# Segurança na Computação em Nuvem: Um Estudo de Caso Sobre a Viabilidade de sua Implantação

**Gabriel Pozzebon**[1]

[1]Curso Superior de Tecnologia em Redes de Computadores – Colégio Técnico Industrial de Santa Maria (CTISM) – Universidade Federal de Santa Maria (UFSM)
Caixa Postal 97015-900 – Santa Maria – RS – Brasil

gabriel.pozzebon@redes.ufsm.br

***Resumo.*** *O presente artigo tem por finalidade realizar um estudo da segurança em Cloud Computing. Devido ao aumento do uso da computação em nuvem, os problemas de segurança foram se agravando, com isso, teve-se a ideia de realizar um estudo bibliográfico sobre o assunto de computação em nuvem e os problemas de segurança existentes e como mitigá-los a ponto de tentar resolver possíveis falhas existentes. Como resultado, esperamos responder as questões de segurança encontradas na nuvem, a fim de viabilizar uma possível implementação de ativos físicos em um ambiente de nuvem seguro.*

**Palavras-chave**: Cloud Computing. Computação em Nuvem. Segurança. Implementação.

***Abstract.*** *This article aims to conduct a study of security in Cloud Computing. Due to the increased use of cloud computing, security issues have worsened, with the idea of conducting a bibliographic study on the subject of cloud computing and existing security problems and how to mitigate them. try to resolve existing flaws. As a result, we expect to address the security issues found in the cloud in order to enable a possible deployment of physical assets in a secure cloud environment*

**Keywords:** Cloud Computing. Cloud computing. Safety. Deployment.

## 1. Conceito de Computação em Nuvem

A Computação em nuvem possibilita acessar recursos computacionais, como por exemplo, servidores e sistemas de armazenamento de maneira prática e a qualquer momento. Para pequenas empresas, por exemplo, adquirir equipamentos e expandir a infraestrutura, bem como adquirir licenças de *software* pode gerar uma grande economia com um ganho no futuro (VERAS, 2012).

## 2. Principais Modelos de Serviços na Nuvem

Serviços na computação em nuvem é o conceito de poder reutilizar componentes, isto é conhecido como "*as a service*" (como um serviço) (VELTE, 2012). Estes modelos de serviços são muito importantes pois definem um padrão de arquitetura para as soluções

 

em computação em nuvem.

Nos últimos anos, a computação em nuvem tem sido responsável por grandes mudanças na área de TI (Tecnologia da Informação), uma vez que essas mudanças têm impactado no crescimento e desenvolvimento de empresas, na medida em que a nuvem oferece cada vez mais serviços, recursos, segurança, facilidades e com custos cada vez mais atraentes para tamanhos diferentes de empresas (OPUS SOFTWARE, 2015).

### 2.1. IaaS – Infrastructure as a Service

IaaS (Infraestrutura como um Serviço) é a capacidade que um provedor de serviços tem de oferecer a clientes uma infraestrutura de armazenamento e processamento de forma transparente. Basicamente, o cliente deixa de adquirir *hardwares* e *softwares* e passa a gerir máquinas virtuais através de virtualização (VERAS, 2012).

### 2.2. PaaS – Plataform as a Service

O ambiente PaaS (Plataforma como um Serviço) fornece uma infraestrutura completa de *hardware*, armazenamento, sistemas operacionais e internet para implantação de aplicativos. Nesse tipo de serviço, o cliente apenas tem que criar e executar suas ações, não precisando se preocupar com detalhes de baixo nível da plataforma (REESE, 2009). O PaaS oferece vários serviços voltados para o desenvolvimento de aplicativos que interagem com dispositivos móveis. (OPUS SOFTWARE, 2015).

### 2.3. SaaS – Software as a Service

O SaaS (Software como um Serviço) é o modelo em que um aplicativo é distribuído como um serviço aos clientes empresariais que o acessam através da internet (VELTE e ELSENPETER, 2012). Exemplos dessa aplicação mais familiares estão as aplicações de gerenciamento de relacionamento com clientes como o *Salesforce*, pacotes de produtividade como o *Google Apps* e o *Dropbox*.

Na figura abaixo, um demonstrativo dos três principais modelos de nuvem, indicando quem pode utilizar tal modelo, os serviços disponíveis e para qual função mais adequada para cada modelo de nuvem.

 

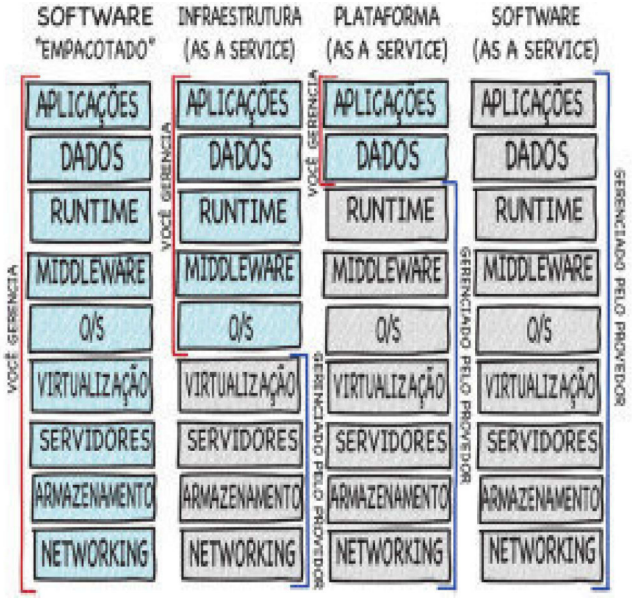


**Figura 1. Modelos de Nuvem SaaS, PaaS, IaaS.**
**Fonte: Opus Software**

## 3. Segurança na Computação em Nuvem

A segurança na computação em nuvem não é diferente da TI convencional, no entanto, com os diferentes modelos de implantação apresentam riscos diferentes (GURKOK, 2014). Muitas das ameaças podem ser combatidas com práticas de segurança simples, enquanto outras exigem soluções mais específicas da nuvem, uma vez que cada arquitetura pode ter diferentes níveis de vulnerabilidade o que afeta diretamente a sua segurança frente os aspectos de gerenciamento da nuvem (*NIST*, 2011). O acesso a recursos podem ser garantidos com práticas que podem aumentar a segurança, como o uso de senhas fortes, *tokens*, cartões de segurança e biometria. A identidade digital um método eficiente de se prover segurança, podendo ser usada não só na nuvem, mas também na rede local o que torna a segurança de dados flexível em um ambiente de TI (VACCA, 2016).

### 3.1. Problemas Importantes de Segurança e Privacidade

Devido ao aumento da utilização da computação em nuvem, muitos problemas foram surgindo em decorrência desse aumento. A computação em nuvem pública representa uma mudança no paradigma das normas convencionais de uma infraestrutura, pois move tudo que era concentrado fisicamente em um ambiente conhecido, para uma infraestrutura de uma organização distante, onde aplicações de diferentes clientes também podem operar.

Governança

A governança implica no controle e supervisão pela organização em relação a políticas, procedimentos e padrões. Com a ampla disponibilidade de serviços de computação em nuvem, a falta de controle sobre funcionários pode ser um problema, embora a computação em nuvem simplifique a aquisição da plataforma, não deixa de exigir

 

menos governança sobre os sistemas. Se ações de governança não forem tomadas, as políticas e procedimentos para privacidade, segurança e supervisão podem não ter a devida atenção, podendo assim, sistemas vulneráveis serem implantados sem consentimento, gerando um custo acima do normal, sublocando recursos para fins diversos que não são autorizados, o que pode prejudicar ou criar problemas.

### Segurança dos Dados

A criptografia é o ponto chave da segurança dos dados, usando de métodos matemáticos, a criptografia mascara as informações e só são reveladas às partes interessadas com o uso de uma chave de descriptografia possuída pela parte autorizada. A criptografia impede que uma pessoa ou parte que não esteja autorizada a ver o conteúdo, tanto quando os dados estão em trânsito ou armazenados na nuvem (VACCA, 2016).

O controle de acesso pode se tornar um problema devido ao modo que a nuvem oferece acesso aos dados nela contida (BUYYA, BROBERG e GOSCINSKI, 2011), com a perda da confidencialidade, integridade ou disponibilidade os clientes devem entender a extensão da proteção que a nuvem oferece para que possam compreender o risco racional, dependendo do nível de impacto, baixo, médio ou alto a nuvem pode oferecer uma determinada proteção aos dados e sistemas de acordo com estes níveis.

As normas da *FIPS* (*Federal Information Processing Standart*) ditam a adequação da nuvem para armazenar e processar os dados dos clientes variando no nível de impacto e as garantias de proteção para estes dados. Essa capacidade de proteger os dados varia de acordo como são acessados os dados, podendo ser em trânsito para um provedor ou de algum provedor onde os dados do cliente devem estar protegidos, da mesma forma se um cliente quiser baixar estes dados, os mesmos devem estar protegidos na transferência (*NIST*, 2010).

### *Hashing*

*Hashing* é utilizado quando necessita de proteção unilateral e não-reversível, isto é, quando um hash é gerado, fica disponível apenas para uma chave, e nenhuma outra chave é gerada para realizar o desbloqueio. Um exemplo de utilização é para a armazenagem de senhas. Além disso pode ser utilizado para proteger os dados na nuvem, incluindo usuários não autorizados e maliciosos e não-autorização de acesso (ERL, MAHMOOD E PUTINI, 2013).

### Segurança de Identidades

A segurança de identidades é a chave para a segurança flexível dos dados em um ambiente de nuvem (BUYYA, BROBERG e GOSCINSKI, 2011). Uma assinatura digital deve assegurar a autenticidade de uma mensagem e o não repúdio, ou seja, deve dificultar uma parte a forjar uma assinatura digital válida e utilizá-la em mensagens diferentes (VACCA, 2016).

 

A criptografa assimétrica é comumente utilizada para esse tipo de segurança em ambientes de nuvem, então se possuir a chave pública gerada e quiser a assinatura digital confiável enviada pela rede, é preciso solicitar a outra ponta que assine ou criptografe estes dados, assim, se for possível descriptografar os dados, é possível saber que estes dados foram criptografados pela parte autorizada, pois só ela conhece a chave privada (VACCA, 2016).

## 3.2. Princípios da Segurança

Em um ambiente de TI convencional é comum observar o detrimento da segurança visando o bom funcionamento dos sistemas. Tal fato, cria um ambiente desprotegido e suscetível a ataques externos. Porém, quando os ativos se encontram na mão de outras pessoas, a segurança deve ser tratada com criticidade (KANDUKURI, 2009).

Os sistemas computacionais nunca estarão livres de terem vulnerabilidades, pois foram projetados e testado por humanos, e estes sempre cometem erros, por exemplo, a construção de um *hardware*, a criação de um *software* sempre haverá uma falha, mais conhecida por vulnerabilidade, ou fraqueza. Essas fraquezas podem ser exploradas por invasores, geralmente tentando obter informações e dados sobre sistemas de empresas (VACCA, 2016).

De modo geral, a computação em nuvem oferece um maior ganho com a sua implementação, reduzindo os custos e aumentando a produtividade das empresas, com um acesso amplo a rede, agrupamento de recursos e serviços tornou a computação em nuvem popular na TI. Além desses pontos, a segurança é crucial para a computação em nuvem. A segurança na computação em nuvem não é diferente da TI convencional, no entanto, com os diferentes modelos de implantação apresentam riscos diferentes (GURKOK, 2014).

Seguindo o contexto de comprometer os princípios de segurança na nuvem, alguns pontos críticos encontrados na nuvem não são encontrados na computação convencional, fazendo com que a computação em nuvem possa ser vista como um obstáculo ou dificultador na TI.

### Complexidade dos Sistemas

Um ambiente de computação em nuvem pública é uma plataforma mais complexa que uma TI convencional, devido a seus recursos e componentes que resulta em uma grande superfície de ataque. A segurança não depende apenas de correções e eficácia dos componentes, já que a inclusão de novos e mais recursos a nuvem, aumentam a sua complexidade, o que aumenta uma demanda de manutenções e gerenciamento, o que geralmente se relaciona inversamente com a segurança, dando uma maior vulnerabilidade.

### Ambiente Compartilhado

O compartilhamento de nuvem entre multiusuários pode ser usada como uma brecha de

 

segurança, uma vez que a nuvem coloca uma dependência maior da separação lógica em várias camadas da pilha de aplicativos em vez de uma separação física dos recursos. Um cliente pode explorar as vulnerabilidades dentro da nuvem, ultrapassar as barreiras de separação e obter acesso a dados restritos, o que também pode ser expor os dados a outros clientes da nuvem ou bloquear o acesso a clientes que antes eram autorizados.

Serviços Orientados para a Internet

O serviço em nuvem pública são distribuídos pela internet, o que expõe as interfaces utilizadas pra realizar os acesso a nuvem, agora, os serviços que antes estavam protegidos dentro do *firewall* da empresa, agora estão em uma nuvem pública enfrentando o risco de ameaças de rede que visam roubar os dados. O desempenho e a qualidade via internet também podem ser afetados.

Perda de controle

Os serviços e dados que antes estava sob domínio da TI local, agora estão migrados para a nuvem, o que acarreta numa transferência de responsabilidades para o provedor e uma certa perda de controle sobre os recursos na nuvem contidos, a falta de um contato direto com o provedor de serviços, aumentam essa perda de controle. Esta situação torna a organização dependente da cooperação entre o provedor da nuvem em realizar atividades que abrangem as responsabilidades, como reportar o monitoramento e incidentes. A perda de controle implica em diminuição da capacidade da empresa em manter a consciência sobre a situação operacional, diante disso, a manutenção de responsabilidades pode ser mais desafiadora frente a TI local (JANSEN, GRANCE, 2011).

| **Princípios da Segurança** | **Risco** | **Questionamentos** |
|---|---|---|
| Autenticidade | Verificação da autenticidade das entidades ativas. | Que ações são tomadas para autenticação e controle de acesso dos usuários? |
| Confidencialidade | Ativos de diversos usuários que dividem o mesmo sistema. | Como é realizada a segregação dos dados? |
| Disponibilidade | Recuperação de dados. | Como é garantida a recuperação dos dados? |
| Integridade | Violação dos dados e leis de proteção. | Quais as garantidas de preservação dos dados? |
| Não-repúdio | Análise das ações executadas por usuários dos ativos. | Os usuários são capazes de negarem suas ações? |

**Tabela 1. Princípios da Segurança**

 

## 4. Questões de Segurança Relevantes

Para a realização de uma implantação em computação em nuvem ou migração de ativos físicos para um ambiente virtual, foram levantadas questões sobre a segurança e de que forma poderiam ser mitigadas e amortecidas no seu uso, métodos eficientes e seguros de acesso, recuperação de desastres, entre outras medidas. A tabela 2 abaixo, mostra questões levantadas pelo autor com base em pesquisas bibliográficas, dúvidas surgidas, o risco impactado na adoção e uma forma de mitigar as dúvidas recorrentes.

| Questões | Dúvidas | Risco | Medida esperada |
|---|---|---|---|
| Formas de acesso | Como prover acesso seguro a nuvem? | Alto | Através de uma *VPN* (*Virtual Private Network*). |
| Recuperação de Dados | Como recuperar eventuais dados perdidos? | Alto | A nuvem deve prover plano de recuperação. |
| Controle de acesso | De que forma é realizado o controle de acesso? | Alto | Geração de *tokens* e identidades digitais para os clientes autorizados. |
| Backup dos ativos | Qual a frequência dos backups dos ativos? | Médio | A nuvem deve possuir *backups* das Máquinas Virtuais pelo menos uma vez ao mês. |
| Registro de controle | É possível ter registros sobre acessos e alterações? | Médio | Através de *LOGs* gerados, podendo ser solicitados esporadicamente pelo cliente ao provedor de nuvem. |

**Tabela 2. Requisitos de Segurança**

## 5. Conclusão

Hoje a internet é usada para praticamente tudo, e como consequência disso, a Computação em Nuvem cresceu nos últimos anos e isso implicou em medidas de segurança mais robustas e eficientes para o meio. Os sistemas computacionais nunca estarão livres de terem vulnerabilidades, pois foram projetados e testado por humanos, e estes sempre cometem erros, por exemplo, a criação de um software sempre haverá uma falha ou fraqueza. Essas fraquezas podem ser exploradas e podem causar danos ou roubo de dados importantes de empresas que utilizam a nuvem. Por isso, não basta apenas ter um controle rigoroso de acesso, se durante o processo de transferência de dados ou armazenagem ocorrem falhas de segurança. É preciso pensar desde o acesso

 

até a forma que é feito a armazenagem e controle do provedor de nuvem. Para a empresa, não faz sentido ter uma forte segurança no acesso, com tokens, por exemplo e no provedor, os dados ficarem expostos a acesso de funcionários não autorizados do provedor de nuvem.

## Referências


Buyya, R., Broberg, J. e Goscinski, A. M. (2010) “Cloud Computing: Principles and Paradigms” 1. Ed. John Wiley & Sons, 660 páginas.

NIST – National Institute os Standards and Technology(2011) “Chapter 14: Cloud Computing Securitu Essentials and Architeture”. Disponível em: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919233

Castro, R., C., C. e Sousa, V., L., P., “Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança”, (2010), 7 páginas, Disponível em: http://infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud(1).pdf

Erl, T., Mahmood, Z. e Puttini, R. “Coud Computing: Concepts, Technology & Architecture” (2013), Prentice Hall, Upper Saddle River, New Jersey, 528 páginas.

Gurkok C., “Network and System Security. Chapter 4. Securing Cloud Computing Systems”. 2. Ed. Elsevier Inc.,(2014), Waltham, 58 páginas.

Jansen, W.; Grance, T., “Guidelines on Security and Privacy in Public Cloud Computing”, (2011), NIST – National Institute os Standards and Technology, 80 páginas, Disponível em: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Kandukuri, Balachandra Reddy, V, Ramakrishna Paturi, RAKSHIT, Dr. Atanu. (2009) “Cloud Security Issues. IEEE International Conference On Services Computing”, Pune, India, n., 520 páginas.

Opus Software Comércio e Representações Ltda, “Computação em Nuvem”, (2015), 1. Ed. Opus Software, São Paulo.

Rao, M. N., “Cloud Computing”, (2015) 1. Ed. PHI Learning Provate Limited, Delhi, 204 páginas.

Reese, G. “Cloud Application Architetures”, (2009), 1. Ed. O’Reilly Media, 206 páginas.

Vacca, J. R., “Cloud Computing Security Foundations and Challenges”, (2016), 1. Ed. CRC Press, Taylor & Francis Groupe, Boca Raton, 496 páginas.

Velte, A. T., Velte, T. J., Elsenpeter, R., “Computação em Nuvem: Uma abordagem Prática”, (2012), Alta Books Editora, Rio de Janeiro, 352 páginas.

Veras, M., “Computação em Nuvem: Nova Arquitetura de TI”, (2012), 1. Ed. Editora Brasport, São Paulo, 215 páginas.


 