REVISTA FATEC SEBRAE EM DEBATE:
Gestão, Tecnologias e Negócios
Volume 05 | Número 09 | JUL - DEZ. 2018 | ISSN: 2358-9817

ANÁLISE DE VULNERABILIDADES EM CLOUD COMPUTING

Estefânia Pianoski Arata

Cristiane Fernandez Rodrigues

Renata Farragoni

Resumo:

Computação em nuvem ou *Cloud Computing é* um termo que surgiu aproximadamente no ano de 2008 e vem ganhando cada vez mais força no mercado e no cotidiano das pessoas, por possuir diversas vantagens. Uma das maiores está em ter acesso às informações de qualquer lugar do mundo, em qualquer dispositivo conectado a internet, pois o armazenamento das informações é feito em equipamentos virtuais. Diante de tantas facilidades a computação em nuvem também está vulnerável a ameaças, sujeito a riscos, os quais podem prejudicar os ativos das organizações. Com isso, este artigo propõe-se apresentar os principais riscos em *Cloud Computing* para as organizações.

Palavras - chave: *Cloud Computing*, riscos, computação em nuvem.

Abstract:

Cloud computing is a term that has emerged approximately in 2008 and has been gaining strength and popularity in the market and in people's the daily life. Amount its many advantages, one of the largest no doubt, is the access to information from anywhere in the world, from any device connected to the Internet, since the information is stored using virtual memory.
However, even though there are many advantages to cloud computing, there is also the danger of being vulnerable to risks and threats, which can, in turn, put organizational assets also at risk.
This article will present the main Cloud Computing risks faced by organizations in today's society.

Keywords: Cloud Computing, Risks, Cloud Computing.

Introdução

Segundo as pesquisas realizadas pela IDC o crescimento, da *Cloud Computing* no Brasil será de aproximadamente 74% até para o fim do ano de 2015 e o *Gartner* estima para 2017 que os negócios na área da computação em nuvem devem gerar uma receita em torno de U$$ 4,5 bilhões.

Diante do crescimento e investimento em *Cloud Computing*, as organizações devem reavaliar os seus conceitos, visto que é possível ter acesso as informações através de um dispositivo móvel como *tablet*, *smartphone* ou um notebook de qualquer lugar do mundo, apenas com acesso a internet.

Embora muitos usuários finais não percebam, eles utilizam os serviços que estão em *cloud* no seu cotidiano, como por exemplo, quando utilizam o NetFlix ou usam Dropbox para compartilhamento de arquivos ou ainda quando acessam os seus e-mails no Gmail.

Os serviços que estão na nuvem são de fácil utilização e transparência e estão presentes em toda a internet, porém muitos usuários finais não sabem que estão utilizando essa tecnologia.

Os usuários finais que tem conhecimento dos serviços que estão em *Cloud Computing* ainda divergem de opiniões quando o assunto é segurança, pois a maioria tem receio em utilizar os recursos disponíveis. Para alguns especialistas no assunto o que há é o desconhecimento sobre o assunto e isso traz a insegurança

Quando o tema é informação corporativa e computação em nuvem, a segurança passa a se concentrar na informação, pois a infraestrutura já não é mais a principal barreira.

Sendo assim, é necessário aplicar controles diferenciados para as informações, como a utilização de soluções de criptografias, controle de acesso e compartilhamento rigoroso. É importante lembrar que a área segurança da informação deve assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações estratégicas para o negócio.

1. FUNDAMENTAÇÃO TEÓRICA

O objetivo desse artigo é apresentar os principais riscos em *Cloud Computing* que as organizações estão enfrentando, porém para contextualizar será descrito o seu conceito, suas vantagens e desvantagens e por fim os riscos apontados por outros autores ou através de análise de riscos.

1.1 O que é *Cloud Computing*

Computação em nuvem é um termo em evolução, separa informações e recursos de sua estrutura básica, e os mecanismos utilizados para entregá-los, Paula M. (2007).

Muitos institutos, autores ou organizações definem o termo Computação na Nuvem, porém o NIST - *National Institute of Standards and Technology*, uma entidade

governamental americana com publicações reconhecidas mundialmente define *Cloud Computing* através da Figura 1.

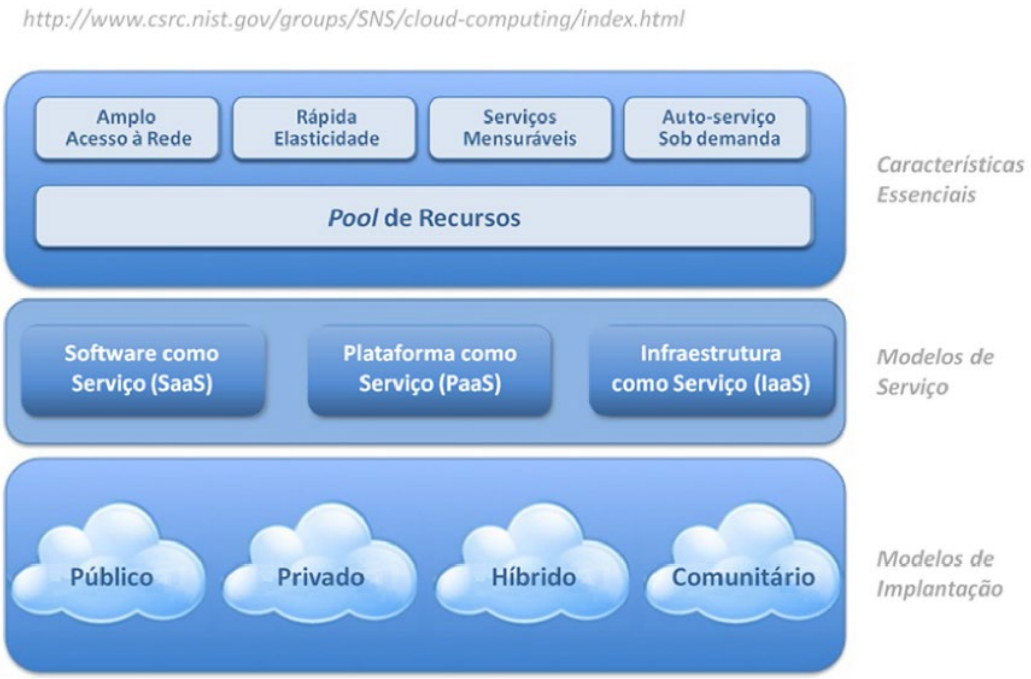

Figura1 - Modelo de Computação em Nuvem segundo NIST.

Por outro lado a CSA - *Cloud Security Alliance*, explica os três modelos de serviços para *cloud*, citados pelo NIST como:

- Saas (*Software* em Nuvem como Serviço), é um formato no qual se usa software para controlar e gerenciar a aplicação em nuvem, sendo as aplicações acessíveis por vários dispositivos através de uma interface simples para o usuário final, cliente, como por exemplo*: Webmail*.

- PaaS (Plataforma como Serviço), que utiliza apenas banco de dados ou WebService. Nessa arquitetura o consumidor tem controle sobre as aplicações implementadas e possivelmente configurações da aplicação referente ao ambiente do servidor;

- IaaS (Infraestrutura como Serviço), quando a nuvem está em uma parte do servidor. Onde o consumidor tem controle sobre o sistema operacional, armazenamento, aplicações implementadas e possivelmente contro-

le limitado de componentes específicos de rede, exemplo: *firewalls* no servidor.

1.2 Vantagens da Computação em Nuvem

A computação em nuvem, quando vista junto com os negócios para uma organização ela melhora a colaboração, agilidade, dimensionamento e disponibilidade, e oferece o potencial para produção através da computação otimizada e eficiente.

A utilização dessa tecnologia também traz como benefício a diminuição dos custos para a organização, pois não há a necessidade de aquisição de um Data Center e ou equipamentos.

Em questão de disponibilidade é possível acessar as informações a qualquer momento e de qual lugar, desde que se tenha permissão e acesso a internet. Utilizando o exemplo do Skydrive, utilizando qualquer dispositivo móvel é um aplicativo de *Cloud Computing,* o usuário final entra com o seu *login* e senha e tem acesso as suas informações.

1.3 Desvantagens da Computação em Nuvem

Com o avanço do*Cloud Computing* há os partidores e opositores. Isso deixa muitos com dúvidas ao usar algumas das tecnologias em “nuvem”, lembrando que muitos utilizam e nem sabem que estão usufruindo da computação em nuvem.

São muitos os usuários da computação em nuvem, que não conhecem a tecnologia mostram as suas desvantagens, afinal são muitos os riscos apresentados pela *cloud*.

Temos a questão da portabilidade dos dados, rastreabilidade em caso de perícia forense entre outros fatores que dependendo da ótica são consideradas grandes desvantagens deste modelo.

1.4 Ativos

Para avaliar um risco é preciso conhecer os ativos da organização, segundo a ABNT NBR ISO/IEC 27001:2006 ativos para a organização é qualquer coisa que tenha valor para a mesma, como: informações impressas e eletrônicas, softwares, hardwares, pessoas, instalações, serviços entre outros.

Sendo assim, conhecendo os ativos e selecionando o que está em *Cloud Computing* o próximo passo é estabelecer a sensibilidade e a importância do ativo para a organização através de uma análise de risco contemplando, dentre outros fatores, os pilares de segurança da informação:

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. [NBR ISO/IEC 27001:2006]

- Integridade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidade ou processo autorizado. [NBR ISO/IEC 27001:2006]

- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. [NBR ISO/IEC 27001:2006]

1.5 Riscos

Embora *Cloud Computing* possua benefícios alguns riscos preocupantes para os usuários e para as organizações que dela utilizam são evidentes.

Risco de segurança da informação conforme a ABNT NBR ISO/IEC 2005:2008 é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou um conjunto de ativos, desta maneira prejudicando a organização.

1.6 *Cloud Computing* e segurança da informação

Atualmente a segurança da informação para o cotidiano tanto da pessoa física como da pessoa jurídica está cada vez mais em alta, afinal o conhecimento e a informação são de grandes valores para ambos. Com isso é de suma importância proteger

as informações em “nuvem”, sabendo que os sistemas em redes estão vulneráveis a diversos tipos de ameaças, como por exemplo, a falta de conectividade, pensando que todas as informações críticas estão disponíveis em um servidor *Web*.

Sabendo dessa grande quantidade de informações que se encontram em *Cloud Computing*, o mesmo se torna alvo de ataques, comprometendo os pilares da segurança da informação, integridade, confidencialidade e disponibilidade, dessa maneira pararem todo o serviço que está na “nuvem”, muitas vezes pode interromper os serviços de uma organização.

1.7 *Cloud Computing* privada

A infraestrutura da nuvem é operada exclusivamente por uma única organização. Ela pode ser gerida pela organização ou por terceiros, e pode existir no local ou fora do ambiente da organização.(Segundo *Cloud Secury Alliance,* 2009).

1.8 *Cloud Computing* pública

A infraestrutura de nuvem é disponibilizada ao público em geral ou a um grande grupo industrial e é controlada por uma organização que vende os serviços de nuvem. (Segundo *Cloud Secury Alliance*, 2009).

2. METODOLOGIA

Para o desenvolvimento deste artigo foram utilizadas bibliografias, sites, normas e outros artigos que referenciam os riscos presentes em Cloud Computing.

Pode-se perceber que em muitos casos é utilizada análise de riscos, baseada na ABNT NBR ISO/IEC 2005:2008 para identificar, classificar e apresentar os maiores riscos nas soluções de computação na nuvem.

No decorrer deste artigo serão apresentados os riscos oferecidos pelo uso da computação em nuvem tanto para usuário final como para organizações.

3. DESENVOLVIMENTO

Compreendido o que é *cloud computing*, seus tipos, vantagens e desvantagem, vem a necessidade de entender quais são os riscos atrelados ao seu uso.

De acordo com as pesquisas realizadas pelo De Paula e a CSA - *Cloud Security Alliance* os riscos são compartilhados tantos com as organizações como para os usuários finais.

No decorrer deste artigo serão explanados os riscos para ambos os cenários, e para os usuários finais algumas dicas de como minimizar os impactos.

3.1 Riscos para as organizações

O crescimento acelerado da computação em nuvem fez com que as organizações começassem a se preocupar com os riscos oferecidos pela nova tecnologia.

Para as organizações esses riscos, muitas vezes, estão ligados as questões contratuais e legais relacionadas ao local onde os dados estão armazenados e, conseqüentemente, submetido a legislação local.

Na Tabela 1 serão expostos alguns riscos identificados por especialistas em *Cloud*, riscos e profissionais da área de Tecnologia da Informação relacionados ao uso dessa nova tendência de mercado para as organizações.

Risco	Descrição
Não atendimento ao requisito contratual	Os contratos com os provedores de serviços na nuvem não estão adequados as necessidades das organizações
	A política para retenção de dados do provedor não está adequada as regulamentações da organização.
Os logs não armazenam todas as informações	Os logs não armazenam todas as informações necessárias para atender os requisitos legais da organização
Acesso indevido	O provedor de serviço pode não realizar o controle adequadamente para atender as necessidades da organização, como no corte de acesso imediato
Indisponibilidade das informações	Não há visibilidade dos controles implementados nos aplicativos para garantir a segurança
Vazamento de informações	Os serviços em *cloud* estão vulneráveis a ataques de DDos
Perda da continuidade da operação	Os provedores de serviço de *cloud* não utilizam ferramentas e interface compatíveis uma com as outras, tornado os seus clientes dependentes.

Indisponibilidade das informações	Como são os provedores realizam a gestão de seus ativos as organizações clientes não tem o controle das atualizações aplicadas nos ativos, ficando refém dos acordos em contrato.
Impossibilidade de rastreamento nos casos de fraude	Como a organização não faz à gestão dos ativos, em caso de fraudes a rastreabilidade é um fator crítico.
Acesso privilegiado de usuários desconhecidos	Muitos usuários que prestam serviço de *cloud* tem acesso de administrador para realizar a gestão do ativo e consequentemente acesso as informações privilegiadas.
Não atendimento ao requisito contratual	Os provedores de serviço não são aderentes a todas as regulamentações o que pode causar problemas legais a organização.
Indisponibilidade das informações	Os provedores têm as suas próprias políticas de recuperação de dados em caso de desastre e esse tempo pode não atender a organização.
Indisponibilidade das informações	Como todas as informações estão trafegando pela internet o tempo de resposta pode não atender as necessidades da organização, causando indisponibilidade

Tabela 1-Riscos e sua descrição para as organizações. Fonte: Próprio autor.

É importante salientar que os riscos citados podem ser alterados dependendo da forma de *cloud* utilizada, se for utilizada uma Nuvem Privada, por exemplo, os riscos tendem a diminuir, pois o ambiente possui uma gerência centralizada e não há o compartilhamento de ativos entre organizações.

O importante é antes de tomar a decisão de contatar provedores de serviço em nuvem é ter a opinião de um especialista em direito e saber exatamente o que será contratado, os SLAs e a forma de gestão desse contrato.

3.2 Riscos para os usuários finais

A grande maioria dos usuários dos serviços disponíveis na internet desconhecem que muitos deles utilizam a tecnologia de computação em nuvem e conseqüentemente não imaginam os riscos atrelados a eles.

A Tabela 2 apresenta os principais riscos atrelados ao uso dos serviços de *cloud* para os usuários finais de acordo com a opinião de especialistas no assunto.

Risco	Descrição	Dicas para minimizar o risco
Roubo de informação	Os usuários podem ter os seus dados roubados devido ao uso de senhas fracas	Utilização de senhas fortes (no mínimo 8 caracteres, contemplando letras, números e caracteres especiais)
Perda da informação	Os usuários, por desconhecimento	Compartilhar somente as in-

	dos termos de uso do site, compartilham seus arquivos de forma arbitrária	formações pertinentes e estar atento aos termos de uso do site.
Exposição da imagem	Os usuários desconhecem os meios de proteção para as suas informações confidenciais	Utilizar meios para proteger as informações, tais como criptografia, uso de senha para compactar arquivos.
Uso indevido do serviço	Os usuários não leem os termos de uso dos sites e em muitos casos utilizam de forma errada o serviço	Realizar a leitura dos termos de uso antes de utilizar os serviços
Roubo de informações	Os dispositivos utilizados pelos usuários não estão com o nível adequada de proteção contra software malicioso	Atualizar ou instalar uma solução contra software malicioso
Acesso indevido	Os usuários utilizam a opção de lembre-me para facilitar o próximo acesso	Retirar a opção de lembre-me
Perda da informação	Os usuários não fazem cópias das informações que disponibilizam na nuvem, mantendo como única cópia	Realizar cópias de segurança em outros locais e/ou dispositivos regularmente.
Acesso desnecessário	Muitos usuários mesmo não utilizando mais um serviço de nuvem mantem o seu acesso ativo desnecessariamente.	Realizar cópias das informações e excluir o acesso ao serviço

Tabela 2–Descrição dos riscos e dicas para minimizar o impacto para os usuários finais.

Fonte:Próprio autor

O que pode-se perceber é que a maioria dos riscos atrelados aos usuários finais estão ligados a falta de conhecimentos em segurança da informação e a falta de leitura dos termos de uso dos serviços.

4. CONCLUSÃO

Cloud Computing é inevitável tanto para os usuários finais como para as organizações, porém percebe-se que há muitas lacunas em relação a segurança das informações.

Os riscos listados apresentam apenas uma pequena parcela do que esta por vir. As organizações devem investir cada vez mais em profissionais com especialidade em C*loud Computing* e riscos, porque não basta ter conhecimento, é preciso gerenciá-los de forma efetiva, porque os riscos estão presentes em todos os lugares, principalmente quando se fala em Tecnologia.

Sendo assim é indispensável que as organizações adotem um processo de gestão de risco, baseado em metodologias disponíveis no mercado, como a ISO 27005

para gerenciar os riscos com uso de *Cloud*. A implementação de normas e procedimentos com foco em segurança da informação completam o processo.

Para os usuários finais dos serviços de *cloud*, medidas de segurança podem ser inseridas no seu dia a dia como ler atentamente os termos de uso e as políticas dos servidores em nuvem, evitando assim surpresas posteriores com o não atendimento de suas necessidades.

Organizações como a *Cloud Security Alliance* estão empenhadas em estudar e desenvolver padrões de computação em nuvem para elevar os níveis de segurança nos serviços que estão na nuvem.

Com base nos estudos dos autores referenciados nesse artigo conclui-se que os usuários finais necessitam de treinamentos voltados para o tema de segurança da informação e jurídico para entender corretamente os termos de uso.

Para as organizações a contratação de especialistas no tema e uma análise de risco podem indicar qual o melhor serviço de nuvem deve ser contratado. No geral os riscos atrelados tanto aos usuários finais como para as organizações vão existir, o importante é ter conhecimento de como minimizá-los.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT, NBR ISO/IEC 27001. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação** — Requisitos. ABNT, 2006.

ABNT, NBR ISO/IEC 27005. **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. ABNT, 2008.

Introducing Guidance for Critical Areas of Focus in Cloud Computing. Disponível em: https://cloudsecurityalliance.org/research/security-guidance. Acesso em 20/08/2014.

CARNEIRO, Ricardo José Gouveia(1); RAMOS, Cleisson C. L. Costa, **A Segurança na Preservação e uso das Informações na Computação nas Nuvens**, Faculdade de Tecnologia de João Pessoa – João Pessoa

Cloud Computing: o poder da nuvem no Brasil. Disponível em: http://stefanini.com/br/2014/04/cloud-computing-o-poder-da-nuvem-brasil/. Acesso em 20/08/2014.

CLOUD COMPUTING + TENDÊNCIAS – Uma nuvem de oportunidades.

Disponível em: https://chapters.cloudsecurityalliance.org/brazil/artigos/. Acesso em 21/08/2014.

CSA – *Cloud Security Alliance* – **Guia de Segurança para Áreas Críticas Focada em Computação em Nuvem**; V2.1; junho 2010.

DE PAULA, Anchises M. G.; **Fog Computing- As falhas e riscos da Computação em Nuvem**; 2011.

IDC apresenta previsões para a evolução do setor das TIC em Portugal: Disponível em:http://www.idc.pt/press/pr_2014-02-10.jsp. Acesso em 24/08/2014.

RITA C. C. de Castro, et al; **Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança**, pp7, Universidade Estadual do Ceará – Ceará.

OUCH! – Using the Cloud Securely, September 2014. Disponível em:

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_en.pdf. Acesso em 10/09/2014.

TAURION, Cesar. **Computação em Nuvem Transformando o mundo da Tecnologia da Informação**, Rio de Janeiro: Brasport (2009).