módulos que compõem o SecSLA, garantindo que os módulos sejam executados na sequência definida. O resultado do processo de gerenciamento e monitoramento do arcabouço é armazenado no banco de dados (Service DB) para efeitos de conformidade com o SLA definido. Também, é responsável pelo gerenciamento da conexão com os bancos de dados (Service DB e Infra DB) para utilização por parte dos módulos do arcabouço. Além disso, é responsável pelo tratamento da sessão do consumidor autenticado no OpenStack no contexto do arcabouço.

- Server: é responsável pelo estabelecimento da comunicação com o módulo (SecSLA Interface) integrado ao serviço Horizon do OpenStack. Bem como, pela recepção e validação dos parâmetros relacionados à identificação da instância do consumidor no ambiente da nuvem, ou seja, suas credenciais.

- Handler: é responsável pela tradução dos parâmetros de segurança definidos no SLA em comandos do OpenStack, referentes aos serviços a serem instanciados para o usuário. Esta tradução ocorre relacionando os parâmetros de segurança recebidos com os respectivos mecanismos de segurança (SecMecs) e serviços definidos na base de dados (Infra DB), e armazenando esta tradução no banco de dados (Service DB). Estes dados armazenados passam por um controle de integridade (*hash*) durante este processo de armazenamento.

- Modeler: é responsável por aplicar a abordagem de defesa em profundidade para os serviços da nuvem, mecanismos e parâmetros de segurança definidos no SLA por parte do usuário. A aplicação da abordagem possibilita definir o fluxo de

execução dos mecanismos de segurança (SecMecs) em conjunto com os comandos do OpenStack. Os dados gerados pelo módulo também são armazenados no Service DB relacionado ao consumidor. Tais dados, também, passam por um controle de integridade (*hash*) durante o processo de armazenamento.

- Runner: é responsável por gerenciar a execução dos comandos gerados para os devidos serviços do OpenStack, e na sequência estipulada. Também é responsável por receber e tratar as mensagens de retorno emitidas pelos serviços.

- Service DB: é responsável por armazenar as informações relacionadas às operações efetuadas pelo arcabouço, bem como operações realizadas pela nuvem.

- Infra DB: é responsável por armazenar as informações pertinentes à infraestrutura e aos recursos da nuvem. Estas informações são: comandos, serviços e mecanismos de segurança (SecMecs).

O arcabouço SecSLA efetua o gerenciamento do SLA definido atendendo às quatro fases propostas no ciclo de vida do SLA, apresentado no Capítulo 3 e ilustrado pela Figura 5. Para ilustrar o funcionamento do arcabouço, são apresentadas as etapas que compõem a sua utilização na Figura 19.

A etapa (**0**) ilustrada na Figura 19 contempla o processo de identificação e classificação dos mecanismos de segurança relacionados aos serviços providos pela nuvem (OpenStack), bem como os comandos da nuvem (OpenStack) relacionados a sua manipulação. Este processo é realizado pelo provedor da nuvem de forma manual, aplicando a abordagem de defesa em profundidade modelada em árvore proposta e seu resultado é armazenado na base de dados (Infra DB), que será utilizado pelo arcabouço SecSLA. Esta etapa não é contemplada de forma automática pelo arcabouço, mas, é fundamental para seu funcionamento, pois, depende do provedor para efetuar o levantamento de forma manual. A abordagem aplicada para levantamento dos recursos da

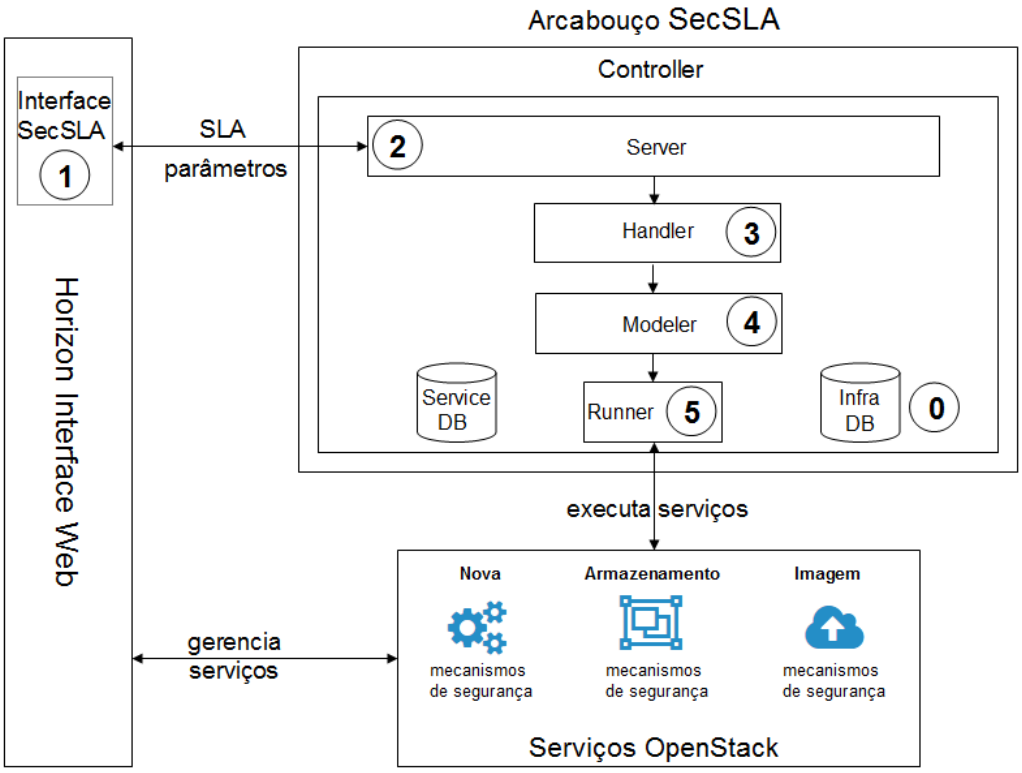

Figura 19: Etapas da Execução do Arcabouço SecSLA.
Fonte: elaborada pelo autor.

nuvem é chamada de defesa em profundidade modelado em árvore, e seu detalhamento será apresentado na descrição detalhada do arcabouço.

Na etapa (1), o consumidor do serviço de nuvem define por meio da interface os mecanismos de segurança e parâmetros que serão aplicados em conjunto com os serviços da nuvem selecionados para sua instância de serviços. Este conjunto de parâmetros definidos para a instância do consumidor é identificada a partir do perfil do próprio consumidor. Os dados do perfil do consumidor são recebidos e verificados na etapa (2) pelo Server, e armazenados no Service DB. Na etapa (3), é feita a tradução do dados do perfil do consumidor em comandos e parâmetros do OpenStack a serem aplicados aos serviços selecionados. Na etapa (4), o Modeler recebe estes comandos e define o fluxo de execução conforme definido pela abordagem de defesa em profundidade modelado em árvore para cada serviço, bem como a etapa do ciclo de vida do SLA do serviço em que o comando será executado, sendo estas informações armazenadas no Service DB. Na etapa (5), os comandos formatados são enviados pelo Runner para os

seus devidos serviços no OpenStack para execução por parte da nuvem. Também, o controle de envios e retornos de execução do arcabouço SecSLA para o OpenStack é realizado, incluindo o registro destas informações de transação no Service DB.

5.2.2 Descrição Detalhada do Arcabouço

Esta seção apresenta detalhes dos componentes da arquitetura do SecSLA. A primeira parte explica a **abordagem de defesa em profundidade modelada em árvore**, que define o processo de identificação e classificação dos mecanismos de segurança dos serviços providos pela nuvem, bem como o fluxo de execução dos mecanismos. Em seguida, é explicado como o consumidor define o SLA de segurança para os serviços desejados. Então, é detalhado como o arcabouço recebe este SLA de segurança e gerencia a entrega dos serviços atendendo aos requisitos definidos. Finalmente, é apresentado como o arcabouço monitora as atividades definidas no SLA, assegurando que os serviços foram entregues pela nuvem conforme o especificado pelo SLA definido pelo consumidor.

5.2.2.1 Integração com a Nuvem

A abordagem de defesa em profundidade consiste na aplicação de múltiplas camadas de proteção ao ambiente, na qual a camada posterior fornece proteção à camada anterior em caso de violação de segurança (KRUTZ; VINES, 2010). Esta abordagem é aplicada para efetuar o levantamento dos serviços e mecanismos de segurança da nuvem (OpenStack) que visam atender os requisitos fundamentais da tríade de segurança (CIA), e são gerenciados pelo arcabouço SecSLA. A aplicação desta abordagem possibilita uma visão clara sobre os mecanismos que podem ser utilizados em cada camada e como estes contribuem para a segurança de todo o ambiente. Esta visão clara dos mecanismos de segurança ofertados pelo provedor da nuvem possibilitam empregar esta abordagem para avaliar a entrega de serviços por parte do provedor com base em

requisitos de segurança definidos em um SLA. Desta forma, possibilitando ao consumidor uma abordagem para avaliar qual provedor atende melhor suas necessidades de segurança. Maiores detalhes sobre como aplicar esta abordagem para avaliar os provedores de serviços estão no Apêndice C (Defesa em Profundidade).

A estrutura em árvore é utilizada para modelar esta abordagem. Este tipo de estrutura possibilita representar as camadas de proteção, bem como a sua relação hierárquica. Assim, é possível a distribuição em camadas dos mecanismos de segurança a serem utilizados pelos serviços durante o processo gerenciado pelo SecSLA. A Figura 20 ilustra a aplicação desta distribuição de mecanismos de segurança em camadas e, também, a representação dos parâmetros de segurança a serem utilizados na entrega do serviço, por meio de quatro etapas de operacionalização.

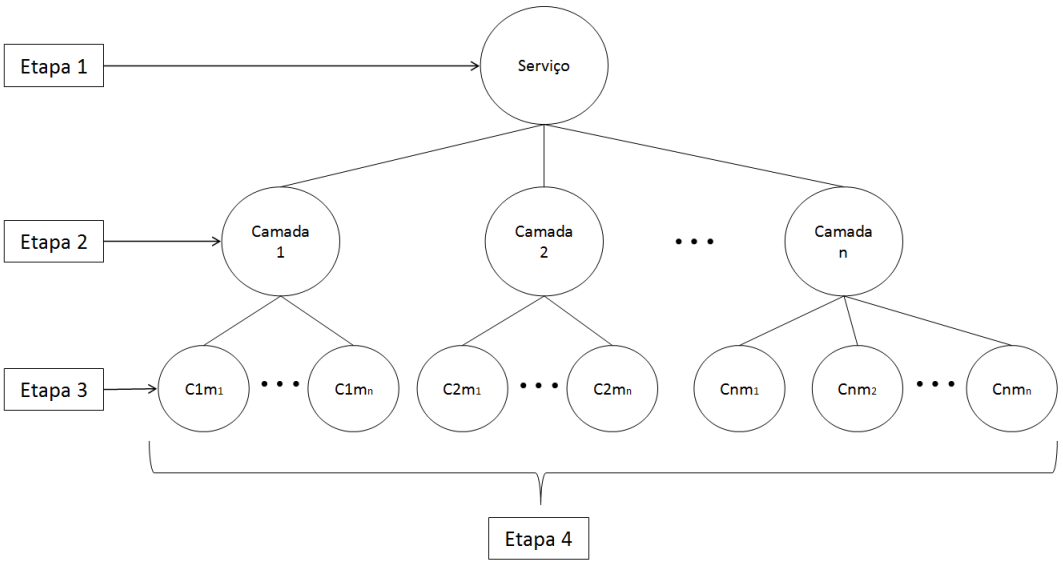

Figura 20: Árvore de defesa em profundidade do serviço.
Fonte: elaborada pelo autor.

Na primeira etapa é definido o serviço da nuvem (por exemplo: máquina virtual, imagens, armazenamento, etc.) que será modelado em árvore e o atributo de segurança relacionado à confidencialidade, integridade ou disponibilidade. Na segunda etapa, são identificadas as camadas de defesa com base nas etapas utilizadas pela nuvem para a entrega do serviço. Na terceira etapa, são identificados os mecanismos de segurança providos pelo ambiente de nuvem para cada camada de defesa, identificados

por Cnm_n, no qual Cn representa a camada e m_n o mecanismo aplicado na camada. Na quarta etapa tem-se a definição de quais mecanismos de segurança devem ser aplicados em cada camada. Esta definição consiste na atribuição de 1 (um) para o mecanismo selecionado e que atende o requisito desejado, e 0 (zero) para o mecanismo que não suporta o requisito desejado ou não é selecionado.

Após a realização das quatro etapas, temos uma árvore que contém a identificação dos mecanismos que devem ser aplicados para suportar a entrega segura de serviços. Temos, também, o fluxo de execução dos respectivos mecanismos, seguindo as camadas de proteção que podem ser aplicadas. Esta árvore gerada consiste na definição de como o SLA de segurança será suportado pelo ambiente de nuvem para atender o estabelecido pelo consumidor. A Figura 21 apresenta um exemplo desta modelagem de defesa em profundidade em árvore, para a definição dos mecanismos que oferecem suporte ao requisito de confidencialidade de um serviço genérico da nuvem.

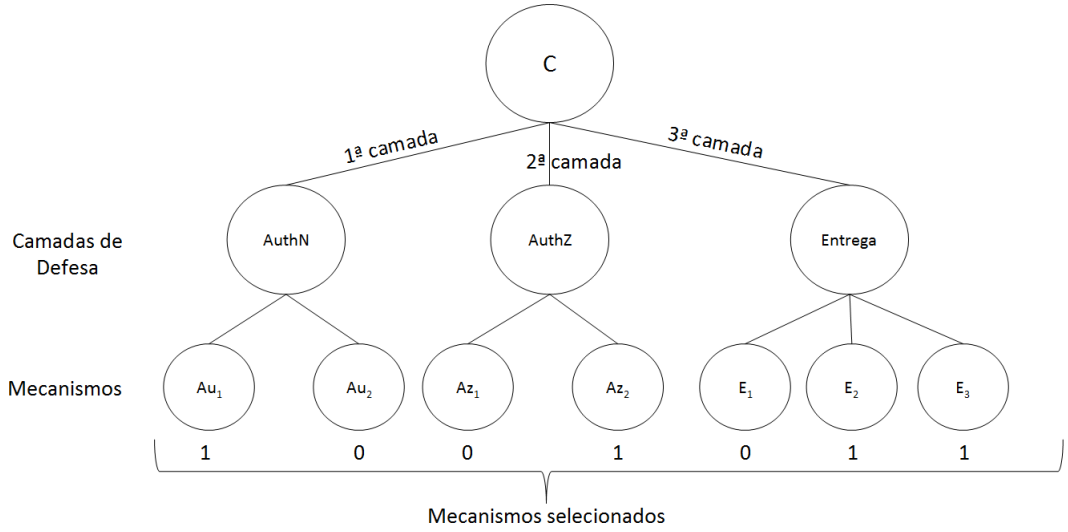

Figura 21: Árvore de defesa em profundidade de um serviço da nuvem.
Fonte: elaborada pelo autor.

No exemplo apresentado na Figura 21, observa-se, como primeira camada de defesa, a autenticação (AuthN) e dois mecanismos de suporte à camada (Au_1 e Au_2). A segunda camada de defesa é constituída pela autorização (AuthZ), e também de dois mecanismos de suporte à camada (Az_1 e Az_2). Na terceira camada é realizada a entrega

do serviço suportada por três mecanismos (E_1, E_2 e E_3). Os mecanismos selecionados para suportar o requisito de confidencialidade para o serviço selecionado foram: o mecanismo Au_1 da primeira camada, o mecanismo Az_2 da segunda camada, e (E_2 e E_3) da terceira camada. Assim, compondo o fluxo de execução dos mecanismos a serem aplicados para a entrega do serviço (S) tem-se: S[AuthN(Au_1),AuthZ(Az_2),E(E_2,E_3)]. Estas informações de serviços, mecanismos e fluxo de execução fazem parte do o perfil de SLA de segurança do consumidor.

Este exemplo ilustra, também, os mecanismos disponibilizados pelo provedor da nuvem que podem ser aplicados ao serviço e atender aos requisitos de segurança (CIA). Os mecanismos podem ser mecanismos concorrentes, que provêm maior ou menor nível de segurança, por exemplo: SHA1 e SHA2 para o caso de controle de integridade. Podem também ser complementares, que corroboram para aumentar o nível de segurança quando aplicados em conjunto, por exemplo: controle de integridade (*Hash*) e controle de confidencialidade (cifragem). Em função do mecanismos de segurança existente para proteção da camada, o mecanismo pode possuir opções de parâmetros, por exemplo se for cifragem, pode-se escolher o algoritmo e tamanho de chave.

O ambiente de computação em nuvem OpenStack foi selecionado para a integração com o arcabouço SecSLA, principalmente por se tratar de um projeto de código aberto e ser uma solução aceita e difundida na comunidade científica e em empresarial. Maiores detalhes sobre os critérios adotados para esta escolha estão disponíveis no Apêndice B (Ambiente de Computação em Nuvem OpenStack). A abordagem de defesa em profundidade apresentada foi aplicada aos serviços providos pelo OpenStack, com o objetivo de identificar as camadas e os mecanismos de segurança disponíveis do ambiente. A Figura 22 ilustra a aplicação desta abordagem para o serviço Nova do OpenStack, responsável pelo gerenciamento de recursos computacionais a serem disponibilizados para os consumidores, na forma de Máquina Virtual (MV).

Observa-se na Figura 22, que aplicando a abordagem para o serviço Nova foram

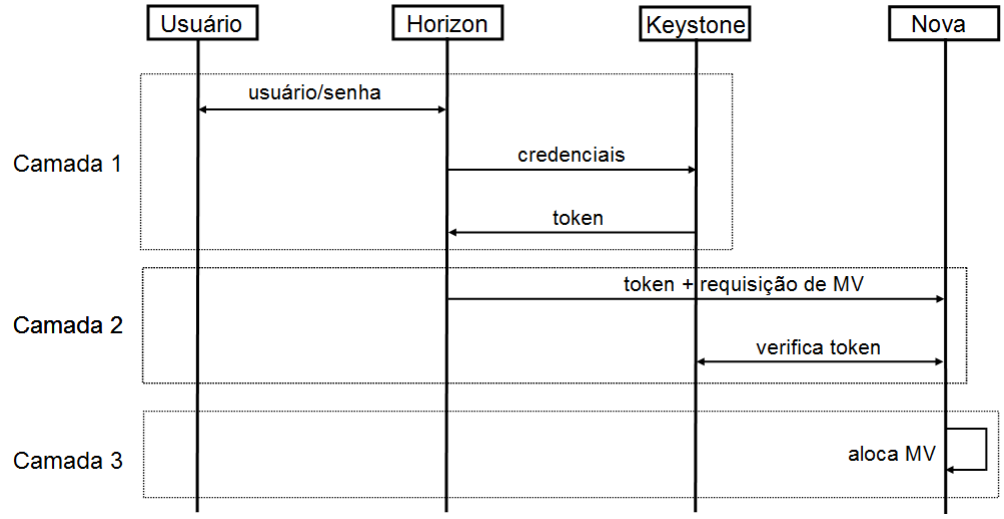

Figura 22: Abordagem de defesa em profundidade aplicada ao serviço Nova.
Fonte: elaborada pelo autor.

identificadas três camadas de proteção: a primeira relacionada à autenticação, a segunda relacionada à autorização e a terceira à entrega do recurso solicitado. Durante este processo, também, foram identificadas as principais funcionalidades e mecanismos de segurança com base na análise do código fonte do OpenStack, bem como em que fase do ciclo de vida do SLA o mesmo pode ser aplicado. Maiores detalhes sobre o gerenciamento da utilização dos mecanismos na respectiva fase do ciclo de vida do SLA são apresentados na sub-seção Gerenciamento do SLA (5.2.2.2).

Durante esta análise foi possível identificar os mecanismos que podem ser aplicados aos serviços do OpenStack, e classificá-los conforme a sua função na tríade de segurança CIA. Também é possível efetuar a análise da granularidade da utilização dos mecanismos definidos no SLA, ou seja, verificar sua abrangência. Foi verificado que os mecanismos podem afetar a configuração da nuvem como um todo, de um grupo de consumidores, de cada consumidor ou de cada ativo (por exemplo: MV, Imagem de SO, etc.). Como um dos requisitos do arcabouço SecSLA é possibilitar que o consumidor defina quais serviços deseja utilizar em conjunto com os mecanismos de segurança para a sua instância da nuvem. Os mecanismos que afetam a nuvem como um todo ou um grupo de consumidores pela sua utilização não foram considerados neste levantamento, ou seja, não permitem que o mecanismos seja aplicado de forma

individual para uma instância de serviços do consumidor, mas, somente para todas as instâncias de consumidores da nuvem. Assim, somente os mecanismos de segurança relacionados aos ativos foram considerados.

Os mecanismos de segurança identificados, sua descrição, sua classificação CIA e fase do ciclo SLA em que pode ser aplicada para os serviços do OpenStack analisado encontram-se na Tabela 6. Com base nas informações apresentadas nesta tabela o banco de dados Infra DB será alimentado pela nuvem, bem como pelos devidos comandos do ambiente para executar esta ações. Este conjunto representa as possíveis opções que o consumidor possuí para definir seu SLA de segurança para este ambiente de computação em nuvem.

Tabela 6: Mecanismo de Segurança do OpenStack por Serviço

Serviço	Mecanismo de Segurança	C	I	A	Entrega	Execução	Finalização	Reutilização
Rede (Neutron)	Firewall	*	*		*			*
	IPSec	*	*		*			*
Imagem (Glance)	Hash		*		*	*	*	*
Armazenamento em Bloco (Cinder)	Cifrar Instância	*			*	*		*
	Cifrar Volume	*			*			*
Armazenamento de Objetos (Swift)	Cifrar	*			*			*

Fonte: elaborada pelo autor.

Constata-se que existem poucas funcionalidades de segurança providas pelo OpenStack, versão Kilo de 2015 (RELEASES, 2016), para os principais serviços por ela disponibilizados para os consumidores. Para um dos principais serviços da nuvem o Nova que é responsável por gerenciar os recursos computacionais da nuvem e instâncias de máquinas virtuais não há um mecanismos que corrobore com a segurança em sua utilização. Além disso, a utilização destas funcionalidades pode ser feita somente pela interface de linha de comando do OpenStack, de forma manual, o que aumenta a complexidade para sua utilização por parte dos consumidores. Este aumento de funcionalidades e parâmetros é importante para o consumidor, pois fornece mais opções, como por exemplo, algoritmos diferentes de cifragem e estes com tamanho de chaves variável. Este exemplo comprova as necessidades levantadas com relação às questões de segurança para o ambiente de computação em nuvem, e também de mecanismos automatizados para sua utilização por parte do consumidor de forma simples e geren-

ciada pelo ambiente de nuvem.

5.2.2.2 Gerenciamento do SLA

Por meio da interface padrão de gerenciamento do OpenStack (Horizon), o consumidor efetua o gerenciamento de sua instância na nuvem. Para possibilitar a integração do OpenStack com o arcabouço SecSLA, a interface Horizon foi modificada, ou seja, criada mais uma opção no menu, possibilitando definir e especificar o SLA de segurança para sua instância, e vincular este SLA a sua instância. Caso o consumidor não deseje especificar um SLA de segurança para sua instância, o fluxo de funcionamento do OpenStack no gerenciamento dos serviços da instância não é afetado. Para a utilização do arcabouço SecSLA, duas etapas de definição são necessárias:

- Gerenciar perfil de SLA: esta funcionalidade foi estendida na interface Horizon, para possibilitar o gerenciamento do perfil de SLA de segurança do consumidor. Este atividade deve ser a primeira etapa do consumidor no processo de utilização do arcabouço SecSLA, e consiste em definir os serviços, mecanismos de segurança e parâmetros dos mecanismos conforme Tabela 6. Também, é definido em que estágio do ciclo de vida do SLA serão aplicados os mecanismos definidos no SLA: no início, em conjunto com a entrega dos serviços, durante o uso do serviço, termino da utilização do serviço ou reutilização de uma instância que possui SLA especificado. Assim que o consumidor definir estas opções e atribuir um nome para o perfil SLA, e solicitar sua criação, estas informações são enviadas para o arcabouço SecSLA para armazenamento; e

- Vincular o perfil a uma instância: esta funcionalidade também foi estendida na interface Horizon, possibilitando que o consumidor escolha a instância desejada e vincule o perfil SLA que deseja aplicar quando esta instância for entregue para ser utilizada pelo consumidor por parte do orquestrador do OpenStack. Assim

que o consumidor fizer esta vinculação estas informações são enviadas para o arcabouço SecSLA para armazenamento.

O diagrama de sequência ilustrado na Figura 23 apresenta esta interação entre o consumidor, o Horizon e o arcabouço SecSLA para a definição do SLA e vinculação com uma instância do consumidor. Este diagrama esta ilustrado na Figura 23.

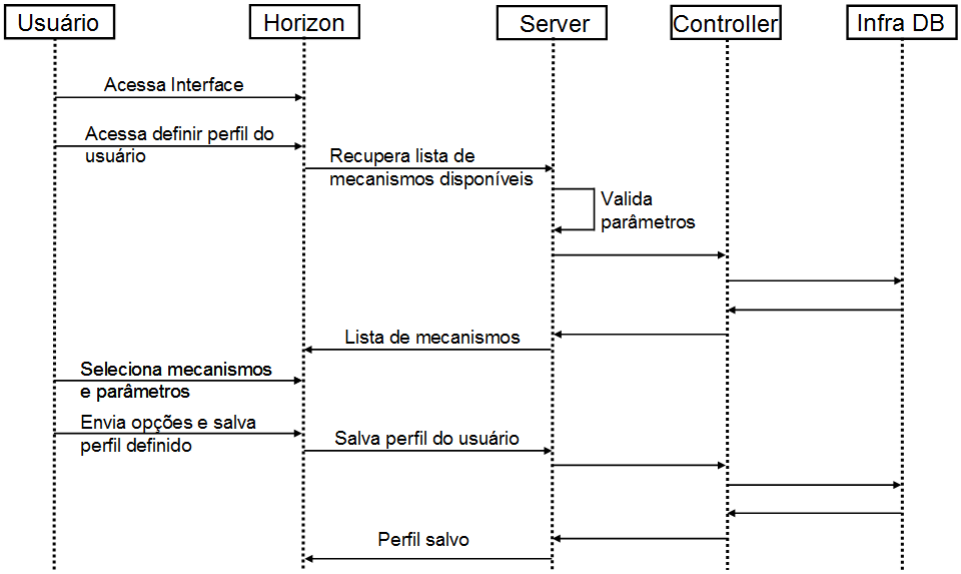

Figura 23: Diagrama de sequência de definição do SLA de segurança.
Fonte: elaborada pelo autor.

Estas informações são enviadas para o arcabouço SecSLA e utilizadas para gerencia o SLA de segurança definido pelo consumidor para a sua instância durante as fases indicadas. Desta forma, como os serviços do OpenStack são gerenciados em conjunto com o SLA de segurança, o arcabouço passa a gerenciar e monitorar o fluxo de aplicação dos mecanismos de segurança em conjunto com a entrega do serviços. O OpenStack continua a enviar dados sobre a instância para o Horizon, dados relativos as atividades extras introduzidas pelo arcabouço são coletadas e armazenadas pelo próprio arcabouço.

O gerenciamento do atendimento ao perfil SLA do consumidor definido em conjunto com o serviços de nuvem é efetuado pelo arcabouço SecSLA em quatro etapas possíveis de operação da nuvem, isso em função do tipo de mecanismo selecionado.

A primeira etapa de operação ocorre durante a entrega do serviço pela primeira vez ao consumidor, este processo está ilustrado pela Figura 24. Para facilitar o entendimento dos passos que compõem o processo e funcionamento do arcabouço SecSLA nesta primeira etapa, vamos considerar o cenário em que o consumidor requisita uma máquina virtual (MV) e uma imagem de SO para ser fornecida pela nuvem, e define o mecanismo de segurança Hash a ser aplicado nesta etapa, estas informações estão armazenadas no perfil SLA do consumidor no arcabouço SecSLA.

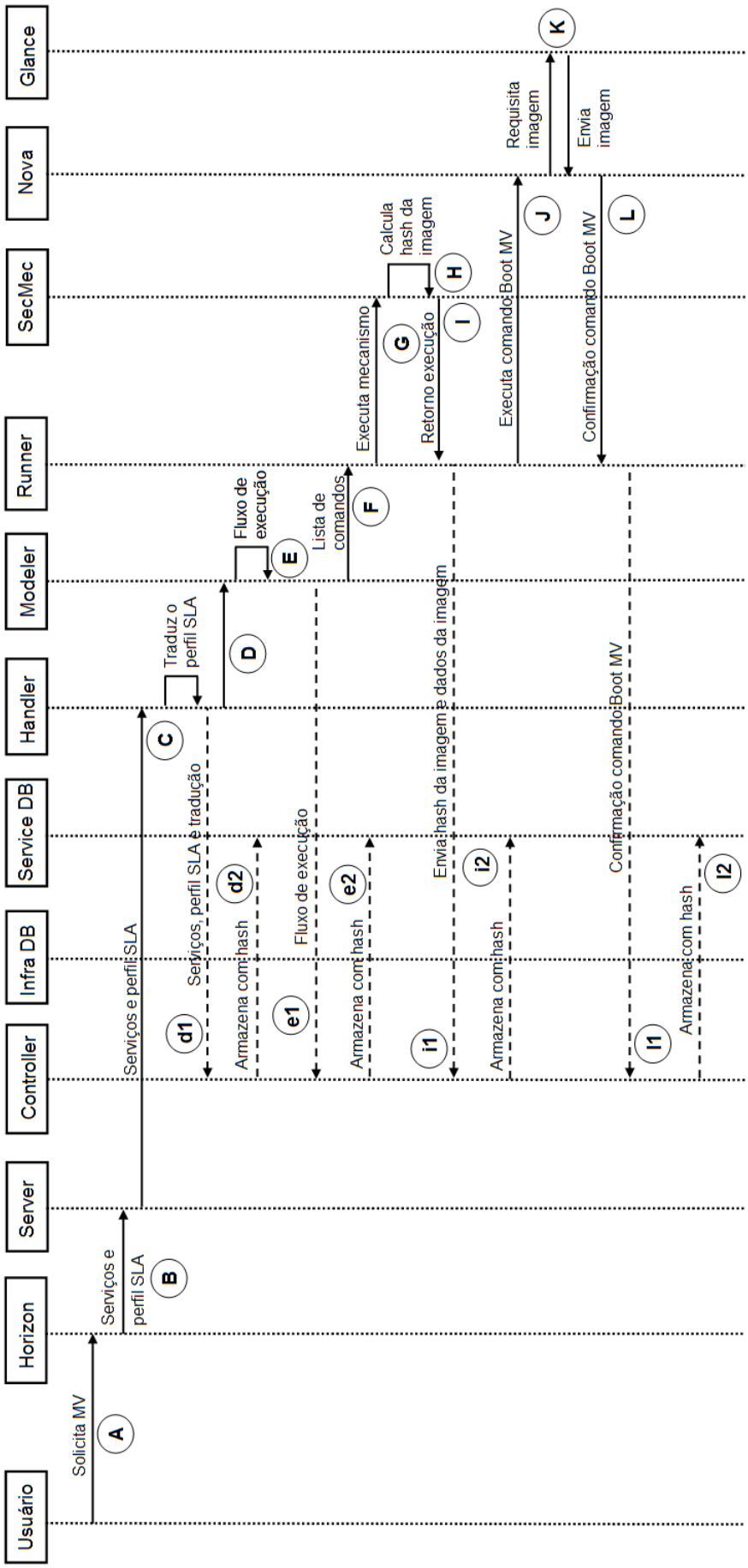

Figura 24: Solicitação de MV utilizando mecanismos de segurança para a imagem de SO.
Fonte: elaborada pelo autor.

No processo ilustrado pela Figura 24 é apresentado o fluxo para assegurar que o mecanismo de segurança definido será aplicado em conjunto com os serviços solicitados pelo consumidor, e na etapa especificada. Este fluxo é constituído pelos passos:

- Passo (A): efetuada a definição do perfil SLA e vinculada a instância do consumidor, é requisita a entrega do serviço. O Horizon customizado envia os dados definidos no perfil SLA em conjunto com os dados da sessão OpenStack (*token*).

- Passo (B): o módulo Server recebe os dados enviados pelo Horizon e efetua a sua consistência. Os dados referentes ao consumidor, parâmetros do perfil SLA e comandos do OpenStack são validados com o objetivo de evitar que requisições mal formadas seja recebidas.

- Passo (C): o módulo Handler recebe os dados e efetua o mapeamento dos parâmetros do perfil SLA em comandos do OpenStack em função do serviço selecionado. Este mapeamento é realizado consultando a base de dados (Infra DB) que contém os possíveis mecanismos a serem aplicados para o serviço definido e comparando com o que esta requisitado no perfil SLA, assim, somente os comandos pertinentes ao serviço e mecanismos do OpenStack são selecionados.

- Passo (D): o módulo Handler encaminha estes dados ao módulo Modeler e dispara a requisição de armazenamento por parte do módulo Controller em (d1). O módulo Controller recebe os dados da instância do consumidor, dados e identificação do perfil SLA, e comandos OpenStack e armazena no banco de dados (Service DB) e efetua um hash em (d2) . Este hash é realizado para ter um controle de integridade sobre os dados recebidos e processados pelos módulos em questão.

- Passo (E): o módulo Modeler recebe os comandos traduzidos e verifica a sua aplicação consultando o banco de dados (Infra DB) da modelagem seguindo a

abordagem em profundidade, para assim definir o fluxo de execução dos mecanismos de segurança em conjunto com os comandos OpenStack. Este dados gerados pela modelagem são encaminhadas para o módulo Controller em (e1) para seu armazenamento no banco de dados (Service DB) com o respectivo controle de integridade utilizando hash em (e2).

- Passo (F): o Runner recebe a sequência de comandos a serem executados e os executa, estes comandos podem esta relacionados aos mecanismos de segurança (SecMec) ou diretamente as operações dos serviços OpenStack.

- Passo (G): os comandos e parâmetros são encaminhados para o mecanismos de segurança (SecMec) e ativam a sua execução.

- Passo (H): no caso apresentado, a primeira sequência de comandos executada esta relacionada ao SecMec de controle de integridade da imagem de SO que será utilizada pelo consumidor em conjunto com a MV especificada. Ela é executa seguindo os passos definidos no mecanismo.

- Passo (I): o respectivo retorno realizado pela operação do SecMec é recebido e tratado pelo módulo Runner, os dados contendo o hash da imagem, e dados que identifiquem a imagem são enviado para o módulo Controller em (i1) para seu armazenamento no banco de dados (Service DB) com o respectivo controle de integridade utilizando hash em (i2) pelo módulo Runner.

- Passo (J): a segunda sequência de comandos esta relacionada a comandos do OpenStack, estes comandos são enviados utilizando a API do OpenStack para comunicação com os serviços, neste caso o Nova, solicitando a inicialização (boot) da MV.

- Passo (K): neste passo o serviço Nova, requisita a Imagem e vincula a sua utilização a MV para ser inicializada.

- Passo (L): o respectivo retorno realizado pelo comando enviado é recebido e tratado pelo módulo Runner, os dados da confirmação com sucesso da operação são enviados para o módulo Controller em (11) para seu armazenamento no banco de dados (Service DB) com o respectivo controle de integridade utilizando hash em (12) pelo módulo Runner.

Na segunda etapa do processo ilustrado pela Figura 25 de utilização da nuvem em conjunto com o arcabouço SecSLA, é considerado o processo de reutilização de uma instância da nuvem com o perfil SLA já definido, bem como os serviços. Também, considera-se o mesmo cenário apresentado da primeira etapa, MV com controle de integridade de imagem de SO.

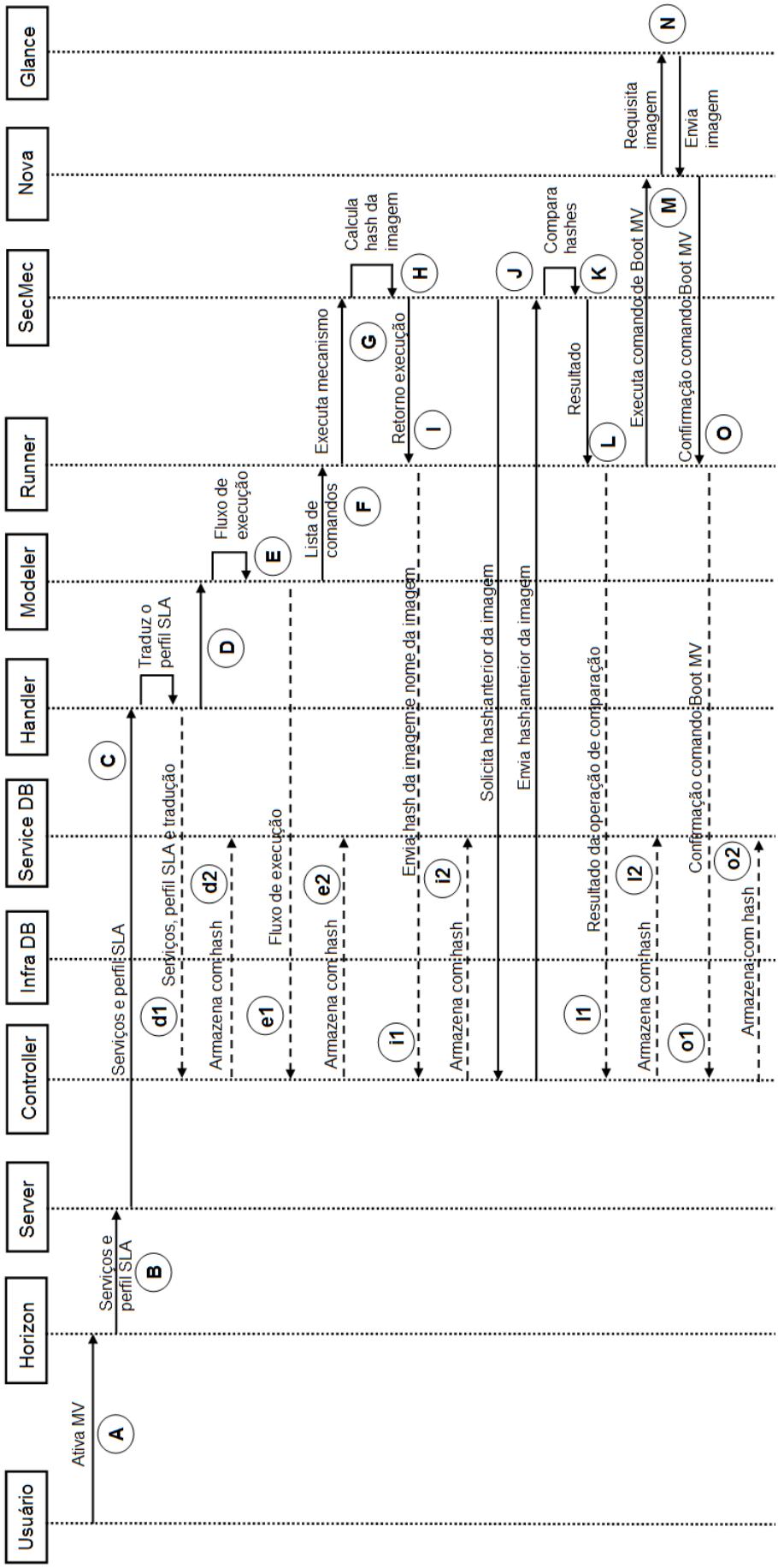

Figura 25: Reutilizar MV com SLA de segurança para a imagem de SO.
Fonte: elaborada pelo autor.

No processo ilustrado pela Figura 25 apresenta-se o fluxo para assegurar que os mecanismos definidos para o consumidor em seu perfil SLA são aplicados durante a reutilização dos recursos requisitados. Este fluxo é constituído pelos passos:

- Passo (A): o consumidor requisita a ativação de sua instância já definida. O Horizon envia os dados definidos no perfil SLA em conjunto com os dados da sessão OpenStack (*token*).
- Passo (B): o módulo Server recebe os dados enviados pelo Horizon e efetua a consistência. Os dados referentes ao consumidor, parâmetros do perfil SLA e comandos do OpenStack são validados, com o objetivo de evitar que requisições mal formadas seja recebidas.
- Passo (C): o módulo Handler recebe os dados consistidos e efetua o mapeamento dos parâmetros do perfil SLA em comandos do OpenStack em função do serviço selecionado. Neste mapeamento é verificada a existência deste perfil SLA na base de dados (Service DB), para posterior verificação de que se trata de um perfil ativo e existente, com base nesta informação a base de dados (Infra DB) é consultada, e o mecanismo de segurança para ser aplicado neste caso de reutilização de serviço é selecionada para ser utilizado nesta sessão.
- Passo (D): o módulo Handler encaminha estes dados ao módulo Modeler e dispara a requisição de armazenamento das informações para o Controller em (d1) com o respectivo controle de integridade em (d2).
- Passo (E): o módulo Modeler recebe os comandos traduzidos e verifica a sua aplicação consultando o banco de dados (Infra DB) e define o fluxo de execução em função dos mecanismos de segurança, bem como os comandos OpenStack. Este dados gerados são encaminhados para armazenamento pelo Controller em (e1) e seu controle de integridade em (e2).

- Passo (F): o módulo Runner recebe a sequência de comandos a serem executados.
- Passo (G): o mecanismo de segurança (SecMec) é executado como os parâmetros necessários.
- Passo (H): o SecMec realiza o controle de integridade da imagem de SO que será utilizada pelo consumidor em conjunto com a MV especificada, calculando seu hash.
- Passo (I): o respectivo retorno é recebido e os dados enviados para armazenamento pelo módulo Controller em (i1) com controle de integridade em (i2).
- Passo (J): o SecMec solicita o hash armazenado no banco de dados (Service DB) para comparação.
- Passo (K): o SecMec compara o hash atual com o recebido pela consulta, para verificar se o mesmo é íntegro.
- Passo (L): o resultado da comparação é encaminhado para o módulo Controller no passo (l1) com controle de integridade em (l2). Havendo divergência no processo de comparação, o processo é cancelado e uma mensagem é gerada para este caso.
- Passo (M): e executado o comando solicitando a inicialização da MV.
- Passo (N): neste passo o serviço Nova, requisita a Imagem e vincula a sua utilização a MV para ser inicializada.
- Passo (O): o retorno da mensagem (N) é recebido e tratado pelo módulo Runner, e tem a solicitação de armazenamento enviada para o módulo Controller em (o1) com controle de integridade em (o2).

Na terceira etapa do processo, ilustrado pela Figura 26, de utilização da nuvem em conjunto com o arcabouço SecSLA, considerar-se o caso de atendimento ao SLA definido de um recurso durante seu processo de utilização, ou seja, enquanto os recursos estão em uso. Este recurso pode ser aplicado para um cenário de utilização contínua de um recurso da nuvem por parte do consumidor, assim a verificação de segurança do ambiente necessita ser realizada durante a utilização do recurso.

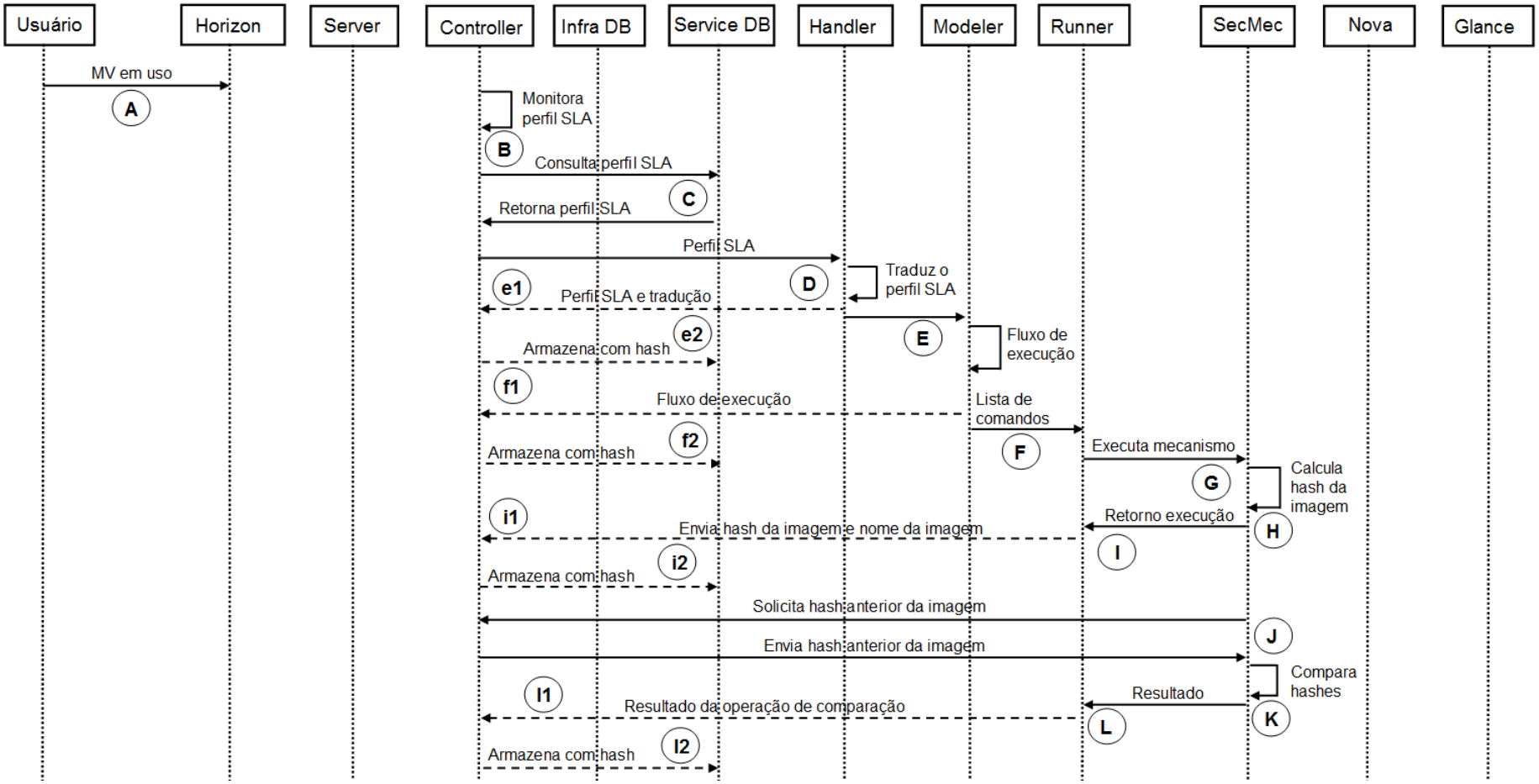

Figura 26: Monitora MV com SLA de segurança definida para a imagem de SO.
Fonte: elaborada pelo autor.

No processo ilustrado pela Figura 26 apresenta-se o fluxo para assegurar que os mecanismos definidos para o consumidor em seu perfil SLA são aplicados durante o uso, em tempo real. Neste caso a periodicidade da verificação é definida no perfil SLA do consumidor. Este fluxo é constituído pelos passos:

- Passo (A): ilustra que a instância definida pelo consumidor está ativa e em uso.
- Passo (B): o módulo Controller tem a função de monitorar e gerenciar os perfis ativos no banco de dados (Service DB), processo indicado no passo (C) que gerenciam este tipo de monitoração de segurança e periodicidade de execução. Este gerenciamento pode ocorrer mantendo uma lista contendo o SecMec a ser utilizado, nome do perfil SLA e periodicidade em que deve ser executado. A informação do perfil SLA é enviado para o módulo Handler, passo (D).
- Passo (E) a Passo (L): nestes passos as operações efetuadas pelos módulos são similares aos diagramas de sequência explicados e ilustrados nas Figura 24 e Figura 25.

Na quarta etapa do processo ilustrado pela Figura 27 de utilização da nuvem em conjunto com o arcabouço SecSLA, considera-se o caso de liberação dos recursos definidos na instância do consumidor, ou seja, quando o consumidor não vai mais utilizá-los. Este processo é aplicado para um cenário de utilização onde o consumidor deseja que após a entrega dos recursos seja feita uma nova verificação de segurança.

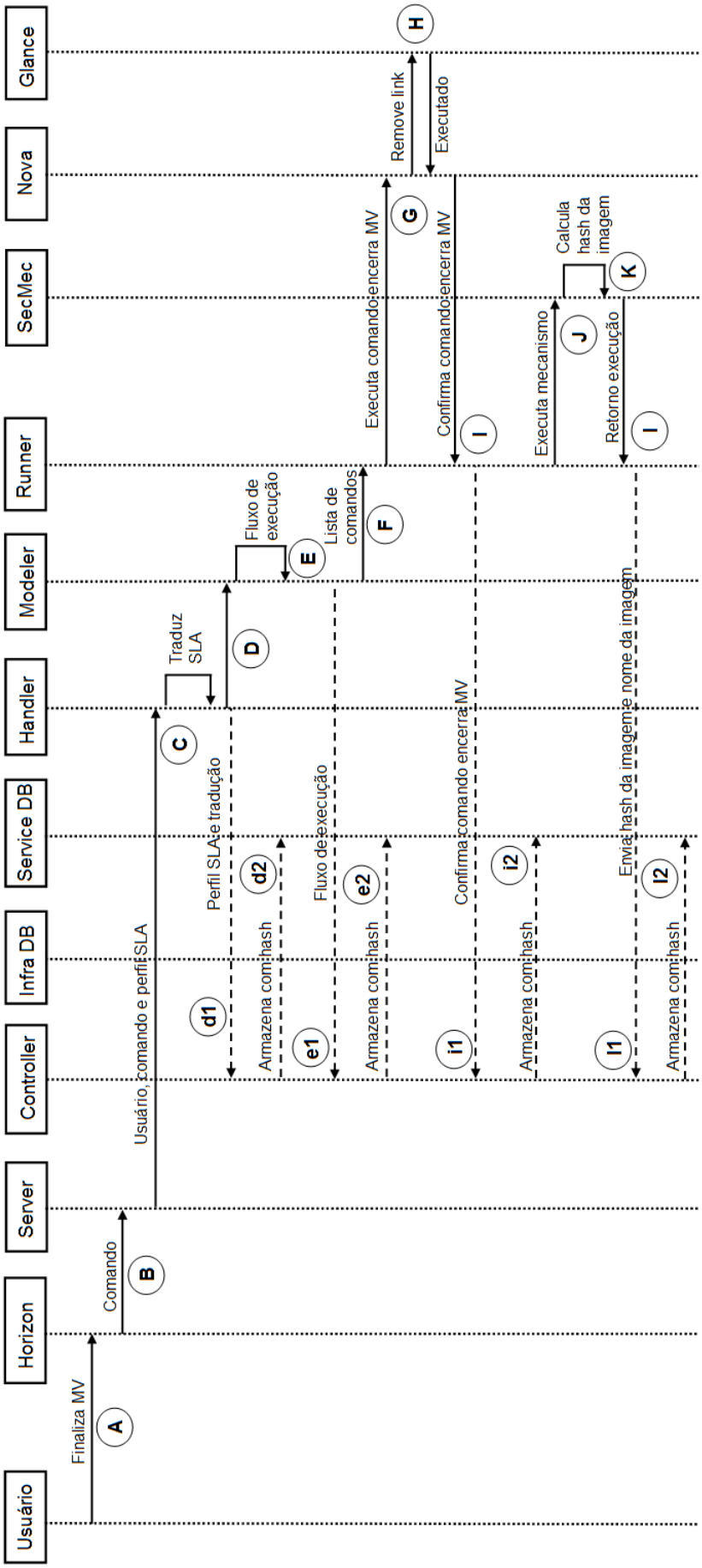

Figura 27: Libera MV com verificação de SLA de segurança para a imagem de SO.
Fonte: elaborada pelo autor.

No processo ilustrado pela Figura 27 é apresentado o fluxo para assegurar que os mecanismos definidos para o consumidor em seu perfil SLA são aplicados na fase de encerramento de uso dos recursos requisitados. Este fluxo é constituído pelos passos:

- Passo (A): o consumidor envia o comando solicitando a finalização de sua instância e liberação dos recursos.
- Passo (B) a Passo (D): as operações efetuadas pelos módulos são similares aos diagramas de sequencia apresentados nas Figuras 25 e 26.
- Passo (E): o módulo Modeler recebe estes dados e especifica o fluxo de execução para atender esta requisição, neste caso, para ser executado após a confirmação de finalização dos recursos por parte da nuvem (Nova), e encaminha este fluxo para o módulo Runner no passo (F), e solicita o armazenamento destas informações com controle de integridade.
- Passo (F) a Passo (L): os passos das operações efetuadas pelos módulos são similares aos diagramas de sequência apresentados. Assim, efetuam o encerramento do serviço, e em seguida calculam a integridade da Imagem de SO utilizada e armazenam a informação com controle de integridade.

Por meio dos quatro modos de operação dos mecanismo de segurança em conjunto com os serviços da nuvem, incluindo a definição do perfil SLA, verifica-se que o arcabouço SecSLA atende aos ciclos de gerencia de um SLA, conforme ilustrado na Figura 5. A Fase 1 é atendida pela capacidade de definir recursos de segurança a serem aplicados a serviços da nuvem. A Fase 2, 3 e 4 são atendidas pelos módulos Handler, Modeler e Runner em conjunto com o mecanismos de segurança definidos para atender a necessidade de cada fase. Assim, tem-se mecanismos para atender a Fase 2 que é implantação dos recursos solicitados. A Fase 3 que é monitorar o serviço, ou seja, verificar se o SLA de segurança está sendo atendido pela nuvem continuamente.

Finalmente na Fase 4, que após a desativação do serviço, é possível assegurar o SLA especificado. Também, todas as operações realizadas pelo arcabouço são armazenadas em banco de dados com controle de integridade, assegurando para o consumidor e provedor a possibilidade de comprovar o atendimento ao SLA.

5.3 Considerações do Capítulo

Neste capítulo foi apresentado o arcabouço SecSLA para prover serviços de computação em nuvem tendo como base requisitos de segurança definidos em um SLA. Este arcabouço foi projetado considerando os requisitos funcionais e não-funcionais especificados na Subseção 5.1. A arquitetura do arcabouço é composta de módulos funcionais que suportam: o ambiente cliente, constituído pela interface agregada ao Horizon, utilizada para definição dos requisitos de SLA de segurança para a instância do consumidor; e o ambiente de gerenciamento do arcabouço SecSLA, que compreende os módulos para atender os requisitos definidos no SLA e assegurar que tais requisitos foram atendidos pelo ambiente de nuvem.

Apresenta-se a descrição geral dos módulos do arcabouço e como os mesmos são utilizados em conjunto com mecanismos e serviços da nuvem. Na descrição detalhada, Subseção 5.2.2 foi apresentada a aplicação do modelo de defesa em profundidade modelado em árvore como abordagem para efetuar o mapeamento das etapas de entrega dos serviços em camada, mecanismos de segurança aplicados na camada e fluxo correto de execução destes mecanismos. Esta estrutura também é a base para a orquestração dos mecanismos de segurança definidos no SLA a serem empregados na entrega de serviços e servido de suporte para os módulos do arcabouço, provendo garantida de execução do SLA para o consumidor e provedor. Em suma, trata-se da estrutura principal de suporte ao arcabouço proposto, bem como uma abordagem que pode ser utilizada para outras soluções de computação em nuvem, com relação a levantamento de mecanismos de segurança.

Por fim, foi apresentado diagramas de sequencia ilustrando o gerenciamento do SLA efetuado pelo arcabouço SecSLA para as quatro etapas de operação relacionadas com o gerenciamento do ciclo de vida do SLA. Assim, verifica-se que o arcabouço SecSLA proposto suporta e atende as quatro fases propostas pelo ciclo de vida de um SLA, neste caso o SLA de segurança.

6 AVALIAÇÃO DO ARCABOUÇO

Este capítulo apresenta a avaliação do arcabouço SecSLA. Neste sentido, a avaliação é composta pela apresentação de cenários de uso do arcabouço, análise de ameaças do arcabouço que objetiva verificar o impacto de segurança que o arcabouço representa por si próprio e pela sua integração com o OpenStack, e finalmente a análise de atendimento aos requisitos por parte do arcabouço.

6.1 Cenário de Uso do Arcabouço

O arcabouço SecSLA foi projetado para gerenciar a entrega de mecanismo(s) de segurança em conjunto com o serviço de nuvem desejado, conforme as quatro fases do ciclo de vida do SLA propostas e ilustradas na Figura 5. Desta forma, assegurando o provimento dos serviços de nuvem atendendo os requisitos de segurança especificados, requisitos almejados neste ambiente computacional.

Esta seção exemplifica por meio de um cenário de uso à aplicação do arcabouço SecSLA, este cenário consiste no provimento de recursos computacionais da nuvem aplicando mecanismos de segurança durante o ciclo de vida do SLA. Os recursos computacionais fornecidos compreendem: computação (máquina virtual), armazenamento (espaço para armazenamento de dados) e imagem (imagem de disco da máquina virtual). Em conjunto com estes recursos são aplicados os respectivos mecanismos definidos no perfil de SLA do consumidor durante as quatro fases do ciclo de vida de gerenciamento do SLA. Este cenário de uso foi selecionado por tratar-se de uma das

principais aplicações das nuvem de infraestrutura (IaaS).

6.1.1 Definir e especificar o SLA do cenário de uso

Para o cenário de uso em questão é necessário definir o perfil do SLA do consumidor, esta ação faz parte da primeira fase do gerenciamento do ciclo de vida do SLA. O perfil definido é composto pelos serviços da nuvem e respectivos mecanismos de segurança disponibilizados pelo provedor da nuvem. Com base nesta definição o arcabouço SecSLA efetua o gerenciamento das demais fases do ciclo de vida. Esta definição ocorre por meio da interface gráfica do OpenStack (Horizon), as opções de mecanismos de segurança que podem ser empregados para os serviços selecionados neste cenário de uso encontram-se na Tabela 7.

Tabela 7: Serviços de Nuvem e Mecanismo de Segurança

Serviço	Mecanismo de Segurança	C	I	A	Entrega	Execução	Finaliza
Máquina Virtual	Infraestrutura confiável (TPM[1]-base)	*	*	*	*		*
	Hash (TPM)		*		*		*
	Lacrar (TPM)	*	*		*	*	*
	Hash		*		*		*
	Cifragem	*	*		*		*
Imagem	Hash (TPM)		*		*	*	*
	Hash		*		*	*	*
	Autorização	*			*	*	*
	Redundância			*	*		
Armazenamento	Hash (TPM)		*		*		*
	Hash		*		*		*
	Cifragem	*	*		*	*	*

Fonte: elaborada pelo autor.

Na Tabela 7, além dos serviços e mecanismos de segurança, verifica-se qual requisito de segurança da tríade CIA será objetivado. Também é possível verificar em quais fases do ciclo de vida o mecanismo será empregado. O sombreamento ilustrado na tabela representa a escolha de qual mecanismo de segurança será utilizado pelo arcabouço SecSLA para gerenciamento das fases do ciclo de vida do serviço. Desta forma, para cada serviço do cenário de uso selecionado um mecanismo de segurança será aplicado e seu ciclo gerenciado pelo arcabouço.

6.1.2 Máquina Virtual Segura

A necessidade por recursos computacionais entregues na forma de máquinas virtuais é uma dos principais serviços fornecidos pela computação em nuvem, também consistindo em um dos grandes atrativos e impulsionadores da adoção deste modelo computacional por parte dos consumidores. Assim, os consumidores podem solicitar para os provedores de serviços de nuvem o provimento deste serviço computacional conforme a sua demanda.

Neste cenário de provimento de recursos de máquina virtual, existe a demanda por parte dos consumidores de se assegurar que este recurso atenda requisitos de segurança definidos em um SLA, em especial os serviços providos pela tríade CIA. Neste contexto, a adoção do arcabouço SecSLA propicia que esta demanda por segurança seja fornecida de forma transparente por parte do provedor de serviço de nuvem e durante as fases dos ciclo de vida do serviço, com base na definição dos mecanismos a serem aplicados ao serviço e definidos no perfil do consumidor. Neste caso, o mecanismo selecionado foi lacrar com base nos recursos providos pelo módulo TPM disponível na infraestrutura provida por parte do provedor de serviços de nuvem. O mecanismo lacrar efetua a cifragem dos dados com base na chave RSA relacionada ao módulo TPM, além disso especifica o estado (memória, registradores e arquivos de sistema) na qual a máquina virtual deve se encontrar para possibilitar o processo inverso (decifrar). Este mecanismo permite assegurar a confidencialidade e integridade durante o provimento do recurso máquina virtual, bem como nas etapas: utilização do recurso e processo de liberação do serviço.

Outro benefício apresentado pelo arcabouço SecSLA é com relação as verificações e validações realizadas durante o gerenciamento das fases do ciclo de vida aplicadas ao serviço, estas são armazenadas no banco de dados (Service DB) e podem ser utilizadas por parte do consumidor e provedor como prova que os mecanismos de segurança definidos no SLA foram aplicados aos serviços utilizados. Assim, o arcabouço SecSLA

possibilita a auditoria do processo contratado, assegurando que o SLA foi atendido por parte do provedor do serviço, bem como o contrato firmado entre ambos.

6.1.3 Imagem Segura

O serviço de imagem permite que a nuvem forneça para o consumidor a possibilidade de utilizar em conjunto com a máquina virtual selecionada um sistema operacional já disponibilizado (e.q. Ubuntu, Debian, etc.) pelo provedor ou subir uma imagem personalizada com as suas necessidades ao ambiente de nuvem e utilizá-la. Este serviço é também um dos principais e mais utilizados serviços do ambiente de computação em nuvem.

Neste cenário, a adoção do arcabouço SecSLA permite que a nuvem forneça este serviço levando em consideração premissas de segurança definidas no perfil do consumidor, neste caso aplicando o mecanismo de segurança *hash*, assim, elevando o nível de segurança com relação a integridade da imagem utilizada. Esta imagem pode ser a disponibilizada pelo provedor ou personalizada pelo consumidor, assim, assegura-se que a mesma imagem seja utilizado em conjunto com a máquina virtual e não uma imagem corrompida ou alterada.

A utilização destes serviços também possibilitam assegurar que o SLA foi atendido conforme especificado pelo consumidor, em função das informações que são armazenadas pelo arcabouço. Além disso, possibilita utilizar estas informações para efeitos de auditoria.

6.1.4 Volume Cifrado

No cenário de serviços de computação em nuvem, a necessidade de armazenar dados por parte das aplicações e consumidores é uma demanda crescente, bem como compartilhá-los. Sendo assim, o provimento deste tipo de serviço por parte dos provedores é uma das principais aplicações deste modelo computacional.

Neste contexto, a adoção do arcabouço SecSLA permite que o provimento deste serviço possa ser efetuado atendendo premissas de segurança definidas no perfil do consumidor (neste caso, a cifragem do volume onde os dados serão armazenados) e assim elevar o nível de segurança (confidencialidade e integridade) no tratamento dos dados dos consumidores por parte da nuvem. Também, durante a utilização do serviço por parte da aplicação ou consumidor é efetuada a verificação se o mecanismo de segurança continua a ser aplicado ao volume de dados. Esta verificação pode ocorrer por demanda do consumidor ou aplicação a qualquer momento, ou em períodos de tempo definidos no perfil do consumidor. Finalmente, na liberação do serviço efetua-se uma verificação se o serviço continua atendendo as premissas de segurança definidas. Este serviço também utiliza as informações armazenadas para assegurar que o SLA foi atendido conforme especificado no perfil o consumidor. Bem como, possibilita utilizar estas informações para efeitos de auditoria.

6.2 Análise de Ameaças do Arcabouço

Com o objetivo de verificar os impactos de segurança que o arcabouço proposto pode apresentar por si próprio, bem como, pela sua integração com o OpenStack para o ambiente de computação em nuvem, o método de análise de ameaças foi utilizado. Este método foi desenvolvido para auxiliar no desenvolvimento de uma especificação segura de um sistema e mitigar suas potenciais ameaças (SWIDERSKI; SNYDER, 2004)(SHOSTACK, 2014).

A aplicação do método de análise de ameaças não é empregada para o arcabouço do OpenStack, pois, dentro do contexto do projeto OpenStack, o grupo de segurança esta aplicando o método ao arcabouço. O grupo já aplicou o método para levantar as ameaças do módulo de gerenciamento de identidade e controle de acesso (Keystone), e encontra-se em estágio inicial a análise do módulo Nova (OSSG, 2016).

O método de análise de ameaças é constituído de três etapas (SWIDERSKI; SNYDER, 2004). A primeira etapa consiste em compreender o ponto de vista do adversário, a segunda na caracterização de segurança do sistema e a terceira em determinar as ameaças. Estas etapas são empregadas na análise do arcabouço proposto e sua integração com o OpenStack.

6.2.1 Etapa 1 - Compreensão do ponto de vista do adversário

Segundo Swiderski e Snyder (2004), uma aplicação não pode ser atacada a menos que o adversário tenha um meio para interagir com ela. Esta premissa norteia o processo de análise de ameaças do arcabouço proposto, bem como, sua integração com o OpenStack.

Com base nesta premissa faz-se necessário definir os adversários do arcabouço e seus respectivos pontos de vista. Devido a integração do arcabouço proposto com o OpenStack, duas classes de adversário são definidas e ilustradas na Figura 28.

- **Externo**: o adversário externo pode explorar as interfaces que provem acesso aos serviços da nuvem. O OpenStack possui duas interfaces para acesso aos seus serviços de forma externa (OPENSTACK, 2016). A interface Web, conhecida pelo componente Horizon que é acessado por meio de um navegador, identificado na Figura 28 por (**A**) e a CLI (*Command Line Interface*) que é acessada por meio de linha de comando, identificado na Figura 28 por (**B**).

- **Interno**: o adversário interno pode explorar as interfaces que provem acesso aos serviços internos da nuvem. No contexto de nuvem temos dois tipos de adversários, um relacionado ao modelo multi-inquilino de operação do ambiente, identificado na Figura 28 por (**C**) e o outro relacionado à operação da nuvem, identificado na Figura 28 por (**D**). O adversário relacionado ao modo multi-inquilino está vinculado ao modo de entrega dos serviços da nuvem (IaaS, PaaS

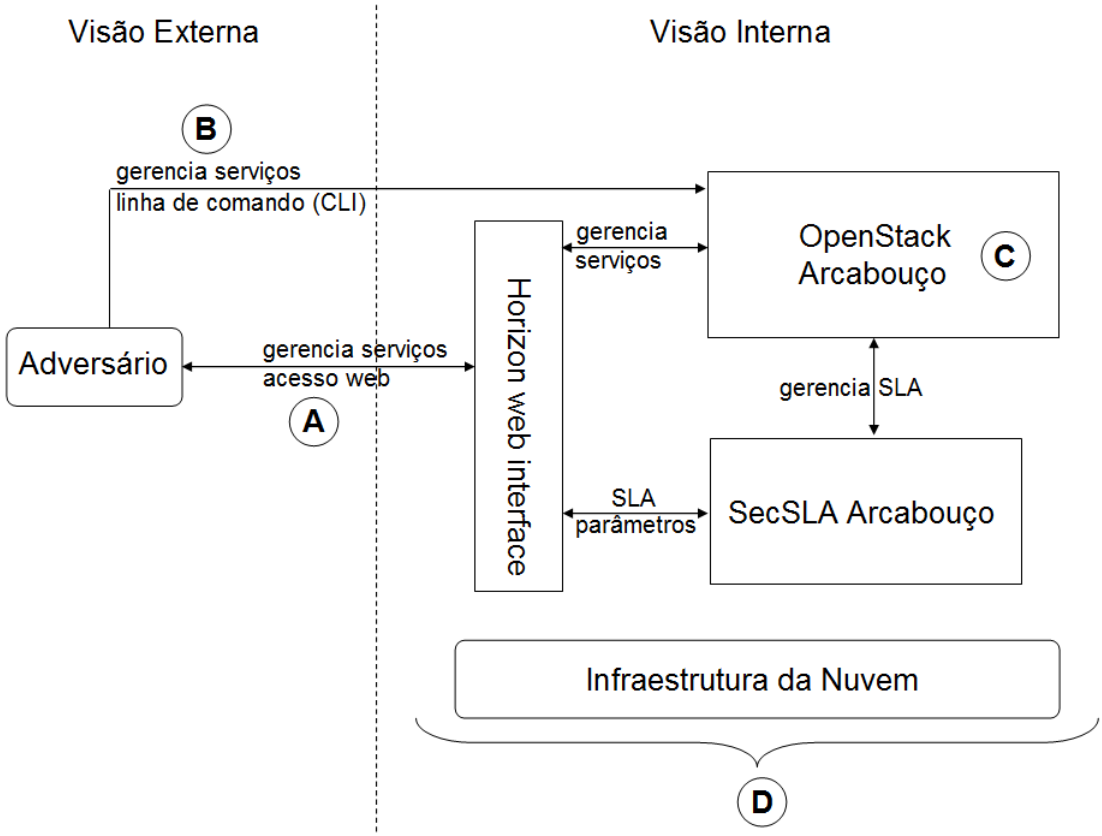

Figura 28: Classes de adversários da nuvem.
Fonte: elaborada pelo autor.

e SaaS). Neste modelo de serviço, o nível de privilégio varia em função to tipo de entrega, no caso de IaaS o privilégio para executar códigos arbitrários é ilimitado. Para o caso de PaaS este privilégio é limitado, em SaaS é extremamente limitado ou nulo. Para este trabalho o modelo de entrega de serviço IaaS será analisado perante o ponto de vista do adversário, ou seja, o adversário é um consumidor da nuvem que pode solicitar os recursos computacionais, e compartilhar os recursos fornecidos pela nuvem com outros consumidores. O adversário relacionado a operação da nuvem engloba os funcionários e contratados que administram o provedor. Como administradores estes consumidores tem acesso técnico aos dados e aplicações gerenciadas pelo provedor. Por meio deste acesso é possível atacar intencionalmente o ambiente, desconfigurando o ambiente, provendo acesso indevidos, prejudicar os demais consumidores, etc. Existem duas abordagens para mitigar estas ameaças causadas por este adversário: aplicando

criptografia ou contratualmente (SHOSTACK, 2014). A abordagem contratual domina o cenário atual, e para a maioria dos riscos envolvidos verifica-se que um contrato entre as partes é suficiente. Este trabalho enquadra-se em propor um arcabouço para tratar o SLA em ambiente de computação em nuvem, definindo e aplicando requisitos de segurança definidos no SLA, onde este SLA é parte deste contrato, ou seja, visa dar suporte a abordagem contratual. As abordagens que empregam criptografia, como cifrar os dados antes de enviá-los à nuvem ou efetuar computações com os dados cifrados na nuvem empregando criptografia homomórfica (NAEHRIG; LAUTER; VAIKUNTANATHAN, 2011), bem como outras, apresentam considerações quando utilizadas em ambiente de computação em nuvem. Tratar destas abordagens e respectivas considerações não faz parte deste trabalho. Neste trabalho as ameaças relacionadas a operação do ambiente não são levadas em consideração e analisadas. Neste trabalho assume-se um provedor que cumpre o contrato assinado pertinente a operação do ambiente, ou seja, que dados e aplicações que estão em posse do provedor não vão sofrer ataques em função deste acesso privilegiado por parte dos administradores.

A compreensão do ponto de vista do adversário com relação ao sistema é uma fase importante do método. Esta compreensão implica em identificar os pontos de acesso do sistema, ativos de interesse e níveis de confiança necessários para acessar os dados.

6.2.1.1 Identificação dos pontos de acesso do sistema

Os pontos de acesso do sistema são locais onde ocorre a transferência de dados ou controle entre o sistema analisado e outros sistemas. Para identificar os pontos de acesso, é necessário verificar como o adversário pode interagir como os componentes do sistema, independentemente do seu nível de privilégio de acesso. Os pontos de acesso representam os locais passíveis de ataque ao sistema por parte do adversário. Como exemplos de pontos de acesso, é possível citar: portas de conexão abertas (*soc-*

kets), interfaces RPC (*Remote Procedure Call*), interface de serviço Web, e dados lidos a partir do sistema de arquivos.

A Figura 29 ilustra a interação entre o OpenStack e o arcabouço proposto (SecSLA), bem como a interação entre o consumidor e os serviços oferecidos pela nuvem. Baseado na ilustração identificam-se os pontos de acesso da visão externa (visão do consumidor) e visão interna (visão da nuvem).

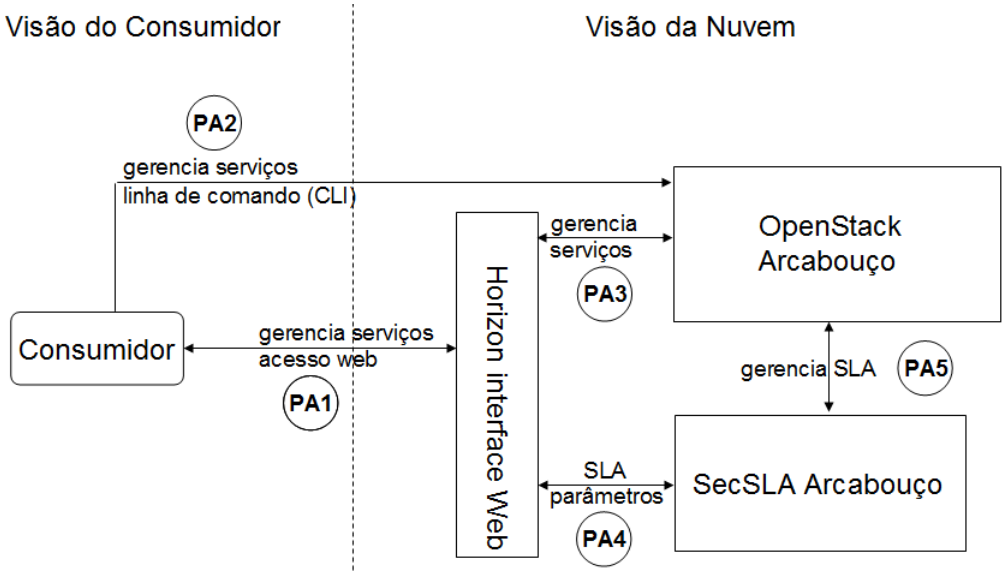

Figura 29: Pontos de acesso do arcabouço.
Fonte: elaborada pelo autor.

Os pontos de acesso identificados por **PA1** e **PA2** são considerados externos, pois, possibilitam que as informações de gerenciamento dos recursos da nuvem trafeguem entre o domínio da nuvem a o mundo externo por meio destas duas interfaces. Estes pontos de acesso ficam disponíveis para conexão por parte da Internet, seja para consumidores da nuvem ou possíveis adversários, ambos são interfaces do OpenStack para acesso ao sistema por parte dos consumidores. O ponto de acesso **PA1** é constituído pela interface padrão Web provida pelo serviço Horizon, responsável pelo gerenciamento dos recursos da nuvem por parte do consumidor ou administrador da nuvem. O ponto de acesso **PA2** é constituído pela interface CLI de gerenciamento de recursos da nuvem por parte do consumidor. O acesso externo ao arcabouço SecSLA é feito exclusivamente por meio da interface Horizon, constituindo assim, a única forma

de interagir com o arcabouço. Não é possível interagir com o arcabouço SecSLA diretamente por meio da interface CLI, pois o arcabouço SecSLA não foi projetado para suportar esta interação. Asim, por meio da CLI é possível acessar diretamente só os serviços do OpenStack.

Os pontos de acesso identificados por (**PA3**), (**PA4**) e (**PA5**) são considerados internos, pois, a comunicação entre estes ocorre por meio de suas interfaces, estas restritas ao domínio do provedor da nuvem. Estes pontos de acesso ficam disponíveis para conexão somente por parte dos componentes internos da nuvem e definidos pelo provedor e aplicações. O ponto de acesso (**PA3**) é composto de um lado pelo Horizon e de outro o acesso ao serviços providos pelo OpenStack, para cada serviço existe uma interface de comunicação definida. O ponto de acesso (**PA4**) é composto pela interface web do arcabouço SecSLA incorporada ao Horizon e o acesso ao módulo do arcabouço SecSLA que irá tratar das definições de mecanismos de segurança a serem empregadas na provisão dos serviços solicitados da nuvem. O ponto de acesso (**PA5**) é composto de um lado pelo arcabouço SecSLA e de outro lado pelo arcabouço OpenStack. Por este ponto de acesso os mecanismos do arcabouço SecSLA comunicam-se com os serviços da nuvem para efetuar a entrega e monitoração dos serviços solicitados, atendendo os requisitos de segurança definidos no SLA.

6.2.1.2 Ativos de interesse

Os ativos de interesse são os recursos que o sistema deve proteger de uso indevido ou não autorizado. Estes recursos podem ser tangíveis como, por exemplo, portas de comunicação (*sockets*) ou abstratos como, por exemplo, tratamento de consistência de dados. Os ativos são a base para as ameaças, pois, é impossível a existência de uma ameaça sem um ativo correspondente, já que estes são os principais alvos das ameaças (SWIDERSKI; SNYDER, 2004).

Considerando os adversário e seus respectivos pontos de vista, é possível identifi-

car os ativos de interesse por parte de um atacante ou que devem ser salvaguardados em caso de uso indevido. A Figura 30 ilustra os ativos de interesse identificados.

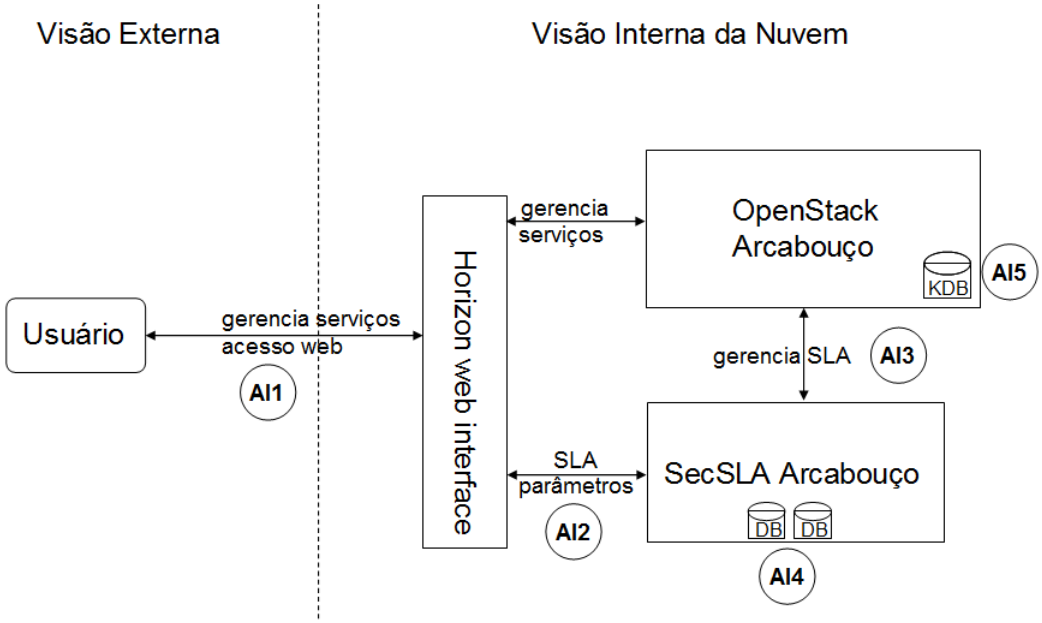

Figura 30: Ativos de interesse do arcabouço.
Fonte: elaborada pelo autor.

Os ativos do tipo porta de comunicação identificados são: a interface web do Horizon, identificada por **AI1**; as portas de comunicação entre o Horizon e o SecSLA, identificadas por **AI2**; e as portas de comunicação entre o SecSLA e serviços do OpenStack, identificadas por **AI3**.

A Figura 30 também ilustra ativos do tipo banco de dados (*Service DB* e *Infra DB*) do arcabouço SecSLA, identificados por **AI4**. Estes ativos podem conter as informações referentes ao gerenciamento do SLA, registro das operações realizadas por parte do OpenStack. O primeiro ativo é responsável pelo armazenamento das informações referentes às operações que devem ser executadas com base no SLA definido, e respectivo controle de execução. O segundo ativo é responsável pelo armazenamento das informações referentes aos recursos providos pela infraestrutura (serviços, mecanismos de segurança e plataforma segura). Também ilustra o ativo do tipo banco de dados, que é referente aos dados mantidos pelo *Keystone*, identificado por **AI5**.

6.2.1.3 Níveis de confiança

Níveis de confiança ou categorias de acesso definem como as entidades externas conhecidas são caracterizadas para o sistemas. Esta caracterização está relacionada com os privilégios que a entidade externa pode ter para, de forma legítima, ter acesso a um ponto de acesso do sistema. Os níveis de confiança são empregados para definir qual entidade externa pode possuir privilégios para acessar um determinado ativo por meio de um ponto de acesso (SWIDERSKI; SNYDER, 2004).

Com base na Figura 29, são identificados os níveis de confiança para a interação entre o arcabouço e as entidades externas. Esta interação ocorre por meio dos pontos de acesso (**PA3**), (**PA4**) e (**PA5**). No ponto de interação (**PA3**) ocorre a comunicação entre os serviços do OpenStack e a sua interface de gerencia Horizon. No ponto de interação (**PA4**) ocorre a comunicação entre o módulo do SecSAL integrado ao Horizon, responsável pelo gerenciamento da definição dos parâmetros de SLA de segurança que são aplicados durante o processo de entrega do serviço, e o módulo no arcabouço SecSLA que armazena estas definições no banco de dados *(Service DB)*, esta operação é realizada empregando as credenciais do consumidor valido da nuvem. Este consumidor válido tem o processo de autenticação realizado pelo OpenStack por meio do ponto de acesso (**PA1**), em termos do arcabouço proposto esta autenticação é suficiente para assegurar que trata-se de um consumidor legítimo que está realizando a operação. Este consumidor também é empregado na solicitação de entrega de recursos da nuvem com os níveis de segurança definidos no SLA. No ponto de interação (**PA5**) é realizado o gerenciamento dos recursos providos pelo OpenStack com base no SLA definido pelo consumidor, esta operação é realizada pelo administrador do arcabouço, bem como garante que a entrega dos recursos solicitados por parte do consumidor ocorram conforme definido no SLA. Este administrador também é responsável por alimentar os ativos *Service DB* e *Infra DB* com os dados da operação realizada pelo consumidor válido do OpenStack. O ponto de acesso (**PA2**) não possui interação com o arcabouço

SecSLA.

6.2.2 Etapa 2 - Caracterização da segurança do sistema

A caracterização de segurança consiste em coletar informações sobre as dependências de segurança consideradas críticas do sistema, bem como o entendimento do funcionamento interno do sistema (SWIDERSKI; SNYDER, 2004). Esta caracterização esta de acordo com as informações para o entendimento da modelagem de ameaças, e consiste em: definir cenários de uso, identificar suposições e dependência, e modelar o sistema.

Este passo do processo de análise de ameças já foi contemplado pela descrição da arquitetura do sistema efetuada no Capítulo 5 e ilustrada pela Figura 18. O cenário de uso foi descrito no Capítulo 6, Seção 6.1 e respectivos subitens.

6.2.3 Etapa 3 - Determinação de ameaças

Esta etapa é composta de duas atividades, sendo considerada uma etapa chave do método (SWIDERSKI; SNYDER, 2004). A primeira atividade consiste em identificar e classificar as ameaças que o arcabouço em análise pode sofrer. A segunda atividade consistem em apresentar como estas ameaças identificadas devem ser mitigadas ou são mitigadas pelo arcabouço proposto.

A identificação de ameaças consiste em analisar os pontos de acesso do sistema identificados na Figura 29 e ativos de interesse identificados na Figura 30. Após a identificação das ameaças a sua respectiva classificação é efetuada empregando a abordagem STRIDE (***S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege*), respectivamente relacionadas com os serviços de segurança (Autenticação, Integridade, Não-Repúdio (irretratabilidade), Confidencialidade, Disponibilidade, Autorização) (SWIDERSKI; SNYDER, 2004)(SHOSTACK, 2014).

Neste levantamento, as duas atividades, identificar e analisar, são realizadas em conjunto para as ameças descritas. Realiza-se também uma análise das ameaças em função da definição dos adversários do arcabouço em externo e interno.

6.2.3.1 Identificação e Análise - Adversário Externo

A relação contendo as ameaças e suas respectivas análises com base no ponto de vista do adversário classificado por externo, é apresentada. Esta relação consiste na ameaça identificada, descrição da ameaça, classificação da ameaça, pontos de acesso e ativos envolvidos pela ameaça, e finalmente a análise do tratamento a ser dado a ameaça identificada.

- Ameaça 1: Captura de Credenciais.
  - Descrição: O adversário pode capturar usuário e senha de um consumidor legítimo da nuvem, empregando por exemplo, um ataque de *phishing*. De posse desta credencial, pode realizar operações que o consumidor legítimo está autorizado. Bem como, realizar ações visando elevar o seu nível de privilégio no ambiente da nuvem.
  - Classificação: Confidencialidade e Autorização são as categorias de ameaça. A confidencialidade, pois, permite acesso a dados de outro consumidor sem a devida autorização. A autorização, pois, o consumidor pode buscar elevar o seu nível de privilégio, afetando as políticas de autorização definidas pela nuvem.
  - Pontos de Acesso: (**PA1**) e (**PA2**), são os pontos de acesso alvos desta ameaça.
  - Ativos: O ativo (**AI5**) é alvo desta ameaça, pois, contém a base de usuários da nuvem e políticas de autorização da nuvem.

  - Análise: Para mitigar esta ameaça, o provedor da nuvem deve empregar no seu ambiente política de senha com alta entropia (e.g., tamanho da senha, diversidade de caracteres a serem utilizados, prazo de validade), autenticação multifator ou Kerberos. O OpenStack suporta estas três alternativas para autenticação externa.

- Ameaça 2: Adivinhar Usuário e Senha.

  - Descrição: O adversário pode tentar adivinhar usuário e senha de um consumidor legítimo da nuvem por tentativa e erro *online* ou empregando por exemplo, técnicas de força bruta ou ataque de dicionário. E realizar ações as quais o consumidor esta autorizado na nuvem, bem como buscar elevar o seu nível de privilégio.
  - Classificação: Confidencialidade e Autorização são as categorias de ameaça. A confidencialidade, pois, permite acesso a dados de outro consumidor sem a devida autorização. A autorização, pois, o consumidor pode buscar elevar o seu nível de privilégio, afetando as políticas de autorização definidas pela nuvem.
  - Pontos de Acesso: (**PA1**) e (**PA2**), são os pontos de acesso alvos desta ameaça.
  - Ativos: O ativo (**AI5**) é alvo desta ameaça, pois, contém a base de usuários da nuvem e políticas de autorização da nuvem.
  - Análise: Para mitigar esta ameaça, o provedor da nuvem deve empregar no seu ambiente política de senha forte, em especial a questão relacionada ao número de tentativas de falha ao informar a senha. O OpenStack tem suporte a estação em sua política de senha forte para autenticação externa.

6.2.3.2 Identificação e Análise - Adversário Interno

A relação contendo as ameaças identificadas e sua respectiva análise com base no ponto de vista do adversário interno é apresentada. Bem como, os demais dados relacionados.

- Ameaça 3: Captura de Credenciais.
  - Descrição: Um adversário pode capturar o usuário e senha de outro consumidor da nuvem por meio de um ataque de escuta do meio de comunicação (*eavesdropping*) entre os serviços da nuvem. Bem como *tokens*, credenciais e códigos de autorização. De posse desta credencial pode realizar ações que o consumidor legítimo estava autorizado a realizar no ambiente. Além de poder personificar o consumidor e buscar elevar seu nível de privilégio no ambiente.
  - Classificação: Confidencialidade e Autorização são as categorias de ameaça. A confidencialidade, pois, permite acesso a dados de outro consumidor sem a devida autorização. A autorização, pois, possibilita ao adversário buscar elevar o seu nível de privilégio, afetando as políticas de autorização definidas.
  - Pontos de Acesso: **PA3**, **PA4** e **PA5**, são os pontos de acesso alvos desta ameaça. Pois, nestes pontos informações trafegam para o arcabouço SecSLA e OpenStack diretamente e indiretamente.
  - Ativos: Os ativos **AI4** e **AI5**, são os envolvidos por esta ameaça, pois, contém a base de usuário e políticas de autorização da nuvem. Também a base de dados do SecSLA onde são armazenados os perfis de SLA definidos para os consumidores.
  - Análise: O OpenStack deve ter mecanismos para revogar usuário/senha, *tokens*, credenciais e códigos de autorização no caso de detecção de com-

prometimento destes dados. Por parte do arcabouço SecSLA, o mesmo deve implementar dupla verificação dos dados recebidos desta natureza, ou seja, fazer uma nova verificação destes dados recebidos antes de realizar alguma atividade no sistema.

- Ameaça 4: Captura de Informações Confidencias no Meio de Comunicação.
  - Descrição: Um adversário pode capturar informações confidenciais por meio de um ataque de escuta do meio de comunicação (*eavesdropping*) entre os serviços da nuvem.
  - Classificação: Confidencialidade é o serviço que podem vir a a ser comprometidos por esta ameaça. Pois, o adversário teria acesso a informações as quais ele não tem acesso.
  - Pontos de Acesso: **PA3**, **PA4** e **PA5**, são os pontos de acesso alvos desta ameaça. Pois, por meio destes pontos de acesso ocorre a troca de informações entre o arcabouço SecSLA e OpenStack, de interesse de um adversário.
  - Ativos: Os ativos **AI4** e **AI5** são os envolvidos nesta ameaça, pois, é para onde estas informações confidenciais são enviadas para armazenamento nas respectivas bases de dados.
  - Análise: O OpenStack deve garantir que as transmissões confidenciais realizadas entre os pontos de acesso são protegidas utilizando mecanismos da camadas de transporte como TSL (*Transport Socket Layer*) e SSL (*Secure Socket Layer*), ou da camada de rede, com o IPSec (*Internet Protocol Security*).

- Ameaça 5: Impersonificação de Informações.
  - Descrição: Com base em *tokens*, credencias e códigos de autorizações adquiridas um adversário pode alterar informações armazenadas nos bancos

de dados do arcabouço SecSLA. Desta forma violando a integridade das informações de gerenciamento e monitoração do SLA armazenadas.

- Classificação: Integridade é o serviço comprometido por esta ameaça, pois, permite ao atacante alterar dados armazenados do consumidor.
- Pontos de Acesso: (**PA4**) e (**PA5**), são os pontos de acesso alvos desta ameaça. Pois, através destes pontos de acesso é fornecido o acesso as bases de dados do SecSLA que armazenam estas informações.
- Ativos: (**AI4**) é o ativo envolvido nesta ameaça. Pois, contém os dado armazenados referente ao gerenciamento e monitoração do SecSLA.
- Análise: O arcabouço SecSLA pode utilizar o mecanismo de *hash* para garantir a integridade das informações armazenadas. Desta forma, as informações armazenadas possuem este controle para o caso de operações não realizadas pelo mecanismo do arcabouço e desta forma identificar possíveis violações.

- Ameaça 6: Impersonificação de Informações e Parâmetros do SLA no Meio de Comunicação.
  - Descrição: Um adversário pode capturar informações e parâmetros definidos pelo consumidor no SLA durante o processo de armazenamento destas informações no banco de dado do arcabouço SecSLA, e alterá-las. Por exemplo, pode informar o nome de outra imagem de sistema operacional a ser utilizada, e esta imagem estar comprometida por algum código malicioso.
  - Classificação: Confidencialidade e Integridade são as categorias de ameaça.
  - Pontos de Acesso: (**PA4**) e (**PA5**), são os pontos de acesso alvos desta ameaça. Pois, é por meio deste pontos que estas informações são encaminha-

das pelos processos para seu respectivo tratamento por parte do arcabouço SecSLA ou OpenStack. O (**PA4**) contém os parâmetros e informações, enquanto o (**PA5**) contém os comandos a serem realizados pela nuvem, bem como o retorno dos mesmos.

  - Ativos: (**AI4**) é o ativo envolvido nesta ameaça. Receber os parâmetros alterados no caminho e armazenar no banco de dados, como se fossem legítimos.
  - Análise: O OpenStack deve garantir que as transmissões realizadas entre os pontos de acesso são protegidas utilizando mecanismos da camadas de transporte como TSL e SSL, ou da camada de rede, com o IPSec.

- Ameaça 7: Impersonificação de Informações por meio de Ataque as bases de dados do SecSLA

  - Descrição: Um adversário pode tentar executar ataque as bases de dados do arcabouço SecSLA empregando a técnica *SQL Injection*, com o objetivo de capturar ou alterar informações referente ao gerenciamento e monitoração do SLA definido.
  - Classificação: Confidencialidade e Integridade são as categorias de ameaça.
  - Pontos de Acesso: (**PA4**) e (**PA5**) são os pontos de acesso alvo desta ameaça. Pois, possibilitam o acesso as bases de dados do arcabouço SecSLA.
  - Ativos: (**AI4**) é o ativo envolvido nesta ameaça, pois, contém as bases de dados de interesse do adversário.
  - Análise: O OpenStack deve garantir que as transmissões realizadas entre os pontos de acesso são protegidas utilizando mecanismos da camadas de transporte como TSL e SSL, ou da camada de rede, com o IPSec. O arcabouço SecSLA possui o mecanismo de *hash* para garantir a integridade das

informações e transações armazenadas.

A Tabela 8 resume a aplicação do método de análise de ameaça no arcabouço SecSLA e sua integração com o OpenStack. Ela é composta pelas ameaças identificadas, sua respectiva análise e classificação, e definição da responsabilidade por mitigar a ameaça.

Tabela 8: Resumo da Análise de Ameaças do Arcabouço

Ameaça	Análise da Ameaça				Mitigar	
	Adversário	Pontos de Acesso	Ativos de Interesse	Classificação	OpenStack	SecSLA
1	Externo	PA1 e PA2	AI5	Confidencialidade e Autorização	*	
2	Externo	PA1 e PA2	AI5	Confidencialidade e Autorização	*	
3	Multi-inquilino	PA3, PA4 e PA5	AI4 e AI5	Confidencialidade e Autorização	*	*
4	Multi-inquilino	PA3, PA4 e PA5	AI4 e AI5	Confidencialidade	*	
5	Multi-inquilino	PA4 e PA5	AI4 e AI5	Integridade		*
6	Multi-inquilino	PA4 e PA5	AI4	Confidencialidade e Integridade	*	
7	Multi-inquilino	PA4 e PA5	AI4	Confidencialidade e Integridade	*	*

Fonte: elaborada pelo autor.

A Tabela 8 apresenta que as ameaças 1 e 2 estão relacionadas ao arcabouço OpenStack diretamente, especificamente ao processo de autenticação de consumidores da nuvem. Apesar de declarar que a análise não contempla o arcabouço OpenStack, é necessário realizar esta análise devido a integração do módulo de definição e especificação de SLA do arcabouço SecSLA com o *dashboard* Horizon, caracterizando-se em uma ameça indireta. Verifica-se conforme a análise efetuada que este módulo do arcabouço não introduz nenhuma ameaça ao serviço do OpenStack ao qual é integrado, mas, este serviço apresenta ameaças aos consumidores do arcabouço SecSLA. Nas ameças com base na visão interna, verifica-se que as ameaças 4 e 6 estão ligadas diretamente a infraestrutura de comunicação do arcabouço OpenStack e o arcabouço SecSLA. Nestes casos a responsabilidade de mitigar as ameaças é exclusivamente da alçada do OpenStack. As ameaças 3 e 7 tem a responsabilidade pelas ações de mitigação compartilhadas entre os arcabouços OpenStack e SecSLA. Já o responsável pela mitigação da ameaça 5 é exclusivamente o arcabouço SecSLA. Neste cenário de

visão interna, é possível verificar a existência de somente uma ameaça relacionada exclusivamente ao arcabouço SecSLA, que pode ter impacto para os serviços do consumidor e não do OpenStack. Com relação as demais ameaças verificou-se que estão relacionadas aos arcabouços OpenStack e SecSLA, e devem ser mitigadas por ambos.

Ao todo, na Tabela 1, foram verificadas três tipos de ameaças: confidencialidade com seis ocorrências, autorização com três ocorrências e integridade com três ocorrências. O arcabouço OpenStack está envolvido em seis ameaças do tipo confidencialidade, três ameaças do tipo autorização e duas ameaças do tipo integridade, totalizando o envolvimento com onze tipos de ameaças em seis ameaças identificadas (1, 2, 3, 4, 6, e 7). O arcabouço SecSLA está envolvido em duas ameaças de confidencialidade, uma de autorização e duas de integridade, totalizando o envolvimento em cinco tipos de ameaças em três ameaças identificadas (3, 5 e 7).

Diante destas informações verifica-se que o arcabouço SecSLA introduz três ameaças, sendo que uma exclusiva de seu ambiente e as demais relacionadas a integração com o arcabouço OpenStack. Já o arcabouço OpenStack introduz seis ameaças, cinco relacionadas a integração com o arcabouço SecSLA e uma relacionada a sua infraestrutura de comunicação. Assim, pode-se constatar que SecSLA introduz um número pequeno de ameaças que podem a vir a comprometer o funcionamento do arcabouço do OpenStack, já a integração com o OpenStack apresenta um número maior de ameaças que podem vir a comprometer o funcionamento adequado do arcabouço SecSLA. Estas ameaças também podem ser consideradas para a integração do arcabouço OpenStack com qualquer outro arcabouço, já que em sua maioria estão relacionadas a infraestrutura de comunicação entre os arcabouços.

6.3 Considerações sobre o Cumprimento de Requisitos

Esta seção tem por objetivo verificar se os requisitos funcionais e não funcionais foram satisfeitos. São descritos cada requisito e informa-se se o mesmo é ou não satisfeito pelo arcabouço SecSLA.

- RF1: o arcabouço deve fornecer uma interface de interação entre o consumidor e o provedor do serviço de nuvem. A interface deve possibilitar a definição dos níveis de SLA necessários para o fornecimento do serviço, bem como os mecanismos a serem empregados.
  - Atendimento ao requisito: Sim.
  - Justificativa: Conforme ilustrado pela Figura 18, tem-se a interface do SecSLA incorporada ao Horizon, para suportar a definição do perfil SLA do consumidor, que contempla os serviços e mecanismos de segurança que devem ser utilizados em conjunto para assegurar um operação na nuvem mais segura.
- RF2: o arcabouço deve permitir a integração com várias plataformas de computação em nuvem, não estando restrito a uma plataforma específica.
  - Atendimento ao requisito: Parcialmente.
  - Justificativa: O arcabouço permite a integração com plataformas de computação em nuvem, esta integração é efetuada por meio do processo de levantamento de recursos para suportar o SLA de segurança de forma manual, empregando a bordagem de modelagem de defesa em profundidade modelada em árvore. No cenário apresentado, a integração foi efetuada com o OpenStack, que possibilita que este tipo de levantamento e mapeamento seja efetuado. Também é possível aplicar a mesma abordagem para efetuar

o levantamento de mecanismos providos por outras soluções de computação em nuvem.

- RF3: o arcabouço deve tratar os parâmetros de entrada definidos no SLA pelo consumidor. O tratamento desses parâmetros inclui a definição dos mecanismos de segurança que são necessários para fornecer os níveis de SLA especificados.
  - Atendimento ao requisito: Sim.
  - Justificativa: O arcabouço conta com o módulo Handler para efetuar o mapeamento dos parâmetros definidos no SLA, e transforma-os nos mecanismos necessários para atender o SLA definido pelo consumidor. O Handler utiliza para isto o resultado do mapeamento de mecanismos de segurança utilizando a abordagem de modelagem de defesa em profundidade.
- RF4: o arcabouço deve definir a ordem de execução dos mecanismos de segurança, atendendo o nível de SLA especificado.
  - Atendimento ao requisito: Sim.
  - Justificativa: O módulo Modeler efetua a definição da ordem correta que os mecanismos devem ser utilizados para atender os requisitos definidos no SLA, este fluxo correto também é resultante do mapeamento de mecanismos de segurança utilizando a abordagem de modelagem de defesa em profundidade.
- RF5: o arcabouço deve assegurar ao consumidor o atendimento dos níveis de SLA especificados.
  - Atendimento ao requisito: Sim.
  - Justificativa: O arcabouço, executa o registro de todas as operações realizadas no banco de dados (Service DB), estas operações servem para assegurar ao consumidor que o que ele definiu no SLA foi realizado pela nuvem.

- RF6: o arcabouço deve assegurar o gerenciamento das fases do ciclo de vida de um SLA.
  - Atendimento ao requisito: Sim.
  - Justificativa: O ciclo de vida de um SLA contém quatro fases: definição, entrega, monitoração e finalização. Por meio dos diagramas de sequencia apresentados na seção Gerenciamento do SLA (Subseção 5.2.2.2), pode-se comprovar que o arcabouço executa o gerenciamento envolvendo o ciclo de vida do SLA definido com requisitos de segurança.
- RF7: o arcabouço deve possibilitar a auditoria das operações realizadas pelo arcabouço e também da nuvem.
  - Atendimento ao requisito: Sim.
  - Justificativa: As informações referentes as operações dos mecanismos de segurança são armazenadas no banco de dados (Service DB) e os possíveis mecanismos e serviços no banco de dados (Infra DB). Estas informações possibilita efetuar a rastreabilidade da execução dos passos definidos no perfil SLA, servindo como prova de auditoria. As informações também são armazenadas com um controle de integridade, o que garante que as informações estão com seu conteúdo intacto e com as informações de data e hora de execução da operação.
- RF8: o arcabouço deve prover contabilização relacionada às suas próprias operações, aos mecanismos executados, aos serviços entregues e às ações executadas na nuvem.
  - Atendimento ao requisito: Parcialmente.
  - Justificativa: Todas as operações e seu respectivos retornos são armazenados no Service DB, estas informações podem ser utilizada para contabilizar

a utilização de recursos da nuvem e do arcabouço, isso de forma manual, pois o arcabouço não efetua esta contabilização de forma automática.

- RNF1: o arcabouço deve fornecer uma interface de comunicação interna e externa transparente para interagir com qualquer tipo de interface.
  - Atendimento ao requisito: Parcialmente.
  - Justificativa: No arcabouço implementado foi previsa somente a interface de comunicação interna, ou seja, entre o arcabouço SecSLA e o OpenStack, para o gerenciamento das atividades definidas no perfil SLA. A possibilidade de acesso externo direto ao arcabouço foi desconsiderada por questões de segurança e necessidade de controles adicionais para atender este acesso.

Com base na análise de requisitos apresentado, é possível verificar que um requisito funcional apresentou atendimento parcial, que não afeta a funcionalidade do arcabouço, mas, sim sua operacionalização por parte do provedor. E verificou-se um requisito não funcional com atendimento parcial, que também não impacta no arcabouço SecSLA. Sendo assim, pode-se afirmar que os requisitos foram satisfeitos com base na descrição detalhada do arcabouço SecSLA.

6.4 Considerações do Capítulo

Neste capítulo foi apresentada a validação do arcabouço SecSLA proposto para gerenciar serviços de computação em nuvem tendo como base requisitos de segurança definidos em um SLA, durante as fases do ciclo de vida do SLA. Por meio de um cenário de uso que envolve a utilização de três serviços do OpenStack em conjunto com três mecanismos de segurança (CIA), foi possível verificar que o arcabouço SecSLA atende as necessidades de gerenciar os serviços de computação em nuvem (OpenStack) com base em requisitos de segurança definidos no SLA. O exemplo apresentado ajuda

a entender a utilização do arcabouço em um cenário real e comum no ambiente de nuvem, bem como, os benefícios que este gerenciamento traz para o consumidor e provedor de ambiente de nuvem. Provendo assim, confidencialidade e integridade dos dados e instância de uso da nuvem ao consumidor.

A análise de segurança foi realizada para o arcabouço proposto, seguindo o método de modelagem de ameaças. Deste modo, foram realizadas três etapas que compreendem a metologia: compreensão do ponto de vista do adversário, caracterização da segurança do sistema e determinação de ameaças do sistema. Com base nestas informações, é possível verificar que o arcabouço possuí ameaças pertinentes ao próprio ambiente e relacionadas a sua integração com o ambiente de nuvem OpenStack, e que soluções para mitigar das ameaças que afetam o funcionamento correto do sistema e sua integração já foram contempladas no próprio projeto dos módulos do arcabouço.

Finalmente, as considerações sobre o cumprimento dos requisitos funcionais e não funcionais especificados para o arcabouço foi efetuada. Verificou-se que os requisitos foram satisfeitos com base na descrição detalhada do funcionamento do arcabouço e cenários de uso apresentados.

7 CONSIDERAÇÕES FINAIS

A solução proposta de "arcabouço para entrega de serviços de computação em nuvem de infraestrutura com base em acordo de nível de serviço de segurança"apresentada nesta tese teve sua avaliação realizada com base na análise de cenários de uso do arcabouço e análise de atendimento de oito requisitos funcionais e um requisito não funcional. Desta análise é possível verificar um requisitos funcional e um requisito não funcional com atendimento parcial, que não afetam o funcionamento do arcabouço. Desta forma, pode-se concluir que a solução apresentada atingiu os objetivos definidos com relação ao gerenciamento de serviços de nuvem de infraestrutura com requisitos específicos de segurança durante as etapas do ciclo de vida de um SLA.

Com o objetivo de verificar a especificação segura do arcabouço SecSLA e mitigar as suas potenciais ameaças relacionadas ao próprio arcabouço, bem como, pela sua integração a um ambiente de nuvem, o método de análise de ameaças foi aplicada nesta proposta. Deste modo, foi possível constatar que as ameaças que comprometem o funcionamento do arcabouço e respectivas integrações já foram mitigadas pelos módulos que contemplam o arcabouço, e pelo atendimento aos requisitos especificados.

Baseado nos objetivos definidos que refletem as necessidades apontadas pelas comunidades acadêmica e científica, de mercado e órgãos de padronização esta tese foi desenvolvida, seguindo as diferentes etapas estipuladas pelo método adotado. As principais contribuições alcançadas neste desenvolvimento foram:

1. Revisão da Literatura e Análise: nesta etapa os Capítulos 2, 3 e 4 fornecem a base

teórica necessária para o desenvolvimento da etapa Projeto e Desenvolvimento.

- Capítulo 2: possibilitou a identificação dos desafios que envolvem a computação em nuvem com relação à segurança, em especial os problemas de SLA, motivando a necessidade de um entendimento mais detalhado dos problemas e soluções para SLA de segurança no contexto a computação em nuvem.
- Capítulo 3: As contribuições deste capítulo são: a) Uma proposta de ciclo de vida consolidando as existentes, auxiliando no entendimento e elucidação das fases que compõe o ciclo de vida de um SLA, bem como as atividades que compõem cada fase. Também possibilita que o consumidor e provedor definam critérios, controles e métricas para o gerenciamento de cada fase, por meio de uma visão holística do processo de gerenciamento de um SLA.; b) Análise quantitativa dos problemas e soluções relacionados a SLA. Esta análise permite o entendimento quantitativo dos principais problemas e soluções neste contexto e, assim, identificar os principais pontos a serem considerados em um SLA, bem como quais são os principais requisitos de segurança que devem fazer parte de um SLA.; c) Apresenta uma taxonomia de SLA atualizada, favorecendo o entendimento das categorias relacionadas. Esta abordagem possibilita uma visão completa dos problemas, e serve como base para que os atores envolvidos na negociação da SLA analisem os requisitos que devem ser tratados em um SLA.
- Capítulo 4: As contribuições deste capítulo são: a) Identificar das práticas, obrigações, recomendações e benefícios que envolvem a questão de tratamento de requisitos de segurança por parte dos provedores. Esta identificação auxilia na compreensão da importância de tratar requisitos de segurança em um SLA e, também, do cenário atual deste assunto com base na visão do provedor de nuvem. Assim, contribuindo para a transparência

destes requisitos e transição para a nuvem.; b) Apresentar o estado da arte com relação aos trabalhos realizados sobre SLA de segurança e sua relação com o ciclo de vida do SLA. Este levantamento possibilita identificar quais fases do ciclo de vida tem soluções propostas, bem como quais tipos de solução foram apresentadas. Desta forma, podemos constatar que não existe até o momento uma solução que contemple o gerenciamento de todas as fases do ciclo de um SLA de segurança.

2. Projeto do Arcabouço: apresenta a principal etapa do método, que consiste no projeto da arquitetura do arcabouço SecSLA atendendo os requisitos advindos da necessidade de gerenciar um SLA de segurança durante seu ciclo de vida para o ambiente de computação em nuvem. O Capítulo 5 apresenta as principais contribuições desta etapa.

    - Capítulo 5: As contribuições deste capítulo são: a) A proposta da abordagem de defesa em profundidade em árvore, que possibilita mapear as etapas para efetuar o gerenciamento de um serviço, bem como os mecanismos empregados por estas etapas e, assim, determinar o fluxo de gerenciamento para o provimento de um serviço em conjunto com os mecanismos de segurança necessários, sistematizando o processo necessário. Esta forma estruturada apresentada pela abordagem proposta possibilita o mapeamento de recursos da nuvem para que possam ser utilizados em um SLA e gerenciados, independentemente de plataforma computacional de nuvem utilizada.; b) A descrição do arcabouço e sua descrição técnica detalhada.

3. Validação: a validação da proposta arcabouço SecSLA esta descrita no Capítulo 6.

    - Capítulo 6: A principal contribuição deste capítulo é com relação a validação do arcabouço proposto no Capítulo 5.

As contribuições desta tese oferecem uma visão mais clara e crítica das questões que envolvem SLA de segurança em ambiente de computação em nuvem. Também permite identificar desafios e oportunidades de pesquisa, necessários para aumentar a transparência dos processos do ambiente de nuvem, e assim corroborar com a sua adoção em maior escala, de forma segura.

7.0.1 Publicações

Esta seção lista as publicações existentes, patentes ou artigos previstos do autor que estão relacionados diretamente ou indiretamente a esta tese. Estes resultados são frutos do envolvimento do autor em projetos de pesquisa nacionais e internacionis, sendo eles: a) FIBRE (*Future Internet Testbeds Experimentation between Brazil and Europe*) relacionada à experimentação em Internet do futuro, e *Science DMZ* voltada à infraestrutura de redes para as aplicações científica.; b) *Credential Management Architecture for Cloud Computing* e *Cloud Security SLA*, ambos voltados para segurança em computação em nuvem, com focos no gerenciamento de credenciais e SLA de segurança respectivamente.; c) *Smart V-WAN Hypervisor for Inter Data Centre Network* e *Energy-Efficiency to Clouds*, ambos relacionados à eficiência energética, respectivamente com foco em Data Center e computação em nuvem.

Como resultado, foram realizadas as seguintes publicações:

- Publicação de Artigos diretamente relacionados ao tema da tese:
  - **Rojas, M. A. T.**; Gonzalez, N.M.; Sbampato, V. F.; Redigolo, F. F.; Carvalho, T. C. M. B.; Ullah, K. W.; Näslund, M.; Ahmed, A. S.; *A Framework to Orchestrate Security SLA Lifecycle in Cloud Computing*. In: CISTI´2016 – 11th Iberian Conference on Information Systems and Technologies. Canaries, Spain, June, 2016.
  - **Rojas, M. A. T.**; Gonzalez, N.M.; Sbampato, V. F.; Redigolo, F. F.; Car-

valho, T. C. M. B.; Nguyen, K. K.; Cheriet, M.; *Inclusion of Security Requirements in SLA Lifecycle Management for Cloud Computing*. In: 2nd International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE 2015). August 24 – 25, 2015.Ottawa, Canada; 2015.

  - **Rojas, M. A. T.**; Gonzalez, N.M.; Sbampato, V. F.; Redigolo, F. F.; Carvalho, T. C. M. B.; Ullah, K. W.; Näslund, M.; Ahmed, A. S.; *Orchestrating the Security SLA Lifecycle in Cloud Computing*. In: Kacprzyk, J. (Ed). Developments and Advances in Intelligent Systems and Applications.Studies in Computational Intelligence: Springer 2016. (submetido)

  - **Rojas, M. A. T.**; Gonzalez, N.M.; Sbampato, V. F.; Redigolo, F. F.; Carvalho, T. C. M. B.; Ullah, K. W.; Näslund, M.; Ahmed, A. S.; *A Framework to Orchestrate Security SLA Lifecycle in Cloud Infrastructure as a Service*. In: IEEE Transactions on Dependable and Secure Computing, November, 2016. (submetido)

  - **Rojas, M. A. T.**; Gonzalez, N.M.; Sbampato, V. F.; Redigolo, F. F.; Carvalho, T. C. M. B.; Ullah, K. W.; Näslund, M.; Ahmed, A. S.; *A Survey of Security SLA issues for Cloud Computing*. In: IEEE Communications Surveys and Tutorials, 2016. (em desenvolvimento)

- Publicação de Artigos, Patentes e Capítulos de Livro relacionados indiretamente à tese:

  - *Network Prediction Driven DVFS*. Patent Application Number: PCT/SE2016/050721. July/2016, Swedish Patent and Registration Office.

  - *Traffic-Driven Datacenter Power Management*. Patent Application Number: PCT/SE2016/050686. July/2016, Swedish Patent and Registration Office.

– Rodrigues, B. B., **Rojas, M. A. T.**, Gonzáles, P. K., Nascimento, V. T., Carvalho, T. C., C. Meirosu. *Green Service Levels in Software Defined Networks*. In: 34th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2016). June, 2016. Salvador Brasil.

– Barros, B. M.; **Rojas, M. A. T.**; Simplicio, M. A.; Carvalho, T. C. M. B.; Redigolo, F. F.; Andrade, E. R.; Magri, D. R. C.; *Applying Software-defined Networks to Cloud Computing*. In: 33nd Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2015). Book Chapter. Vitória/ES: Sociedade Brasileira de Computação, 2015, v. 1, p. 1-57.

– Magri, D. C.; Carvalho, T. C. M. B. C.; Redigolo, F. F.; **Rojas, M. A. T.**; Junior, M.S.; Ciuffo, L. N.; Dias, G. N.; Moura, A. S.; Vetter, F.; *Science DMZ: Support for e-science in Brazil*. In: The 10th IEEE International Conference on e-Science (e-Science Workshop of Works in Progress). São Paulo, Brazil, October, 2014.

– **Rojas, M. A. T.**; UEDA, T.; Carvalho, T. C. M. B. *Modelagem e Verificação de Regras de Segurança em Ambiente OpenFlow com Rede de Petri Colorida*. In: CISTI´2014 - 9th Iberian Conference on Information Systems and Technologies. Barcelona, Spain, June, 2014.

– Miers, C. C.; Junior, M. S.; Carvalho, T. C. M. B.; Koslovski, G.; **Rojas, M. A. T.**; Rodrigues, B.; Iwaya, H. L.; Barros, B. *Análise de Segurança para Soluções de Computação em Nuvem*. In: 32nd Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2014). Book Chapter. May, Florianópolis, Brasil: 2014.

– Carvalho, T. C. M. B.; Redigolo, F. F.; **Rojas, M. A. T.**; Magri, D. C. *DMZ Científica: Desafios e modelos de gerenciamento de aplicações de alto volume de dados no contexto de e-ciência* In: 32nd Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2014). Book

Chapter. May, Florianópolis, Brasil: 2014.

– Schwarz, M. F.; Penteado, R. V. S.; **Rojas, M.A.T.**; Redígolo, F. F.; Carvalho, T. C. M. B.; *Experimentação em SDN/OpenFlow Utilizando o Testbed Emulab/ProtoGENI*. XXXIX Conferencia Latinoamericana de Informática (CLEI), Outubro, Venezuela: 2013.

– Gonzalez, N. M.; **Rojas, M. A. T.**; Silva, M. V. C.; Redigolo, F. F.; Carvalho, T. C. M. B.; Miers, C. C.; Näslund, M.; Ahmed, A. S. *A framework for authentication and authorization credentials in cloud computing*. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13). Melbourne, Australia, July 2013.

– **Rojas, M. A. T.**; Carvalho, T. C. M. B. *Proposta de Mecanismo de Controle de Acesso para o ambiente SDN/OpenFlow*. CISTI'2013 - 8th Iberian Conference on Information Systems and Technologies. Lisbon, Portugal. June, 2013.

– Schwarz, M. F.; **Rojas, M. A. T.**; Miers, C. C.; Redigolo, F. F.; Carvalho, T. C. M. B. *Emulated and Software Defined Networking Convergenc*e. 13th International Symposium of Integrated Network. Belgium, Ghent. May, 2013.

– Gonzalez, N. M. ; Miers C.; Redigolo, F. F. ; **Rojas, M. A. T.**; Carvalho, T. C. M. B. *Segurança nas Nuvens Computacionais: Uma visão dos principais problemas e soluções*. Revista USP, v. 1, p. 27-42, 2013.

– Haidar, F. ; **Rojas, M. A. T.** ; Gonzalez, N. M. ; Redigolo, F. F.; Carvalho, T. C. M. B. *Aplicação de Credenciais para Segurança de Computação em Nuvem e Integração ao OpenStack*. In: IV Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2013), 2013, São Carlos. Anais da IV Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2013),

2013.

– Bueno, W. M.; **Rojas, M. A. T.**; Gonzalez, N. M.; Redigolo, F. F.; Carvalho, T. C. M. B. *Sistema de Gerenciamento de Credenciais para Computação em Nuvem Integrado com OpenStack*. In: IV Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2013), 2013, São Carlos. Anais da IV Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2013), 2013.

7.0.2 Trabalhos Futuros

A área de SLA de segurança no contexto de computação em nuvem, possui um grande potencial para a geração de pesquisas. Com relação à problemática de gerenciamento de SLA de segurança, podem derivar diversos trabalhos futuros relacionados a adição, refinamento ou extensão de funcionalidades do arcabouço, bem como a questão que envolve a integração com a nuvem e seus mecanismos de segurança. Uma relação com as direções para onde este trabalho pode evoluir e trabalhos futuros é apresentada:

- Investigar a integração e descoberta automática de recursos providos pela nuvem para suportar o SLA, como por exemplo: novos mecanismos de segurança, ou novos parâmetros para os mecanismos de segurança existentes. Por exemplo, um novo hardware como o Intel SGX[1] pode ser adicionado ao ambiente da nuvem, este novo recurso pode prover novos mecanismos de segurança;

- Pesquisar e propor um método para alterar o perfil de SLA de forma automática para o arcabouço proposto, no arcabouço só é possível criar e remover um perfil. Para suportar esta alteração é necessário um estudo das características dos mecanismos de segurança e propor um processo que efetue esta troca, assim, um novo SecMec pode ser desenvolvido para atender esta alteração;

[1] https://software.intel.com/en-us/sgx

- Propor um processo de auditoria de conformidade com base nas informações geradas no arcabouço. Esta informação é importante para efeitos de relatório de conformidade exigidos pelas empresas;

- Propor um processo de contabilização das operações de gerenciamento realizadas pelo arcabouço, mecanismos e serviços da nuvem envolvidos para quantificar o consumo de recursos computacionais decorrentes desta necessidade de gerenciamento do SLA e utilização de mecanismos;

- Pesquisar como aumentar a granularidade de mecanismos de segurança para que o modelo de defesa em profundidade seja utilizado em mais camadas, e não somente na camada dos serviços, ou seja, mecanismos para a camada de autenticação, autorização, comunicação. Desta forma aumentar a segurança provida ao consumidor por meio de um SLA, bem como avaliar como as novas tecnologias, como por exemplo, enclaves (Intel SGX), micro segmentação e SDN (*Software-Defined Networking*) podem contribuir para este aumento;

- Pesquisar como expandir a arquitetura do arcabouço para suportar o atributo disponibilidade da tríade CIA;

- Pesquisar como expandir a arquitetura do arcabouço para suportar a inclusão de atributos relacionados a privacidade;

- Expandir o modelo de defesa em profundidade proposto para possibilitar a quantificação do nível de segurança provido pela nuvem em função dos mecanismos de segurança definidos no SLA;

- Pesquisar novos modelos de arquitetura para o arcabouço, visando mitigar a questão do provedor malicioso;

- Pesquisar como mitigar a questão do provedor malicioso com relação ao ambiente de execução do arcabouço SecSLA. Esta abordagem de pesquisa pode ser

empregando novas tecnologias, criptografia ou novos componentes;

- Investigar a aplicação do arcabouço para o cenário de federação de nuvens privadas e/ou híbridas.

REFERÊNCIAS

ABDULLAH, R.; TALIB, A. M. Towards integrating information of service level agreement and resources as a services (raas) for cloud computing environment. In: *Open Systems (ICOS), 2012 IEEE Conference on*. [s.n.], 2012. p. 1–5. Disponível em: <http://dx.doi.org/10.1109/ICOS.2012.6417613>.

AIB, I.; DAHEB, B. Sla driven network management. In: ____. *Management, Control and Evolution of IP Networks*. ISTE, 2010. p. 219–246. ISBN 9780470612118. Disponível em: <http://dx.doi.org/10.1002/9780470612118.ch11>.

BADGER, L. et al. *Roadmap Volume II Release 1.0 (Draft) Useful Information for Cloud Adopter*. Gaithersburg, MD, November 2011. Disponível em: <http://www.nist.gov/itl/cloud/upload/$SP_500_293_volumeII.pdf$>.

BAUDOIN, C. et al. *Public Cloud Service Agreements: What to Expect and What to Negotiate*. [S.l.], March 2013. Disponível em: <http://www.cloud-council.org/publiccloudSLA.pdf>.

BENEDICTIS, A. d. et al. Rest-based sla management for cloud applications. In: *2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*. [S.l.: s.n.], 2015. p. 93–98. ISSN 1524-4547.

BIANCO, P.; LEWIS, G.; MERSON, P. *Service Level Agreements in Service-oriented Architecture Environments*. Carnegie Mellon University, Software Engineering Institute, 2008. (Technical note). Disponível em: <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8615>.

BISHOP, M. A. *Computer Security: Art and Science*. [S.l.]: Addison-Wesley Professional, 2002.

BOUCHENAK, S. et al. Verifying cloud services: Present and future. *SIGOPS Operating Systems Review*, ACM, New York, NY, USA, v. 47, n. 2, p. 6–19, July 2013. ISSN 0163-5980. Disponível em: <http://doi.acm.org/10.1145/2506164.2506167>.

BRUNETTE, G.; MOGULL, R. *Security Guidance for Critical Areas of focus in Cloud Computing V2.1*. [S.l.], December 2009. Disponível em: <https://cloudsecurityalliance.org/csaguide.pdf>.

CASOLA, V. et al. Per-service security sla: A new model for security management in clouds. In: *2016 IEEE 25th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. [S.l.: s.n.], 2016b. p. 83–88.

CASOLA, V. et al. Automatically enforcing security slas in the cloud. *IEEE Transactions on Services Computing*, PP, n. 99, p. 1–1, September 2016a. ISSN 1939-1374.

CASOLA, V. et al. A reference model for security level evaluation: Policy and fuzzy techniques. *J. UCS - Journal of Universal Computer Science*, v. 11, n. 1, p. 150–174, 2005. Disponível em: <http://dblp.uni-trier.de/db/journals/jucs/jucs11.htmlCasolaPRT05>.

CATTEDDU, D.; HOGBEN, G. *Cloud Computing: Benefits, risks and recommendations for information security*. [S.l.], November 2009. Disponível em: <http://www.enisa.europa.eu>.

CPNI. *Information Security Briefing 01/2010 - Cloud Computing*. [S.l.], March 2010. Disponível em: <http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB$_c loud_c omputing.pdf$>.

CSAPLAR, D. *Who is adopting the Public Cloud Faster ? North America or Europe ?* [S.l.], July 2013. Disponível em: <http://www.aberdeen.com/Aberdeen-Library/8565/AI-public-cloud-adoption.aspx>.

DAMM, G. et al. *GB917 - SLA Management Handbook Version 3.0*. [S.l.], November 2012. Disponível em: <http://www.dmtf.org/sites/default/files/standards/documents/DSP2029%20$_1$.0.0$a.pdf$>.

DASTJERDI, A. V.; BUYYA, R. An autonomous reliability-aware negotiation strategy for cloud computing environments. In: *Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (Ccgrid 2012)*. Washington, DC, USA: IEEE Computer Society, 2012. (CCGRID '12), p. 284–291. ISBN 978-0-7695-4691-9. Disponível em: <http://dx.doi.org/10.1109/CCGrid.2012.101>.

DEKKER, M.; HOGBEN, G. *Survey and analysis of security parameters in cloud SLAs across the European public sector*. [S.l.], December 2011. Disponível em: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector/at$_d ownload/fullReport$>.

DING, J.; ZHAO, Z. Towards autonomic sla management: A review. In: *International Conference on Systems and Informatics (ICSAI 2012)*. [S.l.: s.n.], 2012. p. 2552–2555.

DMTF, T. F. *Cloud Management for Communications Service Provider*. [S.l.], January 2013. Disponível em: <http://www.dmtf.org/sites/default/files/standards/documents/DSP2029

FANIYI, F.; BAHSOON, R. Self-managing sla compliance in cloud architectures: a market-based approach. In: GRASSI, V. et al. (Ed.). *ISARCS*. [S.l.]: ACM, 2012. p. 61–70. ISBN 978-1-4503-1347-6.

FERREIRA, A. S. *Uma Arquitetura para Monitoramento de Segurança baseada em Acordos de Níveis de Serviço para Nuvens de Infraestrutura*. Dissertação (Dissertação de Mestrado) — Instituto de Computação, Universidade Estadual de Campinas, UNICAMP, 2013.

FICCO, M.; RAK, M.; DI MARTINO, B. An intrusion detection framework for supporting sla assessment in cloud computing. In: *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on*. [S.l.: s.n.], 2012. p. 244–249.

FREITAS, A. L.; PARLAVANTZAS, N.; PAZAT, J.-L. Cost reduction through sla-driven self-management. In: *European Conference on Web Services (ECOWS)*. Lugano, Suisse: [s.n.], 2011. Disponível em: <http://hal.inria.fr/inria-00600289>.

GARCIA, J. L. et al. A security metrics framework for the cloud. In: LOPEZ, J.; SAMARATI, P. (Ed.). *SECRYPT*. SciTePress, 2011. p. 245–250. ISBN 978-989-8425-71-3. Disponível em: <http://dblp.uni-trier.de/db/conf/secrypt/secrypt2011.htmlLunaGGS11>.

GONZALEZ, N. M. et al. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, v. 11, n. 1, p. 1–18, 2012.

GONZALEZ, N. M. et al. Segurança das nuvens computacionais: Uma visão dos principais problemas e soluções. *Revista USP*, v. 1, n. 97, p. 27–42, 2013. Disponível em: <http://www.usp.br/revistausp/97/SUMARIO-97.html>.

HENNING, R. R. Security service level agreements: quantifiable security for the enterprise? In: KIENZLE, D. M. et al. (Ed.). *NSPW*. [S.l.]: ACM, 1999. p. 54–60. ISBN 1-58113-149-6.

HOGBEN, G.; DEKKER, M. *Procure Secure: A guide to monitoring of security service levels in cloud contracts*. [S.l.], April 2012. Disponível em: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector/at$_d$*ownload*/*fullReport*>.

HUBBARD, D.; SUTTON, M. *Top Threats to Cloud Computing*. [S.l.], March 2010. Disponível em: <http://www.cloudsecurityalliance.org/topthreats.html>.

IRVINE, C.; LEVIN, T. Quality of security service. In: *Proceedings of the 2000 Workshop on New Security Paradigms*. New York, NY, USA: ACM, 2000. (NSPW '00), p. 91–99. ISBN 1-58113-260-3. Disponível em: <http://doi.acm.org/10.1145/366173.366195>.

ITU-T-FG. *Focus Group on Cloud Computing Technical Report Part 1*. [S.l.], 2012. Disponível em: <http://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx>.

JAATUN, M.; BERNSMED, K.; UNDHEIM, A. Security slas â an idea whose time has come? In: QUIRCHMAYR, G. et al. (Ed.). *Multidisciplinary Research and Practice for Information Systems*. Springer Berlin Heidelberg, 2012, (Lecture Notes in Computer Science, v. 7465). p. 123–130. ISBN 978-3-642-32497-0. Disponível em: <http://dx.doi.org/10.1007/978-3-642-32498-$7_1$0>.

JANSEN, W.; GRANCE, T. *SP 800-144. Guidelines on Security and Privacy in Public Cloud Computing*. Gaithersburg, MD, United States, 2011.

JEGOU, Y. et al. Managing ovf applications under sla constraints on contrail virtual execution platform. In: *Network and service management (cnsm), 2012 8th international conference and 2012 workshop on systems virtualiztion management (svm)*. Las Vegas, NV: [s.n.], 2012. p. 399–405.

JIANG, Q. *CY13-Q4 Community Analysis â OpenStack vs OpenNebula vs Eucalyptus vs CloudStack*. [S.l.], January 2014. Disponível em: <http://http://www.qyjohn.net/?p=3432>.

JRAD, F.; TAO, J.; STREIT, A. Sla based service brokering in intercloud environments. In: LEYMANN, F. et al. (Ed.). *CLOSER*. SciTePress, 2012. p. 76–81. ISBN 978-989-8565-05-1. Disponível em: <http://dblp.uni-trier.de/db/conf/closer/closer2012.htmlJradTS12>.

KANDUKURI, B. R.; PATURI, V.; RAKSHIT, A. Cloud security issues. In: *Services Computing, 2009. SCC '09. IEEE International Conference on*. [S.l.: s.n.], 2009. p. 517–520.

KEN, R. et al. *Security for Cloud Computing: 10 Steps to Ensure Sucess*. [S.l.], August 2012. Disponível em: <http://www.cloud-council.org/Security$_f or_C loud_C omputing - Final_0$80912.$pdf$>.

KIRKHAM, T. et al. Risk based sla management in clouds: A legal perspective. In: . [S.l.: s.n.], 2012. p. 156–160.

KLINGERT, S.; SCHULZE, T.; BUNSE, C. Greenslas for the energy-efficient management of data centres. In: *2nd International Conference on Energy-Efficient Computing and Networking*. [S.l.: s.n.], 2011. p. 21–30.

KRUTZ, R. L.; VINES, R. D. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. [S.l.]: Wiley Publishing, 2010. ISBN 0470589876, 9780470589878.

KYLE-BOWLSBEY, E.; ZARET, D. Quantifying trust: data integrity metrics. In: *Military Communications Conference, 2005. MILCOM 2005. IEEE*. [S.l.: s.n.], 2005. p. 3142–3147 Vol. 5.

LUNA, J. et al. Quantitative assessment of cloud security level agreements - a case study. In: *In Proceedings of the International Conference on Security and Cryptography*. SciTePress, 2012a. (SECRYPT 2012), p. 64–73. ISBN 978-989-8565-24-2. Disponível em: <http://www.deeds.informatik.tu-darmstadt.de/fileadmin/user$_u pload/GROUP_D EEDS/Publications/conf/secLA_e val.pdf$>.

LUNA, J.; LANGENBERG, R.; SURI, N. Benchmarking cloud security level agreements using quantitative policy trees. In: *Proceedings of the 2012 ACM Workshop on Cloud Computing Security Workshop*. New York, NY, USA: ACM, 2012b. (CCSW '12), p. 103–112. ISBN 978-1-4503-1665-1. Disponível em: <http://doi.acm.org/10.1145/2381913.2381932>.

LUNA, J. et al. Quantitative reasoning about cloud security using service level agreements. *IEEE Transactions on Cloud Computing*, PP, n. 99, p. 1–1, 2015. ISSN 2168-7161.

MAVROGEORGI, N. et al. Content based slas in cloud computing environments. In: CHANG, R. (Ed.). *IEEE CLOUD*. [S.l.]: IEEE, 2012. p. 977–978. ISBN 978-1-4673-2892-0.

MEEGAN, J. et al. *Practical Guide to Cloud Service Level Agreement*. [S.l.], April 2012. Disponível em: <http://www.cloudstandardscustomercouncil.org/2012$_{P}ractical_{G}uide_{t}o_{C}loud_{S}LAs.pdf$>.

MELAND, P. H. et al. Expressing cloud security requirements in deontic contract languages. In: LEYMANN, F. et al. (Ed.). *CLOSER*. SciTePress, 2012. p. 638–646. ISBN 978-989-8565-05-1. Disponível em: <http://dblp.uni-trier.de/db/conf/closer/closer2012.htmlMelandBJUC12>.

MELL, P.; GRANCE, T. *The NIST Definition of Cloud Computing*. [S.l.], September 2011. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

MODIC, J. et al. Novel efficient techniques for real-time cloud security assessment. *Computers Security*, v. 62, p. 1 – 18, 2016. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404816300682>.

MONAHAN, B.; YEARWORTH, M. *Meaningful Security SLAs*. [S.l.], October 2008. Disponível em: <http://www.hpl.hp.com/techreports/2005/HPL-2005-218R1.pdf>.

MYERSON, J. M. *Best practices to develp SLAs for cloud computing*. [S.l.], January 2013. Disponível em: <http://www.ibm.com/developerworks/cloud/library/cl-slastandards/cl-slastandards-pdf.pdf>.

NAEHRIG, M.; LAUTER, K.; VAIKUNTANATHAN, V. Can homomorphic encryption be practical? In: *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*. New York, NY, USA: ACM, 2011. (CCSW '11), p. 113–124. ISBN 978-1-4503-1004-8. Disponível em: <http://doi.acm.org.ez67.periodicos.capes.gov.br/10.1145/2046660.2046682>.

ONLINE. Cloud security alliance - csa. *Online: https://cloudsecurityalliance.org/*, 2014.

OPENSTACK. *OpenStack Dashboard*. [S.l.], March 2016. Disponível em: <http://docs.openstack.org/user-guide/intro-user.html>.

OSSG. *Security/Threat Analysis*. [S.l.], March 2016. Disponível em: <https://wiki.openstack.org/wiki/Security/Threat$_A$*nalysis*>.

PATEL, S. G.; JETHAVA, G. B. A review on sla and various approaches for efficient cloud service provider selection. *International Journal of Engineering Research & Technology*, v. 1, n. 1, November 2012. Disponível em: <http://www.ijert.org/view.php?id=1564title=a-review-on-sla-and-various-approaches-for-efficient-cloud-service-provider-selection>.

PRODANOV, C. C.; FREITAS, E. C. d. *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico*. Novo Hamburgo, RS, Brasil: Editora Feevale, 2013. ISBN 978-85-7717-158-3.

RAK, M.; CUOMO, A.; VILLANO, U. A proposal of a simulation-based approach for service level agreement in cloud. In: *Proceedings of the 2013 27th International Conference on Advanced Information Networking and Applications Workshops*. Washington, DC, USA: IEEE Computer Society, 2013. (WAINA '13), p. 1235–1240. ISBN 978-0-7695-4952-1. Disponível em: <http://dx.doi.org/10.1109/WAINA.2013.208>.

RANK, M.; LICCARDO, L.; AVERSA, R. A sla-based interface for security management in cloud and grid integrations. In: *Information Assurance and Security (IAS), 2011 7th International Conference on*. [S.l.: s.n.], 2011. p. 378–383.

RELEASES, O. *OpenStack Releases*. [S.l.], August 2016. Disponível em: <https://releases.openstack.org/>.

RIGHI, R. R.; KREUTZ, D. L.; WESTPAHALL, C. B. Sec-Mon: Uma Arquitetura para Monitoração e Controle de Acordos de Níveis de Serviço Voltados á Segurança. In: *XI Workshop de Gerência e Operação de Redes e Serviços (WGRS'2006)*. Curitiba, Brasil: [s.n.], 2006.

RIGHI, R. R.; PELISSARI, F. R.; WESTPAHALL, C. B. Sec-sla: Especificação e validação de métricas para acordos de níveis de serviço orientados á segurança. In: *IV Workshop em Segurança de Sistemas Computacionas (WSeg2004)*. Gramado, RS, Brasil: [s.n.], 2004.

ROCHA, F.; GROSS, T.; MOORSEL, A. van. Defense-in-depth against malicious insiders in the cloud. In: *Cloud Engineering (IC2E), 2013 IEEE International Conference on*. [S.l.: s.n.], 2013. p. 88–97.

SAMPAIO, R.; MANCINI, M. C. Estudos de revisão sistemática: Um guia para síntese criteriosa da evidência científica. *Revista Brasileira de Fisioterapia*, v. 11, n. 1, p. 83–89, 2007.

SCHNJAKIN, M.; ALNEMR, R.; MEINEL, C. Contract-based cloud architecture. In: *Proceedings of the Second International Workshop on Cloud Data Management*. New York, NY, USA: ACM, 2010. (CloudDB '10), p. 33–40. ISBN 978-1-4503-0380-4. Disponível em: <http://doi.acm.org/10.1145/1871929.1871936>.

SHOSTACK, A. *Threat Modeling: Designing for Security*. Indianapolis, Indiana, USA: John Wiley Sons, Inc., 2014. ISBN 978-1-118-80999-0.

SILVA, C. A. d.; FERREIRA, A. S.; GEUS, P. L. d. A methodology for management of cloud computing using security criteria. In: IEEE. *1st Latin American Conference on Cloud Computing and Communications (LatinCloud)*. Porto Alegre, Brasil, 2012. p. 49–54.

SINTON, M. Sla handbook and introduction to joing initiative. *The Open Group Conference*, The Open Group, Paris, France, 2002. Disponível em: <http://archive.opengroup.org/public/member/q202/documentation/forums/qos/sinton.pdf>.

SU, M. et al. A service level agreement for the resource transaction risk based on cloud bank model. *2012 International Conference on Cloud and Service Computing*, IEEE Computer Society, Los Alamitos, CA, USA, v. 0, p. 198–203, 2012.

SUN, L.; SINGH, J.; HUSSAIN, O. K. Service level agreement (sla) assurance for cloud services: a survey from a transactional risk perspective. In: PARDEDE, E.; TANIAR, D. (Ed.). *MoMM*. [S.l.]: ACM, 2012. p. 263–266. ISBN 978-1-4503-1307-0.

SWEET, C. Securing hybrid cloud applications. *ISACA Journal*, v. 4, n. 1, 2012. Disponível em: <http://www.isaca.org/Journal/Past-Issues/2012/Volume-4/Documents/12v4-Securing-Hybrid-Cloud-Applications.pdf>.

SWIDERSKI, F.; SNYDER, W. *Threat Modeling*. Redmond, WA, USA: Microsoft Press, 2004. ISBN 0735619913.

TAHA, A. et al. Ahp-based quantitative approach for assessing and comparing cloud security. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. [S.l.: s.n.], 2014. p. 284–291. ISSN 2324-898X.

THEILMAN, W. et al. A reference architecture for multi-level sla management. *Journal of Internet Engineering*, v. 4, n. 1, p. 289–297, 2010. Disponível em: <http://jie-online.org/index.php/jie/article/viewFile/78/41>.

TORKSHAVAN, M.; HAGHIGHI, H. Cslam: A framework for cloud service level agreement management based on wsla. In: *6Â´th International Symposium on Telecommunications (IST'2012)*. IEEE, 2012. p. 577–585. ISBN 978-1-4673-2072-6. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6483055>.

TRAPERO, R. et al. A novel approach to manage cloud security {SLA} incidents. *Future Generation Computer Systems*, p. –, 2016. ISSN 0167-739X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167739X16301844>.

ULLA, K. W. *Automated Security Compliance Tool for the Cloud*. Dissertação (Master) — Department of Telematics, Norwegian University of Science and Technology, NTNU, 2012.

UNIVERSITY, C. M. *Service Measurement Index*. Moffett Field, CA, United States, 2011.

VENTERS, W.; WHITLEY, E. A. A critical review of cloud computing: researching desires and realities. *JIT*, v. 27, n. 3, p. 179–197, 2012.

WHITESIDE, F. et al. *Challenging Security Requirements for US Government Cloud Computing Adoption*. [S.l.], November 2012. Disponível em: <http://www.nist.gov/customcf/get$_pdf.cfm?pub_id$ = 912695>.

WINKLER, V. J. R. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. [S.l.]: Syngress, 2011. ISBN 1597495921.

YEARWORTH, M.; MONAHAN, B.; PYM, D. *Predictive Modelling for Meaningful Security SLAs*. [S.l.], October 2008. Disponível em: <http://www.hpl.hp.com/techreports/2006/HPL-2006-50R1.pdf>.

ZHANG, Z.; WU, C.; CHEUNG, D. W. A survey on cloud interoperability: Taxonomies, standards, and practice. *SIGMETRICS Perform. Eval. Rev.*, ACM, New York, NY, USA, v. 40, n. 4, p. 13–22, April 2013. ISSN 0163-5999. Disponível em: <http://doi.acm.org/10.1145/2479942.2479945>.

APÊNDICE A – DEFINIÇÃO E CONCEITOS BÁSICOS DE COMPUTAÇÃO EM NUVEM

A computação em nuvem é um paradigma de computação proposto em 2006, que apresenta benefícios e desafios para a sua adoção em larga escala. Este capítulo introduz os principais conceitos relacionados à computação em nuvem.

A.1 Definição e Conceitos Básicos

O NIST (*National Institute of Standards and Technology*) e ENISA (*European Network and Information Security Agency*) são organizações que trabalham no processo de evangelização dos principais conceitos relacionados à comutação em nuvem, auxiliando na desmitificação e no entendimento deste paradigma por parte das comunidades acadêmica-científica e técnica de modo geral. O NIST atuando mais na padronização do conceito genérico de nuvem, enquanto o ENISA tem seu foco maior nas questões que envolvem a segurança no ambiente de nuvem. As definições de computação em nuvem propostas por ambas as agências são:

- **NIST:** É um modelo que habilita o acesso por rede, de forma ubíqua, e sob demanda a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo: redes, servidores, armazenamento, aplicações e serviços), que

podem ser prontamente provisionados e liberados, com o mínimo de esforço administrativo ou necessidade de interação por parte do provedor de serviços (MELL; GRANCE, 2011);

- **ENISA:** É um modelo de serviços sob demanda para provisionamento de recursos de Tecnologia da Informação (TI), tendo como base as tecnologias de virtualização e computação distribuída (CATTEDDU; HOGBEN, 2009).

Em ambas as definições é realçada a característica de provisionamento de recursos sob demanda do modelo, além da utilização de recursos compartilhados de infraestrutura de TI em ambiente distribuído. Na qual aborda-se o aspecto operacional do paradigma de computação em nuvem com relação às atividades administrativas de gerenciamento do ambiente, o que implica na redução e na facilidade das atividades administrativas para ambos, usuário/consumidor e provedor. Na definição proposta pelo NIST (MELL; GRANCE, 2011) também são apresentados três modelos de serviço e quatro modelos de implantação. Neste trabalho a definição do NIST é adotada, por refletir a flexibilidade da nuvem na provisão de recursos computacionais e por ser amplamente aceita e difundida.

A.1.1 Modelos de Serviço

Os modelos de serviço propostos pelo NIST são conhecidos por modelos SPI (Software, Plataforma e Infraestrutura) e têm, por objetivo, classificar os possíveis serviços oferecidos pela nuvem, além da forma em que estes serviços serão entregues ao consumidor (MELL; GRANCE, 2011). Os três modelos de serviço são:

- **Software como serviço** (*Software as a Service*, SaaS): A nuvem é implantada, entregue, operada e gerenciada pelo provedor de serviços, cabendo ao consumidor a utilização da aplicação por meio de uma interface padrão (e.g.,

HTTP/HTTPS através de uma navegador web) e/ou responder pelo gerenciamento da aplicação e dados relacionados;

- **Plataforma como serviço** (*Platform as a Service*, PaaS): A nuvem oferece um ambiente para o desenvolvimento e execução de aplicações. Este ambiente de desenvolvimento pode ser constituído de linguagens de programação, bibliotecas e ferramentas suportadas pelo provedor. Neste modelo, o provedor tem a responsabilidade de gerenciar ou controlar as camadas subjacentes de serviços, incluindo rede, servidores, sistemas de armazenamento e sistemas operacionais. Cabe ao consumidor a responsabilidade pela configuração do ambiente de desenvolvimento entregue, além das aplicações e dados relacionados;

- **Infraestrutura como serviço** (*Infrastructure as a Service*, IaaS): Os serviços oferecidos pela nuvem são basicamente recursos de infraestrutura e ferramentas, por exemplo: processamento, armazenamento, máquinas virtuais e rede. O consumidor é responsável por todo o gerenciamento da infraestrutura oferecida pelo provedor, podendo executar diferentes aplicativos ou sistemas operacionais nesta infraestrutura. Cabe ao provedor o gerenciamento e o controle do ambiente de virtualização que disponibiliza a infraestrutura entregue.

De forma geral o modelo de serviços SPI define papéis e responsabilidades que devem ser assumidos pelo consumidor e provedor em função do modelo de serviço a ser adotado. Neste contexto o consumidor é o usuário que contrata um serviço da nuvem, já o provedor é o responsável por atender a solicitação do consumidor e entregar os serviços contratados. O modelo de implantação é o cenário em que estas definições de papéis e responsabilidades serão aplicados.

A.1.2 Modelos de Implantação

Os modelos de implantação tem, por objetivo, apresentar os tipos de nuvens que podem ser adotadas: tal adoção depende das características do negócio ou do tipo de informação a ser armazenada ou processada na nuvem. Segundo o NIST, os modelos de implantação de nuvens podem ser classificados da seguinte forma (MELL; GRANCE, 2011):

- **Nuvem pública:** A infraestrutura de nuvem é disponibilizada para uso aberto ao público em geral a partir da Internet. Pode ser administrada e controlada por uma empresa, uma instituição acadêmica, organização governamental ou um provedor de serviços. Como exemplos, podem-se citar os casos da Amazon e Google;

- **Nuvem privada:** A infraestrutura de nuvem é provisionada para utilização exclusiva de uma organização, por múltiplos consumidores (por exemplo, unidades de negócio). É administrada e controlada pela própria organização ou por um terceiro. Como exemplo, pode-se citar o caso do CloudUSP. Que é uma nuvem privada adquirida, implantada e administrada pela própria Universidade de São Paulo (USP) e possui diversos consumidores, incluindo unidades administrativas, escolas e faculdades;

- **Nuvem comunitária:** A infraestrutura de nuvem é provisionada para uso exclusivo por uma comunidade especifica de consumidores de várias organizações que apresentam interesses semelhantes. A nuvem pode ser controlada, gerenciada e operada por uma ou mais organizações participantes ou por um terceiro. Como exemplo, pode-se citar a nuvem criada para fins de desenvolvimento de um projeto por um consórcio formado por universidade e empresas; e

- **Nuvem híbrida:** A infraestrutura de nuvem é composta pela combinação de infraestruturas de nuvem com diferentes modelos de implantação. A integração

desses modelos é efetuada por meio do emprego de tecnologias padronizadas e proprietárias, que visam garantir a portabilidade entre dados e aplicações através da infraestrutura heterogênea. Como exemplo, pode-se citar uma empresa que usa o serviço de armazenamento da Amazon para determinada aplicação, mas continua a manter o armazenamento no ambiente local dos dados operacionais do cliente.

Os modelos de implantação a ser empregado deve ser selecionado tendo como critério principal o maior alinhamento com os objetivos da empresa e com as suas necessidade em termos de tratamento dos dados. Os modelos apresentados também ilustram o modelo compartilhado de operação da nuvem, que apresenta desafios e responsabilidades relacionadas com cada modelo, tanto para o consumidor como para o provedor de serviço.

A computação em nuvem, por meio dos modelos de serviço e implantação, apresenta uma visão clara da segregação de funções entre provedor e consumidor, bem como aplicações e recursos computacionais empregados. Os benefícios da adoção da computação em nuvem são: flexibilidade, agilidade, resiliência, colaboração, redução de custos, otimização de recursos computacionais, disponibilidade, entrega rápida de recursos computacionais, escalabilidade, provisionamento de recursos computacionais sob demanda e suporte as demandas de TI requeridas por na definição de estratégias de negócio (WINKLER, 2011)(HUBBARD; SUTTON, 2010)(BRUNETTE; MOGULL, 2009).

APÊNDICE B – AMBIENTE DE COMPUTAÇÃO EM NUVEM OPENSTACK

Para avaliação o arcabouço proposto de entrega de serviços de nuvem aplicando um SLA de segurança, é necessário selecionar um ambiente de nuvem. Este ambiente deve suportar a validação e a integração do arcabouço proposto, bem como o levantamento dos mecanismos de segurança providos pelo ambiente e serviços oferecidos. Tal levantamento deve ser realizado de forma minuciosa e detalhada, sendo imprescindível a escolha de um ambiente de código aberto de nuvem para suportar estas atividades.

No trabalho (JIANG, 2014) é realizada a comparação dos ambientes de nuvem de código aberto OpenStack, OpenNebula, Eucalyptus e CloudStack. Esta comparação leva em consideração a quantidade de consumidores, a comunidade de desenvolvedores e a comunicação da comunidade de desenvolvedores, buscando identificar a mais ativa em discussões e participação no desenvolvimento do código. Como ilustração do estudo efetuado por Jiang (2004) tem-se a Figura 31.

Na Figura 31, é possível verificar o número de participantes dos projetos ativos, constatando-se que o número de participantes do projeto OpenStack é significativamente superior ao segundo projeto que é o CloudStack. A Figura 32 apresenta a população acumulada por projeto.

Na Figura 32 é apresentado o número total de consumidores e desenvolvedores que participaram da comunidade por meio de fórum de discussões ou listas de e-mail.

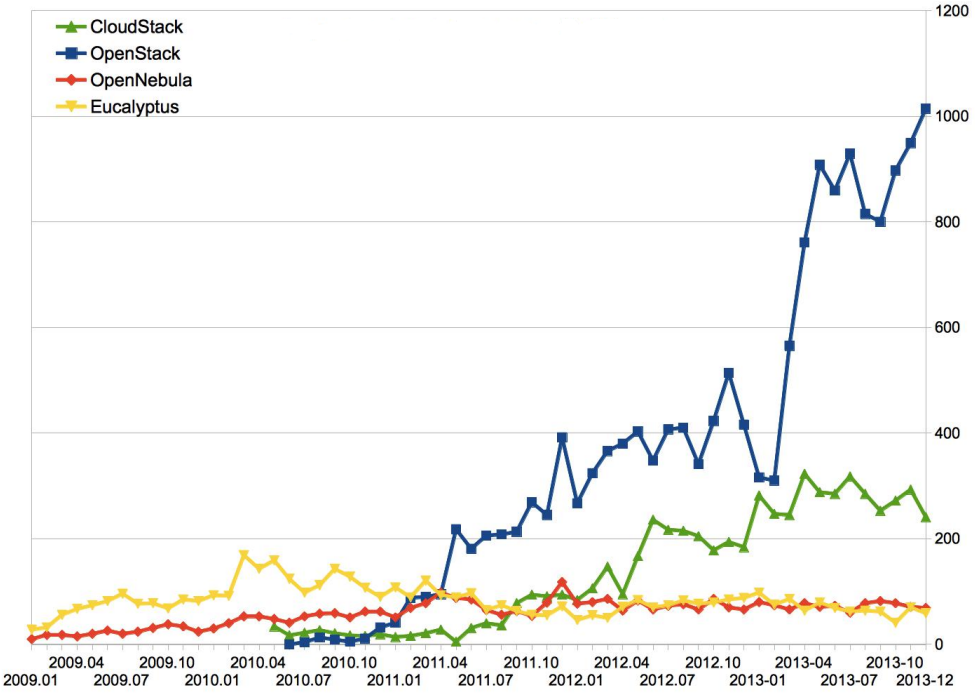

Figura 31: Número de participantes por projeto.
Fonte: (JIANG, 2014)

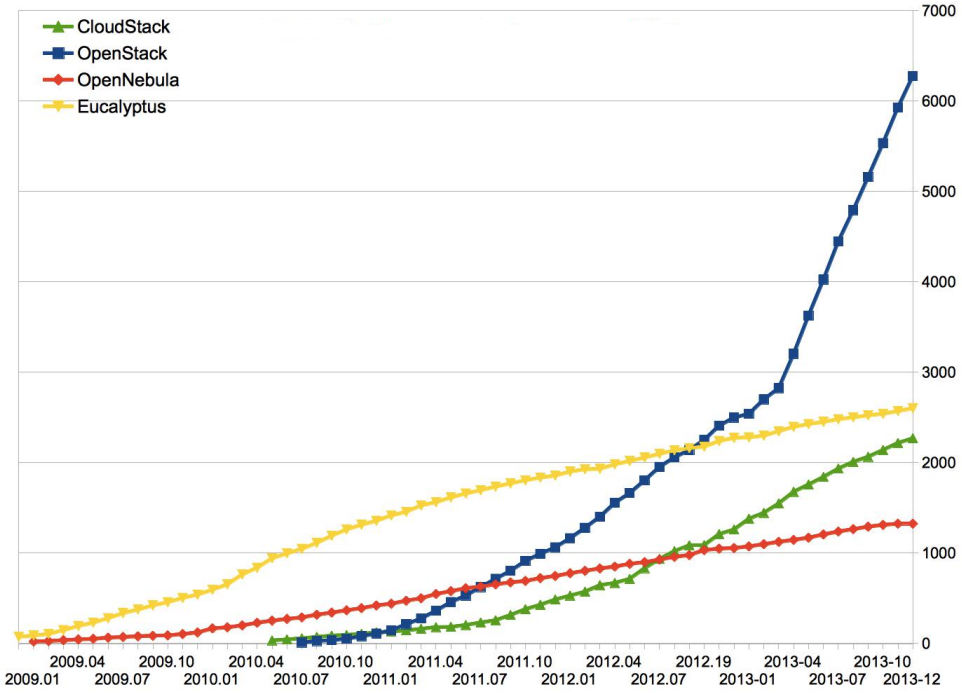

Figura 32: População acumulada da comunidade.
Fonte: (JIANG, 2014)

Verifica-se que todas as comunidades tiveram crescimento, mas a comunidade OpenStack apresentou um crescimento intenso e superior aos demais projetos. A Figura 33 apresenta a população ativa da comunidade por projeto.

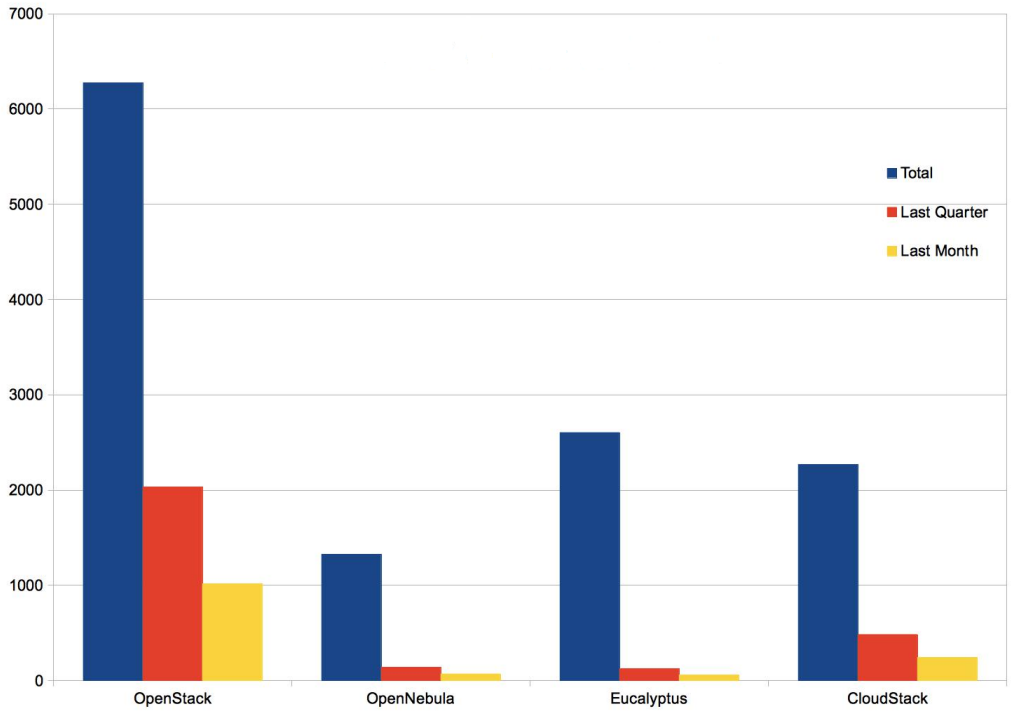

Figura 33: População ativa da comunidade.
Fonte: (JIANG, 2014)

Na Figura 33 apresenta o total da população da comunidade, número de participantes ativos do quadrimestre passado e número de participantes ativos no ultimo mês dos quatro projetos avaliados. Com base na ilustração pode-se verificar que o OpenStack possui a maior população, a maior população ativa e também a maior e mais ativa no ultimo mês.

A conclusão do estudo de Jiang (2014) é que o OpenStack é atualmente o projeto mais ativo, seguido do CloudStack, OpenNebula e Eucapyptus. Esta conclusão serve para endossar a escolha pelo OpenStack como ambiente de nuvem a ser empregado na validação do arcabouço proposto, além de ser um ambiente de nuvem conhecido e empregado no LARC (Laboratório de Arquitetura e Redes de Computadores) para pesquisa e ensino.

APÊNDICE C – DEFESA EM PROFUNDIDADE

Tomando como ponto de partida a visualização dos mecanismos de segurança ofertados pelo provedor da nuvem para entrega de seus serviços, esta abordagem pode ser empregada para avaliar a entrega de serviços por distintos provedores que suportam requisitos de segurança. Isso permite que o consumidor possa avaliar qual provedor atende melhor suas necessidades de segurança. Esta abordagem está ilustrada na Figura 34, bem como as etapas para efetuar a avaliação do ambiente com relação ao requisito de segurança desejado, com foco em confidencialidade e/ou integridade.

Este exemplo ilustra, também, quais mecanismos o provedor do serviço disponibiliza que atendem os requisitos de segurança do consumidor na camada específica, bem como os mecanismos que não atendem o requisito de segurança desejado por parte do consumidor. Os mecanismos selecionados devem compor o SLA de segurança a ser firmado por ambos, usuário e consumidor. Tomando como ponto de partida a visualização dos mecanismos de segurança ofertados pelo provedor da nuvem para entrega de seus serviços, esta abordagem pode ser empregada para avaliar a entrega de serviços por distintos provedores que suportam requisitos de segurança. Possibilitando ao consumidor avaliar qual provedor atende melhor suas necessidades de segurança. Esta abordagem está ilustrada na Figura 34, bem como as etapas para efetuar a avaliação do ambiente com relação ao requisito de segurança desejado, com foco em confidencialidade e/ou integridade.

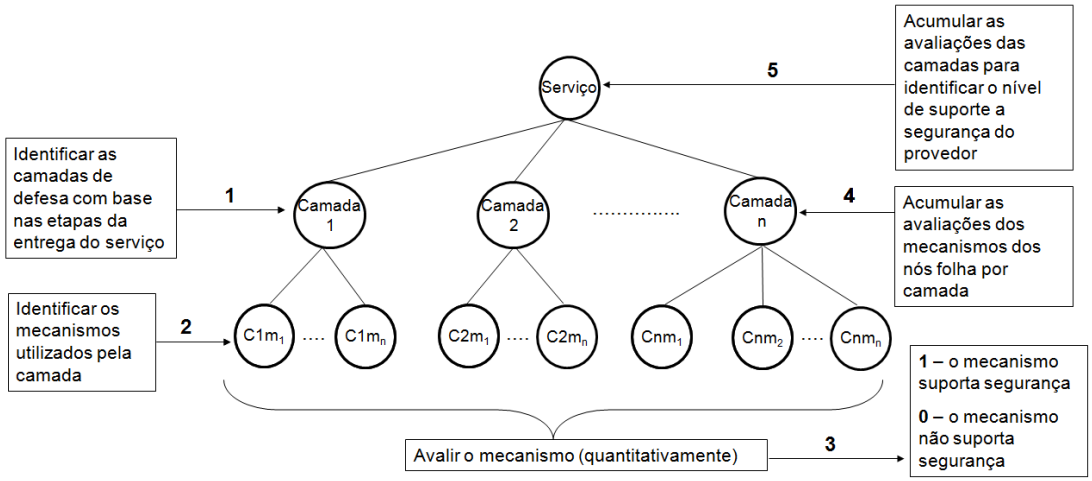

Figura 34: Árvore de avaliação de requisitos de segurança do ambiente.
Fonte: elaborada pelo autor.

Nas cinco etapas apresentadas pela Figura 34, tem-se descrito o processo para avaliar como o provedor pode suportar as necessidades de segurança requeridas pelo consumidor. Este processo pode, também, ser empregado pelo consumidor para avaliar a situação atual dos mecanismos de segurança suportados pelo provedor na entrega dos serviços solicitados. Também pode ser utilizado para apontar mecanismos a serem incorporados no processo de entrega segura e, desta forma, melhorar a adoção de mecanismos de segurança por parte do ambiente de computação em nuvem. A Figura 35 ilustra um exemplo da aplicação do método apresentado pela Figura 34.

No exemplo ilustrado pela Figura 35, o provedor suporta segurança (confidencialidade, o C da raiz) a partir de somente 4 (quatro) mecanismos empregados para a entrega de serviço (assinalados com 1), sendo que três mecanismos não dão suporte à confidencialidade (assinalados com 0). A partir destas informações, o cliente tem uma medida de avaliação de como está o atendimento dos requisitos de confidencialidade por parte do provedor para a entrega do serviço contratado. Além disso, esse mesmo cliente tem uma visão sobre quais mecanismos necessitam ter suporte à confidencialidade por parte do provedor, para que seu atendimento à confidencialidade tenha outro patamar de conformidade.

Nesse método, a proposta para avaliação dos mecanismos de segurança oferecidos

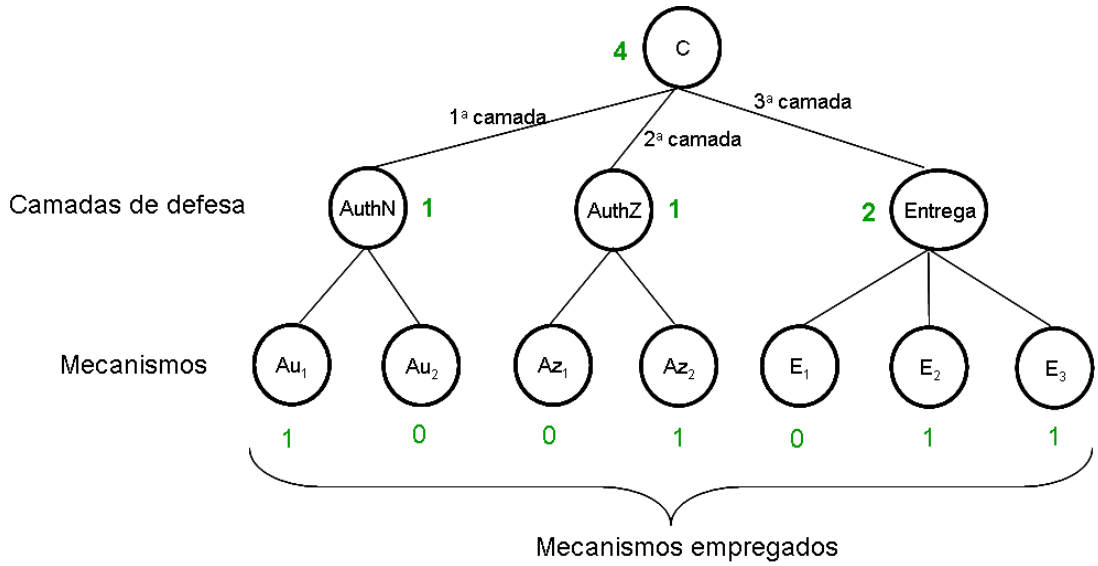

Figura 35: Avaliação do atendimento ao requisito de segurança por meio do método defesa em profundidade.

Fonte: elaborada pelo autor.

pelo provedor apresenta aspectos que não foram levados em consideração. O primeiro aspecto a ser considerado refere-se à questão qualitativa dos mecanismos, ou seja, todos os mecanismos só informam se suportam determinado requisito de segurança. Não é levando em consideração se um mecanismo é mais eficiente do que outro, ou se existem mecanismos distintos que dão suporte a mesma funcionalidade, os mesmos não são comparados. O segundo aspecto esta relacionado à divisão em camadas, ao seu impacto para o ambiente de computação em nuvem e à comparação entre as camadas, com relação a segurança fornecida por cada camada. Um estudo aprofundado sobre estes aspectos é necessário para que o método proposto seja mais robusto, permitindo levar estas considerações no seu processo de avaliação e na comparação da entrega de serviços. Este estudo faz parte das atividades futuras a serem desenvolvidas no contexto desta tese.

A inspiração para a proposta do método aplicando a abordagem de defesa em profundidade em conjunto com a modelagem em árvore é proveniente dos artigos: *Quantifying Trust: Data Integrity Metrics* de (KYLE-BOWLSBEY; ZARET, 2005), *Bechmarking Cloud Security Level Agreements Using Quantitative Policy Trees* de (LUNA; LAN-

GENBERG; SURI, 2012b); e *Defense-in-depth Against Malicious Insiders in the Cloud* de (ROCHA; GROSS; MOORSEL, 2013). O primeiro artigo apresenta uma técnica analítica para enumerar e quantificar ataques conhecidos com base em sua probabilidade de sucesso, e apresenta, também, uma quantificação do requisito integridade. O segundo artigo apresenta um método quantitativo para avaliar SLA de segurança em ambiente de nuvem, levando em consideração a base de dados que trata desta questão disponibilizada pela *Cloud Security Alliance (CSA)* conhecida por *Security, Trust & Assurance Registry (STAR)*. O terceiro artigo aborda a aplicação de camadas de defesa para tratar da questão de ataques maliciosos internos no ambiente de nuvem.