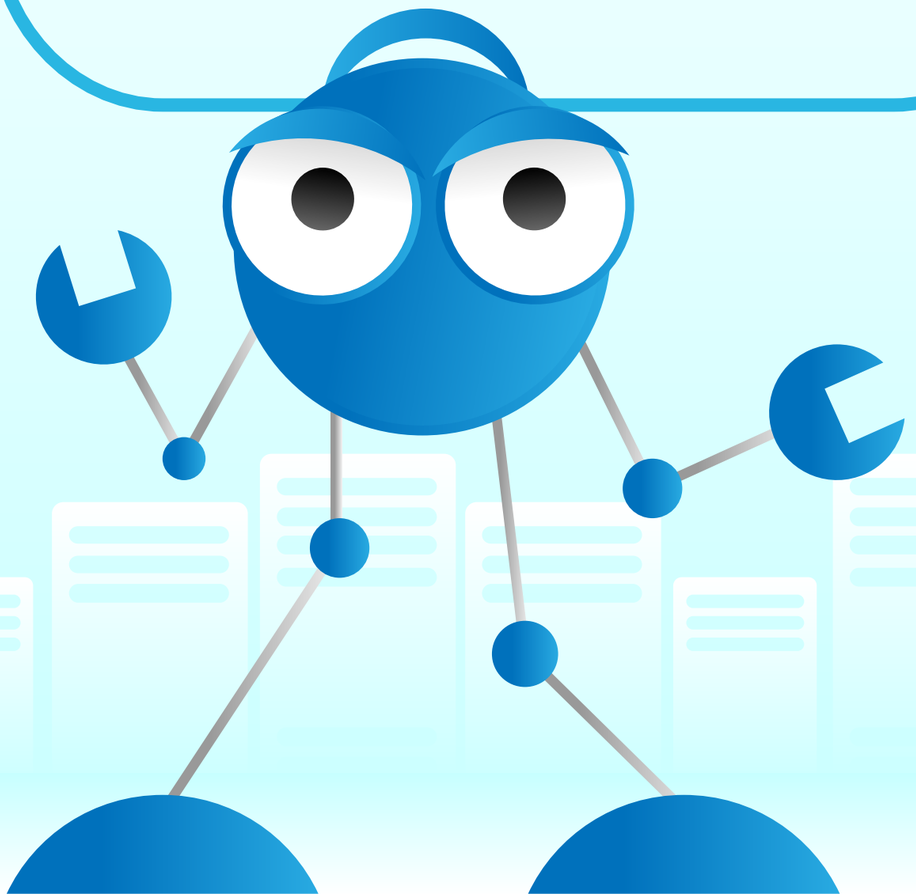
SEGURANÇA EM CLOUD COMPUTING

DESAFIOS E GERENCIAMENTO DE RISCOS



INTRODUÇÃO

No panorama atual vemos o que acontece com as tendências da computação e percebemos que elas percorrem cada vez mais o *caminho do conectar, transmitir* e *compartilhar*. Assim se pararmos para pensar nos damos conta que realmente estamos todo o tempo *conectados, transmitindo e compartilhando* tudo o que diz respeito á informação sobre nossa vida, a sociedade, a ciência, entre outros.

O termo *cloud computing* teve seu *boom* em meados de 2008, desde então ele vem colocando-se em pauta e tende a não sair de cenário tal cedo.

Sua essência está ligada a ideia de utilizarmos, em qualquer lugar e de forma independente de plataforma, as mais diversas aplicações por meio da internet com a mesma facilidade de tê-las instaladas em nossos próprios computadores.

Agora, com a **Computação em Nuvem**, para uma empresa que precisa utilizar um *software* específico que demanda de alto poder computacional, não precisaria mais investir em diversas máquinas poderosas para rodá-lo. Tudo pode ser feito através da nuvem. A organização paga pelo tempo de utilização ou número de acessos ao *software* e não se preocupa mais com gastos de manutenção e *hardware*. O fornecedor dos serviços é quem se preocupa com isso.

E é exatamente este ponto que este ebook prentende discorrer.

Por Domingos Teruel

SOCIALBASE

1. O QUE É CLOUD COMPUTING

Oficialmente *Cloud Computing* é um modelo para permitir acesso **sob-demanda** de forma onipresente e **conveniente** via rede a um "*pool*" **compartilhado** de recursos computacionais configuráveis (ex: redes, servidores, armazenamento, aplicativos e serviços) que podem ser **rapidamente** provisionados e lançados com o mínimo esforço de **gestão** ou integração com o **provedor** de serviço - (NIST).

Entende-se por *Cloud Computing* a evolução conjunta de infra-estrutura (rede e hardware) e sistemas computacionais em uma "única" central, de forma "virtual". Ou seja, sem a necessidade de reservas de espaços para servidores e data centers em empresas. Segundo Rita de Castro e Verônica de Sousa (2010), *hardwares*, *softwares* e gestão de dados de informação deixam de ser considerados ativos da instituição e figuram como ferramentas de trabalho, deixando a administração e ônus da infraestrutura nas mãos de fornecedores do serviço.

Com a *Cloud Computing* os aplicativos outrora armazenados em servidores ficam disponíveis em nuvem e sendo acessados através de um simples navegador web, não sendo necessário um ambiente físico (computadores, notebooks, etc) ou licenças para programas instalados nestes equipamentos. Ficando, ao fornecedor a responsabilidade pela instalação, armazenamento, manutenção, atualização, escalonamento, *backups* e outros serviços relacionados. Ao usuário compete apenas acessar e utilizar os arquivos.

2. CARACTERÍSTICAS DA CLOUD COMPUTING

Tal como já informado, uma das vantangens da *cloud computing* é a possibilidade de se utilizar as aplicações diretamente da internet, sem que elas estejam instaladas no computador do usuário, em outras palavras, redução de custos com TI (servidores; licenças de programas; equipamento; etc). Mas há outros ganhos significativos:

- Na maioria dos casos é possível acessar determinadas aplicações independente de sistema operacional ou *hardware*.

- Ao usuário não é preciso preocupar-se com a estrutura para a execução - *hardware*, procedimento de *backup*, controle de segurança ou manutenções - são de responsabilidade de fornecedor do serviço.

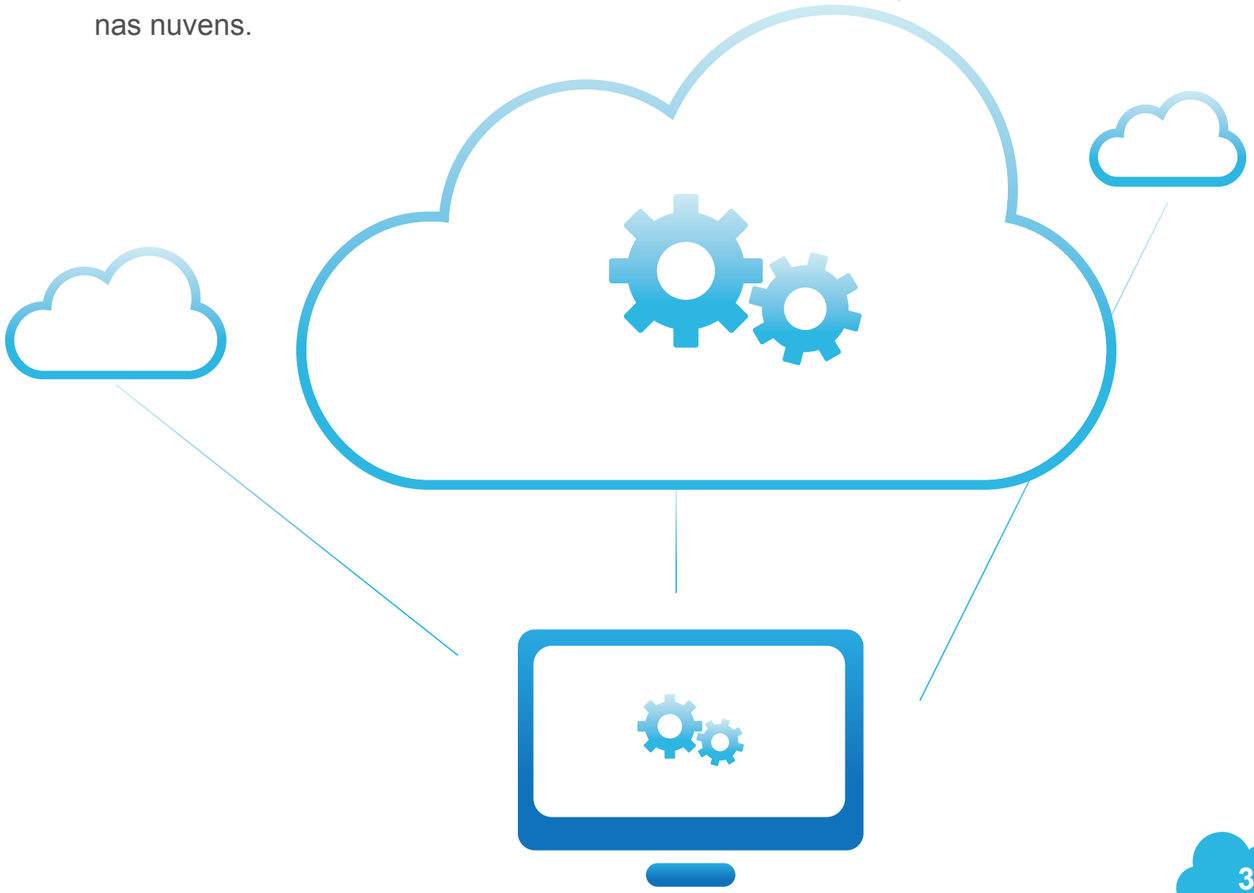
- Compartilhamento de dados e o trabalho colaborativo torna-se mais fácil, uma vez que todos acessam e arquivam os dados no mesmo local.

- A maioria dos fornecedores possuem sistemas duplicados, ou seja, caso haja problema no acesso a um servidor específico outro é ativado sem que haja perda de tempo ou de dados ao contratante.

- Maior controle de gastos. Há inúmeros serviços gratuitos de *Cloud Computing* e mesmo os serviços pagos possuem controle por meio de utilização de tempo ou espaço contratado, dependendo do contrato.

- Mesmo os serviços que requerem, em alguns casos, a instalação de um aplicativo (*Dropbox* ou *Google Drive*) os dados e arquivos mantêm-se em nuvem.

Independente da aplicação utilizada, o usuário não necessita de conhecimento especializado prévio sobre a estrutura que mantém em funcionamento o sistema. Ou seja, não há necessidade do usuário saber quantos servidores executam uma ferramenta, qual configuração de *hardware* é utilizada ou como é feito o escalonamento. O usuário apenas precisa saber que a aplicação está disponível nas nuvens.



3. MODELOS DE SERVIÇO EM CLOUD COMPUTING

Ambientes de computação em nuvem podem ser compostos por até 8 modelos diferentes de serviços que definem o padrão arquitetural de soluções em *Cloud Computing*. Castro e Sousa (2010) destacam que os riscos e benefícios de cada um é tratado dependendo do serviço e tipo de implantação contratado.

SAAS - SOFTWARE COMO SERVIÇO (SOFTWARE AS A SERVICE)

O modelo está relacionado a contratação de um software para sanar determinada necessidade da empresa (Rede Social Corporativa; Intranet; email; CRM; etc), sem que haja a necessidade de adquirir *hardwares*, licenças de *softwares* ou mesmo instalar aplicativos, basta acessar o serviço por meio do endereço fornecido pelo contratado. Nesse modelo, o cliente paga o serviço e não o produto.

Deste modelo, o mercado naturalmente expandiu o conceito de Saas como forma de diferneciar os seus serviços. São elas:

PAAS - PLATAFORMA COMO SERVIÇO (PLATFORM AS A SERVICE)

Trata-se de um tipo de solução SaaS mais amplo para determinadas aplicações, incluindo todos (ou quase todos) os recursos necessários à operação, como armazenamento, banco de dados, escalabilidade (aumento automático da capacidade de armazenamento ou processamento), suporte a linguagen de programação, segurança e assim por diante.

DAAS (DATABASE AS A SERVICE)

Banco de Dados como Serviço. O nome já deixa claro que esta modalidade é direcionada ao fornecimento de serviços para armazenamento e acesso de volumes de dados. A vantagem aqui é que o detentor da aplicação conta com maior flexibilidade para expandir o banco de dados, compartilhar as informações com outros sistemas, facilitar o acesso remoto por usuários autorizados, entre outros.

IAAS - INFRAESTRUTURA COMO SERVIÇO (INFRASTRUCTURE AS A SEVICE)

Parecido com o PaaS, nesse modelo o foco é a infraestrutura como serviço, ou seja, estrutura de *hardware* e virtualização, contudo ao invés de adquirir elementos físicos (racks, roteadores, etc) a tarifa alimenta-se por números de servidores virtuais, dados trafegados ou armazenados e tempo de uso. Geralmente oferece uma interface única à administração do sistema; provisionamento dinâmico de serviços; alta disponibilidade e balanceamento das máquinas virtuais.

DEVAAS - DESENVOLVIMENTO COM SERVIÇO (DEVELOPMENT AS A SERVICE)

Esse modelo apoia-se no compartilhamento de ferramentas de desenvolvimento e serviços. Extremamente flexível permite a mescla de conteúdos de diversas fontes para criar um novo serviço.

CAAS – COMUNICAÇÃO COMO SERVIÇO (COMUNICATION AS A SERVICE)

O modelo estabelece uma comunicação unificada por meio de um "*data center*", ou seja, garante que a comunicação da empresa fique alocada em um sistema central.

EAAS – TUDO COMO SERVIÇO (EVERYTHING AS A SERVICE)

Unifica a infraestrutura, plataformas, *software* e suporte em um único serviço.

TAAS – ENSAIO COMO SERVIÇO (TESTING AS A SERVICE)

Oferece um ambiente onde os usuários possam simular o comportamento de execução de aplicações e sistemas, sendo comumente usado para testes de segurança antes desses serviços serem implantados.

4. MODELOS DE IMPLEMENTAÇÃO DE COMPUTAÇÃO EM NUVEM

A implementação dos serviços de computação em nuvem basicamente são compostos por dois lados: o provedor da solução e o usuário - pessoa ou empresa. Sobretudo, os modelos de implementação referem-se ao acesso e disponibilidade de ambientes de computação em nuvem. A definição do modelo depende do processo de negócio de cada organização, do tipo de informação e do nível de visão desejado. O NIST (*National Institute of Standards and Technology*) divide assim os modelos de *Cloud Computing*:

4.1. NUVEM PRIVADA (PRIVATE CLOUD)

4.2. NUVEM PÚBLICA (PLUBIC CLOUD)

4.3. NUVEM HÍBRIDA (HYBRID CLOUD)

4.4. NUVEM COMUNITÁRIA (COMMUNITY CLOUD)

4.1 NUVEM PRIVADA (PRIVATE CLOUD)

Também conhecida como *Corporate Cloud*, o serviço, por ser “particular”, é administrado pela empresa ou por um prestador de serviço designado. O modelo é o mais utilizado por instituições que ainda não sentem-se a vontade em trabalhar com nuvens públicas ou híbridas.

Segundo Castro e Sousa (2010), neste modelo de implementação são empregadas as políticas de acesso ao serviço. As técnicas aplicadas para ordenar estas características podem ser em nível gerencial de redes, nas configurações dos provedores de serviços e na utilização de tecnologias de autenticação e autorização.

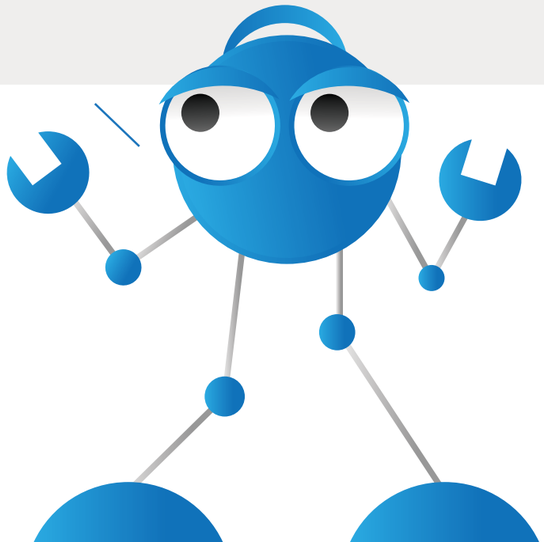
Embora o modelo siga os mesmos desígnios da Nuvem Pública, contra ele, pesa o fato de por estar no ambiente interno da empresa (*firewall* ou mesmo físico), ele exige um profissional ou consultoria especializada na criação e na manutenção da nuvem - afinal uma má implementação pode aferir negativamente a aplicação. Por haver essas necessidades específicas, uma nuvem privada diminui a economia de recursos, obtida em uma nuvem pública.

Além disso, dependendo do modelo contratado, os gastos com equipamentos, sistemas, treinamento e profissionais poderão ser elevados no início. No entanto, os benefícios obtidos a médio, longo prazo com a ampla disponibilidade do sistema, a agilidade dos processos e a segurança compensarão os custos - especificamente se a implantação for potencializada com a virtualização e a padronização dos serviços.

O QUE CARACTERIZA UMA NUVEM PRIVADA

Segundo o Gartner, alguns pontos caracterizam um ambiente como uma nuvem privada. São eles:

- Oferta de recursos como serviços (infraestrutura e aplicações);
- Elasticidade e escala adequada à demanda do cliente;
- Compartilhamento de recursos entre um grande número de usuários;
- Medição e pagamento de acordo com o uso do serviço;
- Utilização de protocolos e tecnologias da internet para acesso aos recursos na nuvem.



4.2 NUVEM PÚBLICA (PLUBIC CLOUD)

É um dos modelos mais conhecidos pelo público em geral, e já popularizado por fornecedores de email e de arquivos como o *Google Drive* e o *Dropbox*. Sua infraestrutura é disponibilizada ao público em geral, sendo acessada por qualquer usuário que conheça o endereço do serviço. Por esse motivo não podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes ou aplicar técnicas de autenticação e autorização. Contudo, é possível gerenciá-la e operá-la com segurança.

A principal vantagem do modelo é a economia proporcionada, pois os recursos de infraestrutura são compartilhados e custeados por várias empresas do mundo todo. Além disso, é possível escalar e provisionar os recursos com menos ônus, uma vez que não é necessário adquirir equipamento e mão de obra.

Por outro lado, a principal vantagem do sistema é o seu principal problema, pois por ser aberto e não haver um controle interno sobre os dados, mutias empresas não sentem-se confortáveis em adquirir o serviço. Também pesa como ponto negativo a necessidade de conexão à internet, muitas vezes, um problema para empresas localizadas em localidades remotas e mesmo para organizações situadas em metrópoles que sofrem com quedas constantes de rede.

4.3 NUVEM HÍBRIDA (HYBRID CLOUD)

Caracterizada pela composição de dois ou mais modelos. A nuvem híbrida permite um maior controle sobre os gastos. A grande vantagem do modelo é a possibilidade de utilizar o que existe de melhor nos outros modelos de implantação.

Por meio dela, por exemplo, é possível manter dados sensíveis em uma nuvem privada e o restante em uma nuvem pública.

Segundo a Penso Tecnologia, a associação de modelos de implantação de nuvem garante uma maior interoperabilidade dos sistemas e recursos de TI possibilitando à empresa:

Redução de custos
É mais barato contratar recursos em nuvem pública do que na privada;

Controle e segurança da informação
Dados e informações críticas estão na nuvem privada, em ambiente controlado pela empresa;

Velocidade e desempenho
Ao replicar em ambiente local o que é muito consultado pelos usuários;

Contingência
A empresa possui recursos contratados em diferentes locais que podem se comunicar e ter redundância de informações.

4.4 NUVEM COMUNITÁRIA (COMMUNITY CLOUD)

No modelo de implantação da nuvem comunitária, a infraestrutura é compartilhada por diversas empresas e oferece suporte a uma comunidade específica que possui interesses semelhantes, tais como: missão, requisitos de segurança, política e considerações sobre flexibilidade. Este modelo pode existir localmente ou remotamente e pode ser administrado por uma empresa da comunidade ou por terceiros. Semelhante ao sistema Privado, é possível definir políticas de acesso e a utilização de tecnologias de autenticação e autorização.

Atualmente, segundo a pesquisa do Grupo Capgemini, não há no país um modelo predominante de Cloud Computing. Empresas de pequeno porte utilizam a pública, enquanto médias e grandes dão preferência às nuvens híbridas.

Aproximadamente 26% dos executivos afirmam não ter nenhuma preferência por um modelo específico de nuvem.

A nuvem pública é o modelo mais atraente, sendo utilizada por 24% das empresas, em seguida vem a privada para as instalações na empresa (18%), híbrida (18% - prevalecendo a junção entre pública e privada) e privada gerenciada por tereceiros (14%).

5. REGRAS DA COMPUTAÇÃO EM NUVEM NO BRASIL

Uma das principais preocupações no uso de serviços de *Cloud Computing* está na segurança da informação que nela circula, segundo Castro e Sousa (2010) adotar sistemas de Computação em Nuvem é totalmente novo às práticas do mercado. Sendo a solução mais adequada, apontada por elas, vincular padrões de governança de TI que permitam as instituições identificar e catalogar as informações que serão armazenadas. “A adequação das políticas de segurança da informação auxiliará a definição de diretrizes para que o consumo dos serviços da nuvem possua um nível de segurança aceitável”.

Em 2013 o projeto de Lei nº 5344/13 ratifica o mercado de computação em Nuvem no país e discorre sobre o desenvolvimento, exploração e segurança da atividade.

> § 1º A computação em nuvem é definida como a exploração da atividade de tratamento, armazenamento, guarda e depósito virtuais, por sistemas eletrônicos ou eletromagnéticos e mediante contrato oneroso ou gratuito, no qual o depositário recebe informações, sistemas, programas, plataformas, ou qualquer espécie de dados do depositante ou titular, sejam codificados ou não, considerados conteúdos ou bens, sendo regido por esta lei e no que aplicável, pelo Código de Defesa do Consumidor, pela legislação específica de proteção de dados, de propriedade intelectual, legislações setoriais e outras aplicáveis.

A lei rege nos artigos 2º (diretrizes da Computação em Nuvem) e 3º (Contrato) sobre as responsabilidades e segurança dos dados alocados em nuvem:

> **Art. 2º**. IV. Reconhecimento da privacidade, intimidade e proteção dos dados e da propriedade intelectual: necessidade de adoção de medidas que reconheçam e que promovam a proteção dos dados de forma clara e transparente em especial aqueles relativos à privacidade e intimidade, em atendimento à garantia constitucional e legal e garantindo a proteção à propriedade intelectual.
>
> V. Clara definição de responsabilidades para os provedores do serviço e seus contratantes, em especial aqueles que por meio do serviço realizam tratamento de dados de terceiros, conforme vier a ser especificado em contrato ou em seu silêncio a assunção plena de responsabilidade do provedor de computação em nuvem por atos de seus subcontratados.
>
> **Art. 3º**. V - responsabilidade do fornecedor do serviço e suas limitações: garantias que podem ser concedidas sobre o conteúdo objeto do armazenamento, guarda edepósito e recuperação deste, em especial sobre padrões de qualidade do serviço e latência.
>
> VIII - forma de sigilo e confidencialidade

Também é descrita na lei (Art. 4º) as responsabilidades ao contratado, sobre os dados do contratante, sendo ele, segundo a lei, responsável pela guarda e conservação dos bens depositados aos seus cuidados.

> § 1º. O responsável pelo depósito do conteúdo deve utilizar medidas técnicas e administrativas capazes de proteger o mesmo que se encontra sob sua responsabilidade da destruição, perda, extravio, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado. Estas medidas devem ser proporcionais ao estado do conhecimento técnico disponível e devem ser informadas ao depositário ou usuário do conteúdo, devendo incluir ao menos um sistema de cópia de segurança e reserva.
>
> § 2º. O conteúdo do depósito terá caráter sigiloso, não podendo ser revelado ou fornecido pelo depositário, salvo por ordem judicial, a requerimento do depositante ou mediante sua autorização ou consentimento prévio e expresso.

O texto completo da lei está disponível aqui.

6. SEGURANÇA EM CLOUD COMPUTING

Geralmente somos habituados a armazenar dados de maneira on premise, ou seja, instalados em nossos equipamentos. Esse cenário muitas vezes provoca um certo “desleixo”, pois acredita-se (senso comum): se está em nossas máquinas está seguro.

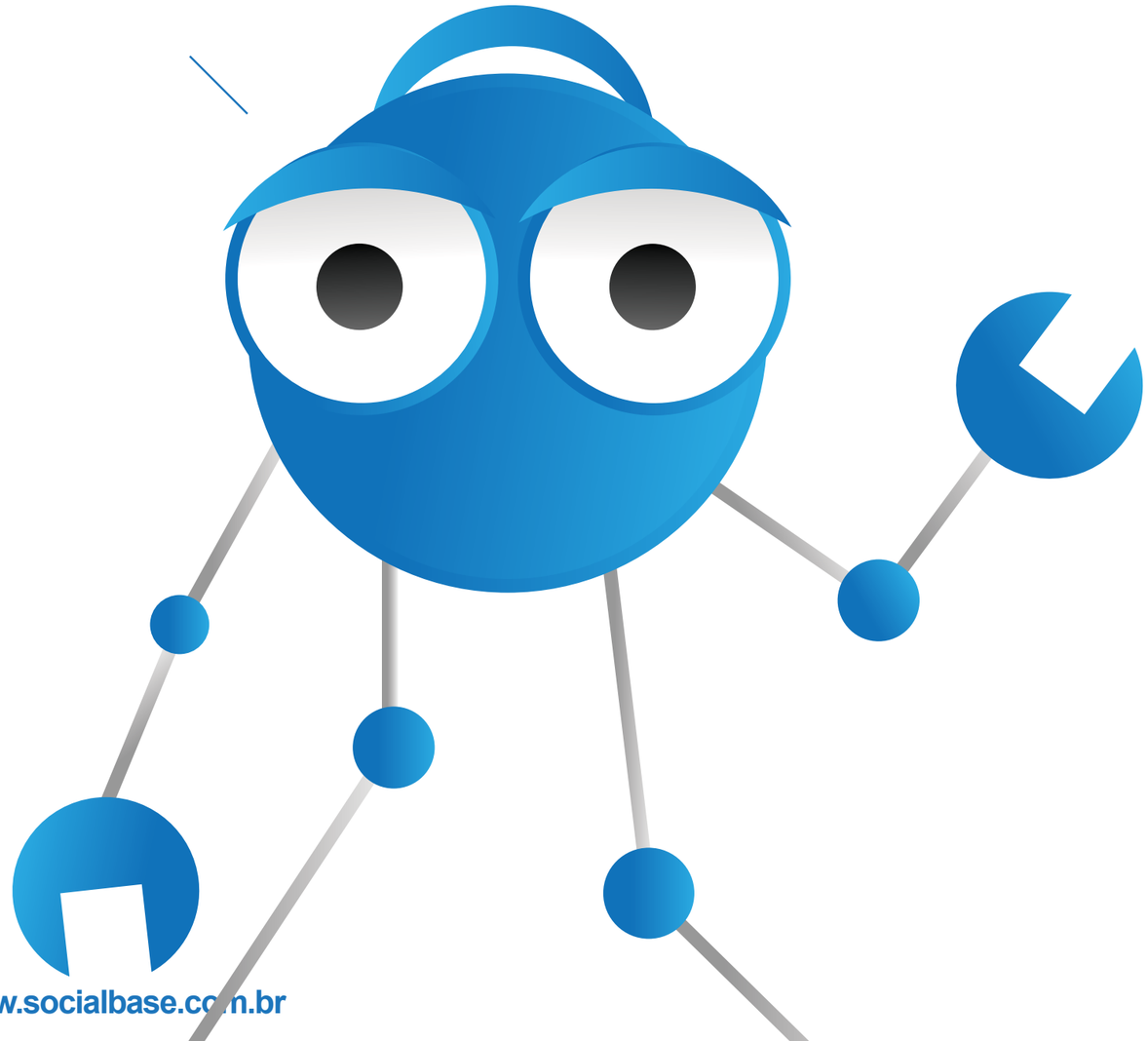
Entretanto, com a **Computação em Nuvem**, alguns cuidados devem ser reequilibrados, uma vez que se pode acessar dados de qualquer plataforma ou local (seguro ou não), esquecer uma senha registrada ou mesmo uma página aberta em uma *Lan House* ou computador de terceiro pode causar uma grande dor de cabeça à empresa.

A segurança na computação em nuvem traz inúmeros desafios a diversas áreas e a gestores de TI, contudo, muitos desses entraves podem ser identificados traçando um bom planejamento de migração de dados.

Segundo a CSA (*Cloud Security Alliance*), é preciso ter ciência sobre quais serviços pode se tirar proveito na Nuvem e quais implicações e regulamentações podem ocorrer na migração de serviços. Muitas vezes, por motivos jurídicos é preferível não migrar alguns serviços, porque os dados precisam estar localizados em um datacenter nacional.

CONHEÇA AS LEIS QUE REGEM SEU NEGÓCIO

CONHEÇA BEM SEU PROVEDOR, SUAS POLÍTICAS DE SEGURANÇA E AS CLÁUSULAS DO CONTRATO DE PRESTAÇÃO DE SERVIÇO.



Muitos dos fracassos ocorridos na implantação ou na migração de dados para um modelo de nuvem acontecem pela falta de planejamento e a escolha do serviço adequado ao negócio. Dependendo do tipo escolhido (SaaS; IaaS; PaaS; etc), uma total readaptação de processos precisa ser feita.

Casos como a aplicação de um modelo de DevaaS não só o serviço sofre uma mutação, mas também a plataforma de desenvolvimento. E, quando se está desenvolvendo para nuvem, qual o modelo de segurança está sendo usado? Todas as áreas que ofereçam vetores de exploração precisam ser levadas em consideração durante a migração. (CSA, 2012).

Além disso é de exímia importância levar em consideração o planejamento de planos de contingência dos termos de níveis de serviço (SLA - *Service Level Agreement*). A avaliação desse ponto não pode passar desapercebida, pois trata de questões relacionadas a:

- Como seu provedor irá reagir em caso de falha;
- Quanto tempo levará para o reestabelecimento do serviço;
- Qual plano de backup em caso de falha;
- Qual o tempo máximo aceitável para o seu negócio e como o provedor irá honrar este tempo.

Segundo a CSA, a partir do momento que se dá início ao processo de migração de aplicações críticas para o seu negócio é de suma importância ter um entendimento e um comprometimento das SLAs utilizadas a cada tipo de incidente. Nem sempre a SLA ofertada pelo provedor irá atender as suas necessidades, principalmente em relação a desastres naturais ou intervenção direta de terceiros (queda de energia, por exemplo).

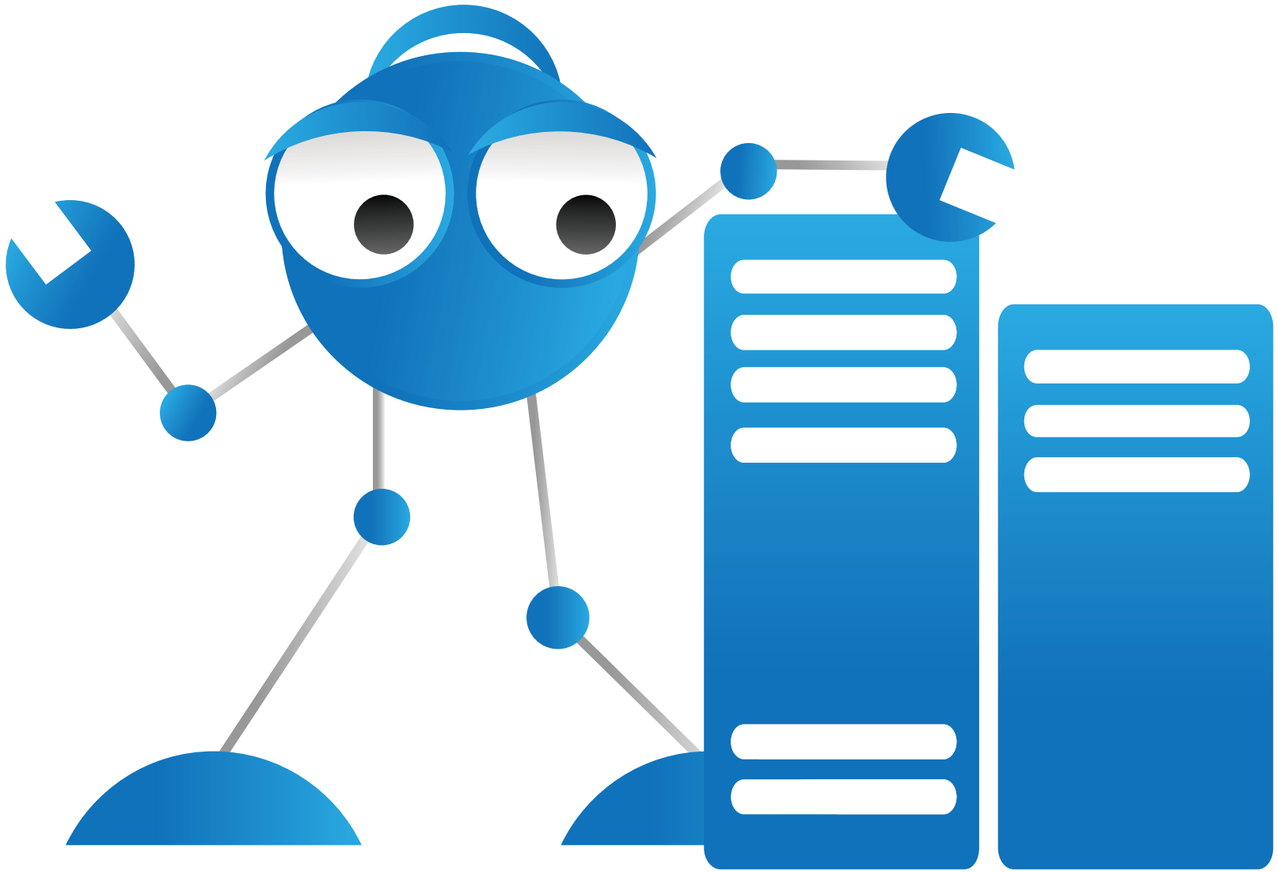
Ainda é necessário que haja, dependendo do modelo utilizado, profissionais treinados para operar as máquinas virtuais, se necessário. Além disso, outros pontos precisam ser avaliados dentro da empresa e no trato com o contratado.

- Quem terá acesso aos dados;
- Qual a política de privacidade e controle é estipulada aos dados;
- Como é feito o isolamento dos dados.

Por fim, destaca a CSA é vital saber onde estão armazenados os datacenters, não é necessário ter ciência do endereço do mesmo, mas a localização geográfica do equipamento. Essa informação é importante pois há outros pontos a serem avaliados em caso de falha do sistema:

- Os dados serão transferidos para fora do país?
- Em caso positivo, para que país?
- Quanto tempo os dados estarão nessa localidade?

Este ponto é notável, pois no papel de contratante, você poderá sofrer restrições jurídicas de um país ou outro quando o dado sair do país de origem.



6.1 QUEBRA DE PARADIGMAS NA SEGURANÇA DE DADOS

Uma vez contratada a empresa, seja ela administradora de nuvem pública, privada ou outro modelo, seus dados estarão em outras mãos. Isto é, seus dados estão sendo manejados por pessoas que você não tem ideia de quem seja. Dentro desse contexto é importante ter ciência de que todas as cláusulas contratuais estão sendo cumpridas.

No entanto alguns pontos podem ser observados para que haja um maior controle e tranquilidade quanto ao serviço prestado:

Um artigo da infoworld.com publicado em 2010 trazia o seguinte subtítulo:
- empregados velhacos e usuários sem noção podem causar mais dados que sujeitos maliciosos vindos de fora - (CSA, 2012). Esta “verdade” infelizmente é uma realidade na maioria das empresas. Dentro disso, há sim riscos reais durante a migração de dados e sobre quem está os administrando. Por esse motivo ao contratante é importante saber qual o treinamento recebido pelos funcionários dos prestador de serviço e quais as ações imediatas em caso de falha humana ou possível vazamento de dados.

• Os dados são de sua propriedade e isso precisa estar bem claro. Embora o manuseio, armazenamento fiquem a cargo do contratado o dado sempre será do cliente e deve estar disponível sempre que necessário.

6.2 PLANEJAMENTO ARQUITETURAL DE NUVEM

Você sabe qual é o caminho para a nuvem? Você tem só um provedor de internet? Se este provedor cair, como irá acessar seus dados em nuvem?

Se você não tem resposta a essas três perguntas, você não tem planejamento. Embora seja necessário e de vital importância questionar seu fornecedor de Nuvem é fundamental preocupar-se com o desenho de como chegar à nuvem e como manter-se conectado a ela.

Esse planejamento perimetral de rede interna é de suma importância para que todo o investimento na migração de dados não seja desperdiçado por falhas no planejamento. Segundo a CSA, é preciso manter uma infraestrutura interna com redundância contra falhas.

CONSIDERAÇÕES FINAIS

Como vimos até agora podemos concluir que qualquer tentativa de definir o que é *Cloud Computing* pode não ser 100% precisa. Isso porque as idéias por trás da noção de computação nas nuvens são recentes e as opiniões de especialistas em computação ainda divergem, mas já seguem um caminho de união. Mas é claro que tentamos facilitar esse entendimento nesse ebook.

A segurança e a privacidade da informação de uma organização, ou mesmo pessoais, é uma preocupação corrente em todas as esferas de negócio. É fato que a computação em nuvem causa, ainda, inúmeras dúvidas e interpretações equivocadas por falta de conhecimento teórico adequado ao o que é e como ela é aplicada. O tema é extenso e acima de tudo dinâmico, assim como a maioria das práticas em TI e novas tecnologias.

Nesse contexto, além de um planejamento e um desenho estrutural das necessidades internas e externas à contração de um serviço de nuvem, ter orientação teórica e técnica de como a tecnologia está sedimentada em questões de segurança e certificados é vital para a concepção de um negócio de sucesso e uma implantação sem problemas ou surpresas.

É claro que ainda há muita coisa por fazer. Por exemplo, a simples ideia de determinadas informações ficarem armazenadas em computadores de terceiros (no caso, os fornecedores de serviço), mesmo com documentos garantindo a privacidade e o sigilo, preocupam pessoas e, principalmente, empresas, motivo pelo qual este ponto precisa ser melhor estudado.

Além disso, há outras questões, como o problema da dependência de acesso à internet: o que fazer quando a conexão cair? Algumas companhias já trabalham em formas de sincronizar aplicações off-line com on-line, mas tecnologias para isso ainda precisam evoluir bastante.

De qualquer forma, o futuro já chegou. Além das mencionadas empresas neste ebook, companhias como Dell, Intel, Oracle e Microsoft já estão trabalhando nas mais variadas soluções para *cloud computing*.

Fontes: Penso Tecnologia; Teleco; Grupo Capgemini; InfoWester; Acom Sistemas; CSA.

“O futuro me interessa porque é o lugar onde vou passar o resto da minha vida”.

Woody Allen

Expediente:
Redação - Ivanir França | Domingos Teruel
Diagramação e Ilustração - Eduardo Castro | Ivanir França
Revisão - Vanessa Eufrásio

Materiais Educativos

Cultura Colaborativa

SOCIALBASE