UNIVERSIDADE PAULISTA - UNIP

Rogério de Lima Occhiuzzi

A COMPUTAÇÃO EM NUVEM E SEUS RISCOS

Limeira

2017

UNIVERSIDADE PAULISTA - UNIP

Rogério de Lima Occhiuzzi

A COMPUTAÇÃO EM NUVEM E SEUS RISCOS

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade de Ciências da Computação da UNIP, como requisito parcial à obtenção do grau de Bacharel em Ciências da Computação sob a orientação dos professores Me. Antônio Mateus Locci, Me. Marcos Vinicius Gialdi e Me. Sergio Eduardo Nunes.

Limeira

2017

Rogério de Lima Occhiuzzi

A COMPUTAÇÃO EM NUVEM E SEUS RISCOS

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade de Ciências da Computação da UNIP, como requisito parcial à obtenção do grau de Bacharel em Ciências da Computação sob a orientação dos professores Me. Antônio Mateus Locci, Me. Marcos Vinicius Gialdi e Me. Sergio Eduardo Nunes.

Aprovado em __ de ____ de 201__.

BANCA EXAMINADORA

_____

Prof. Dr. Nome completo

_____

Prof. Me. Nome completo

_____

Prof. Esp. Nome completo

DEDICATÓRIA

Agradeço em primeiro lugar a Deus que iluminou o meu caminho durante esta jornada, a minha esposa Rose que, com muito carinho e apoio, não mediu esforços para que eu chegasse a esta etapa, e aos meus professores e orientadores pelas diretrizes e incentivo, que foram tão importantes na minha vida acadêmica e tornaram possível a conclusão desta monografia.

Para se ter sucesso, é necessário amar de verdade o que se faz. Caso contrário, levando em conta apenas o lado racional, você simplesmente desiste. É o que acontece com a maioria das pessoas. (Steve Jobs)

RESUMO

A ideia central desta monografia é mostrar um panorama atualizado dos aspectos que envolvem a segurança e a legalidade dos dados e informações que trafegam ou estão armazenados em sistemas de computação em nuvem. Aqui são apresentados casos reais e legais de problemas de segurança e também todo o aparato teórico para que se possa compreendê-los e preveni-los. Por último, é apresentada uma solução legal de segurança para os serviços de computação em nuvem que trabalham com armazenamento e transferência de arquivos.

Palavra-Chave: Computação em nuvem, internet, riscos legais, riscos de segurança.

ABSTRACT

The main idea of this monograph is to show an up-to-date overview of the aspects that involve the security and legality of the data and information that travels or is stored in cloud computing systems, here are presented real cases of security and legal problems and also the whole the theoretical apparatus so that they can be understood and prevented, and finally a security and legal solution is presented for the cloud computing services that work with storage and file transfer.

Keyword: Cloud computing, internet, legal risks, security risks.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

API - *Application Programming Interface*

ARPANET - *Advanced Research Projects Agency Network*

CDN - *Content Delivery Network*

CERN - *Conseil Européen pour la Recherche Nucléaire*

CmaaS - *Compliance as a Service*

CSA - *Cloud Security Alliance*

DDoS - *Distributed Denial of Service*

DNS - *Domain Name System*

DRM - *Digital Rights Management*

IaaS - *Infrastructure as a Service*

IdaaS - *Identity as a Service*

NIST - *National Institute of Standards and Technology*

NSA - *National Security Agency*

NSF - *National Science Foundation*

NSFNET - *National Science Foundation Network*

PaaS - *Platform as a Service*

P2P - *Peer-to-peer*

SaaS - *Software as a service*

SLAs - *Service Level Agreement*

SQL - *Structured Query Language*

SSC - *Secure Shared Cloud*

SSL - *Secure Socket Layer*

StaaS - *Storage as a Service*

TI - Tecnologia da informação

VM - *virtual machine*

VPN - *Virtual Private Network*

WWW - *World wide web*

Sumário

1. INTRODUÇÃO

Analisando a computação em nuvem pelo panorama social atual, pode-se ver a importância dela para o mundo contemporâneo. Setores importantes da sociedade moderna estão atrelados à computação em nuvem, como as finanças de pessoas que utilizam serviços bancários online, os serviços de e-mail que são utilizados por empresas e milhões de indivíduos diariamente e os serviços de armazenamento em nuvem, que muitas vezes guardam documentos e outros arquivos importantes.

Considerando a importância da computação em nuvem para o mundo moderno, vem à tona uma pergunta muito importante sobre a mesma:

Quais são os riscos envolvidos na sua utilização?

Responder esta pergunta é o propósito principal desta monografia e isso será efetivado da seguinte maneira: primeiro, será feita uma breve explicação do que é computação em nuvem para que as pessoas possam ter um conhecimento um pouco mais profundo sobre o assunto; depois, serão tratados os riscos de segurança mais importantes e comuns; o terceiro tópico será sobre os riscos legais que envolvem a computação em nuvem e os dados que trafegam por ela ou estão armazenados nela; por último, será apresentada uma proposta de aplicativo que foca na proteção legal e tecnológica dos dados que estão armazenados na nuvem.

2. O QUE É COMPUTAÇÃO EM NUVEM

A computação em nuvem é uma área da tecnologia da informação muito importante atualmente. Ela está presente em uma grande quantidade de dispositivos computacionais, tais como computadores, smartphones, TVs e uma infinidade de outros aparelhos.

Segundo Sosinsky (2011, p.33) a “Computação em nuvem se refere a aplicações e serviços que são executados em uma rede distribuída usando recursos virtualizados e acessados por protocolos de internet comuns e padrões”. De acordo com esses princípios, a computação em nuvem transforma as tecnologias, serviços e aplicações em uma “ferramenta self-service” e a palavra “nuvem” refere-se a dois conceitos essenciais, que é a abstração – ou seja, a capacidade de esconder do usuário os detalhes do sistema que foi implementado – e a virtualização, a capacidade de o sistema virtualizar aplicações através de agrupamento e compartilhamento de recursos (SOSINSKY ,2011, p.34).

2.1 Princípio e Uso do Termo Computação em Nuvem

Se pensarmos nos conceitos principais da computação em nuvem, que são a abstração e a virtualização, podemos dizer que a computação em nuvem existe há algumas décadas, ela nasceu nos primórdios da internet. Posso citar como exemplo as redes ARPANET/NSFNET, que foram criadas pelo Departamento de Defesa Americano e pela Fundação Nacional da Ciência (NSF), respectivamente (TANENBAUM, 2003 p. 55 a p. 59). Elas podem ser identificadas como um tipo de nuvem, pois essas redes proviam a abstração de seu funcionamento. Em outras palavras, os usuários não precisavam ter o conhecimento de como elas funcionavam por completo para poderem utilizá-las. Eram usadas normalmente por universidades e depois por empresas para o envio e recebimento de informações e dados acadêmicos e/ou de pesquisa. Porém, a nuvem, como a conhecemos atualmente, começou a tomar forma na década de noventa, com a criação da World Wide Web (WWW) pelo físico Tim Berners-lee do CERN (*Conseil Européen pour la Recherche Nucléaire*: Conselho Europeu Para Pesquisa Nuclear) (TANENBAUM, 2003 p. 60), pois a World *Wide Web,* além de prover a abstração de seus serviços, também provê a virtualização dos mesmos serviços. Um exemplo de virtualização mundialmente usado até hoje é a hospedagem de sites, pois em um único servidor podem-se

armazenar vários sites, não deixando transparecer para o usuário final que o site que ele acessa está armazenado junto com outros. De acordo com Sosinsky (2011, p.45):

> A computação em nuvem é uma extensão natural de vários princípios, protocolos e sistemas que têm sido desenvolvidos pelos mais de 20 anos que se passaram. De certa maneira, a computação em nuvem descreve algumas novas capacidades que são arquitetadas dentro de servidores de aplicações os quais têm a capacidade de receber programação dinamicamente, por serem escaláveis e por virtualizarem recursos. [...]

Segundo Giordanelli (2010 p. 6), o termo *nuvem* começou a ser usado pela telefonia, que na década de 1990 era em sua maioria conectada por fios (incluindo o tráfego de internet). Nessa época, as companhias de telefonia começaram a oferecer serviços de comunicação por VPN (*Virtual Private Network*, em uma tradução livre: rede privada virtual). A VPN é um tipo de serviço de proteção nas transmissões dos dados. Esses serviços eram oferecidos com garantias de uma alta banda-larga com custo baixo. As operadoras faziam isso alternando o caminho do tráfego para balancear a utilização, conseguindo assim maior eficiência na largura de banda; porém tornava impossível determinar exatamente qual rota o tráfego iria tomar. Para descrever esse tipo de “networking”, foi usado o termo *telecom cloud* (tradução livre: nuvem de telecomunicação).

De acordo com Giordanelli (2010 p. 6), o primeiro acadêmico que definiu o que era computação em nuvem foi Ramnath K. Chellappa e chamou-a de paradigma onde “os limites da computação serão determinados por razões econômicas em vez de limites técnicos”.

2.2 Computação em Nuvem Segundo a CSA

Segundo a CSA (2011) a computação em nuvem é:

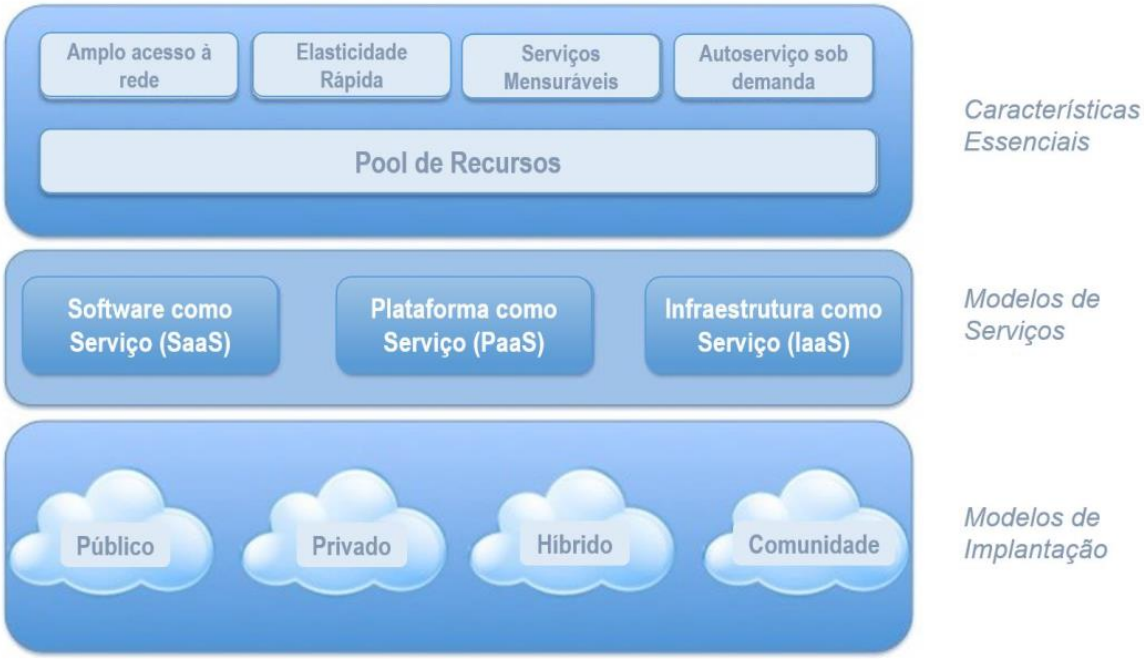
> [...] uma tecnologia disruptiva que tem o potencial de aumentar a colaboração, a agilidade, o dimensionamento e a disponibilidade e fornece as oportunidades de redução de custos através da computação otimizada e eficiente. O modelo em nuvem prevê um mundo onde os componentes podem ser rapidamente orquestrados, provisionados, implementados e desativados e, escalados para cima ou para baixo para fornecer um modelo utilitário de alocação e consumo sob demanda.

Esta interpretação é baseada na interpretação do NIST sobre o que é computação em nuvem, definida no documento *Working Definition of Cloud Computing* (descrito no NIST 800-145).

De acordo com a CSA (2011), a nuvem se caracteriza principalmente pela virtualização de recursos, entretanto nem sempre existe a virtualização em um serviço em nuvem.

2.3 Tipos de Nuvens

Figura 1 – Modelo Visual da Definição da Computação em Nuvem.



Fonte: CSA (2011, p.15).

Os modelos de nuvem tratados nesta monografia serão os que foram definidos pela NIST (The U.S. *National Institute of Standards and Technology*) Mell (2011). Sua escolha se deve ao fato de serem amplamente usados e por retratarem bem a realidade da computação em nuvem. O NIST separa a computação em nuvem em dois modelos, o modelo voltado a serviços e o modelo voltado à implantação. É importante ressaltar a importância dos conceitos de abstração e de virtualização neste modelo. A respeito da virtualização, Sosinsky (2011, p.35) diz:

> O modelo original do NIST não requeria que a nuvem usasse recursos virtualizados, também não existia nenhuma exigência de que a nuvem suportasse *multi-tenancy* nas definições anteriores do que era computação

> em nuvem. [por definição] *Multi-tenancy* é o compartilhamento de recursos entre dois ou mais clientes. A última versão da definição do NIST exige que a nuvem use virtualização e suporte *multi-tenancy*. [...]

Devido à computação em nuvem ter característica altamente dinâmica e evolutiva, é bem possível que este modelo mude com o passar dos anos.

2.3.1 Modelo de Implantação

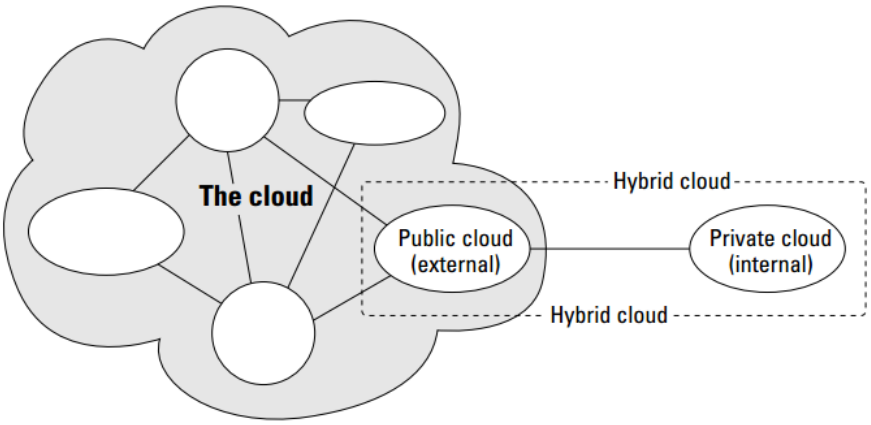
De acordo com Sosinsky (2011, p.37 a p. 39), os modelos de implantação são expressões da maneira como cada uma das infraestruturas é implantada e definem o propósito e a natureza da nuvem de acordo com a localidade dela.

O NIST (MELL, 2011) define quatro modelos de implantação:

Nuvem pública é a infraestrutura que está disponível para uso público ou para uso em grandes grupos industriais, serviços os quais são vendidos por organizações que comercializam serviços em nuvem. De maneira genérica, pode-se dizer que ela é a verdadeira representação de uma nuvem, pois este modelo provê serviços para vários clientes simultaneamente. Normalmente a maioria dos clientes não tem controle sobre ela, nem sabem a localização da mesma.

Nuvem privada é a infraestrutura operada exclusivamente para uso de uma empresa, ou seja, uma nuvem interna – que pode ser gerenciada pela própria empresa ou por uma empresa terceirizada – e pode estar dentro ou fora das instalações da empresa. Alguns detalhes técnicos importantes deste modelo de nuvem: deve ser guardado por um *firewall* controlado pelo departamento de T.I.; o sistema deve ser acessado apenas por usuários autorizados; costuma ter um controle maior sobre os dados que trafegam por ele.

Figura 2- Localização das nuvens de implantação.



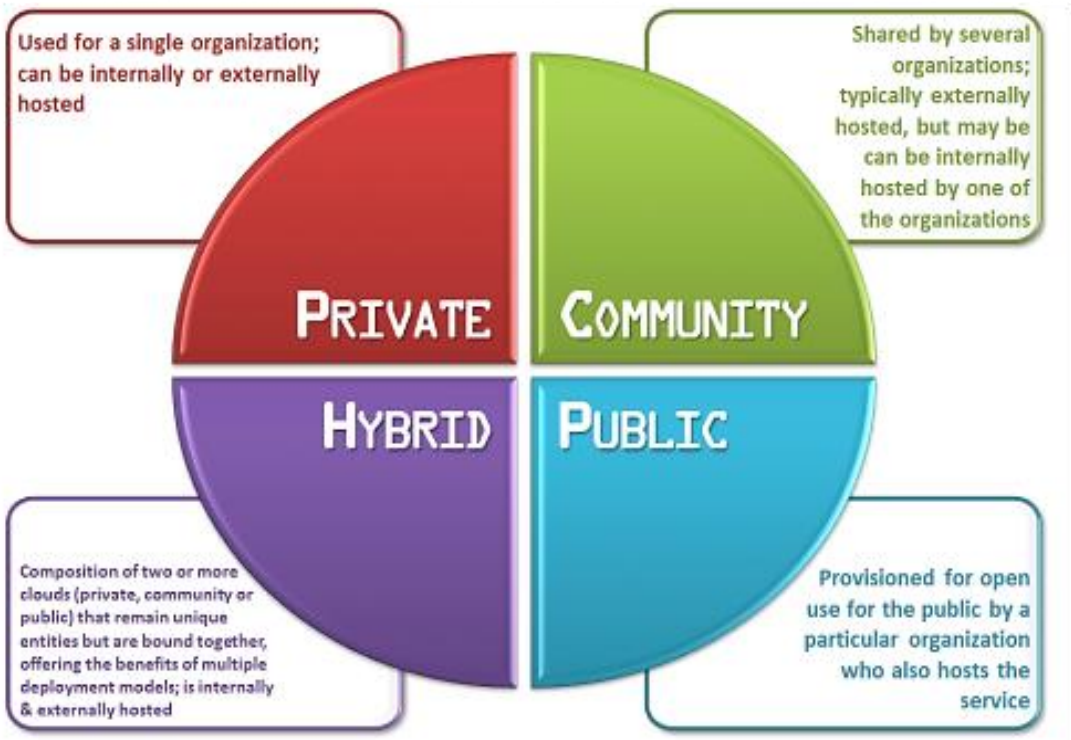
Fonte: Sosinsky (2011, p.38).

Nuvem híbrida é um modelo de nuvem que combina vários tipos, que podem ser nuvem privada, pública ou comunitária, ou seja, é um modelo de nuvem integrada, onde cada um desses tipos está conectado aos outros. Eles têm características únicas, mas trabalham juntos numa unidade. Assim, os benefícios destes vários tipos de nuvem se encontram em um único modelo. A nuvem híbrida pode oferecer padronização ou acesso prioritário a dados ou aplicações e é excelente para aplicativos portáteis. Outra característica é que ela pode terceirizar recursos e componentes não críticos e hospedá-los internamente, fazendo com que esta seja uma boa estratégia para os negócios que tenham uma demanda dinâmica e uma grande necessidade de segurança. Apesar de o modelo de nuvem híbrida ter várias vantagens, ela também tem alguns desafios a serem vencidos, como por exemplo as incompatibilidades de interface das aplicações, problemas de conectividade, complexidade de implementação e custos para a melhoria dos sistemas.

Nuvem comunitária é um modelo de nuvem que está organizada para servir a um propósito ou função comum, pode estar em uma ou várias organizações. Ela utiliza a configuração de multi-inquilino (para vários clientes simultaneamente) , portanto elas compartilham alguns objetivos, sua missão, políticas de utilização, cuidados com a segurança etc. A nuvem comunitária pode ser gerenciada por uma organização constituinte ou por uma organização externa. Esse tipo de nuvem normalmente é utilizado por organizações e negócios que trabalham com empreendimentos em conjunto ou em projetos parecidos.

Embora os quatro modelos de nuvem sejam parecidos, cada um tem suas particularidades e características e, mais importante, cada tipo de nuvem tem um uso específico de acordo com as necessidades e ideais de cada organização ou negócio.

Figura 3 - Os quatro modelos de nuvem com suas características.



Fonte: Reddy (2013).

2.3.2 Modelo de Serviços

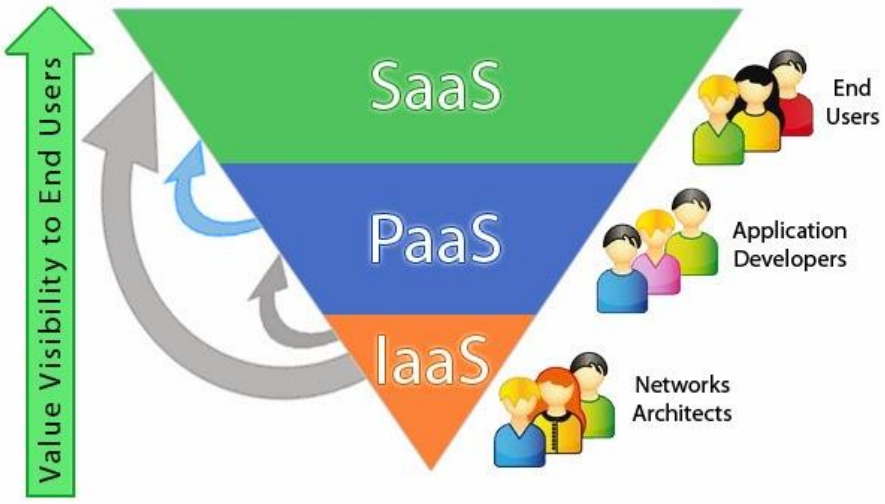
Pode-se dizer que o modelo de serviços é um nível superior do nível de implantação, porque todos os tipos de serviços estão dentro de um ou mais modelos de implantação; porém, o contrário não é verdadeiro, existe essa diferença de terminologia para que se possa ter um entendimento exato do que cada tipo de nuvem pode oferecer. Sendo mais específico na terminologia, *modelo de serviços* trata-se sempre da terceirização de serviços, sendo eles cobrados ou não, enquanto que no modelo de implantação os serviços podem ser feitos para e pelo próprio usuário.

O modelo de serviços é muito importante, pois foi ele que trouxe popularidade e evolução para a computação em nuvem. Atualmente existem serviços em nuvem extremamente populares com número de acessos de até centenas de milhões. De acordo com Scoble (2010), são serviços em nuvem o facebook.com, twitter.com, o Hotmail, que pode ser acessado pelo login.live.com, o youtube.com, o dropbox.com.

Várias outras empresas também prestam tais serviços: Amazon, IBM, Cisco, Dell, HP, Intel, Novell e Oracle. Esses exemplos mostram a importância do modelo de serviços não apenas para a computação em nuvem, mas também para a toda a área de tecnologia em si, pois ele afeta a vida de milhões de pessoas diariamente.

De acordo com Sosinsky (2011, p.39 a p. 43), existem vários tipos de serviços, como o Staas , *Storage as a Service* – em uma tradução livre significa *armazenamento como um serviço* –, Idaas, *Identity as a Service – identificação como um serviço* – e o CmaaS ,*Compliance as a Service*, que não tem uma tradução adequada, mas trata de um tipo de serviço que cuida da área de acesso e restauração dos sistemas em nuvem, e outros; porém existem três tipos de serviços que são muito populares e universalmente aceitos.

Figura 4 - Os tipos de usuários que os serviços atingem.



Fonte: Reddy (2013).

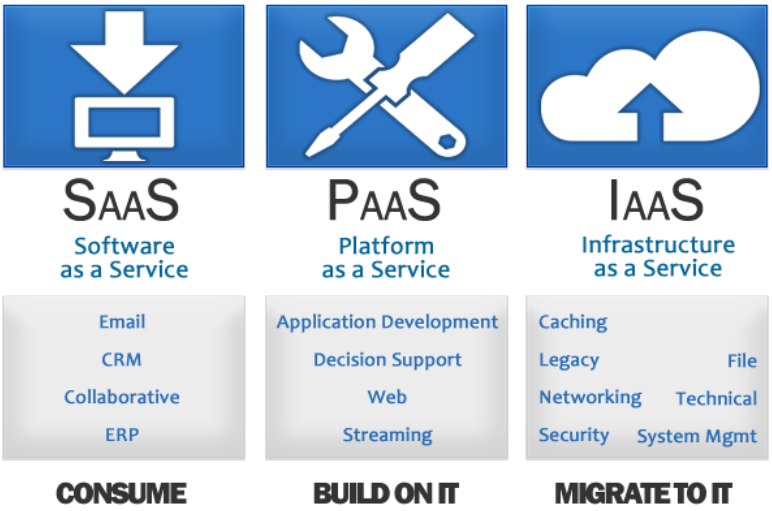
O primeiro é o IaaS, *Infrastructure as a Services*, que pode ser traduzido como *infraestrutura como um serviço, e* provê os serviços de virtualização de vários componentes da infraestrutura como por exemplo, máquina, armazenamento, infraestrutura e outros de que o cliente possa necessitar. As IaaS são responsáveis pelo gerenciamento de toda a infraestrutura enquanto o cliente é responsável pelos outros aspectos da implantação: o sistema operacional, as aplicações e as interações com os usuários. A opção mais comum de armazenamento em IaaS é o armazenamento bruto, que se refere à disponibilidade do meio físico para tal tarefa. Nesse tipo de armazenamento, não existe gerenciamento por parte do provedor. Já

os volumes anexados nas instâncias de IaaS são guardados em discos virtuais. Esses objetos podem ser acessados através de uma API e a rede de entrega de conteúdo pode ser uma CDN (*Content Delivery Network,* ou em tradução livre *Rede de Distribuição de Conteúdo*); em outras palavras, a distribuição de conteúdo por vários nós para que se possa aumentar a velocidade de conexão e de transferência.

O segundo é o PaaS, *Platform as a Services*, cuja tradução pode ser *plataforma como um serviço*, que oferece serviços e gerenciamento de máquinas virtuais, sistemas operacionais, aplicações, desenvolvimento de *frameworks*, controle de estruturas e outros. Na Paas o cliente implanta suas aplicações na infraestrutura da nuvem ou usa aplicações, onde se programa usando linguagens ou ferramentas suportadas pelo serviço oferecido por essa plataforma, sendo o cliente responsável pela implantação e gerenciamento das aplicações. A opções mais comuns de armazenamento em PaaS é a base de dados como um serviço que trata da simples hospedagem de uma base de dados. Aqui pode ser hospedado qualquer tipo de base de dados, SQL ou qualquer outro. Esse serviço é marcado por um grande uso do sistema de multi-inquilino, pois com um único data center podem-se hospedar várias bases de dados. A big data é um tipo de serviço que oferece o processamento de dados, enviados pelo cliente ou de uma base de dados, e a devolução dos resultados de acordo com algoritmos desenvolvidos pelos próprios clientes; e provê também o armazenamento de aplicações simples, por exemplo, a hospedagem de web sites.

O terceiro é o SaaS, *Software as a Service*, traduzido como *software como um serviço*. O SaaS é o mais popular tipo de serviço em nuvem, um ambiente completo com aplicações, gerenciamento e interface com o usuário, ou seja, o servidor é completamente responsável pelo gerenciamento das informações e das interações com os usuários, tudo na infraestrutura é responsabilidade do servidor. As opções mais comuns de armazenamento em SaaS são o armazenamento e o gerenciamento da informação. Esse serviço pode ser uma rede social ou de e-mails e o armazenamento de conteúdo ou arquivos, que pode ser a hospedagem de arquivos ou armazenamento e reprodução de vídeos. São serviços de computação em nuvem muito populares, uma grande parcela da população os utiliza.

Figura 5 - Os tipos de serviços oferecidos.



Fonte: Reddy (2013).

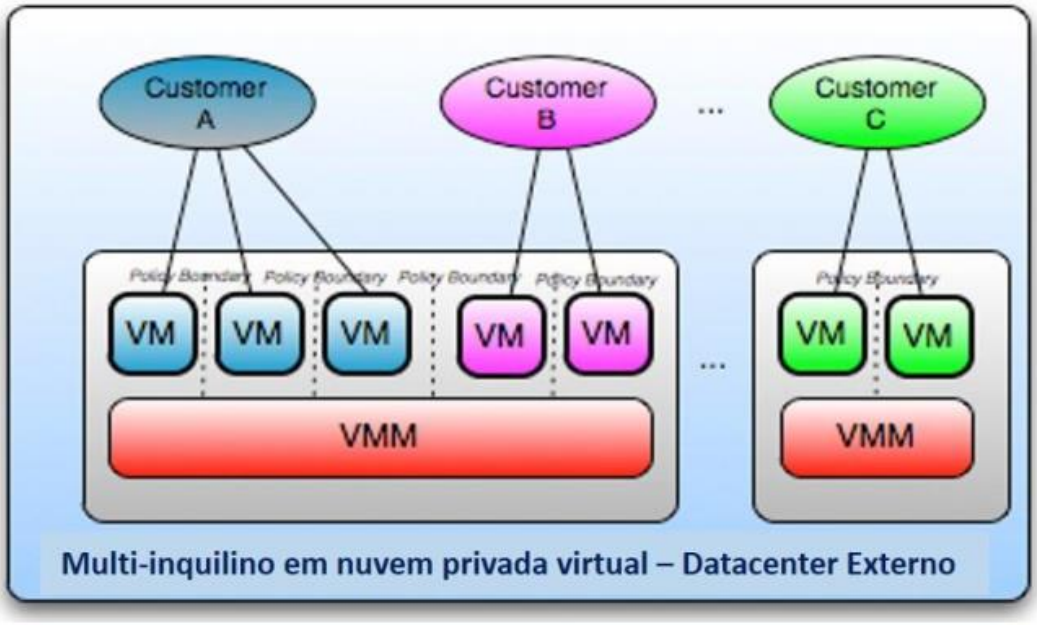
2.3.3 Arquitetura de Multi-inquilinos

Em todos os sistemas de virtualização, existe a necessidade de se utilizar a estrutura de multi-inquilino. Embora o documento do NIST, citado acima, não defina o sistema multi-inquilino como essencial para a computação em nuvem, a CSA considera-o importante para a nuvem.

Ressaltando, o sistema com recurso de multi-inquilino pode compartilhar os mesmos recursos de hardware ou os mesmos aplicativos entre vários usuários ou organizações, o que implica em economia e eficiência, do ponto de vista da organização provedora.

Abaixo, podemos observar o exemplo de uma companhia qualquer com três unidades de negócios; cada uma delas se diferencia entre suas seguranças, governanças e políticas e seus próprios SLAs (contrato de nível de serviço).

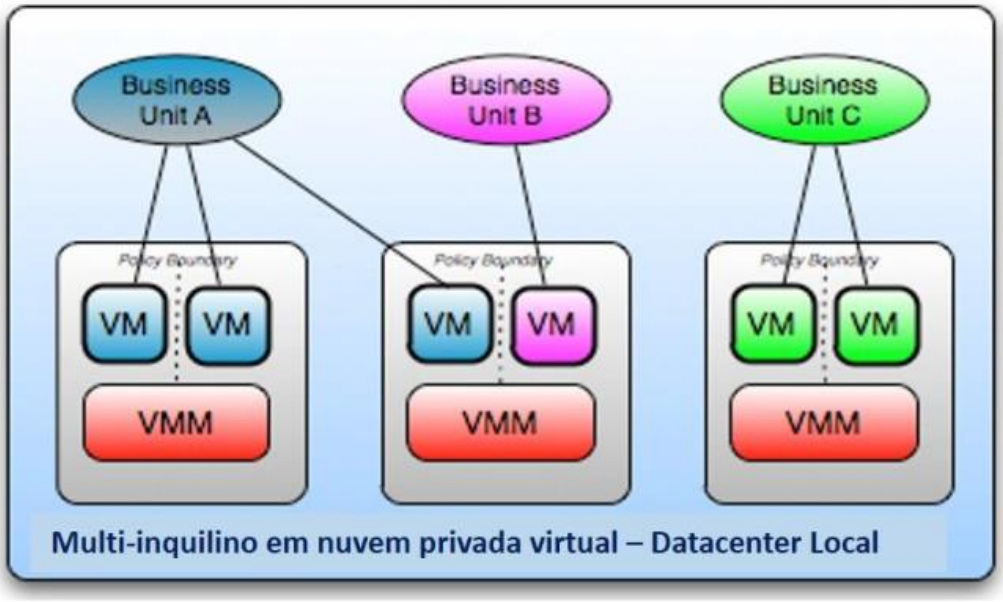
Figura 6 - Exemplo multi-inquilino.



Fonte: CSA (2011 p.17).

Abaixo, é apresentado o esquema de um provedor de nuvem pública com três clientes diferentes; cada um também com suas diferenças entre suas seguranças, governanças e políticas e seus próprios SLAs (contrato de nível de serviço).

Figura 7 - Exemplo multi-inquilino.



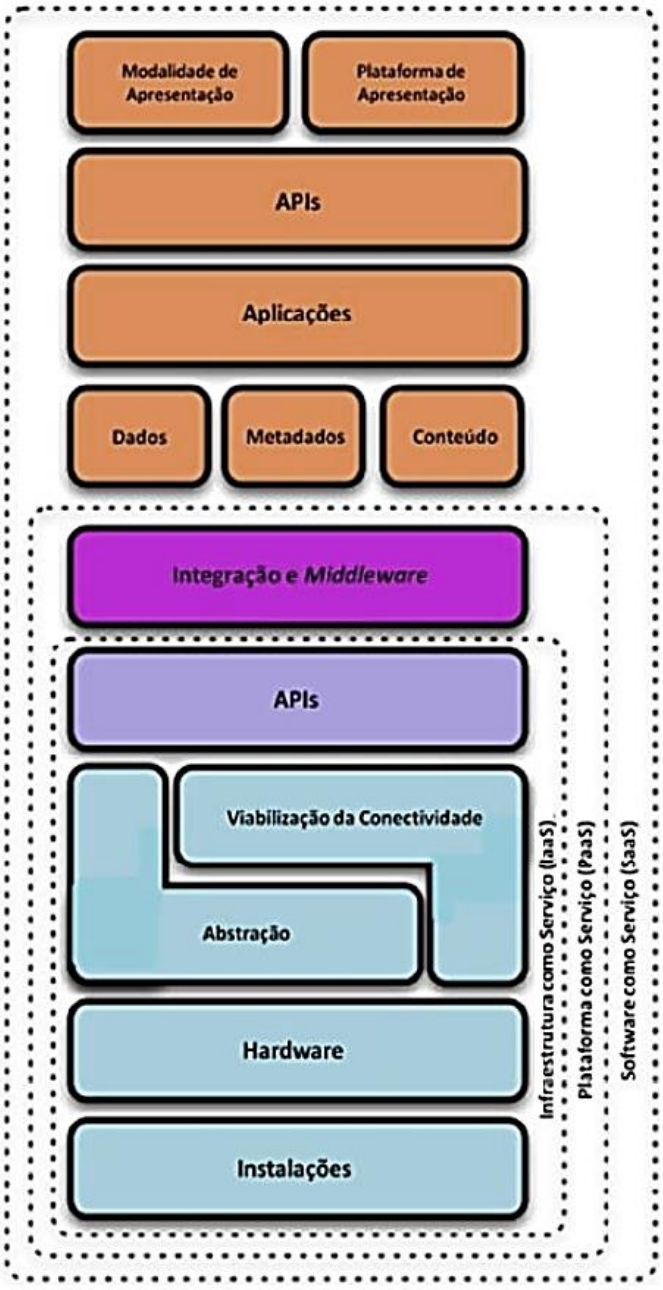
Fonte: CSA (2011 p.17).

2.3.4 Modelo de Referência

O modelo de referência é um modelo teórico de computação em nuvem que serve como base para se estabelecer que tipo de serviço/provedor é usado por cada uma das organizações que usam sistemas em nuvem. O modelo de referência apresentado a seguir, como qualquer outro, pode não corresponder à realidade de algum sistema de computação em nuvem que exista.

A seguir, o modelo de referência em formato de pilha.

Figura 8 - Modelo de referência.



Fonte: CSA (2011 p.16).

A IaaS é a base de todos os serviços em nuvem. Qualquer serviço que seja utilizado em nuvem será fundamentado em uma IaaS. Ela é toda a infraestrutura de um serviço – as instalações e hardware e todas as configurações, que tornam possível inserir alguma plataforma nela, normalmente entregue em forma de APIs.

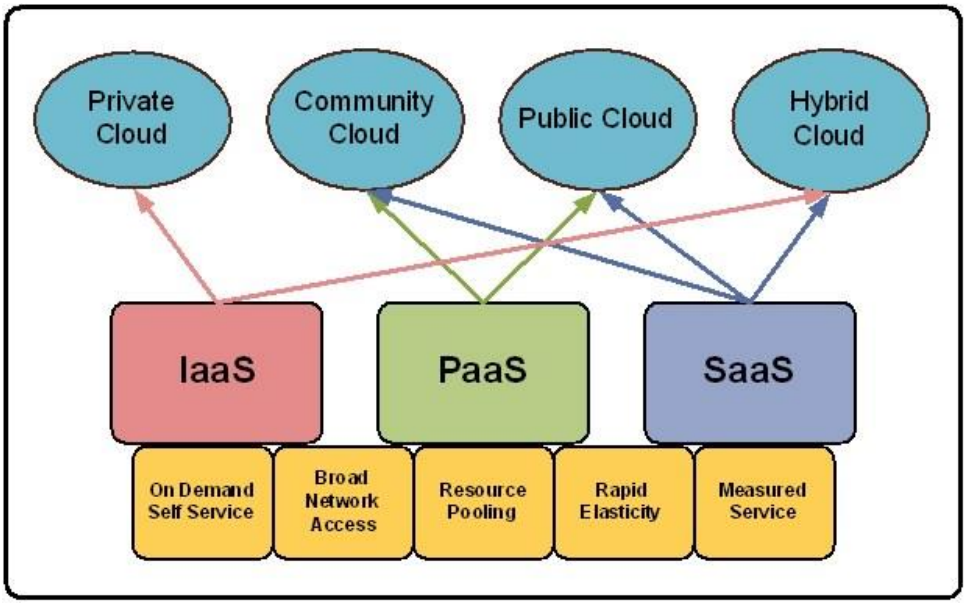
A PaaS é um serviço que adiciona uma camada a mais no sistema em nuvem se comparado a IaaS. Para a eficácia da utilização da PaaS, os provedores de nuvem fornecem ferramentas de integração, middlewares e funcionalidades, como base de dados, por exemplo, que permite aos desenvolvedores hospedarem suas aplicações na plataforma.

A terceira camada é a SaaS, implementada sobre a PaaS. Esse é o tipo de serviço em nuvem mais popular, ele entrega toda a experiência ao usuário, desde o conteúdo até a apresentação.

Os modelos de implantação da CSA são idênticos aos da NIST, por isso não entraremos em detalhas sobre eles.

2.3.5 Fragmentação da Nuvem

Figura 9 - Os quatro tipos de nuvem com suas características.



Fonte: Bishop (2011).

Para o usuário final, a nuvem pode ter a aparência de ser um sistema único, assim como todo sistema distribuído deve ter. Contudo, através de um olhar mais técnico sobre a computação em nuvem, podemos observar que ela é relativamente

fragmentada, e essa fragmentação é necessária a fim de que se consiga especificar qual é a área de abrangência e o cliente final que uma nuvem vai atingir. Uma ótima amostra desta fragmentação está na figura abaixo, onde se constata que serviço está conectado ao tipo de implementação que a computação em nuvem pode usar.

Esta introdução, relativamente extensa, ao tema exposto, objetiva apontar tecnicamente quais áreas da computação em nuvem possui os riscos citados neste trabalho acadêmico, sendo então necessária.

2.4 CSA (Cloud Security Aliance)

A Cloud Security Aliance é uma organização internacional com o objetivo de estabelecer normas e práticas que visem ao aumento da segurança nos ambientes de computação em nuvem. É importante abrir um espaço neste trabalho acadêmico para falar um pouco da CSA, pois ela é uma instituição renomada, com muitos colaboradores e ótimos guias e dicas de segurança que tratam da computação em nuvem.

Ela tem uma visão ligeiramente diferente da NIST, considerando o sistema de multi-inquilino essencial para a computação em nuvem, enquanto o NIST não o vê desse modo.

A CSA provê treinamentos, certificações e eventos. Também possui um blog direcionado a assuntos relativos à segurança da computação em nuvem e um manual completo a esse respeito que pode ser acessado no site oficial “cloudsecurityalliance.org”. Mais adiante, discorreremos sobre os tópicos que ele abrange: riscos, normas e medidas de segurança para os sistemas em nuvem.

Durante esta monografia, algumas vezes será apresentada a visão da CSA sobre tópicos abordados, com a finalidade de se ter uma compreensão mais ampla dos temas desenvolvidos.

3. COMPUTAÇÃO EM NUVEM E SEUS RISCOS

A partir deste tópico serão tratados os riscos a que o uso de computação em nuvem está suscetível. Por não haver espaço suficiente, este trabalho não conterá todos os riscos possíveis, mesmo porque são inumeráveis; serão tratados aqueles de maior gravidade e/ou que atingem uma grande parcela dos usuários.

3.1 Riscos de Segurança

Com a grande popularidade dos serviços em nuvem atualmente, um dos pontos de interesse e discussão mais importantes refere-se à segurança. Segundo CSA (2011, p.24):

> Em sua maior parte, os controles de segurança da computação em nuvem não são diferentes dos controles de segurança em qualquer ambiente de TI. Porém, a computação em nuvem pode apresentar diferentes riscos se comparados com as soluções tradicionais de TI para uma organização, por causa dos modelos de serviço de nuvem empregados e dos modelos operacionais e tecnologias utilizadas para habilitar os serviços em nuvem.

Esses “diferentes riscos” citados anteriormente surgem porque a computação em nuvem é algo relativamente novo, e também pela abstração e virtualização em que são usados os serviços em nuvem. A seguir, serão citados alguns desses riscos.

3.1.1 Ataques DDoS

Esse é um tipo de risco que a maioria das pessoas comuns desconhece, mesmo sendo um tipo de ataque relativamente frequente. Um dos casos foi a ação de crackers que tiraram do ar os serviços online dos videogames em outubro de 2016 (AUGUSTO, 2016).

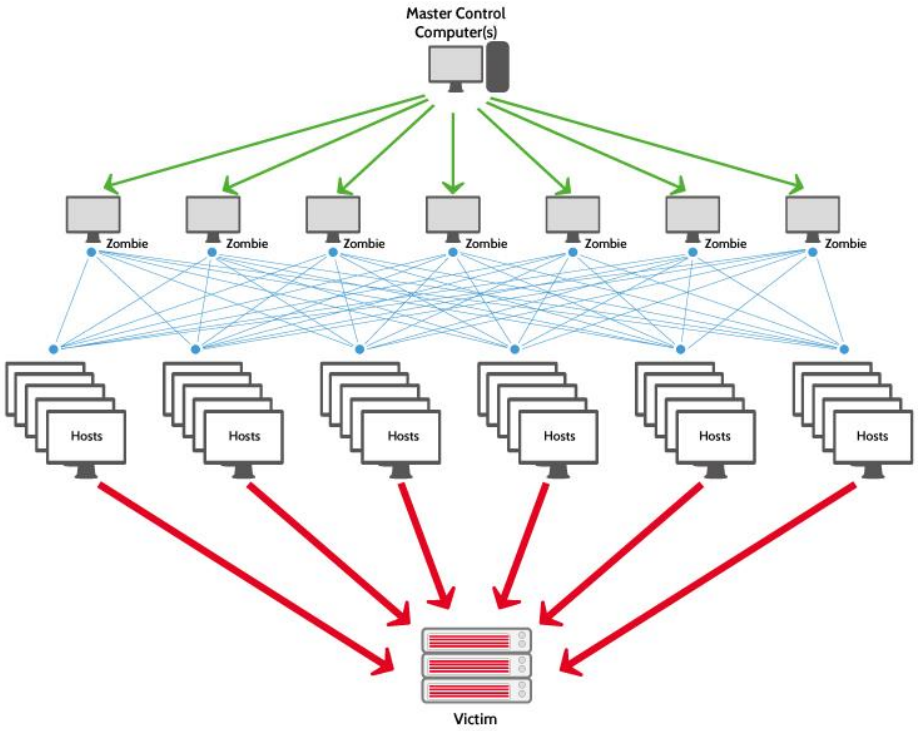
Segundo a Radware (2015), os ataques DDoS (*Distributed Denial of Service /ataque distribuído de negação de serviço)* são um tipo de ataque que tenta tornar os recursos do sistema indisponíveis para seus utilizadores. Os alvos mais comuns são serviços em nuvem, sendo esse ataque não uma invasão, mas sim uma invalidação por sobrecarga.

Um ataque DDoS funciona da seguinte maneira: um computador denominado Master adquire o controle de vários dispositivos que estão conectados à internet, dispositivos chamados zumbis, e a tarefa de atacar o alvo fica a cargo desses zumbis.

Esses zumbis são programados pelo computador Master para acessar determinado recurso de um servidor na mesma data e hora. Como todos os serviços possuem um número limitado de utilizadores a quem podem atender simultaneamente (slots), a avalanche repentina de requisições de acesso atinge o seu limite, fazendo com que o servidor não seja capaz de atender a nenhuma outra requisição.

Dependendo das configurações e do recurso atacado do servidor, ele pode chegar a travar ou se reinicializar automaticamente.

Figura 10 - Funcionamento do ataque DDoS.



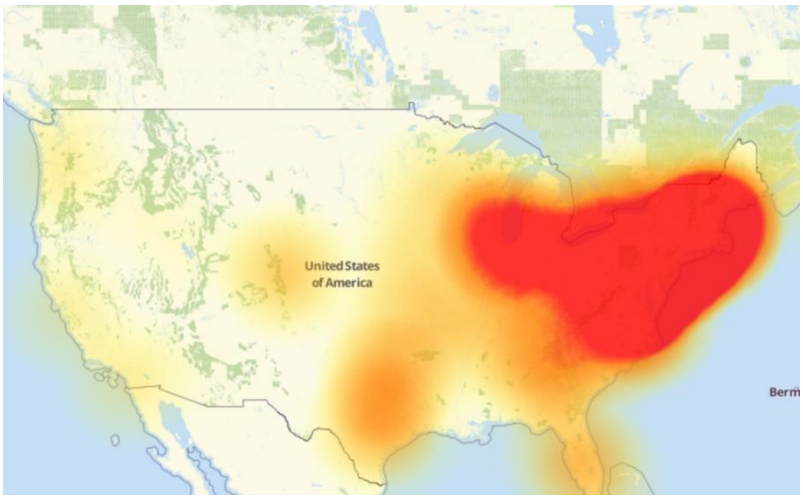
Fonte: ovh.pt (2016).

Abaixo será citado um caso recente de grande impacto.

O ataque DDoS pode parecer um tipo de ataque não muito prejudicial, entretanto isso é apenas aparência porque ele tem um poder muito grande de adquirir máquinas zumbis. Um dos maiores ataques DDoS aconteceu no dia 21 de outubro de 2016 na costa leste dos EUA e atingiu várias empresas multinacionais ao mesmo tempo, como por exemplos: Twitter, Spotify, Vox Media, Reddit, Airbnb, Tumblr, Amazon, and The New York Times.

O acontecimento mostrou um lado preocupante relacionado à segurança, ele mostra que com apenas um ataque várias empresas podem ser afetadas ao mesmo tempo. Nesse caso específico, foi direcionado ao servidor DNS Dyn.

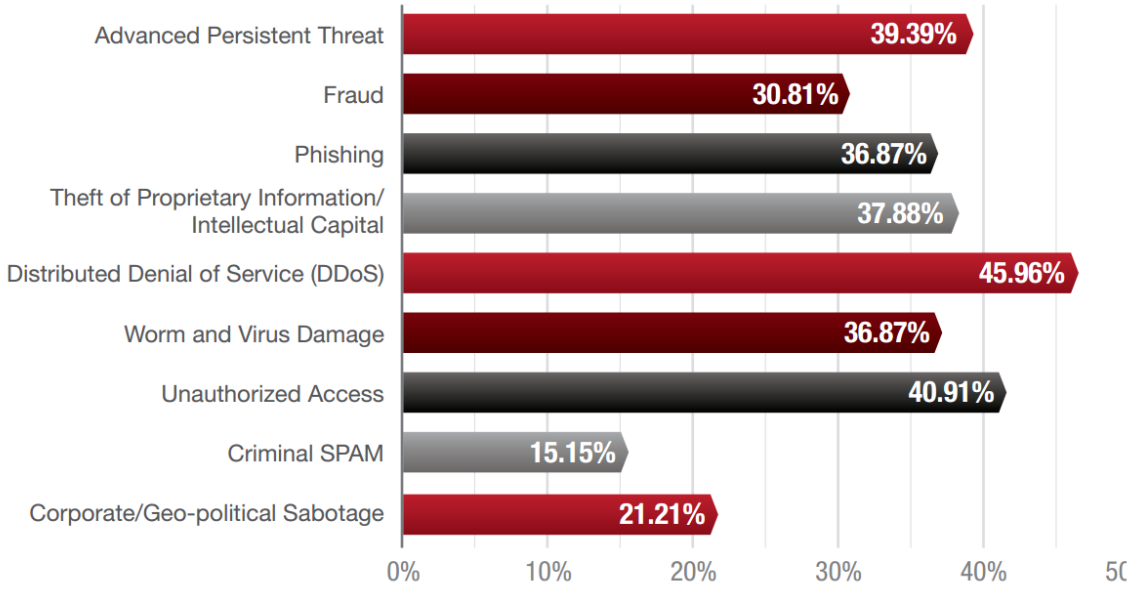
Figura 11 - Este mapa mostra o escopo do problema.



Fonte: the verge (2016).

Para revelar o quanto são preocupantes os ataques DDoS, a empresa Radware (2015) fez um levantamento nos anos de 2014 a 2015 e divulga dados alarmantes:

Figura 12 - Relatório global de segurança em aplicações e internet da empresa Radware nos anos de 2014 e 2015.

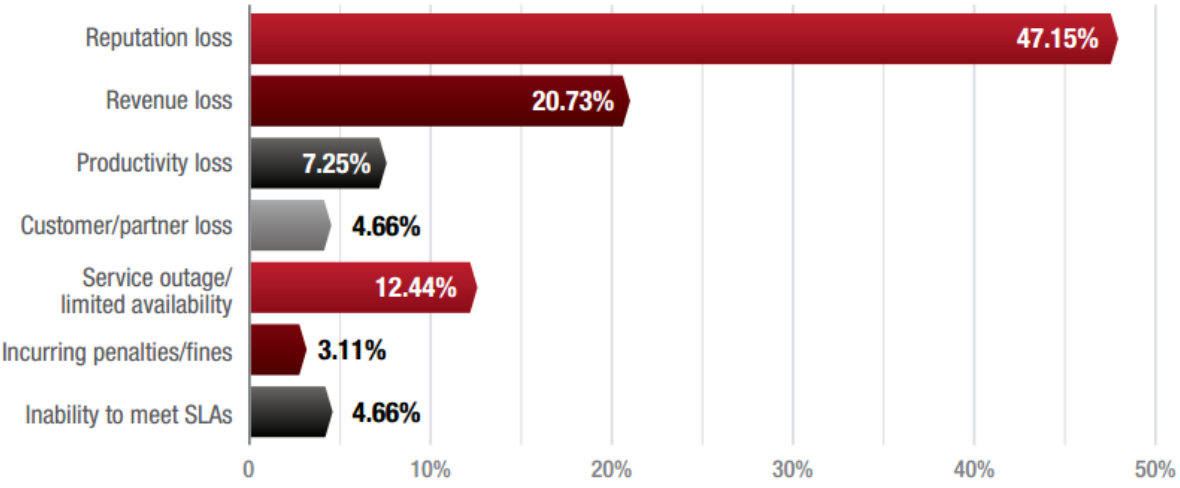


Fonte: Radware (2015 p. 10).

Este relatório estampa a porcentagem dos ataques que causaram maior prejuízo nas empresas. Liderando está o DdoS.

Outro gráfico interessante é exibido abaixo:

Figura 13 - Relatório global de segurança em aplicações e internet da empresa Radware nos anos de 2014 e 2015.



Fonte: Radware (2015 p. 22).

Este gráfico mostra as áreas dos negócios aos quais os ataques DDoS causaram maior prejuízo. Podemos notar que a área mais afetada é a reputação, pois os ataques DDoS costumam ser muito visíveis, normalmente impedem o acesso dos usuários aos serviços, causando-lhes assim frustração.

De acordo com Radware (2015 p.24 e p.25), devido ao fato de as arremetidas DDoS incidirem sobre a área da nuvem SaaS, podemos dizer que não existem perímetro fixos, ou seja, a nuvem atualmente é altamente dispersa, trazendo assim uma série de desafios para a segurança.

O primeiro desafio está relacionado aos perímetros da internet que desapareceram nos últimos anos, porque muitas empresas estenderam a infraestrutura das suas nuvens para uma nuvem pública. A finalidade das empresas é usarem aplicações externamente ou para espelhamento no caso de desastre e o maior desafio é implementar a segurança de uma nuvem privada numa nuvem pública.

O segundo desafio é a expansão do mercado de CDN, *Content Delivery Network*, que significa *entrega de conteúdo de internet*. Esse serviço é um tipo de rede criada por empresas que visam fornecer conteúdos de internet mais rapidamente a mais utilizadores. O CDN faz isso duplicando os conteúdos em vários servidores e depois direciona e distribui os conteúdos de acordo com a localidade dos usuários. A despeito de oferecer grandes vantagens, esse sistema tem um ponto muito vulnerável, que é a utilização de um grande cache. Assim, os hackers podem criar ferramentas de ataque capazes de seguir o rastro dos conteúdos e atacar diretamente no data center que contém os conteúdos originais.

O último desafio refere-se a um tipo específico de vulnerabilidade de multi-inquilino, a vulnerabilidade baseada em disponibilidade, que ocorre nas virtualizações dos data centers. Mesmo que alguns aplicativos para uso privativo ou corporativo hospedados em nuvem estejam protegidos por tecnologias de alta qualidade, ainda assim estão suscetíveis a sofrerem ataques baseados em disponibilidade, pois é muito provável que esses aplicativos privados ou corporativos compartilhem recursos virtualizados com aplicativos de uso público ou de pouca segurança, o que faz com que eles sejam o elo fraco de todo o data center. Este tópico será tratado mais especificamente à frente.

Segundo o manual da Radware (2015 p.32), as empresas podem tomar algumas medidas de segurança.

Antes de sofrerem algum ataque, as empresas devem entender que nenhuma está a salvo. Não é uma questão de se a empresa vai ou não ser atacada, mas quando. Ter certeza de que as ferramentas de detecção estão em local adequado é essencial; pode-se dizer que só se pode estar protegido do que pode ser detectado. E mais: esteja certo de que o time de segurança sabe o que tem de ser feito e o que não pode ser feito; tenha uma lista de fácil localização para quando estiver sob ataque; se existe esse risco em um website público, prepare uma mensagem de explicação e desculpa para o caso de um ataque ocorrer (atitude que não pode ser tomada antes de acontecer alguma investida); não crie regras somente com propósitos estéticos, entenda os riscos e necessidades; não implemente várias ferramentas de fornecedores diferentes, apenas o faça se essas ferramentas forem capazes de se

“comunicar” entre si e passarem informações relevantes para uma detecção otimizada.

Durante o ataque, deve-se fazer o seguinte para minimizar os danos e as interferências nos negócios: entre em contado com a empresa e/ou fornecedor responsável pela equipe de emergência para se ter certeza de que as melhores decisões estão sendo tomadas; defina um ponto de detecção, tipo de ataque e ferramenta, e decida o melhor processo de atenuação; tenha certeza de que cada passo do ataque está sendo documentado; tenha alguém responsável para falar em público e dar informações aos clientes durante a ocorrência. Da mesma forma, é importante frisar o que não se deve fazer: não entre em pânico; não tome nenhuma decisão antes de consultar a empresa ou provedor de emergência responsável pela segurança; não ignore os clientes e tenha certeza de que há alguém incumbido de tranquilizá-los durante os ataques.

Depois de ocorrido um ataque, pode-se aprender com ele e como se prevenir caso ocorra novamente. Faça uma análise de controle de dano; reveja os relatórios e procure entender o que estava errado para se preparar melhor contra ataques futuros; investigue tudo; otimize a arquitetura de segurança; tenha certeza de que foi sondado cada aspecto do ataque; adapte as tecnologias, políticas e estratégias de solução; informe os clientes com detalhes relevantes; empresas on-line devem considerar campanhas de marketing para recuperar a confiança dos clientes; certifique-se de que os relatórios estão disponíveis em caso de investigações legais; não se deve pensar que depois do ataque pode-se ficar tranquilo; não ignore os clientes e perguntas da imprensa, responda a eles e controle a crise; não adie a implementação dos resultados da investigação do ataque, seja estratégia de segurança, soluções tecnológicas ou políticas.

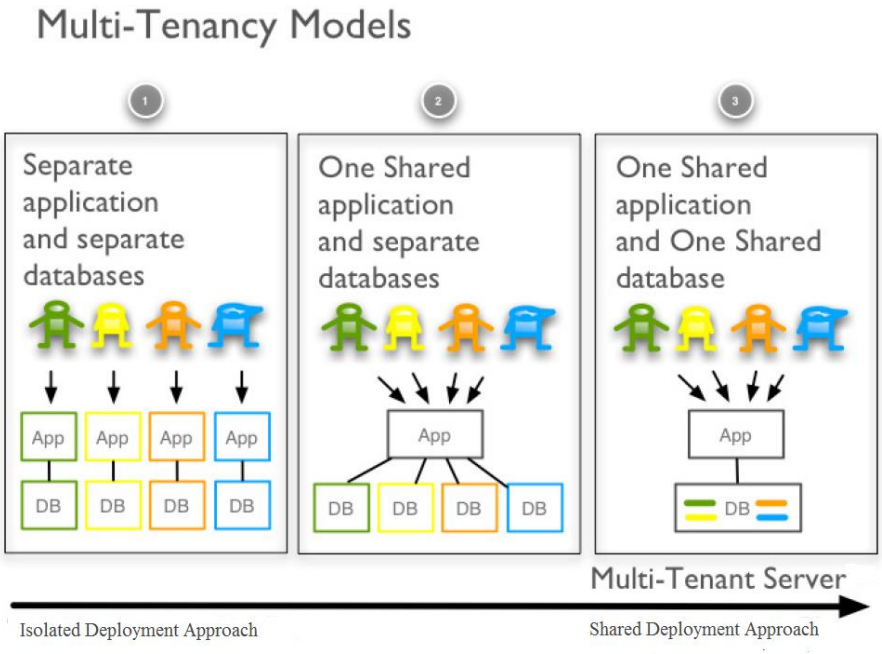
Ficou aqui demonstrado que este tema sobre os ataques DDoS é muito extenso e possui várias nuances que podem ser discutidas e avaliadas em um profundo estudo sobre o tema, todavia o objetivo aqui é dar um panorama desse tipo de problema nos dias atuais e como se prevenir dele.

3.1.2 Risco de Vulnerabilidade Com a Arquitetura de Multi-inquilinos

Essa vulnerabilidade nasceu da necessidade de virtualização dos serviços em nuvem.

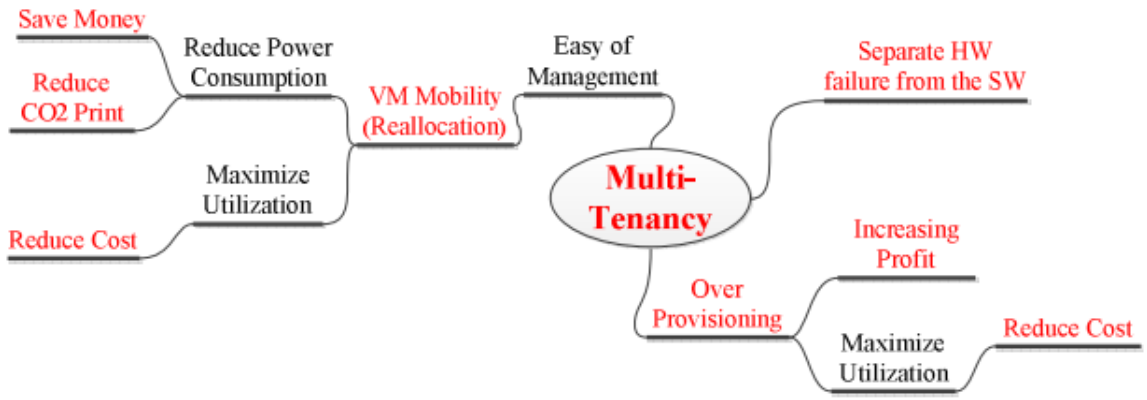
De acordo com Aljahdali (2014), nos servidores de computação em nuvem normalmente se utiliza o sistema de multi-inquilino, que é o compartilhamento dos mesmos recursos entre vários usuários, fazendo apenas uma separação lógica entre o espaço de cada um. Esse sistema facilita muito a abertura para hackers invadirem a conta de outras pessoas, por meio de testes de segurança. Pesquisadores conseguiram recuperar dados de outros usuários em sistemas que utilizam o multi-inquilino.

Figura 14 - Exemplo de como funciona o multi-inquilino.



Fonte: wikispaces, 03 de novembro de 2016.

Figura 15 – Árvore de benefícios da multi-inquilino.



Fonte: Aljahdali (2014 p.4).

De acordo com Mather (2009 p. 33), a virtualização é um dos elementos fundamentais da computação em nuvem:

> A tecnologia de virtualização baseada no modelo de negócios multi-inquilino provê escalabilidade e compartilhamento de recursos da plataforma para todos os inquilinos. Mais importante, ele provê uma visão dedicada dos recursos para os clientes da plataforma. Na perspectiva das empresas, a virtualização oferece a unificação do data center e a melhora na eficiência operacional da área de T.I. [...]

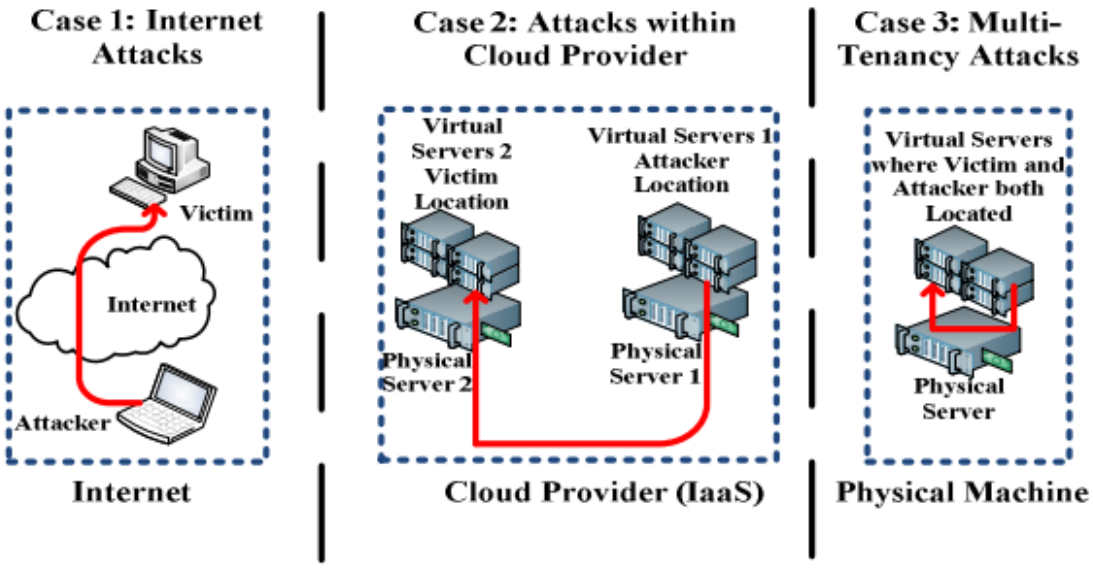
Para Aljahdali (2014 p.3 e p.4), multi-inquilino é um resultado de um esforço para conseguir ganho na computação em nuvem. Com tal objetivo, as empresas utilizam virtualização e permitem o compartilhamento de recursos, porém para cada tipo de serviço oferecido as características do modelo de multi-inquilino mudam.

A multi-inquilino, no modelo de serviços SaaS (*software como um serviço*), possibilita que os usuários usufruam dos mesmos serviços e aplicações sem que eles entendam ou vejam o que acontece na estrutura interna do data center.

Conforme a IaaS (*infraestrutura como um serviço*), o modelo de multi-inquilino proporciona a cada cliente a capacidade de prover e controlar processamento computacional, armazenamento e recursos de rede, porém eles não têm acesso ao equipamento da infraestrutura. Neste modelo, ocorre de haverem duas ou mais máquinas virtuais na mesma máquina física.

Aljahdali (2014 p.4) diz que a multi-inquilino abriu muitos questionamentos sobre a computação em nuvem. Os desenvolvedores de softwares a consideram uma oportunidade, pela eficácia em alocar recursos com muita facilidade. No entanto, para os profissionais que trabalham com segurança, ela é uma vulnerabilidade, pois pode expor a confidencialidade dos usuários. Inclusive alguns especialistas em segurança opinam que deve haver uma mudança drástica na computação em nuvem e eliminar a camada de virtualização para não precisar recorrer à arquitetura de multi-inquilinos; porém essa solução é péssima, elimina muitos dos benefícios de se utilizar multi-inquilino, como a possibilidade de usar máquinas virtuais ou o compartilhamento de recursos. Poderia ser sugerida uma ação das empresas em prover algum tipo de notificação dos riscos para os usuários, com a pretensão de amenizar a referida vulnerabilidade.

Figura 16 – Diferentes tipos de ataques.

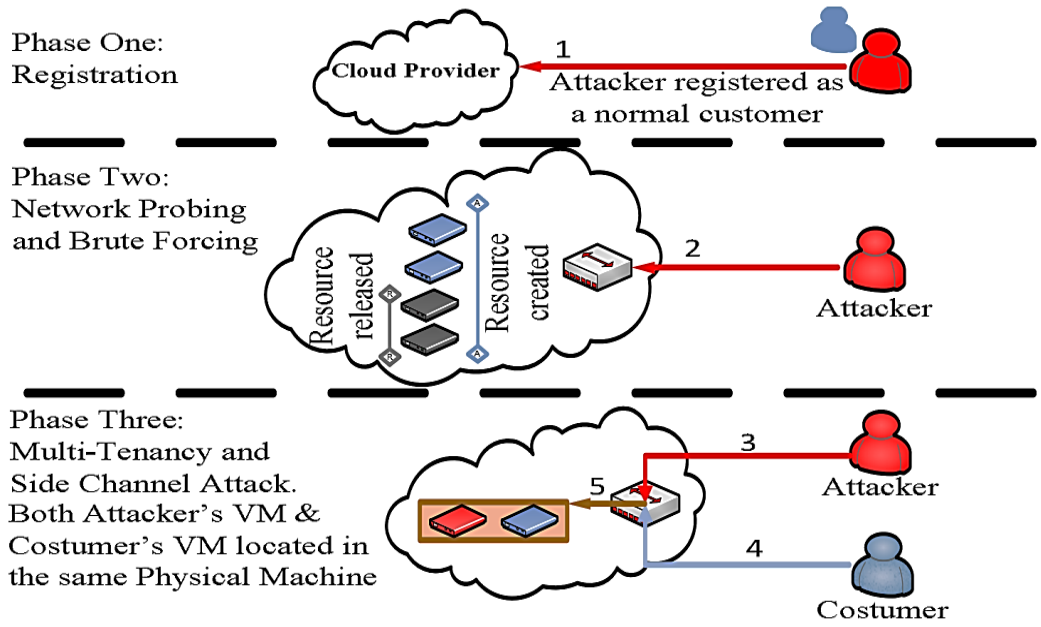


Fonte: Aljahdali (2014 p.4).

Como podemos verficar na figura acima, enquanto os tipos de ataque mais comuns são feitos de fora dos servidores para dentro deles, os ataques de multi-inquilino são feitos de dentro do próprio servidor-vítima. E o que torna grave esse tipo de ataque é a dificuldade de contê-lo, pois as técnicas tradicionais não estão preparadas para fazer a contenção de investidas que partem de dentro do próprio servidor. É um fato muito preocupante já que um único tenancy (inquilino) que foi

acessado pode abrir brecha para todos os outros, podendo assim causar um grande estrago.

Figura 17 – Passo a passo de como ocorre um ataque.



Fonte: Aljahdali (2014 p.6).

Acima vemos um modelo proposto por Aljahdali (2014 p.6) de como ocorre um ataque multi-inquilino. No primeiro passo, o atacante se registra no servidor como um usuário normal; depois obtém as informações sobre as técnicas de alocação de recursos e que sondagem de rede é utilizada no servidor em nuvem; conseguindo as informações sobre a alocação de recursos, requisita-os e deixa de usá-los; além do mais, o invasor pode chegar a dados sobre a infraestrutura do servidor em nuvem e que tipo de sistema e técnicas ele usa; no passo três, o atacante pode usar força bruta para ter acesso à alocação da multi-inquilino; após essas ações, é possível criar um canal lateral para conseguir os dados da vítima.

3.1.3 Avaliação de Riscos e Outros Aspectos da Segurança

Segundo CSA (2011), o passo primordial para saber qual tipo de nuvem é a melhor a ser implantada e os riscos aos quais poderá estar exposta, é avaliar os ativos que ela processará. Existem dois tipos de ativos, o primeiro são dados, podem ser de quaisquer tipos ou formatos, valores com campos e/ou conjuntos de informações; o segundo são aplicações/funções/processos, ou seja, qualquer tipo de sistema que use processamento. De acordo com CSA (2011 p.10), “Ou estamos movendo informações

para a nuvem, ou realizando transações/processamentos (de todas as maneiras, de funções parciais até aplicações completas)".

Para a CSA (2011), o próximo passo importante é avaliar qual a importância de cada ativo, dando prioridade ao risco que deve ser evitado e onde deve haver mais proteções. A partir daí examinar que modelo de nuvem se enquadra melhor para os ativos que serão hospedados – os modelos são os quatro vistos anteriormente. Em seguida, avalie os riscos na camada SPI. Nessa fase, é interessante mapear o fluxo de dados entre a organização, o serviço em nuvem e todos os clientes e outros nós; se possível, esboce o fluxo de dados para todas as opções aceitáveis de riscos, isso é ótimo para identificar os pontos de exposição aos riscos.

Para ativos de baixo valor, não é necessário controle de riscos muito alto, porém, para ativos de alto valor, é necessário controle severo, como por exemplo inspeções locais e esquemas de criptografia complexos. Tudo isso deve ser decidido por uma avaliação cuidadosa de todo o cenário da implantação do sistema em nuvem.

3.1.3.1 Avaliação de Riscos no Modelo de Referência

Em uma primeira visão, a SaaS é o tipo de serviço mais seguro, por diminuir a autonomia dos usuários e pelo fato de o servidor ser o único responsável pela segurança. Na PaaS, os desenvolvedores devem criar os seus próprios sistemas de segurança, o provedor é responsável apenas pela segurança mais básica da plataforma, enquanto que na IaaS o nível de segurança é mínimo e pode chegar a não haver segurança nenhuma a nível de software, sendo o fornecedor encarregado apenas da segurança do hardware, de acordo com CSA (2011 p.18):

> O principal argumento para a arquitetura de segurança é que, quanto mais abaixo na pilha o provedor de nuvem para, mais os consumidores são responsáveis por implantar e gerir os recursos de segurança e de gerenciamento por conta própria.

Embora, em um primeiro momento, pareça desvantajoso, do ponto de vista da segurança, utilizar serviços em nuvem mais "crus", eles podem trazer vantagens que compensem a sua utilização. Um custo mais baixo para implementar um sistema de segurança ou uma otimização especial para o tipo de sistema que vai ser hospedado são exemplos de ganho, além de muitas vezes ser mais barata sua utilização.

Dentro do modelo de referência, podem surgir várias questões sobre a segurança dos ativos: se os ativos estão hospedados internamente ou externamente, quais os tipos de ativos, recursos e informações, quem os controla e como, entre outras. Aludindo à questão dos ativos, a CSA elaborou uma tabela muito útil em relação à confiabilidade dos serviços (CSA 2011 p. 21), apresentada a seguir:

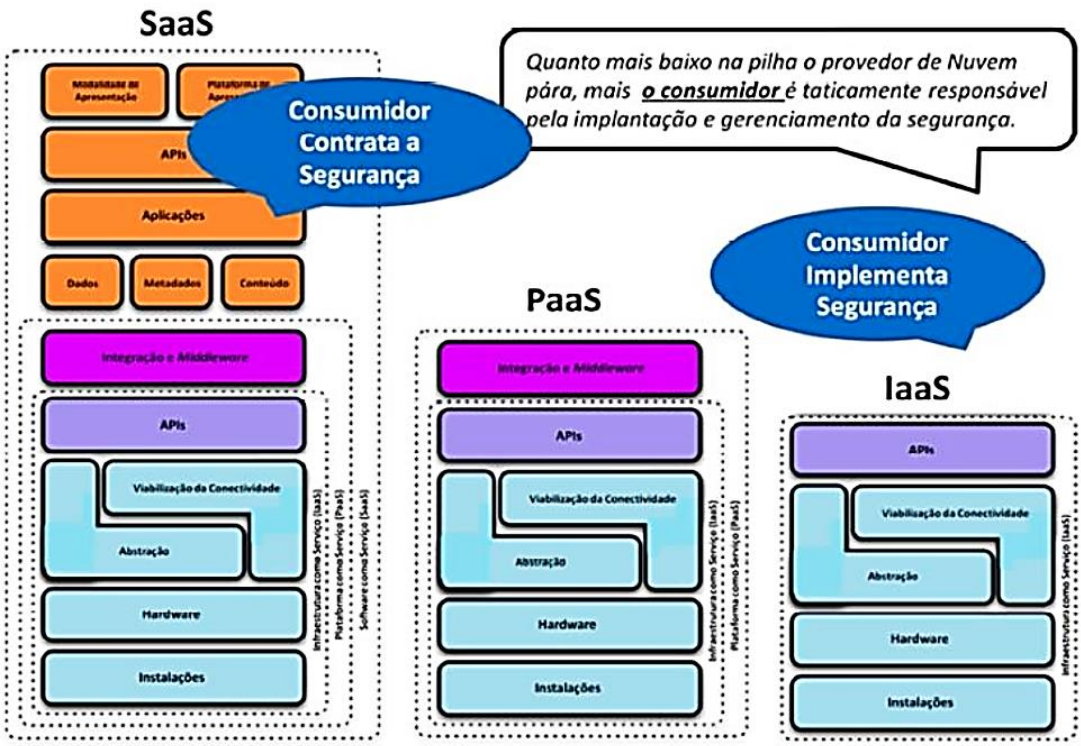
Figura 18 - Confiabilidade nos modelos de implantação.

Fonte: CSA (2011 p.21).

Na figura acima, observa-se que o *gerenciamento* da infraestrutura inclui a governança, a segurança etc; a *propriedade* da infraestrutura inclui infraestrutura física, rede, equipamentos de armazenamento etc; a *localização* da infraestrutura é a localização física e também a localização relativa para o gerenciamento organizacional; a maior ou menor *confiabilidade* está ligada ao acesso, se é acessada e consumida por vários tipos de clientes, incluindo empregados, contratados e parceiros de negócios, a confiabilidade diminui; se for acessada por um nicho mais restrito de clientes, a confiabilidade aumenta. Sobre a segurança dos modelos de serviços a CSA (2011 p.22) afirma:

> [...]A não ser que os provedores de nuvem possam facilmente revelar ao consumidor os seus controles de segurança – e até que ponto eles são implantados – e o consumidor saiba quais controles são necessários para manter a segurança de suas informações, há um enorme potencial para decisões de gerenciamento de risco equivocadas e resultados negativos.

Figura 19 - Níveis de segurança de acordo com o serviço prestado.



Fonte: CSA (2011 p.25).

A figura acima mostra qual a responsabilidade dos clientes e dos provedores de acordo com o modelo de referência.

3.1.3.2 Governança e Gerenciamento de Risco

De acordo com CSA (2011 p. 24), a segurança em ambientes em nuvem, na sua maior parte, não é diferente da maioria dos outros ambientes em TI. Em ambientes em nuvem mais especificamente, podem haver riscos adicionais pelos modelos de serviços existentes ou tecnologias usadas. Para medir a segurança de uma organização, é necessário analisar a maturidade do sistema de segurança, a eficiência do mesmo e a integridade dos controles de segurança. Ela será eficiente se esses controles forem implantados desde a camada física até a camada de aplicações, lembrando que os níveis de segurança fornecido pelos provedores diferem de acordo com o tipo de serviço prestado.

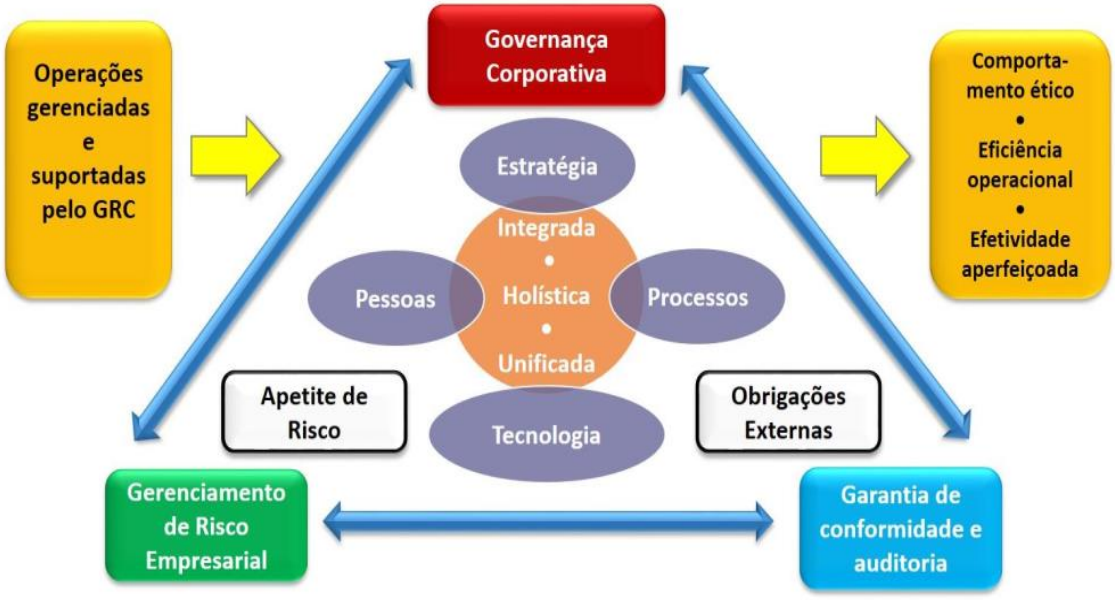
A CSA (2011 p.50) define a governança corporativa como gerenciamento consistente e aplicação coesa de políticas e controle, que viabiliza deliberações relativas à segurança dos serviços. Quanto ao gerenciamento de risco empresarial, a

CSA (2011 p.50) o define como os meios utilizados pelas organizações para se tomar decisões baseadas na identificação de certos eventos que afetam a segurança do sistema de computação em nuvem, sempre monitorando os processos.

A garantia de conformidade vem da adesão das empresas pelas obrigações “[...]responsabilidade social corporativa, ética, legislações aplicáveis, regulamentações, contratos, estratégias e políticas[...]” (CSA 2011 p.50), e por sempre iniciar e manter as ações necessárias pela segurança.

Através da figura abaixo, constatamos como a governança corporativa e o gerenciamento de riscos se relacionam com a conformidade aos riscos.

Figura 20 - Conformidade de riscos.



Fonte: CSA (2011 p.50)

Sobre o gerenciamento de risco empresarial, a CSA (2011 p.34) define como o “processo de identificar e compreender a exposição ao risco e a capacidade de gerenciá-lo”. Ainda de acordo com a CSA (2011 p.38), a gerência de risco deve ser transparente diante dos investidores e acionistas, deve ter conhecimento da interdependência dos riscos inerentes e comunicá-los aos clientes de maneira clara, e deve inspecionar e considerar os riscos herdados de outros membros mais baixos da pilha do modelo de referência.

A CSA (2011 p.36) dá algumas dicas sobre governança e gerenciamento de riscos; por exemplo, investir as economias adquiridas por se utilizar serviços em computação em nuvem nas áreas de segurança da organização.

Os analistas de riscos devem identificar estruturas colaborativas de prevenção aos riscos de segurança, e ela deve estar dentro dos contratos de serviços. Dessa maneira, o departamento de segurança precisa estar envolvido durante o acordo sobre o nível de serviço, para assegurar que os requisitos de segurança sejam aplicáveis contratualmente.

Recomenda-se estabelecer métricas de eficiência e desempenho da segurança antes de mover ou instalar alguma aplicação ou plataforma em um novo sistema em nuvem. Como medida adicional, pode ser criada auditoria e feitas avaliações suplementares de segurança para o novo sistema que será utilizado. Também, se possível, pensar antecipadamente na sobrevivência do novo sistema em nuvem que será implementado e em como fazer a portabilidade dos dados e de aplicações se acontecer caso de emergência, para que não haja nenhuma surpresa na hora da utilização do novo sistema.

Os clientes devem sempre se questionar se a tolerância aos riscos é adequada e se é aceitável qualquer risco residual resultante da utilização de serviços em nuvem, sempre procurar lacunas na gestão de risco. Com base na governança de segurança, a CSA (2011 p.37) diz:

> Clientes de serviços de computação em nuvem e provedores de serviço devem desenvolver uma governança robusta de segurança da informação, independentemente dos modelos de serviço ou implantação. A governança de segurança da informação deve ser uma colaboração entre clientes e fornecedores para alcançar as metas acordadas que suportem a missão empresarial e o programa de segurança da informação. A governança deve incluir revisões periódicas e o modelo de serviço pode sofrer ajustes nos papéis e nas responsabilidades definidas na governança colaborativa e na gestão de risco de segurança da informação (com base no respectivo escopo de controle para o usuário e para o prestador de serviços), enquanto o modelo de implantação pode definir a responsabilidade e as expectativas (com base na avaliação de risco).

3.1.4 Segurança dos Dados

Segundo a CSA (2011 p. 60), a segurança dos dados é dividida em três seções, que são a detecção e a prevenção de ataques antes de migrar os dados para a nuvem, proteção enquanto estão migrando para a nuvem e enquanto estiverem hospedados em nuvem.

Para que se tenha certeza de que os dados que serão movidos para a nuvem são confiáveis, existem dois controles que podem ser utilizados. Um deles é o monitoramento para grandes migrações de dados e arquivos – o monitoramento da atividade de uma base de dados que serve para detectar se algum administrador ou algum outro usuário está movendo uma grande quantidade de dados em uma determinada base –, o outro são filtros de gateway de segurança e prevenção de perda de dados; este tipo de filtragem monitora e previne que usuários não autorizados se conectem aos serviços em nuvem e serve para verificar as permissões dos destinos para onde os dados estão sendo enviados.

A proteção dos dados em trânsito é muito importante, tanto de um cliente para uma nuvem ou o contrário, e também de uma nuvem para outra ou de instâncias dentro da mesma nuvem. Existem três opções de proteção mais usadas. A primeira é a criptografia de cliente ou de aplicação, feita nos clientes ou nos serviços de computação em nuvem; os dados podem ser criptografados tanto por aplicações quanto por terminais. A segunda é a criptografia de rede, técnicas padrão de criptografia como a SSL ou as VPNs. Se possível, a criptografia deve ser de ponta a ponta. A terceira pode ser a criptografia no servidor proxy, uma técnica em que esse servidor se encarrega de criptografar os dados; esta menos utilizada.

A proteção de dados na nuvem vem principalmente de criptografias, desde as camadas mais baixas da estrutura; por exemplo, desde a criptografia dos discos rígidos até a criptografia das aplicações. Também é importante ter prevenção contra a perda de dados e fazer o monitoramento de atividades tanto administrativas quanto de movimentação de dados. A fim de proteger os dados a serem distribuídos, pode ser usado o DRM. Uma informação muito importante é que a maioria das falhas relevantes de segurança de dados é referente a uma gestão de segurança ineficiente.

É relevante destacar que compreender o tipo de arquitetura do serviço em nuvem é útil na descoberta de onde estão os pontos críticos de riscos de segurança

e que se deve, sempre quando possível, usar sistema de armazenamento de dados com dispersão.

3.1.4.1 Dispersão de Dados

De acordo com a CSA (2011 p. 56), uma técnica que pode melhorar a segurança dos dados é a sua dispersão. Por exemplo, um arquivo qualquer é dividido em vários fragmentos, e os fragmentos são assinados digitalmente e enviados para vários servidores. Para o usuário recuperar o arquivo, é indispensável acessar os servidores e recuperar todos os fragmentos. Esse sistema pode ser mais trabalhoso, todavia o nível de segurança aumenta drasticamente, pois, se o hacker pretende conseguir o arquivo, ele tem de *hackear* os vários servidores, recuperar todos os fragmentos e ainda quebrar a criptografia que os fragmentou.

3.2 Riscos Legais

Aqui serão abordados os aspectos e riscos legais da computação em nuvem com base na legislação brasileira.

Na Lei Nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet em seu artigo 2, são especificados os fundamentos da internet no Brasil:

> I. O reconhecimento da escala mundial da rede;
> II. Os direitos humanos e o exercício da cidadania em meios digitais;
> III. A pluralidade e a diversidade;
> IV. A abertura e colaboração; e
> V. A livre iniciativa, a livre concorrência e a defesa do consumidor.

O marco civil teve como motivação ser uma lei que pudesse preservar as bases para a promoção da liberdade e dos direitos na internet no Brasil, de maneira que não fosse repressiva; demonstrando assim que os próprios órgãos governamentais entendem que a internet é uma questão que abrange o mundo todo e não apenas o Estado brasileiro.

O marco civil garante algumas leis muito importantes para a população brasileira, porém ele traz alguns problemas. Diz Souza (2016, p. 9) que “Passados mais de dois anos desde a aprovação do Marco Civil da Internet, não faltam controvérsias sobre a sua interpretação e o destino que os tribunais reservam para alguns dos mais inovadores dispositivos constantes da lei.”, e uma das questões mais polêmicas do texto trata da proibição e suspensão de aplicativos, tal como a do watsapp que aconteceu em fevereiro de 2015 (LOPES, 2015).

3.2.1 Questionamentos

O marco civil da internet institui uma liberdade de iniciativa com relação às atividades econômicas desenvolvidas na internet. Ele diz “liberdade dos modelos de negócios promovidos na Internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei” (Lei 12.965/2014, artigo 3º, VIII). Isso significa que as empresas são livres para determinar os seus modelos de negócios e executar atividades econômicas.

Nesse contexto, podemos notar alguns pontos relevantes e o primeiro deles é se, por exemplo, houver alguma dúvida a respeito de uma intervenção estatal em algum setor de atividade econômica. Porém, a interpretação do texto é de que a intervenção deve ser a favor do livre comércio.

Outro ponto importante é a solução de problemas jurídicos envolvendo a implantação de novos serviços. O marco civil diz em seu artigo 4, inciso 3, que no uso da internet no Brasil deve-se priorizar a promoção “*da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso*”. Entretanto, Souza salienta (2016, p.49 e p. 50):

> Infelizmente, até o presente momento, tem-se observado postura oposta de detentores de interesses investidos e até mesmo de autoridades públicas. É o caso dos projetos de lei que buscaram combater aplicativos que oferecem alternativas de transporte privado individual no Município de São Paulo e em outras entidades da federação.

Esse trecho revela uma lamentável realidade brasileira que talvez ocorra em razão de uma cultura que teme inovações, julgando que possam prejudicar a economia brasileira. E, pior, vai contra o marco civil da internet que determina que as autoridades públicas devem proteger o empreendedor que inova na internet, assumindo uma postura aberta com relação a isso.

Um ponto importante a se ressaltar é a necessidade de se criar proteções especiais para os empresários e empreendedores que desenvolvem atividades na internet. Isso é imprescindível para que os riscos da exploração de tais atividades econômicas não sejam altos, viabilizando assim o investimento e a inovação.

3.2.2 Neutralidade da Internet

O tema que gera mais debates no marco civil da internet é sobre as exceções à neutralidade da rede.

Segundo Souza (2016), sendo a internet uma arquitetura "*end-to-end*", o transporte de dados obedece à ordem de endereçamento definida pelo próprio pacote, não interferindo no seu destino, ou seja, ficando neutra com relação ao destino dos pacotes, não sendo nem possível privilegiar ou não o envio de acordo com o conteúdo deles. Em outras palavras, para que a rede seja totalmente neutra, ela não pode conferir tratamento discriminatório aos pacotes trafegados por ela.

Um caso que fere a neutralidade da rede é aquele que ficou conhecido internacionalmente em que a NSA (National Security Agency) interceptava os pacotes de dados que passavam pelas redes de internet americanas. O tal episódio foi intitulado "Arquivos Snowden". Segundo Cerqueira Filho (2014), no período em que Edward Snowden trabalhou para a NSA, ele capturou milhares de documentos confidenciais e divulgou-os no início de junho de 2013. Com a ajuda dos jornalistas Glenn Greenwald e Laura Poitras, ele "revelou ao mundo o maior conjunto de programas de vigilância já realizados na história." (CERQUEIRA FILHO, 2014).

Sobre o problema da neutralidade da internet, Sousa diz (2016, p.140):

> Um dos temas mais importantes do mundo contemporâneo é justamente os limites do uso da tecnologia para fins de vigilância. Nossos celulares e computadores não são meros produtos de consumo. São as mais poderosas ferramentas de vigilância e escuta já criadas. Sem que a lei respeite um balanço adequado entre privacidade e investigação criminal, estaremos sujeitos a um estado de vigilância.

Com relação ao marco civil da internet, a neutralidade pode ser considerada um dos princípios mais importantes, porque sem neutralidade não é possível garantir os demais princípios, e agora a neutralidade está prevista em lei.

3.2.3 Direito ao Esquecimento

Com os mecanismos de busca na internet que existem hoje, é muito fácil conseguir informações e, muitas vezes, informações relativamente privadas. Mas, independente dessa facilidade, as pessoas dispõem de direito a ter sua privacidade preservada e é nesse contexto que se insere o "direito ao esquecimento".

Atualmente existe uma grande discussão a respeito do “direito ao esquecimento”. Nas palavras de Souza (2016, p. 125), o direito ao esquecimento é uma “espécie de tutela jurídica que concederia autorização para que as pessoas buscassem meios para que não se disponibilize ao público fatos indesejados”; em termos técnicos, seria a desindexação de certos termos referentes às pessoas que querem ser “esquecidas” dos resultados dos provedores de busca e, dessa maneira, houvesse uma grande baixa ao acesso à informação que deve ser “esquecida”.

3.2.4 Cibercrimes e o Marco Civil da Internet

Uma grande discussão que envolve o marco civil da internet é a tutela dos dados pessoais e a necessidade de se suprimir ordem judicial que permite a aquisição do IP de alguém. Essa discussão aumentou como consequência dos cibercrimes, pois, a disponibilidade dos IP e dos dados pessoais para as autoridades, auxiliam a investigação e o combate aos cibercrimes.

Em 2012 foi aprovada a lei 12.737, popularmente conhecida como lei Carolina Dieckmann. Segundo Souza (2016), “Essa lei dispôs sobre a tipificação criminal dos chamados “delitos informáticos”, criando modalidades criminais próprias para os crimes na internet.”

A lei citada acrescentou ao código penal os artigos 154-A ao 154-B, que tratam dos crimes contra a liberdade individual, especificadamente dos crimes contra a inviolabilidade dos segredos profissionais (Borges, 2013). O artigo 154-A acentua:

> *Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*
>
> *Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. [...]*

O artigo 154-B trata da abrangência do Código Penal[1].

Esses artigos mostram o quão sério é levado os cibercrimes atualmente, e com a crescente popularização dos serviços em nuvem os cibercrimes tendem a aumentar,

[1] Artigos 154-A e 154-B disponíveis em, https://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940.

tornando assim indispensáveis meios de proteção cada vez mais sofisticados aos usuários de serviços em nuvem.

3.2.5 Questões Legais Segundo a CSA

A CSA (2011) dá algumas dicas para se proteger legalmente ao se utilizar algum serviço em nuvem. Os clientes devem sempre formalizar um contrato; se não existir a exigência de um contrato padrão, o cliente pode negociar os termos com o provedor de serviços; se apenas o contrato padrão existir, o cliente deve analisar os riscos e verificar se são aceitáveis.

Uma ótima prática a ser adquirida é monitorar o cenário técnico regulatório do local de implantação do serviço em nuvem, pois as regulações estão sujeitas a mudanças extremas em um curto período de tempo, portanto as partes necessitam sempre estar alinhadas com as leis aplicáveis.

Em caso de algum problema legal com os serviços de computação em nuvem, sempre existirá uma grande dificuldade de se fazer uma análise forense, pois os provedores sempre obstaculizam o acesso aos hardwares e, nos piores casos, é impossível fazer essa análise por causa dos tipos de dados hierárquicos que os hardwares contêm.

Uma questão realmente difícil de se constatar é a autenticidade de alguns dados na nuvem. Por exemplo, se alguma inspeção forense achou um e-mail no ambiente de algum usuário, é muito difícil os técnicos em segurança determinarem com precisão se foi o próprio usuário ou outra pessoa quem escreveu esse e-mail, muitas vezes a autenticação de identidade não garante isso.

4. SSC (SECURE SHARED CLOUD)

Como se pôde notar até então, existem vários riscos para a utilização de serviços em nuvem. Nesse contexto, podem ser muito úteis aplicativos que têm foco na proteção legal e também na proteção tecnológica dos dados dos usuários. É válido destacar a existência de um aplicativo que foca nesse aspecto, o Secure Shared Cloud.

O Secure Shared Cloud (GITHUB, 2017) é um projeto para criar um aplicativo de código aberto que forma uma nuvem de computadores para o compartilhamento de arquivos entre eles. Essa nuvem tem foco na proteção legal e tecnológica dos dados do usuário, através de criptografia de chave pública e também de um controle avançado de identificação dos dados que o usuário disponibiliza para os outros; o controle em tempo real chama-se *blockchain*.

4.1 De Quais Riscos Ele Protege

Ele protege de riscos de ataques DdoS, por ser uma rede distribuída – se um nó é atacado os outros servem de espelhamento daquele nó. É capaz de defender os multi-inquilinos, usando um sistema distribuído onde cada rede virtual é salvaguardada por uma chave criptográfica diferente; se um nó for atingido os outros continuam intactos.

O Secure Shared Cloud também foi projetado para oferecer proteção legal aos arquivos, empregando o esquema de blockchain para identificar quem enviou e quem recebeu os arquivos e aplicando criptografia para garantir a integridade destas informações.

4.2 O Que O Secure shared Cloud É Tecnicamente

O Secure Shared Cloud é um sistema de computação em nuvem baseado em um complexo de arquivos distribuídos. Tecnicamente, ele é um SaaS (software como um serviço) que se baseia em uma rede pública, privada ou híbrida.

Ele pode ser definido como um sistema de computação em nuvem, pois se conecta a uma rede através de protocolos padrões, que no caso são o TCP/IP; oferece a abstração de seu funcionamento – para usar o Secure Shared Cloud o usuário não precisa ter um conhecimento avançado em informática – e, ainda, propicia um sistema de virtualização. O Secure Shared Cloud tem a capacidade de virtualizar várias redes

de distribuição de arquivos, cada uma com sua criptografia, autenticação e blockchains respectivos.

Além disso, pode ser hospedado em desktops, notebooks ou em servidores que rode os sistemas operacionais Windows (7, 8, 10), ou Linux. A condição para executar o software é que o computador tenha a máquina virtual do java instalado.

4.2.1 O Que é Blockchain?

O blockchain é uma espécie de Log que funciona em tempo real e foi desenvolvido em 2008, junto com o bitcoin, por uma pessoa ou grupo de pessoas (não se sabe a identificação real de quem seja) chamada Satoshi Nakamoto (ANTONOPOULOS, 2014). Em seu uso original, ele guarda o histórico de todas as transações em tempo real. De acordo com Antonopoulos (2014, p. 163), o blockchain é “uma estrutura de dados ordenada através de uma lista vinculada de blocos de transações” e pode ser guardado em texto plano ou em uma base de dados simples. No caso do bitcoin, o cliente central guarda os meta-dados do blockchain na base de dados da google, o LevelDB (ANTONOPOULOS, 2014).

Em termos menos técnicos, chama-se blockchain (*cadeia de blocos*) porque, conforme as transações vão ocorrendo, os blocos de informações referentes a elas vão sendo adicionados ao blockchain de maneira linear e cronológica. Outra parte essencial do blockchain é o fato de que, se um nó da rede adulterar alguma parte ou integralmente seu blockchain, o restante da rede excluirá esse nó da e invalidará seu blockchain.

O blockchain utilizado no Secure Shared Cloud é, em sua maior parte, baseado nos blockchains utilizados pelas criptomoedas; contudo, em vez de guardar informações das transações financeiras, ele guarda as informações dos arquivos baixados pelas pessoas que fazem parte dos grupos, garantindo assim a propriedade e a legalidade dos arquivos compartilhados.

4.2.2 Licença GNU GPLv3

Assim como o blockchain e o bitcoin, o Secure Shared Cloud também tem o código aberto. No caso específico do Secure Shared Cloud, ele usa uma licença de distribuição que garante os direitos sobre o software, mesmo este sendo de livre uso. A licença pertence ao projeto GNU e é denominado tecnicamente *GPLv3*. De acordo com (GNU.ORG 2017a), “O sistema operacional GNU é um sistema de software livre

completo, compatível com o Unix. GNU significa “*GNU's Not Unix*” (GNU Não é Unix)”. O projeto GNU foi anunciado em setembro de 1983 por Richard Matthew Stallman, seu criador, e foi concebido com a intenção de recriar o espírito cooperativo que a computação perdeu com o tempo. Em 1985, foi publicado o “Manifesto GNU”, contendo as bases do projeto e ?? expandido em conteúdo. Segundo (GNU.ORG 2017a), o nome GNU foi escolhido porque “em primeiro lugar, é um acrônimo recursivo para “GNU's Not Unix”, depois, porque é uma palavra real e, finalmente, é divertido de falar (ou Cantar)”.

Conforme dito em (GNU.ORG 2017a), a palavra “*Free*” em “*Free Software*” vem de liberdade e não de grátis. Sendo assim, os usuários dos softwares podem ou não pagar pelo uso deles. A fonte citada acima diz também que, ao usar um software “Livre”, existem quatro liberdades: “a liberdade de executar o programa como você desejar; a liberdade de copiá-lo e dá-lo a seus amigos e colegas; a liberdade de modificar o programa como você desejar, por ter acesso total ao código-fonte; a liberdade de distribuir versões melhoradas e, portanto, ajudar a construir a comunidade”; e mais, a pessoa que distribui fica livre para cobrar ou não por cópias do software.

O software Secure Shared Cloud usa a licença GNU GPLv3 que foi lançada em 29 de junho de 2007 (GNU.ORG 2017b). A GPLv3 é composta de quatro fundamentos que são:

> ●a liberdade do uso do software para qualquer propósito;
>
> ●a liberdade de mudar o software de acordo com as necessidades;
>
> ●a liberdade de compartilhar o software com os amigos e vizinhos;
>
> ●a liberdade de compartilhar as mudanças feitas.
>
> Quando um programa oferece todas essas liberdades, nós podemos chamá-lo de ‘software livre’.

Garante desta maneira tanto a proteção intelectual do software quanto a liberdade de uso e mudança do mesmo.

4.2.3 O Que é P2P?

A sigla P2P vem de *Peer-To-Peer* do inglês *Par-a-Par*, que é um tipo de arquitetura de rede que se caracteriza por cada ponto ou nó da rede servir tanto como um cliente quanto como um servidor, não necessitando de um servidor centralizado – como é o caso da web. Para que um sistema computacional se conecte a uma rede P2P, é exigido um software que gerencie essa conexão. Um exemplo de uso para a rede P2P é o sistema de torrentes.

Tecnicamente falando, os nós da rede P2P têm os mesmos privilégios com tarefas e cargas divididas igualmente. Fazendo assim, a arquitetura P2P configura-se como uma arquitetura de alta disponibilidade, pois, se um nó falho, há vários outros ainda funcionando. Esse também é um ponto positivo quanto à segurança, já que é uma arquitetura imune a ataques centrais.

Pode-se dizer que a arquitetura P2P é um tipo de sistema distribuído que, se otimizado de forma adequada, resulta em excelente performance, porque a performance do sistema é igual à soma de todas as performances individuais, enquanto na arquitetura de servidor centralizado a performance do sistema é igual à do servidor central.

4.2.4 Java

O software Secure Shared Cloud está sendo desenvolvido na linguagem de programação java que pertence à empresa Oracle Corporation. O fato de ela ser uma linguagem orientada a objetos, garantindo assim a segurança e reusabilidade do código; depender de uma máquina virtual para ser executada; ser altamente portável, fazendo com que, para ser executada em vários tipos de sistema, tenha que ter apenas pequenas alterações no código, são algumas características dessa linguagem de programação.

4.2.5 Criptografia

A criptografia serve para a proteção de sistemas, pois envolve métodos desenvolvidos com o objetivo de cifrar e codificar informações, de modo que pessoas não autorizadas possam ter acesso aos dados em sua forma original; essa codificação pode ser feita por meio de diversos tipos de algoritmos.

O Secure Shared Cloud irá usar criptografia para proteger os dados que serão transferidos de um nó para outros. Atualmente ela ainda está sendo implementada.

4.2.6 Servidor de Arquivos

Um servidor de arquivos é um tipo de software ou hardware, ou a integração dos dois, que tem a função de armazenar e compartilhar arquivos de qualquer tipo que se necessite. Além desse papel, um servidor de arquivos tem de garantir a segurança e integridade de seus arquivos.

Quanto à utilidade, um servidor de arquivos pode ser apenas um lugar de armazenamento de arquivos, sem nenhuma interface gráfica – por exemplo o servidor de arquivos ftp – ou ser um sistema de armazenamento pago com aplicativos de vários tipos para garantir o acesso aos arquivos e segurança de alto nível, como o Google Drive ou o Dropbox, por exemplos.

Em se tratando do Secure Shared Cloud, é possível dizer que ele é um servidor de arquivos distribuídos, onde os arquivos podem estar em uma ou mais máquinas simultaneamente. A qualquer um que tenha acesso e seja um usuário autenticado, é permitido chegar a todos os dados ou informações da rede distribuída. O Secure Shared Cloud também oferece a opção a cada usuário de pertencer a mais de uma rede ao mesmo tempo, fornecendo a tecnologia blockchain como modo de confiança das transferências realizadas na rede distribuída.

4.3 Como Funciona o SSC

O Secure Shared Cloud é um projeto que está continuadamente se aperfeiçoando. Atualmente, funciona usando a internet para se conectar a outros computadores. Ele faz a conexão através de uma rede p2p como dito anteriormente, porém apenas são criadas conexões com nós que pertençam ao mesmo grupo. Para pertencer a algum grupo, o nó precisa saber o nome do grupo e a chave de segurança referente ao mesmo. Então, basta colocar o nome do grupo e a chave nos campos do aplicativo e se conectar; a partir daí cada nó tem acesso irrestrito para fazer o download de qualquer dado que pertença ao grupo ao qual ele está conectado e que está devidamente autenticado. Outra função importante é o uso do blockchain. Neles são guardadas as informações de quem faz os downloads dos arquivos que estão na rede distribuída.

Com o tempo e ajuda da comunidade que apoia o código livre, há a probabilidade de que outras funcionalidades sejam desenvolvidas, como interações sociais ou mudanças nas restrições para participar de um grupo.

4.3.1 Como Usar o SSC

Figura 21 – Tela da utilização do Secure shared cloud.

Fonte: Github, 22 de abril de 2017.

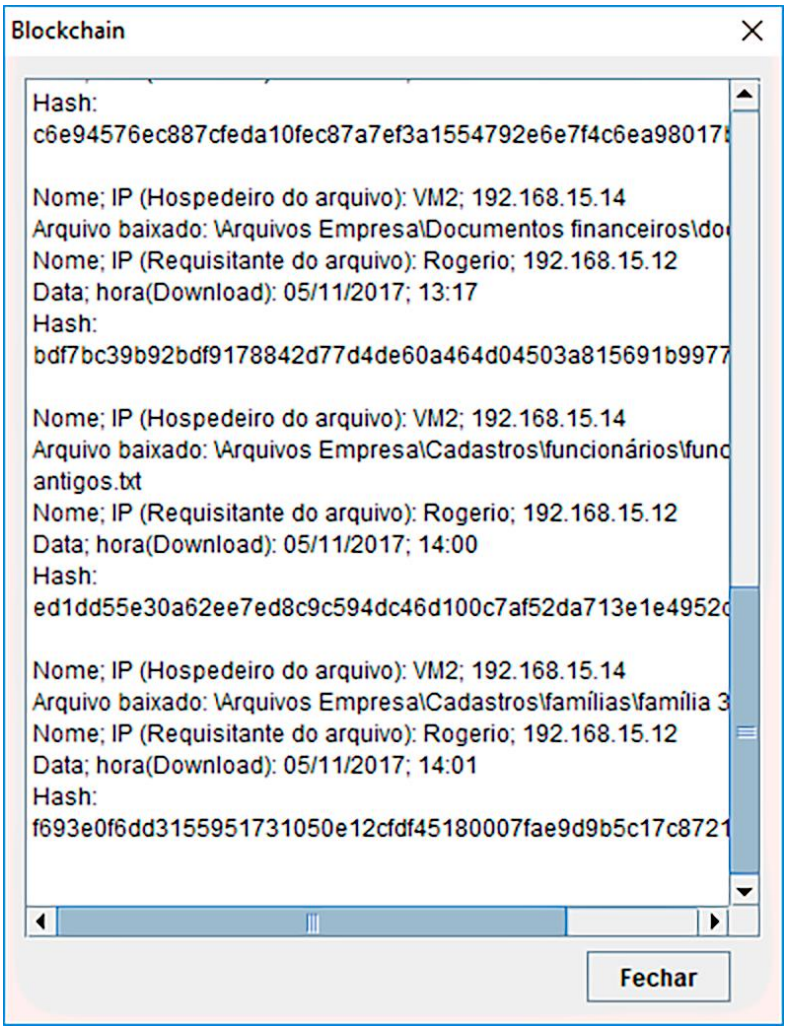
O funcionamento do Secure Shared Cloud (GITHUB, 2017) é relativamente simples, ele oferece funções que facultam a criação de grupos ou a entrada em grupos já existentes, visando ao compartilhamento seguro dos arquivos. Antes de usar qualquer função do software e realizar qualquer ação referente aos grupos, o usuário deve primeiro fazer um cadastro, uma ação muito importante, pois o cadastro garante a legalidade dos arquivos e, dessa forma, a informação do nome completo pode ser guardada nos seus devidos blockchains. Não se devem colocar apelidos nem CPF.

Para compartilhar seus próprios arquivos, são indicados os passos a serem dados: clique em “Criar novo grupo”, adicione o nome do grupo e os arquivos que deseja compartilhar na pasta criada para o grupo.

Para baixar os arquivos, primeiro clique em “entrar em um grupo”, adicione o nome do grupo e a chave pública para ter acesso.

Ele oferece também opções de sair de grupos, gerenciar aqueles criados pelos usuários e ver estatísticas referentes aos grupos.

Figura 22 – Exemplo de como funciona o Blockchain.



Fonte: Github, 22 de abril de 2017.

Como destaque de seu funcionamento, o Secure Shared Cloud (GITHUB, 2017) tem a segurança legal e tecnológica. Ele se utiliza de dois dispositivos, o primeiro é a criptografia de chave pública, o segundo é o blockchain, onde ele guarda todos os

arquivos que foram baixados para que seus proprietários possam garantir a localização de seus documentos.

4.3.2 Quais Tipos de Usos Pode Ter o SSC

O projeto como um todo foi pensado com a finalidade de proteger tanto legalmente como tecnologicamente os arquivos que estarão disponíveis para a distribuição. Logo, pode-se dizer que o Secure Shared Cloud serve para todos os clientes e usuários que necessitam desse tipo de proteção. Um dos usos mais interessantes é o comercial, pois o Secure Shared Cloud tenta garantir confiança na posse dos arquivos distribuídos. Outro emprego que pode ser proveitoso é na distribuição multimídia, uma área onde existe o risco de pirataria; e ainda a distribuição de arquivos pessoais para indivíduos de confiança, como na criação de um grupo familiar que tenha esse intento.

Além das aplicações já citadas, há outras menos óbvias: utilizar algum módulo em um outro projeto, se devidamente referenciado, ou para monitoramento de aquisição de dados, entre outras.

5. CONCLUSÃO

Durante a pesquisa, notou-se que os riscos para os usuários de serviços e plataformas de computação em nuvem são iminentes e atingem uma parcela considerável da população. O ideal é que os esquemas de proteção melhorem com o tempo. Este cenário é bem preocupante, pois cada vez mais os sistemas em nuvem fazem parte do dia a dia das pessoas, tornando assim a preocupação com a segurança um dos aspectos mais importantes da utilização dos referidos sistemas. Espera-se que, não apenas a parte corporativa deste cenário, mas também a parte pública, entenda essa importância e siga de maneira adequada as normas e dicas de segurança.

A experiência adquirida mostra que, na esfera legal, principalmente em território brasileiro, existem muitas brechas para o abuso de autoridade e a perda de privacidade com relação à nuvem. Sem dúvida, um ponto em que é necessário fazer evoluir a discussão.

Como trabalhos futuros, sugere-se o aprofundamento dos temas acima citados e a criação de sistemas que protejam melhor os usuários, garantindo assim a sua segurança sem a perda da privacidade. É fundamental que os sistemas de segurança da computação em nuvem sempre estejam atualizados e uma amostra deles é o sistema apresentado nesta monografia, pois o melhor caminho é a criação de novas tecnologias que salvaguardem usuários e consumidores. Da mesma maneira como os riscos aumentam e ficam cada vez mais complexos, a computação em nuvem precisa progredir a fim de ser capaz de proteger o usuário desses riscos.

6. REFERÊNCIAS

ANTONOPOULOS, Andreas M. **Mastering Bitcoin.** ISBN: 978-1-449-37404-4. Publicado por O'Reilly Media, Inc. 2014.

AUGUSTO, Cesar. **Ataque DDoS está afetando alguns aplicativos do Xbox Live e da PSN**. Disponível em: <http://www.universoxperience.com/2016/10/21/ataque-ddos-em-massa-esta-afetando-alguns-aplicativos-xbox-live-e-da-psn/>. Acessado em: 13 de abril de 2017.

ALJAHDALI, H. et al. **Multi-tenancy in cloud computing**. ISBN 978-1-4799-2504-9. Oxford, Reino unido. 2014.

BISHOP, Jerry. **Cloud or Not: 4 Cloud Deployment Models.** Disponível em: < http://blog.thehigheredcio.com/cloud-deployment-models/>. Acessado em: 01 de jul. de 2017.

BORGES, Abimael. **Lei Carolina Dieckmann - Lei nº. 12.737/12, art. 154-a do Código Penal.** Disponível em: <https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal>. Acessado em: 14 de abril de 2017.

CSA, Cloud Security Alliance, **Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem**, Disponivel em: < http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf >. Acessado em: 14 de abril de 2017.

CERQUEIRA FILHO, Carlos Roberto de Almeida. **Os arquivos Snowden: o episódio e os reflexos no Brasil.** Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia (CAEPE). Rio de Janeiro, 2014.

COGNOSYS SOFTWARE. Cloud Compliance Service. Disponível em: < http://www.cogno-sys.com/cloud-azure-amazon-open-stack/cloud-compliance-service/>. Acessado em: 02 de jul. de 2017.

LOPES, Marcelo Frullani. **Suspensão do Whatsapp**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 20, n. 4275, 16 mar. 2015. Disponível em: <https://jus.com.br/artigos/37170>. Acessado em: 13 de abril de 2017.

Lei nº. **12.965**, de 24 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em: 09 de abril de 2017.

GIORDANELLI, Raffaele et Mastroianni, Carlo. **The Cloud Computing Paradigm: Characteristics, Opportunities and Research Issues.** Palermo, Itália. Consiglio Nazionale delle Ricerche – Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR). 2010.

GNU.ORG, a. Visão Geral do Sistema GNU. Disponivem em:< https://www.gnu.org/gnu/gnu-history.html>. Acessado em :13 de ago. de 2017.

GNU.ORG, b. A Quick Guide to GPLv3. Disponivel em:< https://www.gnu.org/licenses/quick-guide-gplv3.html>. Acessado em:13 de ago. de 2017.

MATHER, Tim; Kumaraswamy, Subra; Latif, Shahed. **Cloud Security and Privacy: Na Enterprise Perspective on Risks and Compliance**. O'Relly.Sebastopol, E. U. A. 2009.

MELL, Peter. Grace, Timothy. **The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology.** National Institute of Standards and Technology (NIST). Gaithersburg, E. U. A. Special Publication 800-145. 2011.

Occhiuzzi, Rogério de Lima. **SSC: Secure Shared Cloud.** Disponível em: <https://github.com/RogerioOcchiuzzi/SSC>. Acessado em: 22 de abril de 2017.

OVH. **Figura: exemplo de como funciona o ataque DDoS**. Disponível em: <https://www.ovh.pt/anti-ddos/principio-anti-ddos.xml>. Acessado em: 03 de novembro de 2016.

RADWARE LTD. **DDos handbook: the ultimate guide to everything you need to know about DDoS attacks**. [S.N.] [S.L.].2015.

REDDY, Bala Narayana. Cloud Computing – Types of Cloud. Disponível em: < http://bigdatariding.blogspot.com.br/2013/10/cloud-computing-types-of-cloud.html>. Acessado em: 30 de abr. de 2017.

SCOBLE, Robert. **Examples of Cloud Computing Services.** Disponivel em: < https://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/examples.html >. Acessado em: 02 de jul. de 2017.

SOSINSKY, Barrie. **Cloud Computing Bible.** ISBN: 978-0-470-90356-8. Wiley publishing, inc. 2011.

SOUZA, Carlos Affonso; **LEMOS**, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editora Associada Ltda, 2016.

TANENBAUM, Andrew S. **Redes de compuitadores.** 4ª ed. Amsterdam, Holkanda, Tradução: Vandenberg D de Souza. Campus. 2003.

THEVERGE. **Figura: mostra o escopo do ataque de 21 de outubro de 2016**. Disponível em: <http://www.theverge.com/2016/10/21/13357344/ddos-attack-websites-shut-down> acessado em: 03 de novembro de 2016.

VICTORIES, Victor. **4 Types of Cloud Computing Deployment Model You Need to Know.** Disponivel em: < https://www.ibm.com/developerworks/community/blogs/722f6200-f4ca-4eb3-9d64-8d2b58b2d4e8/entry/4_Types_of_Cloud_Computing_Deployment_Model_You_Need_to_Know1?lang=en>. Acessado em: 01 de jul. de 2017.

WIKISPACES. **Figura: exemplo de como funciona o multitenancy**. Disponível em: <http://multitenancy-in-saas-paas.wikispaces.asu.edu/>. Acessado em: 03 de setembro de 2016.