



**FACUDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE  
SERGIPE – FANESE**

**NUCLEO DE POS-GRADUAÇÃO E EXTENSÃO LATO SENSU  
MBA EM REDES E SEGURANÇA DA INFORMAÇÃO**

**“CLOUD COMPUTING”  
UMA ABORDAGEM PRÁTICA**

**ADRIANO BARROS PEREIRA**

**ARACAJU-SE**

**2016**

**ADRIANO BARROS PEREIRA**

**“CLOUD COMPUTING”  
UMA ABORDAGEM PRÁTICA**

Artigo Científico apresentado ao núcleo da Pós-Graduação e extensão da Faculdade de Administração e Negócios de Sergipe como exigência para obtenção do Trabalho de Conclusão do Curso de Pós Graduação Lato Sensu MBA em Redes e Segurança da Informação.

**ARACAJU – SE**

**2016**

## **Resumo**

Neste artigo veremos como surgiu a nova tecnologia para solucionar alguns problemas como troca de informações, armazenamento dos arquivos, downloads, uploads, sites de músicas, vídeos, entre outros tipos de arquivos, assim evitando estar transportando hardware como HD's, Pen Drive, etc. e sim ter acesso de qualquer lugar do mundo apenas basta ter acesso à internet, entretanto nos dias de hoje a tecnologia vem se inovando a cada dia que passa, um exemplo para ter acesso a internet pode ser através dos smartphones (celulares) independente do modelo do mesmo basta ter apenas o aplicativo que venha a dar acesso à tecnologia chamada 'Cloud Computing', em português Computação em Nuvem.

Palavras Chaves: Tecnologia. Armazenamento. Cloud Computing. Internet

## **Abstract**

In this article we will see how the new technology has emerged to solve some problems with information sharing, file storage, downloads, uploads of music sites, videos, and other types of files, thus preventing be carrying hardware such as hard drives, USB flash drive, etc. but access from anywhere in the world just enough to have access to the internet, but these days the technology has been innovating every day, an example to access the internet can be through smartphones (cell) regardless of model the same just have only the application that will give access to the technology called "Cloud Computing" in Portuguese Cloud Computing

Key Words: Technology. Storage. Cloud Computing. Internet

## 1. Introdução

Até a pouco tempo atrás a “cloud computing” era tido como uma tendência que ninguém iria precisar fazer mais instalação dos programas em seu computador para fazer as tarefas básicas (como planilhas) ou mesmos os trabalhos mais complexos, pois seria feito tudo através da internet [1].

A ideia central da Computação em Nuvem ou em inglês “Cloud Computing” é para permitir a transição da computação tradicional para o um novo modelo onde o consumo dos recursos computacionais como exemplo: armazenamento, processamento, banda de entrada e saída dos dados será feito através dos serviços prestados por uma empresa que faça esse tipo de serviço. Uma forma de mostrar como demonstrar esse tipo de serviço é no final do século XIX, durante a Revolução Industrial que as grandes indústrias tinham que fabricar a sua própria energia elétrica ou mecânica, mas nos dias de hoje as fabricas de grande porte faz com que a energia venha de outras empresas que preste serviço de energia elétrica ou mecânica e tenha que pagar pelo que for consumido.

O seguimento da computação em Nuvem vem daí, pois os recursos passarão a ser de empresa que tenha a especialização, assim ficando com a responsabilidade da gestão e comercialização através de serviços especializados.

A função desse artigo é descrever como surgiu, como serão no futuro, alguns riscos, as vantagens, a segurança e alguns tipos de ataques mais comuns na rede, assim obtendo o uso desse tipo de serviço que são utilizados por empresas de pequeno, médio e grande porte.

## 2. Desenvolvimento

### 2.1 O que é Computação em Nuvem?

O conceito mais resumido é que a computação em nuvem é toda operação realizada entre um computador e algum serviço de armazenamento on-line como servidores.

O conceito mais real é que todos os seus arquivos podem ser acessados pela internet, livrando o computador da instalação de aplicativos para a realização das tarefas, pois é tudo feito através da internet, quando conectado no serviço da “nuvem”, assim podendo salvar ou acessar o trabalho que você fez de qualquer lugar ou em qualquer hora que desejar usar um desses arquivos que estejam na “nuvem” daí que vem o termo “Computação na Nuvem”.

Outro conceito é uma nova tecnologia que permite acesso remoto a programas (softwares), arquivos (documentos, músicas, jogos, fotos, vídeos) e serviços por meio da internet, porque os arquivos estão sempre à disposição dos usuários a hora que for possível, assim esses arquivos ficam disponíveis na internet, e sem que precise fazer instalação de programas e sim apenas um acesso à web.

Fazendo uma análise mais profunda os arquivos que são colocados na nuvem ficam em um servidor que está em algum lugar do mundo, assim quando acessa o serviço o computador troca informações com o servidor, assim fazendo a liberação do acesso aos arquivos esse usuário vem a ter todo o direito de observar todos os arquivos do site, algumas empresas como Google, Microsoft, Yahoo entre outros disponibiliza desse tipo de serviços.

A função da computação em nuvem e o corte de custos operacionais, e o mais importante é que as empresas de TI veem a concentrarem nos projetos de estratégias do que ter o Data Center em pleno funcionamento (Antony, 2012).

Na imagem a baixo dá para se ter uma ideia do que é a computação em nuvem, e que pode ser colocado na nuvem através de serviços prestados como se estivesse na própria empresa.

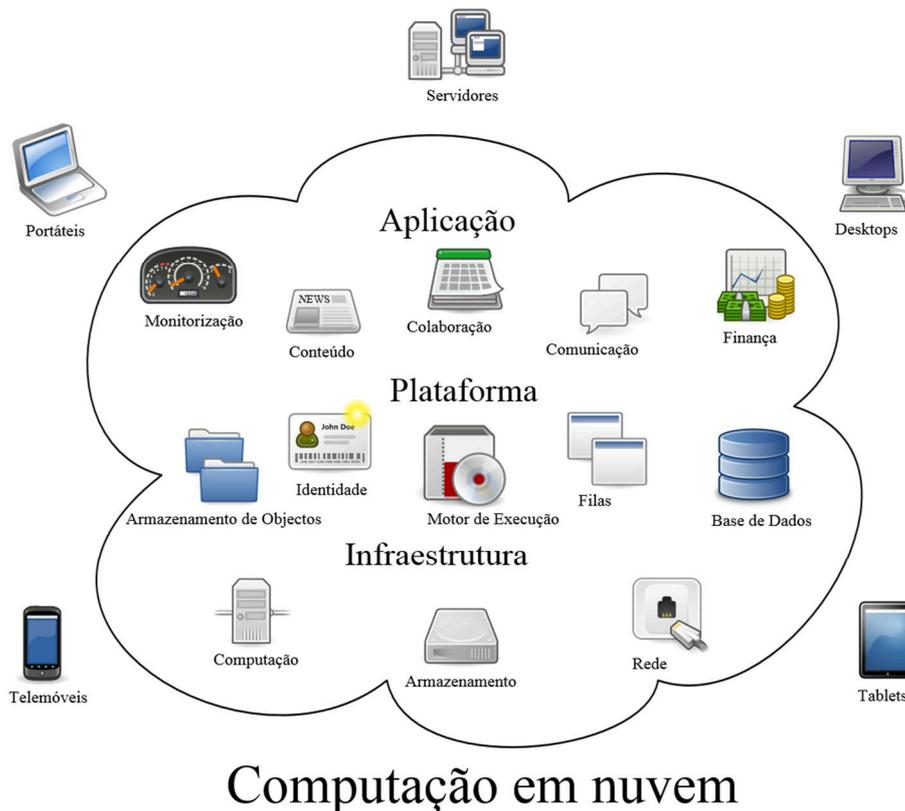


Fig 1. A nuvem (*cloud*) o símbolo da Internet. (Fonte: Wikipédia)

Com esse modo, os supercomputadores são usados somente por aqueles que realmente precisam ter algo na nuvem para que tenha sistema ou mesmos arquivos na nuvem, pois o mundo vem sendo mais conectado e trazendo mais versatilidade, segurança, rapidez, e disponibilidade com esse tipo de tecnologia que vem cada vez mais crescendo nos tempos de hoje.

Os usuários têm a possibilidade de fazer um acesso em qualquer lugar e também com qualquer aparelho que tenha acesso a internet, e deixar os arquivos como fotos, músicas, documentos e ferramentas em unidades físicas tipo, pen drives, HD's, etc. o que precisa é apenas o acesso à internet para acessar os arquivos que estão na nuvem.

Algumas empresas já aderiram esse tipo de tecnologia, a pioneira foi a Google que vinha com o uso gratuito e online desde 2002, que tinha lançado os primeiros programas como agenda e edição de texto tudo online. Hoje em dia, o Google tem os Docs, que são integrados às contas do Google (Gmail)

que é o mais clássico exemplo que pode ser feito online, ou seja, usando a computação na nuvem [4].

O Google vem mostrando um padrão de programas que pode ser usado na nuvem que tem como exemplo o Google Drive. Mas outras empresas vêm abraçando essa ideia que a Google já vem fazendo como a Microsoft, Dropbox, Cubby, entre outras que vem criando os mais diversos serviços e produtos para os usuários da internet.

## **2.2 Surgimentos da tecnologia “Cloud Computing”**

Atualmente em qualquer lugar pode ter acesso a internet só basta ter um aparelho eletrônico como um computador, notebook, smartphone entre outros, também precisa usar a segurança necessária, como senha de acesso, e ter a velocidade boa para fazer o acesso à internet, como a tendência é sempre procurar a melhor velocidade para comunicação a cada dia. A Computação em Nuvem é uma das tecnologias que vem se evoluindo constantemente, permitindo o armazenamento, a gestão, o compartilhamento e disponibilização dos dados tipo: softwares, aplicativos e serviços através da internet.

No ano de 1960 ele disse que “A computação algum dia poderia ser considerada como uma utilidade pública.” John McCarthy assim também discutindo a ideia de que a computação seria compartilhada (time sharing), ou seja, apenas com um computador poderia ser usado por dois ou mais usuários simultaneamente, também tinha que realizar várias tarefas no mesmo momento, aproveitando o tempo ocioso entre cada processamento.

Junto a ele o físico Joseph Carl Licklider, cientista da ARPA (Advanced Research Projects Agency), que era o pioneiro na criação da Internet de forma que conhecemos hoje, também estava a criar outro conceito que iria transformar o mundo que tinha como objetivo a busca de outras utilidades para o computador, Licklider acabou descobrindo outra poderosa forma de conectar com as pessoas, permitindo-lhe a comunicação e o compartilhamento dos dados em grande escala global [5]. Assim foi possível

criar a rede global de compartilhamento e comunicação, a “ARPANET” que com a sua evolução transformou na Internet e possibilitou que a Cloud Computing começasse a tomar forma.

Com a evolução da tecnologia é difícil encontrar uma empresa que não trabalhe com o planejamento da nuvem ou mesmo esteja querendo usa-la. O termo Cloud Computing veio a surgir no ano de 1997 na palestra ministrada por Ramnath Chellappa, que tinha como conceito associado ao nome de John Mccarthy, que são os pioneiros na tecnologia da inteligência artificial e criador da linguagem de programação LISP.

Porém a tecnologia começou a ser oferecida de forma comercial em 2008 quando as empresas de pequeno, médio ou grande porte adotaram as novas tecnologias, e em 2013 já possuía uma aceitação por parte do universo corporativo. Com a aceitação foi transformando o serviço, fazendo com que o processamento e armazenamento dos dados comesçassem a ser tratado da mesma forma que um serviço de fornecimento como o de energia elétrica, que é pago apenas pelo que foi usado durante o mês.

Muitas empresas vêm aderindo essa nova tecnologia como negócio se serviços terceirizados por um fornecedor de Cloud Computing, ou mesmo construindo servidores e Data Centers dentro da própria companhia para atender a demanda dos processos que roda nas empresas que as contrata os serviços.

Enquanto isso, as companhias se preparam para atender os usuários e as corporações que desejam entrar na Nuvem, ou seja, qual for o tipo de empresa como pública, privada ou híbrida. Porém a Cloud Computing é mais vez prova ser uma tecnologia arrojada que surgiu para mudar a forma de fazer negócios e comunicação.

## **2.3 O Futuro da nuvem**

Os especialistas creem que a computação em nuvem é o futuro da TI, na realidade a computação em nuvem é uma espécie de “Box” com diversos tipos de serviços como o SOA, SaaS, virtualização de servidores e

BPM que é oferecido na internet. Essas constatações aparecem nas pesquisas sobre o mercado que vem crescendo a cada ano.

Muitas empresas vêm na busca de soluções com mais benefícios e menos custos, dando atenção especial para a tecnologia em nuvem. Com os orçamentos vem cada vez mais apertados e os desafios maiores os CIOs estão olhando com atenção na computação em nuvem pois pode ter vantagens na busca de redução dos custos e ganhos benéficos nos negócios (Veras, 2012).

Segundo o Gartner (apud CIO, 2010):

*No mundo, os serviços de Cloud Computing vão movimentar 68 bilhões de dólares até o final de 2010, com crescimento de 16,6% em comparação com os 58,6 bilhões de dólares gerados em 2009. As projeções são de estudo da consultoria Gartner. O documento estima ainda que esse mercado alcançará uma receita de 148,8 bilhões de dólares em 2014.*

*Na avaliação do vice-presidente de pesquisas do Gartner, Ben Pring, esse modelo ganhou mais força no ano passado com a crise econômica que obrigou muitas companhias a analisarem a alternativa para reduzir os custos de TI. Gerentes de TI começaram a se interessar pelos serviços na nuvem, estimulando fornecedores a aumentarem as ofertas.*

Este ambiente da economia mundial fará com que os provedores de serviços de computação em nuvem aumentem os serviços fazendo com que a tecnologia tenha um futuro promissor desde que tenha uma confiabilidade, disponibilidade dos serviços, alcançando a maturidade e afastando de desconfianças dos clientes que tem.

De acordo com a instituição de Gartner, por exemplo, um terço dos dados pessoais dos usuários estará armazenado em algum servidor online até o ano de 2016. O resultado é bastante significativo, já que hoje apenas 7% dessas informações são salvas na nuvem. A maior razão para esse tipo de mudança é pela falta de espaço físico nos computadores.

A previsão é que o volume dos conteúdos de multimídia como fotos, vídeos, músicas e textos vem a sobre carregar toda a capacidade do armazenamento nos locais físicos. Em números absolutos, isso tende a representar um salto de 329 exabytes para 4,1 zettabytes (um zettabytes equivale a mais de um trilhão de gigabytes).

## 2.4 Computação em Nuvem no Brasil

Como em vários países a computação em nuvem vem chegando de vagar, no Brasil não foi diferente, mas o mercado atualmente encontra bem mais aquecido, segundo pesquisa do Gartner, os CIOs brasileiros fizeram uma lista com as prioridades dos investimento no ano de 2010.

Com a tendência mundial a Cloud Computing ficou em 1º lugar na lista dos mais citados para prioridades de investimentos, como mostra a baixo.

1. Cloud computing
2. Business Intelligence
3. Virtualização
4. Web 2.0
5. Gestão de TI
6. Mobilidade
7. Soluções orientadas a serviço
8. Networking
9. Business Process Management

Quadro 1 - Prioridades tecnológicas do CIO no Brasil - Fonte: Gartner (2010)

Segundo a vice-presidente do programa executivo do Gartner, Ione Coco, (apud CIO, 2010):

*Hoje o mundo inteiro está de olho no Brasil e existe uma pressão para que o CIO local traga respostas que acompanhem o crescimento esperado das empresas.*

*[...] o Cloud (Computing) garante a flexibilidade para responder mais rapidamente às demandas do negócio.*

Devido ao potencial da redução de custos, dos serviços oferecidos na nuvem ainda a perspectiva do mercado de TI, é bastante atraente não só para o gestor de TI, mas também no alinhamento estratégico das empresas fazendo redução de custos e gerando valores de negócio (Veras, 2015).

Mesmo assim, se tratando de algo relativamente novo ainda carece do amadurecimento dos gestores, fornecedores e clientes trazendo um problema para a adesão da computação em nuvem no curto prazo de implantação.

## **2.5 Riscos e Cuidados**

Os riscos da Cloud Computing têm a possibilidade que algum evento imprevisto como falhas ou mesmo mau uso, venha apareceras ameaça como um objeto de negócio.

Assim, os projetos da Cloud Computing como qualquer outro projeto apresentam características conflitantes. Os objetivos de um projeto de adoção de Cloud Computing devem ser acompanhados dos gerenciamentos dos riscos associados, existindo várias características importantes no modelo do mesmo, a combinação das características fornecidas pelo modelo adotado dos provedores, fazendo os riscos variarem.

O Gartner recentemente sugeriu alguns cuidados que o cliente deve ter para que não aconteça os riscos referente a aquisição de serviços de um provedor de Cloud Computing descrito a seguir:

- ✓ Saber como é feito o acesso dos usuários.
- ✓ Saber como o provedor obedece às normas de regularização.
- ✓ Saber onde se localizam os dados.
- ✓ Saber como os dados são segregados.
- ✓ Saber como os dados são recuperados.
- ✓ Saber como e feito o suporte.
- ✓ Entender a viabilidade do provedor no longo prazo.

O aspecto de chaves tem que ser avaliado na opção da entrega dos serviços de TI para o fornecedor da Cloud Computing, o risco das perdas dos controles e dos dados internos, não deixa de fato existe.

Mesmos os aplicativos que eventualmente continuam a rodar localmente, podendo utilizar os serviços de infraestrutura providos pela nuvem, como o armazenamento dos dados, por exemplo, e tem que está em pleno funcionamento no uso dos serviços providos internamente e externamente, assim os riscos aumentando até nestes casos.

O que tem que ficar claro é que no ambiente da de Cloud Computing é essencialmente diferente do ambiente tradicional da computação, mudando do modelo de equipamentos para o modelo orientado a serviço. Os acordos dos níveis de serviços (Service Level Agreement - SLA) passa ser a interface entre os provedores e as organizações dos clientes. Os SLA podem ser definidos para a aplicação ou para a infraestrutura da TI.

Com a computação baseada nas nuvens públicas adicionarem novos atores a equação da segurança – provedores de serviços terceirizados, fornecedores de infraestrutura e funcionários diminuindo o controle que a TI tem sobre as três áreas.

As ofertas dos serviços da nuvem ainda são confusas como na medida em que estas ofertas vêm crescendo os aspectos da segurança precisam ser rapidamente consideradas de forma que a nuvem serve como opção de data Center corporativo, e é preciso considerar a nova aquisição de serviços de TI.

Esses serviços em nuvem precisam ser elásticos conforme o que o cliente precisa precisando ser adequado a precisão a realidade e as exigências das aplicações que precisam ser oferecidas em diversos locais, tudo isso com toda a segurança possível.

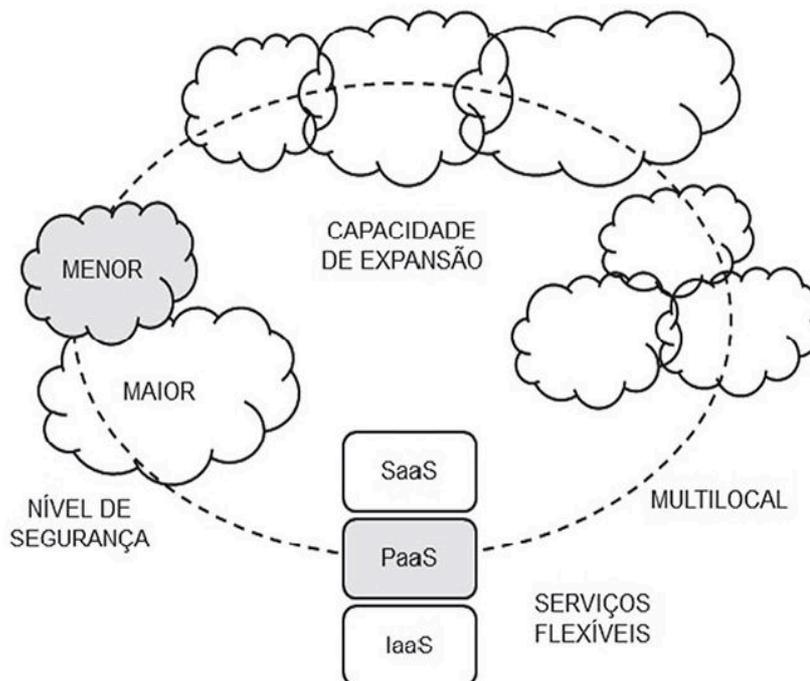


Fig 2: Recursos essenciais de nuvem. (Fonte: RCA)

Os aplicativos que estão na nuvem ainda não são de muita confidencialidade, mas com o crescimento da base das informações digitais, as empresas precisam considerar o fato de que responde boa parte das informações com os termos de segurança, privacidade e confiabilidade. Para se tiver um maior crescimento da nuvem precisa ter também uma segurança mais rígida com o acesso de cada empresa, assegurando a confiabilidade, disponibilidade e a integridade dos dados no momento que forem transmitidos, armazenados ou processados, no serviço da nuvem.

Os tradicionais aspectos de segurança da infraestrutura mudam com a adoção da nuvem, o Data Center na nuvem é controlada por terceiros e estruturas convencionais da segurança não servem mais, passando a ser compartilhada a questão da responsabilidade que vem à tona: como saber quem acessou e quais informações e aplicações? O acesso tem que ser individualizado, pois as empresas trabalham para definir os padrões da segurança na nuvem, a abrangência vem desde a autenticação delegada, do gerenciamento da chave pública, ter proteção contra a perda dos dados e emissão dos relatórios normativos de acesso à nuvem.

Outra questão a ser resolvida é a portabilidade da nuvem, que serão necessários arranjos que permita a portabilidade de identidade das informações entre várias nuvens, as questões de confidencialidade e privacidade são relevantes, abordando o controle do acesso usual nas operações convencionais não podem funcionar na nuvem como deve ser feito. O controle do acesso é baseado no conteúdo e não com a identidade do usuário que não são resolvidas. O que as empresas querem é saber se os provedores de serviços atende a política conforme a relação dos eventos internos e externos (Antony, 2012).

Os níveis de segurança dos dados deverão variar e também atender as diferentes necessidades e confidencialidades que deverá ser mantida durante o ciclo de vida dos dados.

Os principais elementos que são considerados para a proteção da nuvem são:

**Segurança da identidade:** o gerenciamento completo das identidades, a autenticação de terceiros e a identidade que tornaram fundamentais para a segurança, assim preservando a integridade e confidencialidade dos dados e dos aplicativos enquanto deixa o acesso pronto e disponível para os usuários.

**Segurança da Infraestrutura:** a arquitetura da nuvem tem que ser segura independente da mesma ser privada, publica ou mesmo prover os serviços de SaaS, PaaS ou IaaS.

Com a utilização do modelo CSA pode ser feita por três considerações nos modelos importantes nos serviços e na segurança:

**O modelo SaaS** oferece funcionalidades mais integras, que é feita através das ofertas com a menor extensibilidade para o cliente no nível relativamente elevado na segurança, assim o fornecedor assumindo as responsabilidades pela segurança.

**O modelo PaaS** visa permitir que os desenvolvedores façam as suas aplicações na plataforma da nuvem, tornando mais extensível que o

modelo SaaS, e a capacidade da segurança não são completas, tendo a flexibilidade de adicionar uma camada de segurança extra.

**O modelo IaaS** oferece pouca ou nem uma característica do aplicativo de segurança, mas permitindo muita extensibilidade, significando que menos recursos e funcionalidades integras na segurança, neste modelo requer que o cliente proteja e gerencie os sistemas operacionais, aplicativos e conteúdo.

O CAS chama atenção nas modalidades de implantação e consumo da nuvem que devem ser compensadas não no contexto do interno como no externo, nem considerando a localização física dos dados ativos, recursos e informações, mas também no contexto de que os clientes são de responsabilidade da governança, segurança e conformidade com as políticas e padrões da nuvem.

Os aspectos da localização dentro ou fora da empresa do ativo são relevantes na segurança, mas o que chama atenção são os riscos depende também de:

- ✓ Tipo de ativos, recursos e informações que estão sendo gerenciado.
- ✓ Quem, e como as gerencia.
- ✓ Quais controles estão selecionados e como está integrado.
- ✓ Quais conformidades.

Na figura a baixo o mapeamento dos serviços da computação da nuvem pode ser comparada com o modelo de controle da segurança e o de conformidade assim determinando qual controle existe. Assim bem como os requisitos dos negócios da regulamentação e outros requisitos da conformidade padrão, típico do exercício de *gap analysty* (Antony, 2012).

Uma vez *gap analysty* realizada, é baseado em requisitos do controle ou exigência da conformidade, tornando mais fácil determinar o que precisa ser feito em relação aos riscos de aceitação, transferência ou mesmo mitigação. Definindo as melhorias para a execução.

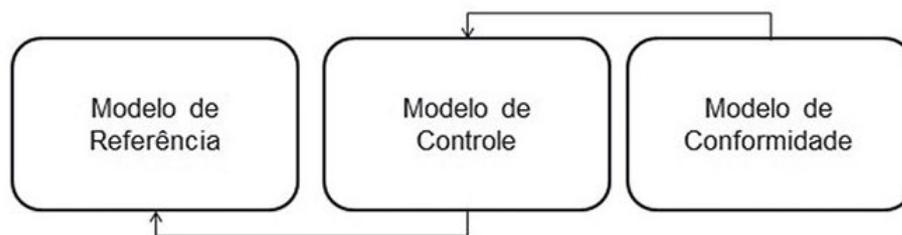


Fig 3: Modelos de referência, segurança e conformidade (Fonte: Guia CSA versão 2.1)

Importante resaltar que os modelos diferem as responsabilidades da segurança do provedor e do cliente para outro. A Amazon EC2 usa o tipo IaaS, toda segurança é relacionada ao sistema da TI, incluindo o Sistema operacional (SO), aplicativo e dados, por conta do cliente. Já no caso da CRM da Sales Force, é fornecido pelo modelo da SaaS, que a responsabilidade é do provedor.

Como ajuda as empresas nas tarefas, tem algumas recomendações:

- ✓ É preciso examinar e avaliar a cadeia de suprimentos do fornecedor, significando a verificação do gerenciamento dos serviços terceirizados pelo fornecedor (Veras 2015).
- ✓ Avaliar os fornecedores de serviços terceirizados que deve concertar-se nas políticas de recuperação dos desastres e continuidade dos negócios, incluindo a revisão das avaliações dos fornecedores destinados cumprindo as exigências das políticas e procedimentos e as avaliações usadas pelo fornecedor, disponibilizando informações do desempenho e a efetividade dos controles.
- ✓ O plano da recuperação dos desastres e continuidade dos negócios do cliente, assim incluindo cenários da perda dos serviços prestados pelo fornecedor e da perda do prestador de serviços terceirizados e da capacidade do mesmo.
- ✓ A regulamentação da governança da segurança das informações, a gestão dos riscos, estrutura e processos tem que ser avaliada.
- ✓ É preciso solicitar documentação como instalações e os serviços do fornecedor que são avaliados quanto aos riscos.

## **2.6 Vantagens do Armazenamento em Nuvem**

Nos dias de hoje já se é possível escolher uma plataforma de armazenamento de arquivos em nuvem, pois já deve ter ocorrido de estar fazendo um trabalho e o PC desligar por falta de energia, agora com a Cloud Computing já é possível ficar livre de inúmeros riscos tendo os arquivos seguros e acessíveis, pois mostraremos algumas vantagens específicas que a nuvem oferece para o armazenamento de arquivos.

### **2.6.1 Segurança Inabalável**

Uma falha mecânica tem enormes chances de representar uma ameaça de produtividade, com um bom uso da plataforma em nuvem os dados ficam seguros das falhas e dos acidentes mantendo sempre disponíveis e atualizados.

### **2.6.2 Envios facilitados**

Trabalhando em conjunto pode não saber qual o arquivo está mais atualizado caso tenha anexos diferentes, usando um sistema de armazenamento na nuvem como o Google Drive, por exemplo, é possível fazer compartilhamento de arquivos com amigos de que seja editado diretamente no documento original, devidamente assinado por quem editou o arquivo.

### **2.6.3 Espaços liberados**

Para a empresa trabalhar pensando o quanto cada um precisa de armazenamento dos arquivos faz parte do pensamento estratégico, assim acumulando muitos documentos pesados, vai chegar um momento que não vai ser mais salvos arquivos algum, por causa do espaço que acabou enchendo os físicos do PC. Com a utilização da plataforma em nuvem, boa parte do desse

acumulo é diminuída por que o serviço passa a atuar como um HD remoto, liberando a memória das máquinas físicas.

#### **2.6.4 Aplicativos Mobile**

A maioria dos sistemas de armazenamento possui bons aplicativos móveis que ajuda na otimização da produtividade, assim passando a ser possível o acesso dos arquivos através do smartphone e tablet, como exemplo, permitindo que trabalhe com os arquivos mesmo estando fora do escritório e longe do computador. Usando o Google Drive, por exemplo, que pode ser acessado de qualquer lugar, tendo apenas acesso à internet e o seu login e senha da conta.

#### **2.6.5 Colaborações simultâneas**

O Google Drive tem se mostrado como um dos melhores que traz algumas vantagens que se destaca trazendo alguns ganhos na produtividade para a equipe da empresa, o aplicativo conta com um chat interno que facilita a comunicação em tempo real entre as pessoas que usa o documento específico. O Drive oferece o controle de alterações mostrando em detalhes de quem fez a alteração exatamente quando.

#### **2.6.6 Disponibilidades de Plataformas**

Independentemente da plataforma que a pessoa use tem um bom aproveitamento, pois no caso do Google Drive, por exemplo, pode ter o acesso independente que use o Windows, Mac ou Linux, pois é possível aproveitar as vantagens de ter os dados de forma remota.

### **2.7 A segurança na Nuvem**

Para a computação em nuvem a questão da segurança ainda é uma grande polêmica para discussão no ponto de vista dos observadores da TI,

pois há quem fale que os usuários que acredita na segurança das nuvens, em quanto isso há muitos que não acreditam no mesmo, Os pessimistas tem como apontar tipos de incidentes a que venha aprovar que existem riscos nas aplicações em nuvem, como mostra as notícias publicadas pelo site CIO (2010).

*“Recentemente a gigante Google admitiu que desde 2007 vinha, por engano, coletando dados de navegação em redes sem criptografia Wi-Fi. Além disso, também foi divulgado que um hacker obteve mais de 300 documentos confidenciais que o Twitter armazenava com o Google Apps. Entretanto, após investigações, foi constatado que esse incidente foi mais culpa de um problema de senhas fracas do que de segurança no Data Center”.*

Pois esses tipos de sistemas são propícios a qualquer tipo de falhas, em muitos dos casos as empresas dizem que os sistemas que tem são mais seguros do que os sistemas de provedores de computação da nuvem, ou seja, que os riscos de armazenar determinados dados fora da própria infraestrutura (Empresa) são maiores o suficiente para refutar a hipótese de deixar disponível na nuvem. A maioria das pesquisas feitas sobre a segurança na nuvem aponta que existe uma desconfiança total no mercado. Segundo o relatório de falhas de segurança realizado por Price Waterhouse Coopers “apenas 17% das empresas confia nas medidas que são feitas pelos provedores baseado em nuvem”. (CIO)

Com esse tipo de preocupação com segurança levaram aos especialistas a criarem a Cloud Security Alliance – CSA “uma organização que não tem fins lucrativos, fundada em 2008 para promover a utilização das melhores práticas para garantir a segurança na Cloud Computing” (CSA). O diretor executivo da CSA, Jim Reais, acha que por mais que novas tecnologias pareçam familiares, basta procurar um pouco e observar um pouco que descobre uma serie de riscos escondidos que existe na rede como toda nova tecnologia.

Com a ajuda de 29 empresas de consultoria e fornecedores da computação em nuvem, os especialistas elaboraram um documento chamado

como os setes pecados mortais da segurança na nuvem, divulgado através do site CIO:

1. Perda de dados ou vazamento - Segundo Reavis, não existe um nível de controle aceitável na nuvem. Alguns aplicativos podem deixar dados vazarem como resultado de um fraco controle de API, geração de chaves incorretas, armazenamento ou gestão ineficiente. Além disso, políticas de destruição de dados podem estar ausentes.
2. Vulnerabilidades de tecnologias compartilhadas - Na nuvem, uma única configuração errada pode ser duplicada em um ambiente nos quais vários servidores virtuais compartilham essa informação. A organização deve aplicar acordos de nível de serviço (SLAs) para o gerenciamento de atualizações e as melhores práticas para a rede e configuração do servidor.
3. Colaboradores mal intencionados - O nível de verificações que os provedores da nuvem realizam em uma equipe pode variar de acordo com o controle de acesso à data center estabelecido pela empresa, segundo Reavis, “muitos deles fazem um bom trabalho, mas é desigual”, completou. A recomendação é realizar uma avaliação de fornecedores e definir um nível de seleção de funcionários.
4. Desvios de tráfego, contas e serviços - Muitos dados, aplicativos e recursos são concentrados na nuvem. Sem autenticação segura, um intruso pode acessar uma conta de usuário e obter tudo o que estiver na máquina virtual daquele cliente, afirma. Para evitar isso, o ideal é monitorar proativamente ameaças de autenticação.
5. Interfaces inseguras de programação de aplicativos - É importante ver a nuvem como uma nova plataforma e não apenas como terceirização quando se trata de desenvolvimento de aplicativos. Deve existir um processo de investigação relacionado aos ciclos de aplicações, no

qual o desenvolvedor entende e aplica certas orientações para controles de autenticação, acesso e criptografia.

6. Abuso da computação em nuvem - Usuários mal intencionados estão cada vez mais preparados, segundo Reavis. Registros indicam que crackers estão aplicando novas ameaças rapidamente, além da habilidade de se adaptar ao tamanho da nuvem. E tudo que é preciso é um cartão de crédito.
7. Perfil de risco desconhecido - A questão da transparência continua preocupando os provedores de nuvem. Usuários de contas interagem apenas com a interface final e não sabem muito sobre as plataformas ou níveis de segurança que os provedores estão empregando, afirma Reavis.

Com a consultoria da Forrester Research através do seu analista James Staten que entrevistou alguns usuários e fornecedores de serviços na nuvem que identificou que as organizações não sabe dizer onde fica a Data Center da nuvem que são usados para armazenar os dados. Com a maior parte dos serviços na nuvem compartilhada o modelo da hospedagem tradicional, significando que os dados dos clientes são gerados e armazenados nos ambientes físicos, sujeito a implicações legais e privados. O especialista alerta que conhecer a localidade dos dados é imprescindível para não há prejuízos.

A falta do conhecimento das empresas está diretamente ligada à falta dos padrões para a gestão das informações e práticas de segurança. Por exemplo, um vendedor não é obrigado a informar aos usuários qual é o País ou o local onde os dados foram armazenados.

*“Não sabemos quais são as condições de segurança praticadas pelas empresas com as quais dividimos a nuvem”, explica o ex-diretor técnico da Agência de Segurança Nacional (da sigla NSA, em inglês) dos Estados Unidos, Brian Snow.*

No momento em que as empresas optam pela nuvem tem que estar ciente dos riscos em relação à forma, ao momento e à aplicação das ferramentas da área de TI. A computação em nuvem ainda tem o problema de por falta de uma retaguarda legal nos modelos contratuais e de controles adequados a segurança.

O modelo também tem falhas pela dificuldade dos processos da auditoria da segurança e da regulamentação dos dados para os backups e das informações que são colocadas na nuvem. Interfaces para a integração adequadas entre serviços da nuvem, os que são hospedados nas empresas que completam a lista da deficiência do modelo da computação em nuvem.

Já os gestores de TI precisam analisar os projetos da adoção da computação em nuvem como qualquer iniciativa que é ligado a área de tecnologia. Isso vem exigindo um grande processo de avaliação dos custos e dos benefícios, quando há um plano bem estruturado para a implementação da estratégia de aperfeiçoamento contínuo. Que cada analista tem que tentar fazer o equilíbrio adequado da melhor maneira possível.

## **2.8 Tipos de ataques**

### **2.8.1 Ataques de negação de serviço (Denial of Service (DoS)):**

Os ataques que tem como objetivo a negação dos verdadeiros usuários, tende a ocorrer por alcançar a inundação da rede com pedidos consumindo os recursos disponíveis e levando a sobrecarga. Para efetuar um DoS, o ataque SYN pode ser colocado e fazendo a exploração no protocolo TCP necessitando de uma resposta do cliente para estabelecer a conexão. Nestes ataques vários pedidos de sincronização (SYN) são feitos pelo atacante nos servidores que responde com o sinal *acknowledge (ACK)*. Assim o atacante não responde ao servidor para fazer que consumisse bastante memória e processamento esperado pela resposta, como exemplo seria a aplicação do uso da fácil escalabilidade do serviço, que normalmente tem uma vantagem, se mal intencionado, podendo sobrecarregar os recursos alocados para o serviço como para os usuários que compartilha da estrutura. Já o dono dos sistemas

atacados terá que arcar com os custos extras, caso não tenha o contrato pague o que usar.

Há também o *DDoS* (*Distributed Denialof Service* – Ataques distribuídos de negação de serviços), Onde o computador mestre comanda vários outros computadores conhecidos como zumbis. Uma maneira de realizar um DDoS, é sequestrando um servidor e desabilitar as *webs services*, exigindo uma recuperação de senha para habilitar novamente, ainda sugerindo o uso de SYN cookies para evitar que a conexão anterior seja descartada.

### **2.8.2 Ataque *man-in-the-middle* (homem no meio)**

É o ataque que tem como objetivo colocar o atacante entre os dois pontos como elemento transparente, com isso o usuário crê que está conversando diretamente com o outro, quando está conversando como o atacante que recebe as informações e repassa se passando do provedor que tem como consequência a leitura e alteração dos dados ao repassa-los.

Assim o atacante descobre as credenciais para fazer o login no serviço da nuvem. A variante desse ataque é *man-in-the-middle*, onde o intruso coloca como receptor de mensagem um e-mail para enviar arquivos maliciosos para descobrir senhas de relatorios, informações privilegiadas que são enviadas por funcionarios de corporações importantes que não pode ser repassadas.

Em 2009, a *Google* teve seu sistema atacado, pelos *hackers* que aproveitaram uma pequena falha do *navegador da Microsoft Internet Explorer* para executar e ter acesso nos servidores da empresa.

## Man in the MailBox (MITMB)

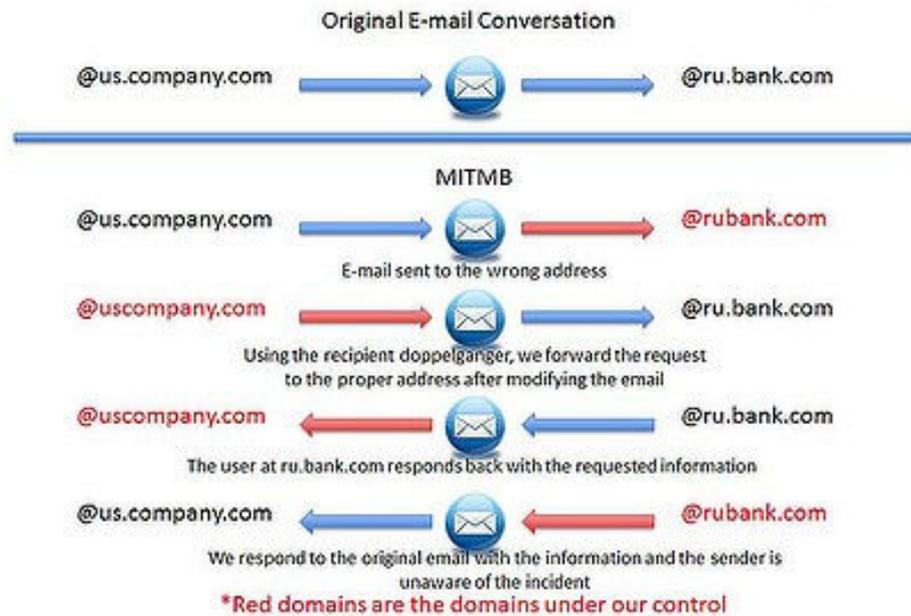


Fig 4: Exemplo do ataque man-in-the-mailbox (Fonte: [10])

### 2.8.3 Injeção de código

Tem como Objetivo de inserir pedaços de códigos no servidor, assim o código mal-intencionado pode fazer com que altere o código do banco de dados (Injeção de SQL – *SQL Injection*), para roubar informações pessoais (*Croos-site scripting*) ou mesmo podendo instalar *malwares* no computador do usuário ou no servidor.

Esses tipos de ataque são os mais comuns em sistema de computação em nuvem.

### **3. Conclusão**

Na descrição do artigo sobre a Computação em Nuvem é um sistema que vem crescendo, pois muitas empresas já vêm usando para fazer armazenamento de dados importantes, do mesmo jeito muitas pessoas vêm usando para armazenar arquivos de multimídia (fotos, vídeos, músicas e documentos).

Assim, fazendo como deve ser usada a segurança que mais convém para que os dados sejam armazenados sem que intrusos tenha acesso indevido a esses tipos de documentos. Por isso foi comentada algumas descrições de ferramentas para se proteger, e os sistemas para ter acesso ou mesmo vindo de aplicativos que pode ser instalados ou não nos aparelhos como smartphone, tablet ou em notebooks, e apenas tendo o acesso à internet para acessar os arquivos que estão remotos, fazendo também o compartilhamento do uso simultâneo dos documentos.

#### 4. Bibliografia:

[1] O que é Computação em nuvem, <http://www.ynternix.com/o-que-e-computacao-em-nuvem/>

[2] *Lauro. Luís Armondi Whately*; Amãpytuna, Computação em Nuvem: serviços livres para a sociedade do conhecimento. Fundação Alexandre de Gusmão Brasília, 2010.

[3] Antony T. Velte, Toby J. Velte, Ph.d.Robert Eisenpeter, Cloud Computing: Computação em nuvem, Uma abordagem Pratica. Brasport Livros e Multimídia Ltda. Rio de Janeiro, 2012.

[4] Computação nas Nuvens, [https://www.oficinadanet.com.br/artigo/923/computacao\\_nas\\_nuvens](https://www.oficinadanet.com.br/artigo/923/computacao_nas_nuvens)

[5] Como surgiu a tecnologia Nuvel Cloud Computing?; <http://blogbrasil.comstor.com/bid/332223/Como-surgiu-a-Cloud-Computing>

[6] O futuro da nuvem; <http://planetamaisinteligente.ig.com.br/2012-09-10/futuro-da-nuvem.html>

[7] [http://www.revistatecnologiagrafica.com.br/index.php?option=com\\_content&id=3928:a-nuvem-e-o-futuro-da-computacao&Itemid=183](http://www.revistatecnologiagrafica.com.br/index.php?option=com_content&id=3928:a-nuvem-e-o-futuro-da-computacao&Itemid=183) Escrito por Andrea Ponce, Seg, 03 de Dezembro de 2012

[8] Augusto Carvalho dos Santos, Bruno Gil Pedrosa, Henrique Santos, Higor Gonçalves Godinho, Leandro Silva, Rafael do Carmo Schettino, Rodrigo Carvalho dos Santos, Sérgio Henrique Amaral Mendes: Computação em nuvem: Conceitos e Perspectivas, TCC Gestão em tecnologia da Informação, BH

[9] Veras Manuel; Computação em nuvem – Nova arquitetura de TI. Brasport Livros e Multimídia Ltda. Rio de Janeiro, 2015.

[10] Laura de Oliveira F. Moraes, Segurança na Nuvem [http://www.gta.ufrj.br/ensino/eel879/trabalhos\\_vf\\_2011\\_2/laura/tipos\\_ataques.php](http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/laura/tipos_ataques.php)