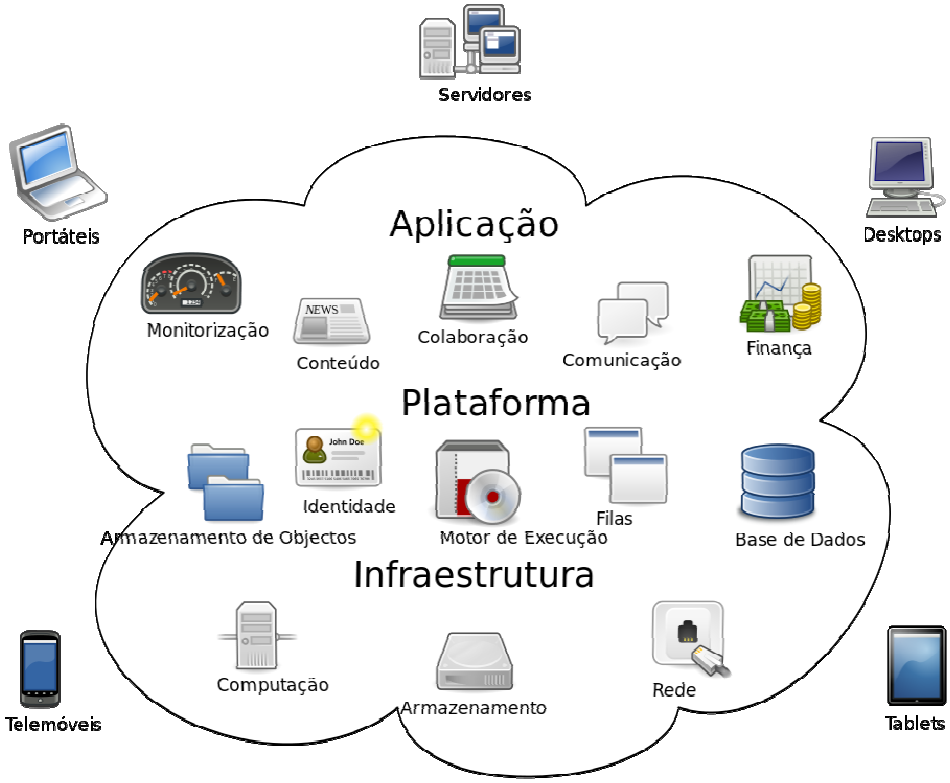

Conceito

Tecnicamente, um conceito bem aceito de computação em nuvem a define como “modelo tecnológico que habilita de forma simplificada o acesso on-demand a uma rede, a qual possui um pool de recursos computacionais configuráveis, como, por exemplo, redes, servidores, storages, aplicações e serviços. Esses recursos podem ser rapidamente provisionados, configurados e liberados com um esforço de gerenciamento mínimo e automatizados, promovendo alta disponibilidade.”

Características essenciais

Autosserviço por demanda: o consumidor pode unilateralmente provisionar recursos computacionais, como servidor de nomes ou espaço em disco, de acordo com sua necessidade, sem precisar de interação humana com o provedor de serviço.

Acesso por banda larga: recursos são disponibilizados pela rede e acessados através de formatos padrões por plataformas clientes heterogêneas, como celulares, laptops e PDAs.

Pool de recursos: recursos do provedor são combinados num modelo de multi-hospedagem, com recursos físicos e virtuais alocados dinamicamente, conforme a demanda. Existe uma sensação de independência de local, em que o consumidor não tem controle ou conhecimento da exata localização dos recursos, senão de uma forma genérica (país, estado ou centro de dados). Exemplos de recursos incluem espaço em disco, processamento, memória, banda e máquinas virtuais.

Elasticidade ágil: capacidades podem ser rápida e elasticamente provisionadas, em alguns casos automaticamente, aumentando ou diminuindo a utilização de recursos. Eles parecem ilimitados e podem ser adquiridos em qualquer quantidade a qualquer hora.

Serviço mensurado: sistemas de nuvem controlam e otimizam o uso de recursos automaticamente, contabilizando o uso de recursos em algum nível de abstração, tal como o uso de espaço em disco, processamento, banda ou contas ativas. O uso de recursos pode ser monitorado, controlado e reportado de forma transparente entre o consumidor e o provedor dos serviços.

Modelos de Serviço

Software como Serviço (SaaS): são oferecidas para o consumidor aplicações rodando em uma infraestrutura de nuvem do provedor, acessíveis por vários dispositivos clientes através de uma interface leve como um navegador de internet. O consumidor não gerencia a infraestrutura, exceto as configurações de usuário da aplicação.

Plataforma como Serviço (PaaS): são oferecidas para o consumidor formas de publicar aplicações geradas ou adquiridas por este, na infraestrutura de nuvem do provedor, criadas por linguagens de programação e ferramentas suportadas. O consumidor não gerencia a infraestrutura, mas tem controle sobre as aplicações e configurações de ambiente.

Infraestrutura como Serviço (IaaS): são oferecidas para o consumidor formas de provisionar processamento, espaço em disco, redes e outros recursos fundamentais onde o consumidor possa instalar software, incluindo sistemas operacionais e aplicações. O consumidor não gerencia a infraestrutura de nuvem, mas tem controle dos recursos provisionados, inclusive algumas configurações de componentes de rede (firewalls).

Modelos de Nuvem

Nuvem Privada: a infraestrutura de nuvem trabalha inteiramente para uma organização. Pode ser gerenciada por esta ou por um terceiro, assim como estar localizada interna ou externamente.

Nuvem Comunitária: a infraestrutura de nuvem é dividida entre várias organizações e tem um conselho para tratar as preocupações comuns, como missão, segurança e políticas. Pode ser gerenciada por esta ou por um terceiro, assim como estar localizada internamente ou externamente às organizações.

Nuvem Pública: a infraestrutura de nuvem está disponível para o público em geral ou um grupo específico e é de propriedade de uma organização que vende serviços de nuvem.

Nuvem Híbrida: a infraestrutura de nuvem é uma composição de mais de um modelo de nuvem que funcionam como entidades separadas, mas usam tecnologias padrões que possibilitam a portabilidade de dados ou aplicações.

Vantagens

Algumas das vantagens do sistema computação em nuvem, detectadas inicialmente são:

a) Disponibilidade – O usuário pode acessar aplicações e dados de qualquer lugar e a qualquer hora.

b) Escalabilidade – O usuário pode a qualquer momento aumentar ou diminuir os recursos alocados (memória, processamento e espaço de armazenamento) de acordo com suas necessidades.

c) Economia – O usuário diminuirá seus gastos como por exemplo: com infraestrutura, equipamentos, licenças de aplicativos proprietários, energia elétrica e manutenção de equipamentos.

A maior vantagem da computação em nuvem é a possibilidade de utilizar softwares sem que estes estejam instalados no computador. Mas há outras vantagens:

- Na maioria das vezes o usuário não precisa se preocupar com o sistema operacional e hardware que está usando em seu computador pessoal, podendo acessar seus dados na "nuvem computacional" independentemente disso;
- As atualizações dos softwares são feitas de forma automática, sem necessidade de intervenção do usuário;
- O trabalho corporativo e o compartilhamento de arquivos se tornam mais fáceis, uma vez que todas as informações se encontram no mesmo "lugar", ou seja, na "nuvem computacional";
- Os softwares e os dados podem ser acessados em qualquer lugar, basta apenas que haja acesso à Internet, não são mais restritos ao ambiente local de computação, nem dependem da sincronização de mídias removíveis.
- O usuário tem um melhor controle de gastos ao usar aplicativos, pois a maioria dos sistemas de computação em nuvem fornece aplicações gratuitamente e, quando não gratuitas, são pagas somente pelo tempo de utilização dos recursos. Não é necessário pagar por uma licença integral de uso de software;
- Diminui a necessidade de manutenção da infraestrutura física de redes locais cliente/servidor, bem como da instalação dos softwares nos computadores corporativos, pois esta fica a cargo do provedor do software em nuvem, bastando que os computadores clientes tenham acesso à Internet;
- A infraestrutura necessária para uma solução de computação em nuvem é bem mais enxuta do que uma solução tradicional de hospedagem ou alojamento, consumindo menos energia, refrigeração e espaço físico e consequentemente contribuindo para a preservação e o uso racional dos recursos naturais.

Desvantagens

A maior desvantagem da computação em nuvem vem fora do propósito desta, que é o acesso à internet. Caso você perca o acesso, comprometerá todos os sistemas embarcados.

- Velocidade de processamento: caso seja necessária uma grande taxa de transferência, se a internet não tiver uma boa banda, o sistema pode ser comprometido. Um exemplo típico é com mídias digitais ou jogos;
- Assim como todo tipo de serviço, ele é custeado.

Sendo a computação em nuvem uma forma de centralizar aplicações e armazenar dados, há uma grande preocupação no que diz respeito à segurança e privacidade. Ao utilizar o sistema, o usuário entrega seus dados e informações importantes aos cuidados de outra empresa, o que para muitos é uma questão bastante complicada, causa uma sensação de vulnerabilidade; ao contrário de hoje que estes dados e informações são bem guardadas por seus proprietários.

A privacidade pode ser comprometida já que um cliente pode se logar de qualquer local e acessar aplicações, para este fim as empresas que fornecem os serviços da computação em nuvem estudam uma forma de proteção, como técnicas de autenticação (usuário e senha); outra forma é empregar um formato de autorização por níveis de permissões, onde cada usuário acessa somente o que lhe é permitido.

A IBM recentemente divulgou uma nova oferta de segurança a qual descreve como a Plataforma de Segurança de Rede Virtualizada Proventia, um dispositivo virtual que consolida aplicativos de segurança como prevenção contra intrusos, além de proteger aplicativos web e oferecer a política de rede em uma única solução.

Gerenciamento da segurança da informação na nuvem.

Sete princípios de segurança em uma rede em nuvem:

- **Acesso privilegiado de usuários** - A sensibilidade de informações confidenciais nas empresas obriga um controle de acesso dos usuários e informação bem específica de quem terá privilégio de administrador, para então esse administrador controle os acessos.
- **Compliance com regulamentação** - As empresas são responsáveis pela segurança, integridade e a confidencialidade de seus próprios dados. Os fornecedores de computação em nuvem devem estar preparados para auditorias externas e certificações de segurança.
- **Localização dos dados** - A empresa que usa cloud provavelmente não sabe exatamente onde os dados estão armazenados, talvez nem o país onde as informações estão guardadas. O fornecedor deve estar disposto a se comprometer a armazenar e a processar dados em jurisdições específicas, assumindo um compromisso em contrato de obedecer aos requerimentos de privacidade que o país de origem da empresa pede.

- **Segregação dos dados** - Geralmente uma empresa divide um ambiente com dados de diversos clientes. Procure entender o que é feito para a separação de dados, que tipo de criptografia é segura o suficiente para o funcionamento correto da aplicação.
- **Recuperação dos dados** - O fornecedor em cloud deve saber onde estão os dados da empresa e o que acontece para recuperação de dados em caso de catástrofe. Qualquer aplicação que não replica os dados e a infra-estrutura em diversas localidades está vulnerável a falha completa. Importante ter um plano de recuperação completa e um tempo estimado para tal.
- **Apoio à investigação** - A auditabilidade de atividades ilegais pode se tornar impossível na computação em nuvem uma vez que há uma variação de servidores conforme o tempo onde estão localizados os acessos e os dados dos usuários. Importante obter um compromisso contratual com a empresa fornecedora do serviço e uma evidência de sucesso no passado para esse tipo de investigação.
- **Viabilidade em longo prazo** - No mundo ideal, o seu fornecedor de computação em nuvem jamais vai falir ou ser adquirido por uma empresa maior. A empresa precisa garantir que os seus dados estarão disponíveis caso o fornecedor de computação em nuvem deixe de existir ou seja migrado para uma empresa maior. Importante haver um plano de recuperação de dados e o formato para que possa ser utilizado em uma aplicação substituta.

Avaliação de riscos para a nuvem

Avaliar corretamente sua tolerância a riscos organizacionais é essencial antes de adotar uma plataforma de computação em nuvem.

Vic Winkler
Adaptado de "Securing the Cloud," publicado pela Syngress, um selo da Elsevier (2011)

É seguro usar uma nuvem pública? Essa é a pergunta prevalece sobre a nuvem de computação. A resposta completa, porém, depende de um entendimento claro do nível da sua organização de aceitação de risco. Noções básicas sobre quanto você pode tolerar o risco depende avaliar os requisitos de segurança e como valor seus ativos de informações como dados, aplicativos e processos.

Somente quando você compreende esses problemas você pode tomar uma decisão informada sobre qual implantação modelos e entrega de serviço são adequados para suas necessidades e tolerância ao risco. Identificação de ativos de informação é importante antes de adaptar um modelo público ou híbrido. Ambas as opções envolverá pelo menos algum grau de controle cedente sobre como essas informações serão protegidas e onde pode residir (local/jurisdição). Aumentou controle organizacional para uma nuvem privada internamente hospedada e operada internamente contra outras combinações.

E não se esqueça que a soma total dos ativos de informação não se limita a informação ou dados. Seus aplicativos e processos podem ser facilmente como confidenciais ou proprietárias como suas informações. Em muitos reinos como inteligência e das finanças, algoritmos ou programas que você usa freqüentemente são proprietárias e altamente secreto para a organização. Sua exposição pode constituir uma dramática perda para a organização.

Avaliar seu risco

Começar com uma análise de risco breve. Você deve fazer as seguintes perguntas:

- Categorização de ameaças: O que pode acontecer com seus ativos de informação?
- Impacto de ameaça: Quão grave que poderia ser?
- Frequência de ameaça: A frequência com que pode acontecer?
- Factor de incerteza: Como alguns estão você em responder a estas três perguntas?

A questão central com risco é expressa em termos de probabilidade de incerteza. O que você realmente quer saber é o que fazer sobre isso (contramedidas ou mitigação de risco). Depois de analisados e dirigida a riscos, você pode pedir várias outras questões:

- Atenuação: O que você pode fazer para reduzir o risco?
- Redução dos custos: O que a redução do risco de incorrer?
- Redução dos custos/benefícios: Mitigação é rentável?

Para ser claro, essas três perguntas são mais retóricas para uma nuvem pública do que para uma nuvem privado ou híbrido. Em uma nuvem pública, você começa o que você paga. O provedor de nuvem é a parte responsável por responder essas três perguntas. Da mesma forma, estas questões também são menos relevantes para Software como serviço (SaaS) do que para a plataforma como um serviço (PaaS), mas mais relevante ainda para infra-estrutura como um serviço (IaaS).

Risco e ativos de informações

A questão central com risco é a incerteza. Aplicando esse fator para sua pergunta, você deve examinar seus ativos de informação um pouco mais detalhadamente. Identificar os ativos de informação pode ser ilusória, especialmente com a "criar uma vez, cópia-frequentemente" aspecto do conteúdo digital.
A organização típica raramente tem controle suficiente sobre sua informação. Isso é muitas vezes mínima garantia de que não há nenhuma outras cópias de qualquer determinado elemento de dados. Do ponto de vista da proteção de dados digitais, que pode ser o pior. A maioria das organizações têm muitos outros problemas que gerenciar seus ativos de informação, embora.

Quando você está pensando em mudar seus ativos de informação para a nuvem, você precisará estar satisfeitos com o processo de categorização classes de informação versus bits específicos de informações. Infelizmente, aqui, também, há geralmente um problema. Isso pode não ser tão ruim se nossos sistemas de computação aplicada informações rotular, mas eles geralmente não. Informações marcação na maioria dos sistemas de computador são baseadas em processos reais de personalidades, que tenham necessidade de conhecer e a limpeza adequada para obter informações.
Isso é organizacionalmente controlada ao longo das linhas de classificação de informações e adicionais de manipulação advertências (tais como projeto x apenas).Os controles apropriados são geralmente insuficientes para impedir a duplicação digital e hemorragia de informação destina ou não intencional.
Lembrando a tríade de fatores de segurança (confidencialidade, integridade e disponibilidade), você pode pedir uma série de perguntas específicas em torno de informações activos nos moldes do que seriam a consequência ser se:

- O ativo de informações foi exposto?
- O ativo de informações foi modificado por uma entidade externa?
- O ativo de informações foi manipulado?
- O ativo de informações tornou-se indisponível?

Se essas questões suscitam preocupações sobre riscos inaceitáveis, você pode querer abordar o problema global, limitando o grau de risco processamento para uma nuvem privado (evitando a introdução de novos riscos). Use a nuvem pública para dados confidenciais de risco. Adopção de uma nuvem privada não eliminam a necessidade de controlos adequados.
Com isso em mente, você pode querer considerar os resultados de:

- Misturando terceirização em uma nuvem pública para dados não confidenciais e reservando sistemas internos de dados confidenciais, você pode ganhar algumas vantagens de custo sem assumir novos riscos.
- No caso de utilização de uma nuvem privada colocaria sem novos riscos para ativos de informação, uso de um híbrido ou modelo de nuvem pública pode.
- Alternar de um tradicional modelo para processamento interno para um modelo de nuvem privado pode reduzir o risco.

Estas são instruções razoáveis que se movem em direção ao alinhamento a importância de nossos ativos de informações em direção a modelos de implantação e os modelos de serviço.

Privacidade e confidencialidade preocupações

Além desses riscos para ativos de informação, você pode ser processamento, armazenar ou transmitir dados que tem assunto para regulamentar e requisitos de conformidade. Quando dados se inscreve no âmbito regulamentar ou restrições de conformidade, sua escolha de nuvem implantação (se privado, público ou híbrido) dobradiças em ser convencido de que o provedor é

totalmente compatível. Caso contrário, você corre o risco de violação da privacidade, regulamentar ou outros requisitos legais.
Esta obrigação para confirmar a gestão segura de dados geralmente recai sobre o inquilino ou usuário. As implicações para a manutenção da segurança da informação são importantes quando se trata de privacidade, negócios e segurança nacional.
Violações de privacidade ocorrem com frequência suficiente dentro de infraestruturas para você se preocupar com qualquer sistema de computação em nuvem — baseados em nuvem ou tradicionais. Isso é especialmente verdadeiro quando você estiver armazenando, processamento ou transmitir informações particularmente sensível tais como financeira ou dados de cuidados de saúde.
Em 2010, houve várias exposições de informações de privacidade de nuvem que ocorreram com um número de serviços baseados em nuvem, incluindo Facebook, Twitter, Inc. e Google Inc. Assim, as preocupações de privacidade com o modelo de nuvem não são fundamentalmente novas.
Como um inquilino de nuvem com as obrigações legais de privacidade, a maneira na qual você lidar com informações de privacidade não vai ser diferente se você usa nuvem ou armazenamento tradicional. Assim como você não iria armazenar essas informações em um servidor que carecia de controles adequados, não selecione qualquer provedor de nuvem sem verificar que se encontram os pontos de referência mesmos para como eles protegem dados em repouso, em transmissão ou enquanto ele é processado.
Isso é não quer para dizer que sua política razoavelmente pode excluir qualquer provedor externo gerenciar essas informações para você, nuvem incluído. E enquanto pode haver uma percepção de que o computador na sua mesa é mais seguro do que um que está em uma nuvem de pública, a menos que você está tomando as precauções técnicas e processuais incomuns com seu computador desktop, é mais apto a ser o único com a segurança mais fraca.

Governança de dados

Você deve reconhecer que a segurança de dados confidenciais e sua governança são duas questões distintas. Como parte da devida diligência, você precisará compreender totalmente o controle de privacidade do provedor juntamente com suas práticas de segurança e orientações.
Informações pessoais estão sujeita às leis de privacidade. Outras classes de informações de negócios e qualquer coisa relacionada à segurança nacional estão sujeita a leis e regulamentos muito mais rigorosos. Processos e informações de segurança nacional beneficiam de um corpo forte e desenvolvido de lei, regulamento e orientação.
Embora a nuvem é um modelo relativamente novo, deve ser amplo para restringir absolutamente qualquer informação classificada de residir em uma nuvem pública um exame estudou as orientações disponíveis. A área de preocupação provável encontra-se com outras funções de governo que não processam dados sensíveis ou confidenciais.
Basta dizer que, quando você examina a possibilidade de utilização de nuvens públicas, há muitas linhas distintas e separadas de negócios do governo

nacional para baixo para jurisdições locais. Dado o tamanho do governo e o número de níveis e jurisdições, parece como se o próprio governo poderia operar uma série de nuvens de Comunidade para seu uso exclusivo, assim, obter os benefícios e evitar problemas com a convivência em uma nuvem pública.
Por outro lado, se o governo é usar uma nuvem pública, esse serviço totalmente deve satisfazer os interesses do inquilino e todas as leis e regulamentos aplicáveis. É possível que um inquilino pode implementar controles de segurança adicionais que atendem aos requisitos regulamentares ou legais, mesmo quando um subjacente IaaS pública ou PaaS totalmente não atender a esses mesmos requisitos.
No entanto, você tem que entender que o intervalo de controles adicionais que podem ser adicionados por um inquilino são limitadas e não pode superar muitas lacunas em alguns serviços público cloud. Manter seu olho na bola quando se trata de segurança é essencial, seja qual for o modelo de nuvem que você escolhe ou consoante o que se adapte às suas necessidades organizacionais.

Fonte:

https://www.serpro.gov.br/inovacao/computacao-em-nuvem

https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem#Vantagens

http://computacaonuvem.blogspot.com.br/2011/03/vantagens-e-desvantagens-da-computacao.html

https://technet.microsoft.com/pt-br/magazine/hh750397.aspx