“Cloud Computing
Segurança e Privacidade da Informação na Nuvem”

António Luís Jesus Mendes da Silva

IESF – Instituto Superior de Estudos Financeiros e Fiscais

Julho 2012

“Cloud Computing
Segurança e Privacidade da Informação na Nuvem”

Abstract

We are in the midst of a revolution in information technologies, under the name of Cloud Computing. Indeed, more than a new technology or a new model of computation, we can consider that it is more like a new business model. Despite the apparently good reception with which companies are facing this new model, are often cited as the main obstacles to its implementation, fears in terms of security, legality and privacy of information. This paper briefly describes the main characteristics of Cloud Computing, and then focuses on key issues related to security and privacy of information in the cloud, highlighting the most important aspects that companies and organizations should aim to ensure, when adopting a model of Cloud Computing.

Resumo

Estamos no meio de uma revolução em termos de tecnologias de informação, que dá pelo nome de Cloud Computing. Com efeito, mais do que uma nova tecnologia ou um novo modelo de computação, podemos considerar que é mais um novo modelo de negócio. Apesar da aparentemente boa recetividade com que as empresas estão a encarar este novo modelo, são frequentemente apontados como principais entraves à sua implementação, os receios em termos de segurança, legalidade e privacidade da informação. Este trabalho descreve resumidamente as principais características da computação na nuvem, e de seguida concentra-se nas principais questões relacionadas com a segurança e privacidade da informação na cloud, realçando os aspetos mais importantes que as empresas e organizações devem procurar garantir, aquando da adoção de um modelo de Cloud Computing.

Palavras-chave

Cloud Computing, Computação na Nuvem, Segurança, Privacidade, Tecnologias de Informação

Introdução

Nos últimos anos, a Cloud Computing – ou computação na nuvem – tornou-se numa tecnologia indispensável, deixando de ser utilizada apenas em meios laboratoriais, tendo passado para as empresas, com a promessa de menores custos, maior flexibilidade na gestão das soluções informáticas, melhorias na eficiência e com a possibilidade de escalabilidade à medida. Contudo, embora esta solução anuncie benefícios significativos, ela vai exigir que as organizações alterem a abordagem da sua plataforma de Tecnologias de Informação (TI).

Este artigo científico pretende abordar os principais pontos relacionados com os temas da segurança, propriedade e privacidade da informação na cloud, numa altura em que cada vez mais as empresas começam a adotar tecnologias de Cloud Computing. Contudo, uma das dificuldades encontradas durante a realização deste trabalho, foi a inexistência de dados concretos sobre a adoção do modelo de Cloud Computing pelas empresas portuguesas, bem como elementos que permitissem evidenciar eventos ocorridos no âmbito das falhas de segurança ou fuga/apropriação indevida de informação.

Cloud Computing é pois uma nova maneira de oferecer recursos de computação, e não uma nova tecnologia. Serviços de computação tais como armazenamento de dados, processamento de software ou tratamento de e-mail, estão agora disponíveis instantaneamente, sem compromisso e sob pedido. Uma vez que estamos numa época de restrições económico-financeiras, este novo modelo económico para a computação encontrou um terreno fértil e está a atrair investimentos maciços a nível global (Balboni, P. et al., 2009).

Com efeito, começa a ser consensual que o modelo de Cloud Computing traz vantagens para a plataforma de TI e para os sistemas de informação das empresas, tais como agilidade, facilidade de utilização, capacidade de expansão e não menos importante, redução de custos. Todavia, existe uma ambiguidade no sentimento das organizações em relação à segurança, pois ela representa quer um objetivo quer uma preocupação quando se trata de migrar para a nuvem, uma vez que os receios relativos à segurança e confidencialidade da informação bem como o controlo sobre os sistemas e as questões de responsabilidade em caso de problemas com a infra-estrutura, são ainda barreiras importantes na altura de considerar a migração para este novo modelo (Balboni, P. et al., 2009).

Revisão Teórica

Conceito de Cloud Computing

Nos últimos anos a tendência nas TI tem sido o caminho da participação colaborativa. A Cloud Computing segue esta tendência, utilizando a memória e as capacidades de cálculo e armazenamento de computadores e servidores partilhados e ligados através da Internet, seguindo o princípio da computação em grelha. O armazenamento dos dados é feito em serviços que podem ser acedidos de qualquer lugar e a qualquer hora, não havendo necessidade de instalação de programas ou de armazenamento local de dados. O acesso a programas, serviços e arquivos é remoto, através da Internet (daí a alusão à nuvem). Desta forma, com um sistema operativo disponível na Internet, a partir de qualquer computador e em qualquer sítio, pode-se aceder a informações, arquivos e programas num sistema único, independentemente da plataforma. O requisito mínimo é um computador compatível com os recursos disponíveis na Internet.

Cloud Computing é um modelo para permitir um acesso à rede, a pedido, omnipresente e conveniente, para um conjunto partilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços). Trata-se de uma tecnologia disruptiva que tem o potencial para melhorar a colaboração, a agilidade, a escalabilidade e disponibilidade, fornecendo oportunidades de redução de custos através da computação otimizada e eficiente. Este modelo prevê um mundo onde os componentes podem ser rapidamente orquestrados, provisionados, implementados e desativados, escalonando-os para cima ou para baixo para fornecer um modelo à medida de consumo e repartição de recursos (Cloud Security Alliance, 2011).

Como esta, existem muitas outras definições de Cloud Computing. Reunindo as definições propostas de vários especialistas (Vaquero, L. M. et al., 2009), chegou-se a uma definição integrada com um mínimo denominador comum. Embora sem uma análise aprofundada de cada uma das propostas individualizadas, foi possível com esta compilação ter uma ideia clara dos diferentes conceitos que os profissionais de TI têm na área de Cloud Computing. Assim, uma definição abrangente de Cloud Computing seria a de um grande grupo de recursos virtualizados facilmente acedíveis e utilizáveis (tais como hardware, plataformas de desenvolvimento e/ou serviços). Esses recursos podem ser dinamicamente reconfigurados para se ajustarem a uma carga variável (escala), permitindo assim uma otimização na utilização de recursos. Este conjunto de recursos é tipicamente explorado por um modelo de pagamento por

utilização, em que as garantias são oferecidas pelo provedor de fornecimento da infra-estrutura, através de níveis de serviços (SLAs) personalizados. Por outro lado, olhando para o mínimo denominador comum, leva-nos a uma definição que não existe, dado que nenhum recurso em particular é proposto por todas as definições. O conjunto de características que mais se assemelham a uma definição mínima seria a escalabilidade, o modelo de pagamento conforme a utilização (pay-per-use) e a virtualização.

Já segundo o National Institute of Standards and Technology (NIST), Cloud Computing é um modelo que permite o acesso em rede omnipresente e adequado, a um conjunto partilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente fornecidos com um mínimo esforço de gestão ou de interação com o fornecedor do serviço. Este modelo de Cloud Computing é composto por cinco características essenciais, três tipos de serviço, e quatro modelos de implementação, abordados nos pontos seguintes (Mell, P., Grance, T., 2011).

Características essenciais

Self-service a pedido: De acordo com as suas necessidades, um utilizador pode prover de forma unilateral e automática, recursos de computação tais como tempo de servidor ou armazenamento em rede, sem necessidade de interação humana com cada fornecedor de serviços.

Acesso por banda larga: Os recursos estão disponíveis na rede e podem ser acedidos através de mecanismos padrão que promovam a sua utilização por diferentes plataformas (por exemplo, telemóveis, *tablets*, computadores portáteis e estações de trabalho).

Conjunto de recursos: Os recursos computacionais do fornecedor do serviço são reunidos para servir vários utilizadores usando um modelo de múltiplos utilizadores, com diferentes recursos físicos e virtuais atribuídos dinamicamente de acordo com os pedidos destes últimos. Há um sentido de independência de localização em que geralmente o cliente não tem nenhum controlo ou conhecimento sobre o local exato dos recursos fornecidos, mas pode ser capaz de especificar o local num nível mais elevado de abstração (por exemplo, país, estado ou centro de dados). Armazenamento, processamento, memória e largura de banda de rede são exemplos destes recursos.

Elasticidade rápida: Os recursos podem ser configurados elasticamente e disponibilizados, em alguns casos automaticamente, muito rapidamente para fora e de uma forma que procura um aperfeiçoamento ativo. Do ponto de vista do consumidor, parece que os recursos disponíveis são muitas vezes ilimitados e passíveis de serem utilizados e apropriados em qualquer quantidade e a qualquer momento.

Serviço medido: Os sistemas de Cloud Computing controlam e otimizam automaticamente a utilização dos recursos, aproveitando uma capacidade de medição num nível de abstração apropriado para o tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de utilizador ativas). O uso dos recursos pode ser monitorizado e controlado, fornecendo transparência quer para o provedor quer para o consumidor final do serviço utilizado.

Tipos de serviço

Software as a Service ou Software como Serviço (SaaS). É disponibilizada ao utilizador, a capacidade de usar as aplicações do fornecedor do serviço, assentes numa infraestrutura na nuvem. As aplicações podem ser acedidas através de vários dispositivos, tais como um navegador Web (no caso por exemplo do Gmail ou do Google Docs) ou através de um programa. O utilizador não gere nem controla a infraestrutura subjacente da nuvem, incluindo a rede, os servidores, sistemas operativos, armazenamento de dados ou até mesmo definições do aplicativo, com a possível exceção de definições de configuração do aplicativo, específicas do utilizador.

Platform as a Service, ou Plataforma como Serviço (PaaS). O recurso fornecido ao consumidor é o de este implementar para a infraestrutura da cloud, aplicativos criados por si usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo fornecedor do serviço. O utilizador não gere nem controla a infraestrutura subjacente da nuvem, incluindo a rede, os servidores, sistemas operativos, armazenamento de dados, mas tem controlo sobre os aplicativos desenvolvidos e sobre as definições de configuração para o ambiente de alojamento de aplicativos.

Infrastructure as a Service ou Infraestrutura como Serviço (IaaS). O recurso fornecido ao consumidor é o de fornecer o processamento, armazenamento, redes e outros recursos fundamentais de computação onde o consumidor é capaz de desenvolver, implementar e executar software, tal como sistemas operativos e aplicações. O utilizador não gere nem controla a infraestrutura subjacente da nuvem, mas tem

controlo sobre sistemas operativos, armazenamento e aplicações instaladas (e possivelmente também poderá ter controlo, embora limitado, de alguns componentes de rede selecionados, tais como firewalls).

Modelos de implementação

Cloud Privada: A infraestrutura da nuvem é configurada para uso exclusivo de uma única organização que compreende múltiplos utilizadores (por exemplo, unidades de negócio). Pode ser de propriedade, gerida e operada pela própria organização, por uma entidade terceira, ou por uma combinação destas duas modalidades. Poderá existir dentro ou fora das instalações da organização.

Cloud de Comunidade: A infraestrutura da nuvem é configurada para uso exclusivo de um conjunto específico de utilizadores, que pertencem a empresas ou organizações que têm interesses comuns (por exemplo, requisitos de segurança, política de privacidade e aspectos de conformidade). Pode ser de propriedade, gerida e operada por uma ou mais das organizações da comunidade, por uma entidade terceira, ou por alguma combinação destas modalidades. Poderá existir dentro ou fora das instalações da organização.

Cloud Pública. A infraestrutura da nuvem é configurada para utilização aberta ao público em geral. Pode ser de propriedade, gerida e operada por uma empresa, instituição de ensino ou organização governamental, ou por alguma combinação destas modalidades. Existe nas instalações do fornecedor da cloud.

Cloud Híbrida. A infraestrutura da nuvem é uma composição de duas ou mais infraestruturas de nuvem distintas (de comunidade, privada ou pública) que se mantêm entidades únicas, mas que estão ligadas por uma tecnologia padronizada ou proprietária que permite a portabilidade dos dados e das aplicações.

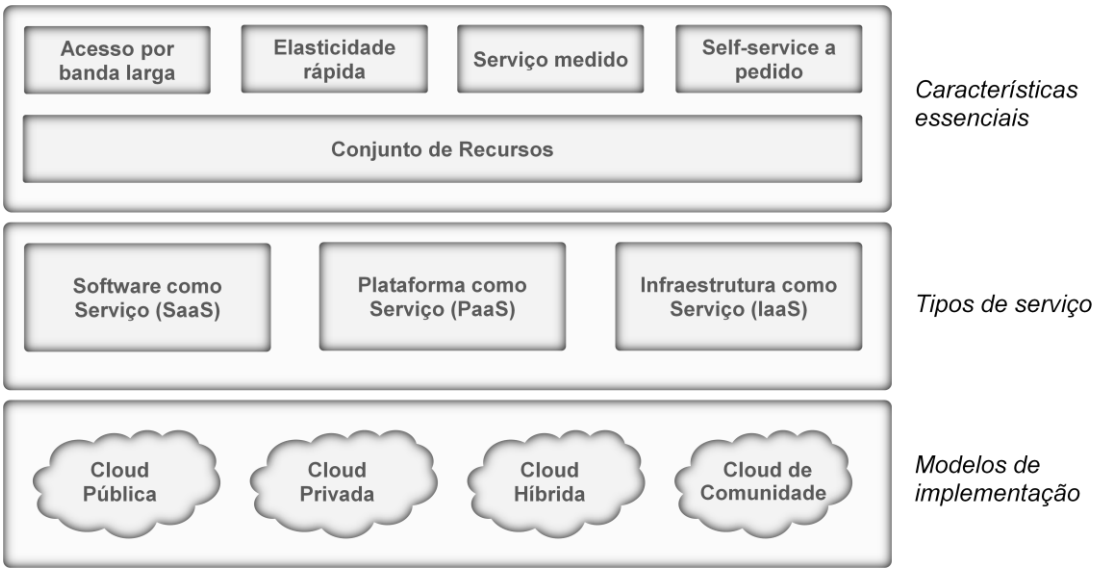

Figura 1 - Modelo visual da definição de Cloud Computing do NIST

Tão ou mais importante que a definição, importa perceber a proposta de valor da Cloud Computing, a qual assenta nas seguintes características-chave: capacidade de escalonamento e aprovisionamento de capacidade de computação, de uma forma dinâmica e economicamente eficiente, aliada à capacidade do consumidor final (seja ele um indivíduo ou uma organização) retirar o maior proveito possível desse poder de computação, sem ter que gerir a complexidade subjacente a essa tecnologia.

Análise Empírica

Segurança e Privacidade da Informação

Em qualquer sistema de computação em rede, a segurança e privacidade da informação é uma questão essencial. A Cloud Computing não é exceção, até porque é executada via Internet, que hoje em dia como sabemos está repleta de perigos e ameaças como vírus, malware ou pirataria informática, que podem destruir dados ou mesmo aceder aos computadores dos utilizadores ou aos seus dados pessoais se não forem tomadas medidas adequadas. É necessário então que os fornecedores de soluções de Cloud Computing, adotem as ferramentas e metodologias de segurança mais sofisticadas e atualizadas existentes atualmente, usando na sua operação elevados níveis de rigor e transparência, de modo a oferecer o nível máximo de segurança possível aos utilizadores e às organizações suas clientes, de modo a dirimir os receios existentes.

Com efeito, se não houver garantia de total segurança, não há motivos nem condições para uma organização fazer a transição para a nuvem.

Problemas de privacidade associados à cloud

O modelo de nuvem tem sido criticado por defensores da privacidade pela maior facilidade com que as empresas de hospedagem de serviços, podem monitorizar à vontade (legal ou ilegalmente), a comunicação e os dados armazenados entre os utilizadores e o provedor do serviço. Situações graves de quebra de confidencialidade de dados pessoais que já ocorreram, fazem com que a incerteza entre os defensores da privacidade cresça, dados os maiores poderes que este modelo dá às empresas de telecomunicações para monitorizar a atividade dos utilizadores. Usar um prestador de serviços na nuvem, pode dificultar a privacidade dos dados, devido à extensão em que a virtualização para o processamento (máquinas virtuais) e armazenamento na cloud são utilizados para implementar serviços em nuvem (Winkler, Vic (J.R.), 2011).

De facto, a virtualização altera a relação entre o sistema operacional e o hardware subjacente - seja este de computação, armazenamento ou mesmo de rede. Isto introduz uma camada adicional - virtualização – a qual deve ser corretamente configurada, gerida e protegida (Hickey, Kathleen, 2010).

Ainda segundo Winkler, a questão é que com este modelo as operações dos utilizadores junto do provedor de serviços, podem levar a que os dados não permaneçam no mesmo sistema, no mesmo centro de dados, ou até mesmo dentro da mesma nuvem ou provedor de serviços. Isto pode levar a questões legais sobre a jurisdição. A computação em nuvem coloca portanto problemas de privacidade, uma vez que o provedor de serviços pode aceder aos dados que estão na nuvem em qualquer ponto no tempo. Eles poderiam inclusivamente, de forma acidental ou deliberada, alterar ou mesmo apagar algumas informações (Ryan, Mark D., 2011).

Questões relacionadas com a segurança da informação

Como seria de esperar de qualquer mudança revolucionária no âmbito da informática e da computação globais, determinadas questões jurídicas surgem, desde violação de marcas registadas, a preocupações com a segurança na partilha de recursos de dados proprietários.

Na medida em se verifica uma crescente popularidade da computação em nuvem, também aumentam as preocupações relacionadas com as questões de segurança introduzidas através da adoção deste novo modelo. A eficácia e eficiência dos mecanismos tradicionais de proteção estão a ser reconsideradas, dado que as características deste modelo de implantação inovador podem diferir amplamente daquelas de arquiteturas tradicionais (Zissis, Dimitrios, Lekkas, Dimitrios, 2010).

Uma perspectiva alternativa sobre o tema da segurança na nuvem, é que este é outro (apesar de bastante amplo) caso de segurança aplicada, e que os princípios de segurança similares que se aplicam aos modelos de segurança para multi-utilizadores de mainframes (computadores de grande porte, grande capacidade) se podem também aplicar à segurança na nuvem (Winkler, Vic (J.R.), 2011).

Com efeito, os controlos de segurança na computação em nuvem não são, na maioria das vezes, diferentes dos controlos de segurança em qualquer ambiente de TI. No entanto, por causa dos modelos de serviços usados na nuvem, os modelos operacionais e as tecnologias utilizadas para permitir os serviços de Cloud Computing, podem fazer com que esta (computação em nuvem) apresente diferentes riscos para uma organização quando comparada com as tradicionais soluções de TI (Cloud Security Alliance, 2011), pois o número de pessoas com acesso aos dados da organização irá aumentar consideravelmente, o que, mais do que um desafio técnico, representa o problema de controlar quem acede à informação.

Mais, segundo o mesmo estudo, a postura de segurança de uma organização caracteriza-se pela maturidade, a eficácia e integridade da segurança ajustada aos controlos de risco implementados. Estes controlos são implementados numa ou mais camadas, que vão desde as instalações de segurança (segurança física), passando pela infraestrutura da rede (segurança da rede) e sistemas de TI (segurança do sistema), até à informação e segurança das aplicações. Além disso, os controlos são implementados ao nível das pessoas e dos processos, tais como separação de funções e gestão da mudança, respetivamente.

De todo o modo, é inegável que uma das maiores preocupações dos profissionais de TI relativamente à adoção e implementação de uma solução de Cloud Computing, é a segurança, sendo este um dos principais desafios que este modelo de computação enfrenta. A Gartner, líder mundial em pesquisa e consultoria em tecnologia de informação, afirma que a Cloud Computing tem atributos únicos que exigem assessoria de risco em áreas como a integridade dos dados, a recuperação de dados e privacidade, bem como uma avaliação de questões legais nas áreas de e-discovery,

conformidade de regulação e auditoria. Como tal, as empresas devem exigir transparência dos fornecedores de soluções cloud, evitando aqueles que se recusem a fornecer informações detalhadas das suas políticas de segurança. De seguida, enumeram-se os sete principais riscos que segundo a Gartner devem ser questionados, antes de se selecionar um fornecedor de serviços na cloud (Brodkin, Jon, 2008):

1. **Acesso privilegiado de utilizadores**: Dados sensíveis processados fora da empresa trazem, obrigatoriamente, um nível inerente de risco. Os serviços terciarizados fogem dos controlos físicos, lógicos e de pessoas, que as áreas de TI exercem quando no ambiente da empresa. O conselho a seguir é conseguir o máximo de informação sobre quem vai gerir os dados e solicitar aos fornecedores que passem informações específicas sobre quem terá privilégios de administrador no acesso aos dados, para assim, poder controlar esses acessos;

2. **Cumprimento de regulamentação:** As empresas são as responsáveis pela segurança e integridade dos seus próprios dados, mesmo quando essas informações são geridas por um provedor de serviços. Os provedores de serviços tradicionais estão sujeitos a auditores externos e a certificações de segurança, pelo que os fornecedores de Cloud Computing que recusem submeter-se a esse tipo de escrutínio, estão a dar uma indicação aos seus clientes que o único uso para o qual se pode confiar neles, é apenas para dados não sensíveis;

3. **Localização dos dados:** Quando uma organização (seja uma empresa ou até um governo) está a usar a cloud, o mais provável é não saber exatamente onde os dados estão armazenados. Na verdade, pode nem se saber qual é o país em que as informações estão guardadas. Os fornecedores deverão pois ser questionados sobre se estão dispostos a comprometerem-se a armazenar e a processar dados em jurisdições específicas, bem como se estão dispostos a contratualizar o compromisso de obedecer aos requerimentos de privacidade desse país, em nome do cliente que representam;

4. **Segregação dos dados:** Os dados de uma empresa quando estão na nuvem, normalmente partilham um ambiente de armazenamento com dados de outros clientes. A criptografia dos dados é eficaz, mas não é a solução para tudo. A

recomendação aqui é no sentido do fornecedor informar quais as medidas usadas para separar os dados e fornecer provas em como a criptografia foi criada e desenhada por especialistas com experiência. De notar que problemas com a criptografia, podem fazer com que os dados fiquem inutilizáveis e mesmo a criptografia normal pode comprometer a disponibilidade dos mesmos;

5. **Recuperação dos dados:** Mesmo se a empresa não sabe onde estão os seus dados, um fornecedor de serviços na cloud deve saber o que acontece com essas informações em caso de desastre. Qualquer oferta de serviços que não replique os dados e a infraestrutura de aplicações em diversas localidades, está vulnerável a uma falha completa. Deverá ser confirmado com o fornecedor se ele tem a capacidade de fazer uma completa restauração dos dados e quanto tempo esta poderá demorar;

6. **Apoio à investigação:** A investigação de atividades ilegais pode ser impossível num ambiente de Cloud Computing. Os serviços na nuvem são especialmente difíceis de investigar, dado que o acesso e os dados dos vários utilizadores podem estar localizados em vários lugares, espalhados numa série de servidores que são alterados constantemente. Se não for possível conseguir um compromisso contratual que suporte formas específicas de investigação, junto com a evidência de que esse fornecedor já tenha feito isso com sucesso no passado, o mais provável é que em caso de existir um problema, os dados sejam impossíveis de recuperar;

7. **Viabilidade a longo prazo:** Num mundo ideal, o provedor de Cloud Computing jamais irá falir ou ser adquirido por uma empresa maior. No entanto, as empresas precisam de garantir que os seus dados estarão disponíveis caso isso aconteça. Como tal, deverá ser questionada a forma de conseguir os dados de volta e se os mesmos estarão num formato que possa ser importado para uma outra aplicação que substitua a anterior.

Conclusões

Sendo certo que a migração para Cloud Computing é tentadora, à semelhança de outras medidas que anunciem reduções nos custos de TI, as vantagens da mudança

não são só financeiras. Há importantes ganhos qualitativos, tais como a redundância, a escalabilidade e a conectividade global.

Contudo, o mover para a nuvem ainda levanta muitas questões sobre a segurança e a privacidade da informação, pelo que as empresas encaram com algumas reservas estes processos de migração.

De facto, a computação em nuvem parece ser uma revolução inevitável que avança a um ritmo rápido. Os pontos abordados mostraram que os serviços de computação em nuvem trazem um grande número de questões legais, juntamente com inquestionáveis benefícios económicos. A proteção de dados e as questões de segurança dos mesmos, são de longe os maiores problemas para os provedores de serviços na cloud e para os seus clientes, quer organizações, quer indivíduos.

Assim, uma das conclusões deste trabalho, é que as economias de escala da nuvem e a sua flexibilidade são quer um amigo quer um inimigo do ponto de vista da segurança. As concentrações maciças de recursos e dados, afiguram-se um alvo mais atraente para os hackers, mas as medidas de defesa de sistemas baseados na nuvem podem ser mais robustas, escaláveis e melhores do ponto de vista custo/benefício.

Como acontece em quase todas as novas tendências tecnológicas, a Cloud Computing apresenta também pontos não amadurecidos, e que deverão ser alvo de aperfeiçoamento num futuro próximo. As melhorias de segurança são necessárias para que as empresas possam confiar dados sensíveis sobre uma infraestrutura cloud (Vaquero, L. M. et al., 2009). Apesar disso, esta solução afigura-se vantajosa para as empresas, que devem no entanto ponderar muito bem todas as questões relacionadas com a privacidade e a segurança da informação, antes de avançar para este modelo.

Os governos e as instituições competentes, deverão estar atentos a este fenómeno crescente e trabalhar em medidas legislativas que regulem e limitem eficazmente os termos em que os provedores de serviços na cloud operam. Hoje em dia, esses fornecedores de serviços têm acesso a informações extremamente detalhadas sobre os seus clientes. Esta informação surge naturalmente a partir dos próprios serviços prestados. Há medida em que a computação em nuvem se torna cada vez mais importante, assistiremos seguramente a um padrão evolutivo semelhante no que respeita aos dados ricos em informação que os prestadores de serviços na cloud terão à sua disposição, originários das atividades dos seus clientes.

No passado, regulamentaram-se intermediários nas questões que envolviam transação de dados, tais como operadores de televisão por cabo, empresas de telecomunicações e bancos, limitando-se as formas pelas quais eles poderiam usar as informações que detinham. Presumivelmente, as mesmas forças que animavam essas preocupações com as regras fundamentais sobre a privacidade do cliente, precisam agora de ser usadas para avaliar os novos intermediários de informação (Picker, R. C., 2008).

Limitações e Investigação Futura

Este é um trabalho essencialmente teórico, dada a inexistência de dados públicos que ilustrem informação referente à adoção da Cloud Computing por parte das empresas. É também um tema relativamente recente, pelo que não há qualquer tipo de histórico que possa servir de sustentação a possíveis análises às questões relacionadas com a segurança e privacidade da informação.

Dada a amplitude do conceito de cloud computing, uma sugestão para investigação futura é segmentar as análises pelos tipos de serviço mais comummente usados, SaaS, PaaS e IaaS, bem como pelos tipos de aplicação de computação na nuvem mais procurados, nomeadamente armazenamento de dados, gestão de e-mail e software aplicacional.

Implicações na Gestão Empresarial

A Cloud Computing é uma tendência que seguramente crescerá nos próximos anos, representando um novo paradigma que oferece diversos benefícios, proporcionando às empresas uma economia de recursos, mantendo o foco nos seus negócios. A comodidade de aceder aos dados a partir de qualquer lugar, com gastos inferiores na utilização de software, dado que o pagamento não é via licenciamento mas sim pela utilização, aliada às atividades que a empresa deixa de ter que suportar, tais como instalação de servidores, manutenção da operação, armazenamento de dados, e oferta/atualização das aplicações, entre outras, são fatores aliciantes para as empresas.

Um recente estudo da IDC (empresa líder mundial na área de serviços de consultoria e organização de eventos para os mercados das Tecnologias de Informação) sobre

"Transformação do negócio nas organizações portuguesas", indica que mais de 90% das grandes organizações portuguesas já desenvolveu ou estão a desenvolver processos de transformação do negócio para reduzir custos e aumentar a competitividade. Este estudo resultante de um inquérito aplicado às 300 maiores organizações portuguesas, públicas e privadas, apurou ainda que dado o atual ambiente de crise económica, entre outras alterações, as empresas estão a apostar na redução de custos e na inovação de processos de negócio. Ainda segundo o mesmo estudo, 60% dos empresários portugueses considera que as tecnologias de informação têm um papel crucial para as organizações avançarem com um processo de transformação e 79% afirma que estas são vitais para o negócio.

Já um recente inquérito da Symantec (líder mundial no fornecimento de soluções de segurança informática) aponta que a partilha de ficheiros online é o grande risco das PMEs, pois com o crescente aumento desta prática, aumentam também as vulnerabilidades das empresas em termos de segurança e perda de dados. Com efeito, muitos colaboradores das empresas começam a adotar livremente soluções cloud para partilha de ficheiros, sem supervisão das equipas de IT, o que poderá levar a graves problemas e colocar em risco a própria sobrevivência do negócio dessas empresas. É urgente nestes casos que as empresas centralizem o armazenamento e a gestão dos ficheiros num sistema online seguro e acessível, implementem controlos de acesso e permissões, garantindo a supervisão de quem acede e partilha os ficheiros, tudo isto de uma forma escalável, de modo a que o sistema possa crescer com a empresa e de acordo com as suas necessidades.

É pois de esperar que dentro deste cenário, as soluções de Cloud Computing representem um papel muito relevante nas estratégias destas organizações, no sentido da redução de custos e da inovação de processos.

Referências

Balboni, Paolo, Mccorry, Kieran & Snead, David: Cloud Computing – Key Legal Issues. em: Cloud Computing Risk Assessment. European Networks and Information Security Agency (ENISA), 2009, disponível em: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Brodkin, Jon (2008). Gartner: Seven cloud-computing security risks. Network World, disponível em: http://www.networkworld.com/news/2008/070208-cloud.html

Cloud Security Alliance, (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

Fibra (2012): Partilha de ficheiros é o grande risco das PMEs, disponível em http://www.fibra.pt/empresas/5387-partilha-de-ficheiros-e-o-grande-risco-das-pmes.html

Hickey, Kathleen (2010): Dark cloud: Study finds security risks in virtualization, disponível em: http://gcn.com/articles/2010/03/18/dark-cloud-security.aspvx

IDC (2012). Principais conclusões do estudo "Transformação do negócio nas organizações portuguesas", disponível em http://www.idc.pt/press/pr_2012-06-27.jsp

Mell, Peter & Grace, Tim: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011, disponível em: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Picker, R. C. (2008). Competition and Privacy in Web 2.0 and the Cloud, 414(June).

Ryan, Mark D. (2011): Cloud Computing Privacy Concerns on Our Doorstep, em Communications of the ACM, Vol. 54 No. 1, páginas 36-38, disponível em: http://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext

Vaquero, L. M., Rodero-merino, L., Caceres, J., & Lindner, M. (2009). A Break in the Clouds: Towards a Cloud Definition, 39(1), 50-55.

Wikipedia [Online] http://en.wikipedia.org/wiki/Cloud_computing

Winkler, Vic (J.R.) (2011): Securing the Cloud - Cloud Computer Security Techniques and Tactics, Syngress, Massachusetts

Zissis, Dimitrios, Lekkas, Dimitrios (2010): Addressing Cloud Computing security issues em Future Generation Computer Systems, Volume 28, Número 3, Março 2012, Páginas 583–592, disponível em: http://dx.doi.org/10.1016/j.future.2010.12.006