Cloud Computing:
Governação, riscos e auditoria dos serviços de TI

Luis Filipe Rocha [1]

1) Diretor Sistemas Informação do Grupo Amorim Turismo e Professor convidado na Universidade Portucalense Infante D. Henrique, Porto

luis.filipe@amorimturismo.pt e luisr@upt.pt

Resumo

Os serviços de computação na "nuvem", vulgarmente conhecidos por *Cloud Computing*, são presença cada vez maior no portfólio de serviços dos *providers* a operar no mercado das TI. A passagem para a "nuvem" relaciona-se frequentemente com uma visão de menores custos e maiores oportunidades de negócio, geradas por um novo modelo de distribuição de serviços de TI. Porém, existem riscos e ameaças que são necessárias mitigar contribuindo para isso uma Governação eficaz desses serviços, a definição de métricas de desempenho e a implementação de mecanismos de monitorização permanente.

Nesse contexto o modelo de *Cloud Computing* reveste-se de particularidades que o distinguem dos tradicionais modelos de computação na "nuvem". Os riscos são diferentes para cada modelo de serviço de TI na *Cloud* e são diferentes para cada modelo de implementação.

Nessa medida é vital uma clarificação do conceito subjacente ao modelo e às áreas críticas de operação, como o caminho para identificar com maior rigor os riscos existentes e assim avaliar o grau de ameaça que representam para as empresas.

Palavras chave: *Cloud Computing*, Governação de TI, Riscos, Auditoria de segurança das TI, *Cloud Services Provider*, *CobIT 5*, *SLA, Computação na "nuvem", SaaS, IaaS, PaaS*

1. Introdução

Nos últimos anos a oferta de serviços de Tecnologias de Informação (TI) em infraestruturas, plataformas e aplicações na *Cloud* tem crescido de forma exponencial, como resposta aos desafios dos mercados, sujeitas a variações extremas que requerem respostas rápidas e flexíveis por parte das TI, mas também devido a constrangimentos económicos que há muito deixaram de ser conjunturais.

O último relatório da Capgemini, "*Word Quality Report 2013-2014*" [1] [ISACA Journal - BIG DATA, 2014], estima que 32% de todos os testes de software se referem a aplicações na *Cloud* enquanto um outro estudo da Gartner "*Gartner Identifies Seven Major Projects CIOs Should Consider During the Next Three Years"* [2] estima que o mercado de *Cloud Computing* atinja os $150 bilhões USD em 2014 pelo que esta tendência não deve ser menosprezada, nem pelos fornecedores de serviços de TI na Cloud, *Cloud Services Providers* (CSP), nem pelas empresas clientes que podem beneficiar e alavancar o seu negócio a partir desses serviços.

As principais razões que levam as empresas a optar pelo *Cloud Computing* estão geralmente associadas às características do serviço, onde se destaca uma maior eficácia na gestão dos recursos de TI, maior agilidade e acesso a tecnologias inovadoras e, por conseguinte, a uma maior competitividade no mercado em que operam e aos menores custos de investimentos em TI.

Os impactos na gestão e nas operações diárias das empresas são, no entanto, inúmeros:

Riscos de segurança, ameaças de exposição da privacidade dos dados sensíveis das empresas, riscos de disponibilidade dos serviços ou riscos de conformidade com requisitos legais e estatutários [Thor Olavsrud, 2012].

As notícias dão-nos conta, quase diariamente, de exemplos como estes que acabámos de referir. Por exemplo a falha em larga escala dos serviços da *Amazon*, em 2011, as vulnerabilidades da *Dropbox* que permitiram o acesso de utilizadores aos dados de outros utilizadores sem autorização ou mesmo os casos recentes discutidos ao nível da *National Security Agency* (NSA), de *Edward Snowden* [ISACA Journal - BIG DATA, 2014]!

Enfim, riscos estimáveis mas que são uma barreira difícil de ultrapassar para as empresas, os *Cloud Services Customer* (CSC), ponderem migrar os seus serviços de TI empresariais para um modelo de *Cloud Computing* [COBIT5 Security, 2012].

Estes aspetos reforçam o argumento da necessidade destes riscos serem tratados e controlados de modo a não interferirem no alinhamento estratégico do *Cloud Computing* com os objetivos do negócio do cliente, o CSC.

Neste artigo iremos refletir sobre esse conjunto de aspetos que devem ser considerados previamente à mudança dos serviços de TI para a *Cloud.* Vamos começar por:

- Definir com maior rigor o conceito *Cloud Computing* de acordo com a definição da *National Institute of Standards and Technology* (NIST) e o atual paradigma BPaaS e ITaaS [3], definidos mais adiante, e os principais aspetos que o caracterizam e distinguem dos tradicionais modelos de computação na "nuvem";
- De seguida iremos identificar os principais riscos e ameaças que pesam sobre as decisões inerentes à passagem dos serviços de TI para a *Cloud*;

[1] www.capgemini.com/thought-leardship/world-quality-report-2013-14

[2] www.gartner.com/newsroom/id/1465614

[3] Business Processes as a Service; IT as a Service

- Por fim identificamos o papel da Governação das TI e a função desempenhada pela Auditoria de Sistemas de Informação (ASI) na identificação e mitigação dos riscos deste modelo de negócio de serviços de TI na *Cloud*.

2. *Cloud Computing*

Cloud Computing não é apenas computação na "nuvem"! Com efeito, de acordo com a definição do *National Institute of Standard and Technology* [NIST 2012], *Cloud Computing* é um modelo que permite o acesso a pedido do cliente (CSC) a um conjunto partilhado de recursos de Tecnologias de Informação (TI), como por exemplo, componentes de rede, servidores, armazenamento e aplicações de computador, rapidamente fornecidos e disponibilizados, com um mínimo de esforço e interação por parte do fornecedor de serviços *Cloud* (CSP) [HARDING 2011]. Qualifica-se desta forma devido às suas cinco características essenciais, aos seus três modelos de serviço e quatro modelos de implementação, ilustrados na figura 1.

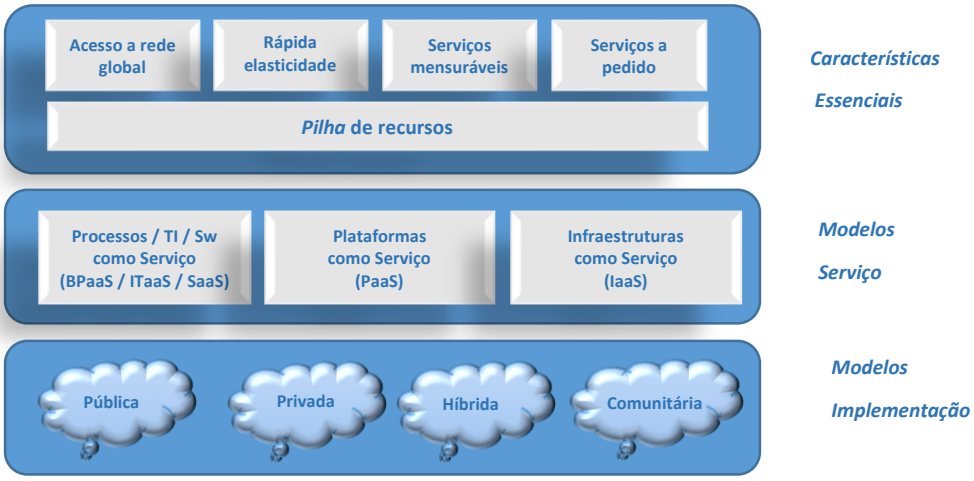

Figura 1 - Modelo visual da NIST de definição de *Cloud Computing*, adaptado [CSA 2012]

O conceito "*as a service*" pode ainda ser aplicado aos processos de negócio, apesar de não estar ainda incluído na taxonomia do modelo de *Cloud Computing* da NIST, (*Cloud Computing 2.0*), como o *payroll*, *CRM* e *billing*, designando-se neste caso, por *Business Process as a Service* (BPaaS) [IBM DeveloperWorks, 2012] . O BPaaS difere do SaaS por incluir serviços na *Cloud* em parte executados por pessoas e não apenas por aplicações de *software* [Mike Kavis, 2013].

A um outro nível temos ainda o *IT as a Service* (ITaaS), desde que fornecido por *Cloud Services Providers* (CSP) que inclui a quantidade de serviços de TI, designadamente *hardware*, software e suporte, para que o *Cloud Services Customer (CSC)* possa gerir o seu negócio e os seus Sistemas de Informação como um todo (SaaS, PaaS e IaaS) [VMWARE CIO, 2012].

Estes aspetos, fundamentalmente os que fazem parte da taxonomia NIST, no seu conjunto e em simultâneo distinguem o *Cloud Computing* de outros modelos tradicionais de computação na "nuvem".

São inúmeras as vantagens económicas e operacionais para as organizações, mas existem também muitos desafios e obstáculos que as empresas, os CSC devem analisar. Vantagens que decorrem da disponibilidade, rapidez, flexibilidade e escalabilidade no fornecimento dos serviços de TI,

que passam a ser disponibilizados a pedido do cliente e à medida das suas necessidades. Por outro lado, a motivação por um CAPEX[4] mais reduzido, uma vez que se adota um conceito *pay-as-you-go*, sem investimento inicial em *hardware* ou *software*, ao mesmo tempo que se liberta a empresa do peso e do ónus da gestão técnica das TI. Mas a migração de uma infraestrutura de TI na parte ou no todo para um CSP não isenta de responsabilidades a empresa cliente, o CSC, perante terceiros, *stakeholders* e *shareholders*, dos resultados e impactos negativos possíveis que daí possam resultar! Quando se opta por serviços na *Cloud* é vital que a empresa tenha o *know-how*, as competências e capacidades internas que assegurem uma adequada monitorização da qualidade dos serviços fornecidos pelo *Cloud Services Providers* (CSP). Este tema será, porventura, um dos primeiros desafios dos profissionais de segurança das TI que passam a ter de lidar com um novo paradigma de serviços, paradigma esse em grande parte relacionado com o nível de abstração que incorpora o modelo *Cloud Computing*, como aliás iremos explicar mais adiante [ISACA Journal - BIG DATA, 2014].

Os desafios seguintes resultam da perda do controlo direto e do sentido de localização física dos dados, dos potenciais riscos associados à partilha de recursos, nomeadamente aplicacionais, devido às características *multitenancy*[5] do modelo, mas também, não menos importante, à dependência e perda de autonomia para terceiros, dos serviços de TI [CLOUD COMPUTING 2012].

3. Riscos do *Cloud Computing*

A segurança e a privacidade são, como vimos, as preocupações mais frequentemente apontadas e também os maiores obstáculos à adoção dos serviços de TI na *Cloud*. Não obstante isso, a análise de riscos do *Cloud Computing* difere também, não apenas em cada um dos modelos de serviço, mas também em cada um dos modelos de implementação que forem adotados.

Relativamente aos vários modelos de serviço, uma das implicações imediatas que decorre da decisão de mudar para a *Cloud* é o facto dos ativos de informação passarem a ser geridos pelos *Cloud Services Providers* (CSP), tornando transparente e abstrata para o cliente, o CSC, a tecnologia e os processos que suportam esses ativos. Esta falta de visibilidade, também designada por camada de abstração, é o denominador comum em todos os modelos de serviço e extremamente importante para uma adequada avaliação de risco [COBIT5 Assurance, 2014].

Cada modelo corresponde a um determinado nível de abstração, conforme podemos observar na figura 2, que vai aumentando à medida que aumenta também o número de camadas de serviço fornecidas pelo CSP.

O modelo *Infrastructure as a Service* (IaaS) corresponde ao menor nível de abstração, uma vez que inclui apenas infraestrutura, como instalações, hardware, storage e recursos de processamento, enquanto o modelo *Software as a Service* (SaaS) corresponde ao mais alto nível de abstração, uma vez que inclui aplicações, plataformas (*middlware*) e toda infraestrutura. Neste último modelo o cliente CSC ignora as camadas que suportam o software aplicacional e isso significa que quanto maior for o nível de abstração, maior será o risco e por conseguinte maiores as ameaças que devem ser levadas em consideração. É este aspeto cumulativo do risco que existe nos modelos de serviço na *Cloud* [CLOUD COMPUTING 2012], que deve ser considerado na análise de risco deste modelo.

---

[4] *Capital expenditure* - despesas de capital ou investimento em bens de capital de uma empresa.

[5] Característica que permite que uma instância de *software* instalado num servidor possa servir múltiplos clientes de várias organizações

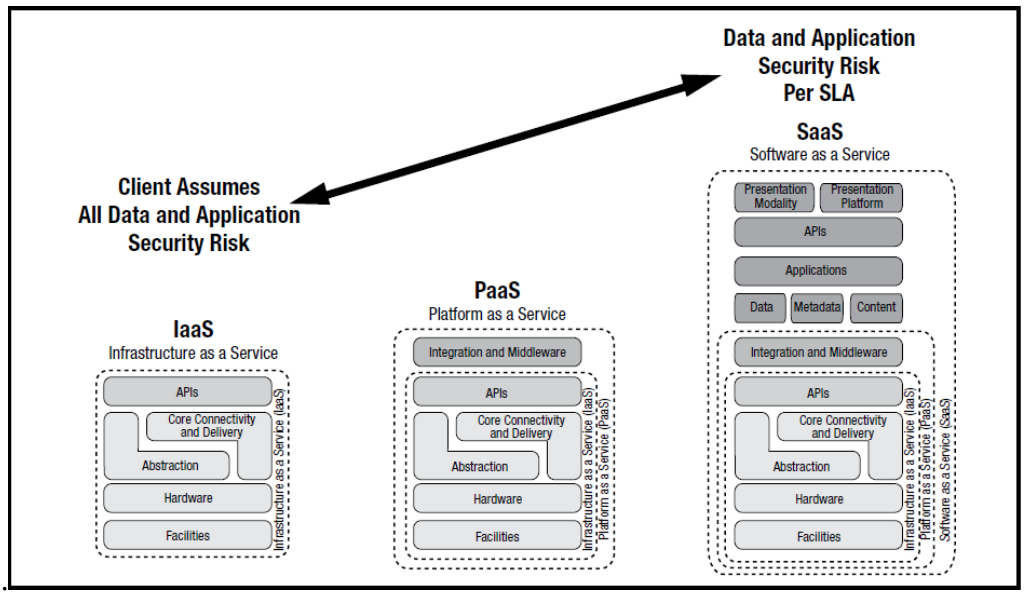

Figura 2 - Modelos de serviço *Cloud computing* fonte: [CLOUD COMPUTING 2012]

De acordo com o *ISACA*, "*Security Considerations for Cloud Computing"* [CLOUD COMPUTING 2012], são identificados e caracterizados os potenciais riscos geradores de eventos com impacto negativo, classificados de acordo com a ameaça produzida ou seja o risco que representam para a empresa cliente, os *Cloud Services Customer (CSC)*. Estes riscos são tipificados em **I**ndisponibilidade da informação, **P**erda, **R**oubo, ou **D**ivulgação de dados sensíveis e são listados a seguir, de acordo com cada um dos modelos de serviço (*IaaS, PaaS, SaaS*) e depois para cada um dos modelos de implementação Publica, Privada, Hibrida e Comunitária.

A) Fatores de risco do modelo de serviço Infraestrutura como Serviço (IaaS)

O modelo de serviço IaaS permite que um CSC use determinada infraestrutura, que pode ir desde as instalações para alojar equipamentos informáticos em ambiente perfeitamente controlado, até aos equipamentos propriamente ditos, como servidores, processadores, memória RAM, espaço para guardar informação (*storage)* e serviços de rede (*switching* e *networking)*. De entre os vários riscos inerentes a este modelo de serviço destacamos os seguintes, de acordo com a *ISACA* em "*Security Considerations for Cloud Computing"* [CLOUD COMPUTING, 2012]:

1. *Requisitos legais transfronteiriços* – assume riscos de Divulgação - quando o *Cloud Service Provider* (CSP) opera fora do território, em países com legislação diferente, é necessário identificar todos os requisitos legais para garantir que o *Cloud Services Consumer* (CSC) não está a violar as leis desse país ao guardar e a processar os seus dados através da infraestrutura do CSP;
2. *Multitenancy e falha de isolamento* – incorpora riscos de Roubo e/ou Divulgação - um dos grandes benefícios da *Cloud* reside na possibilidade de partilha de recursos de *hardware* e *software* por várias entidades (*tenants*). Neste ambiente *multitenant* é fundamental que os recursos partilhados sejam totalmente isolados e protegidos de forma que não haja divulgação de dados por outros *tenants*, por exemplo em situações de realocação de recursos, sendo esse o risco que deve ser controlado e mitigado;
3. *Falta de visibilidade das medidas técnicas de segurança no local* - inclui riscos de Perda, Roubo, Indisponibilidade e/ou Divulgação - é da responsabilidade do CSP fornecer as capacidades contratadas, garantindo que não há falhas de segurança através de uma

adequada governação e política de segurança que vá de encontro às necessidades do cliente;

4. *Ausência de Disaster Recovery Plan (DRP) e backup* – inclui riscos de Indisponibilidade e/ou Perda - este fator implica um alto grau de risco pelo que o CSP deve assegurar estas medidas básicas preventivas alinhadas com as necessidades do CSC;
5. *Segurança física* – integra riscos de Roubo e/ou Divulgação - no modelo IaaS em que os recursos são partilhados por várias entidades, é essencial que o CSP assegure medidas de segurança física [ISO/IEC 27002:2013] que previnam o acesso não autorizado ou a destruição de informação sensível ou vital;
6. *Eliminação dos dados* – inclui risco de Divulgação - o CSP deve garantir medidas adequadas de destruição da informação depois de terminados os contratos, de forma a evitar a recuperação e divulgação de informação critica e sensível do CSC;
7. *Infraestrutura Offshoring* – integra riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - a mudança para uma infraestrutura *offshoring* aumenta a probabilidade de ataques que poderão afetar os ativos *no cloud* da organização. Normalmente estes ataques são perpetuados através das comunicações, expondo tanto a "nuvem" como as infraestruturas internas das organizações, tanto do CSC como do CSP;
8. *Manutenção da segurança das Virtual Machines (VMs)* - riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - uma das funcionalidades do IaaS é permitir que o cliente possa criar VMs (*virtual machines*) em vários estados (ativo, suspenso ou parado) e apesar do CSP poder estar envolvido no processo de manutenção dessas máquinas a responsabilidade é em geral do cliente, i.é., do CSC. Este facto poderá por em causa a segurança de toda a infraestrutura quando forem ligadas as VMs que tenham estado desligadas durante longos períodos, sem as respetivas atualizações de segurança;
9. *Autenticidade do Cloud Servive Provider* – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - é da responsabilidade do cliente dos serviços de TI na *Cloud* a verificação da autenticidade e credibilidade do CSP, nomeadamente quanto à sua "saúde" financeira, rentabilidade dos últimos 3 anos, referências de mercado e garantias de terceiros.

B) Fatores de risco do modelo de serviço Plataforma como Serviço (PaaS)

O modelo de serviço PaaS adiciona uma camada de abstração ao modelo de serviço anterior, o IaaS, em que a infraestrutura física, os sistemas operativos e as ferramentas de desenvolvimento são da responsabilidade do fornecedor, o CSP e as aplicações e os dados processados são da responsabilidade da empresa, o CSC. De acordo com a *ISACA* [CLOUD COMPUTING, 2012], este modelo serviço tem os mesmos riscos que o modelo IaaS, mais os indicados a seguir:

1. *Capacidade instalada* – inclui riscos de Roubo e/ou Divulgação - o risco aumenta para o CSC quando as funcionalidades fornecidas são desproporcionais aos recursos e capacidades do CSP. Esta situação pode introduzir vulnerabilidades e causar comportamentos anómalos ou um défice de desempenho que impacte a organização;
2. *Vulnerabilidades do Service Oriented Architecture (SOA)* – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - a utilização de bibliotecas SOA, da responsabilidade do CSP, reduz o tempo de desenvolvimento e testes na *Cloud*, mas podem introduzir vulnerabilidades nas plataformas, nem sempre visíveis para o cliente.
3. *Desativação das aplicações* – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - os *backups* e cópias de segurança, bem como os originais das aplicações desenvolvidas num ambiente PaaS, devem estar sempre disponíveis e atualizadas, na

posse do CSC, na eventualidade de uma rescisão do contrato ou alteração dos respetivos termos em que os serviços passem a ser prestados.

C) Fatores de risco do modelo de serviço *Software as a Service* (SaaS)

Neste modelo de serviço o CSP fornece a capacidade da empresa CSC usar aplicações informáticas na infraestrutura *cloud*. Toda a infraestrutura, designadamente *hardware*, sistemas operativos e aplicações são do CSP e o CSC apenas responsável pelo tratamento dos dados, com funcionalidades de um *end user*. De acordo com a *ISACA* [CLOUD COMPUTING, 2012], este modelo tem os mesmos riscos que o modelo de serviço anterior, o PaaS, mais os indicados a seguir:

1. *Eliminação de dados* – inclui riscos de Roubo e/ou Divulgação - em caso de rescisão do contrato, os dados introduzidos na aplicação do CSP devem ser imediatamente removidos, com recurso a ferramentas forenses para evitar a divulgação e a violação de confidencialidade;
2. *Falta de visibilidade sobre o SDLC* [6] - integra riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - as empresas que usam aplicativos na *Cloud* nem sempre têm visibilidade sobre o ciclo de vida de desenvolvimento de sistemas (SDLC). Não conhecem em detalhe como as aplicações foram desenvolvidas e desconhecem por isso as medidas de segurança implementadas. Isto pode levar a uma discrepância entre a segurança proporcionada pela aplicação e os requisitos exigidos pelo CSC;
3. *Identificação e gestão de acessos* – incorpora riscos de Perda, Roubo e/ou Divulgação - para maximizar as receitas, o CSP oferece serviço e aplicações para vários clientes numa base de partilha de servidores, aplicações e até de dados. Não obstante, se não existir uma gestão adequada dos acessos, um cliente pode ter acesso aos dados de outro cliente sem o devido controlo e até sem o conhecimento do CSC;
4. *Estratégia de saída e Portabilidade* – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - um dos grandes constrangimentos que se apresenta às empresas na hora de rescindir um contrato com um CSP é a questão de como migrar os dados para outro CSP ou mesmo para serviços *in house* sem perda de dados ou com um mínimo de esforço de reconstrução desses sados. Podem não existir ferramentas que assegurem a portabilidade dos dados ou mesmo a inexistência de aplicações compatíveis que deem continuidade ao seu processamento o que poderá causar disrupção de serviços com prejuízos e impactos que devem ser previstos e mitigados pelo CSC;
5. *Maior exposição das aplicações a ataques* – integra riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - num ambiente de computação na "nuvem", os aplicativos, que muitas vezes interagem com aplicações *no cloud*, têm uma maior exposição a ataques. Nem sempre as *firewalls* de rede standards são suficientes, o que implica a necessidade de medidas de segurança adicionais que limitem o alcance desses possíveis ataques;
6. *Falta de controlo sobre as aplicações* – inclui riscos de Indisponibilidade e/ou Perda - o CSP tem por vezes necessidade de introduzir correções nas suas aplicações de forma rápida, sem esperar pela aprovação formal dos seus clientes. Nestes casos, o CSC pode não ter controlo sobre os processos e ser prejudicado por efeitos colaterais imprevistos;
7. *Vulnerabilidades do browser* – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - na maioria dos casos os serviços SaaS são disponibilizados através de navegadores *web* que, infelizmente, são alvo apetecível para *malware* ou outros ataques

[6] Systems Development Life Cycle do software

de cibernautas. Se o *browser* do cliente for infetado o acesso aos dados e às aplicações pode ficar comprometido.

D) Fatores de risco de um modelo de implementação Publica *(Public Cloud)*

O tipo de implementação não têm a mesmo abstração que os modelos de serviço, dado que neste caso o risco não é cumulativo mas sim particular a cada modelo. Numa implementação pública o CSP fornece uma infraestrutura partilhada por várias empresas e indivíduos sem relação. De acordo com o ISACA, "*Security Considerations for Cloud Computing"* [CLOUD COMPUTING 2012], consideram-se os seguintes riscos:

1. *Partilha total da "nuvem"* – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - a infraestrutura de "nuvem" é partilhada por vários *tenants*, por vários CSC, sem relação, interesses comuns, ou o mesmo nível de preocupações com a segurança, sendo isso um risco potencial acrescido para os CSC que deve ser analisado e mitigado;
2. *Danos colaterais* – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação- numa infraestrutura partilhada se um dado cliente for atacado poderá haver impacto noutros clientes do mesmo CSP, mesmo que não sejam o objetivo do alvo a atingir (por exemplo *DDoS Attack*).

E) Fatores de risco de um modelo de implementação Comunitária (*Community Cloud)*

Neste modelo de implementação os serviços são fornecidos para o uso de um grupo de entidades que partilha um determinado nível de confiança, como por exemplo uma política comum de segurança. . De acordo com a *ISACA* [CLOUD COMPUTING, 2012], os níveis de risco são os apontados a seguir:

1. *Partilha da "nuvem"* – inclui riscos de Perda, Roubo e/ou Divulgação - neste modelo a ameaça existe quando diferentes entidades do mesmo grupo de empresas que partilha uma mesma infraestrutura, têm diferentes requisitos e medidas de segurança. Os procedimentos menos exigentes de uma das entidades podem por em causa os SLAs de outra entidade.

F) Fatores de risco de um modelo de implementação Privada (*Private Cloud)*

Neste modelo os serviços são fornecidos para uso exclusivo de uma entidade, sem qualquer interação com outras entidades na *cloud*. Nestes casos, de acordo com a *ISACA* [CLOUD COMPUTING, 2012], os riscos são os seguintes:

1. *Compatibilidade das aplicações* - incorpora riscos de Indisponibilidade e/ou Perda - neste contexto é necessário identificar e avaliar o grau de compatibilidade de aplicações antigas proprietárias, (*legacy*), com ambientes virtualizados e aplicações que estejam a correr na *Cloud* privada;
2. *Investimentos necessários* – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação[7] - planear e justificar os investimentos numa infraestrutura partilhada, sejam eles de formação e contratação necessária à aquisição de competências na *Cloud*, pode tornar-se tarefa difícil para o CIO se a mensagem não for convenientemente passada à Administração da CSC. É, por isso, necessária uma análise custo-benefício, o

[7] Riscos que podem ser despoletados por este factor

desenvolvimento de um *Business Case*, com o cálculo rigoroso do ROI[8], para determinar se a "nuvem" é uma solução viável, se está alinhada com os objetivos do negócio e se justifica os custos de investimento do projeto;

3. *Competências de TI na Cloud* – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - ainda que a implementação de uma "nuvem" privada dentro da organização possa parecer a melhor opção, em termos de segurança a sua manutenção e gestão requerem competências específicas de TI que podem aumentar os custos inicialmente previstos. Essa análise deve ser tida em conta na elaboração do *Business Case* já referido.

G) Fatores de risco do modelo de implementação Hibrida (*Hybrid Cloud)*

É um modelo de implementação que permite às empresas um *mix* de *cloud* pública, comunitária e privada, dependendo do nível de requisitos de confiança existentes entre as empresas. Por exemplo uma empresa pode decidir que o portal web pode migrar para uma *cloud* publica mas querer manter as suas aplicações de negócio numa *cloud* privada. Esta combinação cria um modelo de *cloud* híbrida, mas os riscos neste caso, de acordo com a *ISACA* [CLOUD COMPUTING, 2012], são os seguintes:

1. *Interdependência da Cloud* – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - se a empresa CSC combina dois ou mais tipos diferentes de "nuvens", serão necessários controlos rigorosos de identidade e credenciais fortes para permitir que uma *Cloud* tenha "acesso" e comunique com a outra. O problema agrava-se e é de difícil gestão quando se tem de conviver com diferentes níveis de segurança, como, aliás, já foi referido antes.

Apesar de tudo o que foi referido até aqui, os riscos identificados para cada modelo de serviço e para cada modelo de implementação não representam um nível de ameaça igual para todas as empresas. Estão sobretudo relacionados com a atividade e a dimensão do CSC e por isso cada organização deve avaliar o risco face aos eventos e aos impactos que possa produzir no seu negócio. As ações terão de passar pela eliminação, mitigação, transferência, ou mesmo aceitação do risco, nos níveis considerados aceitáveis para o negócio, figura 2.

Figura 3 - Medidas de gestão de risco. Adaptado de: [COBIT5 Assurance, 2014]

[8] Return of Investment

4. *IT Governance e* Auditoria de Sistemas de Informação

A Governação das empresas é responsável por definir princípios, comunicar políticas, estabelecer regras, delegar autoridade para fazer cumprir essas regras e monitorizar os resultados para determinar se é necessário algum ajuste ao que foi inicialmente determinado.

A Governação das TI, na tradução portuguesa do termo original *IT Governance* [ITGI - IT Governance Institute® 2008], e não "governança", termo eventualmente mais adequado a uma tradução brasileira, assume-se como um mecanismo subordinado da Governação geral da empresa, com a missão de incorporar o valor intrínseco das TI em todos os aspetos da organização.

Através da Governação das TI a empresa retira todos os benefícios da informação que processa, maximiza os benefícios da utilização das TI, capitaliza oportunidades e ganha vantagem competitiva, através da minimização dos riscos e da otimização dos recursos, figura 4 [COBIT5 Framework 2012].

Figura 4 - Objetivo da Governação, adaptado de [COBIT5 Framework 2012]

A Governação das TI materializa assim as boas práticas de TI, baseadas em *frameworks* próprias de *IT Governance*, como o *Control Objectives for Information and related Technology* do COBIT 5, com foco em processos genéricos de Avaliação, Direção e Monitorização amplamente detalhados na framework do COBIT 5 - *A Business Framework for the Governance and Management of Enterprise IT*. Esses processos têm por objetivo: manter uma *framework* eficaz de Governação das TI; assegurar a entrega de benefícios; assegurar a otimização dos riscos e dos recursos, conforme figura 1; e assegurar uma prática de políticas transparentes para os *Stakeholders* e *shareholders* [COBIT5 Framework, 2012].

Os fatores que relevam também a importância da Governação das TI e dos serviços na *Cloud* seguem um conjunto de linhas de preocupação que elencadas a seguir [COBIT5 Security 2012]:

1. Maior preocupação dos *Stakeholders* e da gestão de alto nível relativamente ao aumento generalizado de investimentos em TI e ao retorno que é possível obter deles;
2. A necessidade de otimizar os custos;
3. Maiores requisitos de conformidade e de controlo das TI em áreas criticas como a privacidade e o reporte financeiro;
4. Necessidade de uma seleção criteriosa dos *Cloud Service Providers* (CSP) para uma maior eficiência e segurança dos serviços de *outsourcing*, aquisição e manutenção;
5. Por fim a necessidade das empresas avaliarem o seu desempenho face a *standards* de referência e da área de atividade da empresa (*benchmarking).*

As auditorias de Sistemas de Informação (ASI), com as suas iniciativas de identificação dos riscos, monitorização contínua, análise e avaliação de métricas associadas à Governação das TI, desempenham um papel fundamental na implementação com sucesso das políticas de Governação das TI de uma organização [CISA 2014].

A garantia de que os riscos de migração ou adoção de serviços na *Cloud* estão identificados e existe uma resposta adequada às ameaças pendentes é dada pelas iniciativas de Auditoria de Sistemas de Informação que garantem que os controlos existem, que estão, portanto, implementados, que são suficientes e estão a ser seguidos conforme esperado, através de uma monitorização continua e sistemática [COBIT5 Assurance, 2014]. O objetivo é fornecer uma garantia de conforto a stakeholders, internos e externos, sobre as matérias auditadas, ou seja todos os fatores internos interligados que contribuam para a concretização dos objetivos da empresa, designados *enablers* pelo COBIT 5 [COBIT5 Assurance, 2014], todos eles com uma dada missão dentro da organização vital para o negócio do CSC, como o são na generalidade dos casos os Sistemas e as tecnologias de Informação.

Os principais objetivos da Auditoria de Sistemas de Informação são, assim, os que indicamos a seguir [COBIT5 Assurance, 2014]:

1. Alinhamento dos SI com a missão, visão, valores, objetivos e estratégia da organização. Em suma, alinhamento da Governação das TI com a Governação da empresa
2. Consecução do desempenho e concretização dos objetivos traçados para os SI
3. Conformidade com requisitos de segurança e privacidade, legais, ambientais e fiduciários
4. Verificação dos investimentos em TI
5. Análise e avaliação dos riscos inerentes ao ambiente de SI como o *Cloud Computing*.

Em suma, o processo de Auditoria de Sistemas de Informação inclui a gestão ao mais alto nível, é transversal a todos os sectores e departamentos da organização e foca-se em dois aspetos fundamentais, conforme figura 5 [CISA 2014]:

- Na conformidade, i.é., no cumprimento de políticas e regulamentos internos e externos e na proteção dos ativos de informação de valor para a organização;
- No desempenho, ou seja, no valor acrescentado que as TI representam e geram para a organização.

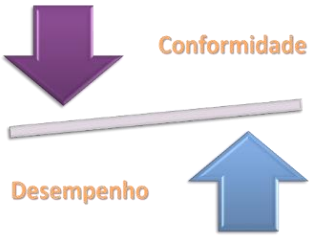

Figura 5 - Foco das Auditorias de Sistemas de Informação

O *Cloud Computing* enquanto *Outsourcing* deve ser governado, gerido e auditado de forma a não comprometer os objetivos do negócio. Neste processo destaca-se a tarefa fundamental de análise e avaliação dos riscos inerentes à adoção de serviços de TI alojados na "nuvem", como forma de mitigar a ocorrência de eventos que comprometam esses objetivos [COBIT5 Security 2012].

A observação de várias empresas de dimensão considerável, em termos de negócio e recursos afetos às TI, mostra-nos que uma das principais razões dos impactos negativos nos serviços de TI fornecidos em *Outsourcing*, pelos *Cloud Service Providers (*CSP*),* relaciona-se, frequentemente, com lacunas na clarificação do âmbito e na definição dos níveis de serviço [COBIT5 Vendor Management. 2014]. Para mitigar esses riscos o primeiro passo é celebrar acordos *Service Level Agreement* (SLA), definir controlos e implementar mecanismos de monitorização. Porém, nesse processo, há um elemento-chave que jamais poderá ser menosprezado: a confiança que deve prevalecer ao longo de todo o ciclo de vida dos serviços, na relação entre o CSP e a empresa

cliente *Cloud Services Customer (CSC)*. A confiança é um elemento fundamental no modelo de negócio de *Cloud Computing*. Sem ele, jamais serão suficientes quaisquer controlos e acordos para mitigar todos os riscos e preocupações que as empresas, os CSC, possam ter acerca deste modelo de gestão das TI empresariais [CLOUD COMPUTING 2012].

Neste processo, a função do auditor passa pela verificação dos seguintes pontos de controlo [CISA 2014]:

1. Determinar se a empresa avaliou as vantagens e desvantagens da opção pelo *Cloud Computing*, face aos seus objetivos
2. Identificar e classificar a criticidade dos dados (privada, publica, sensível, confidencial)
3. Identificar os riscos referidos na secção anterior;
4. Verificar se existe controlo e visibilidade da informação critica para o negócio;
5. Verificar se estão devidamente contratualizados os SLAs ou seja se estamos perante *Strong Service-level Agreements* (SSLAs) [Vaz, et al., 2013]
6. Verificar as boas práticas usadas pelo *CSP, designadamente ISO 15504 Software Process Improvement and Capability (SPICE), CMMI e ITIL;*
7. Verificar se está a ser gerida a mudança, o que implica:
    a. Alteração nos processos de arquivo, alojamento e *backup* da informação;
    b. Revisão das políticas de acesso à informação;
    c. Revisão das competências e função para gerir a relação dos serviços com terceiros (*Outsourcing* e *Cloud*).

A Governação do *Outsourcing* e a auditoria dos serviços de TI na *Cloud* inclui, deste modo, todo o conjunto de responsabilidades, funções, objetivos e controlos exigidos no sentido de antecipar o processo de mudança, gerir a introdução do serviço, a manutenção, o desempenho e os custos do CSP. É um processo interativo que se estende a ambas as partes, CSC e CSP, numa base necessariamente de confiança, com o objetivo de assegurar a continuidade dos serviços de TI com níveis adequados de rentabilidade e segurança.

5. Conclusão

A Governação das TI, enquanto mecanismo subordinado à Governação geral da empresa, assume-se como instrumento sistemático de boas práticas para suporte às grandes decisões estratégicas e à maximização dos investimentos em TI. A eficácia da Governação está intimamente ligada à utilização de *frameworks* globalmente aceites e que são independentes da dimensão ou ramo de atividade.

O *Cloud Computing* deve ser uma consequência de decisões estratégicas e exige práticas de controlo e monitorização permanente ao longo de todo o ciclo de vida dos serviços, em que a Auditoria de Sistemas de Informação desempenha uma função vital com foco aspetos fundamentais como a conformidade e o desempenho.

A confiança na relação que se estabelece entre o cliente-empresa e o CSP, fornecedor dos serviços de computação na "nuvem é também fundamental em todo o ciclo de serviços da *Cloud*.

Mas é na identificação e avaliação prévia dos riscos para o negócio nas suas vertentes específicas, i.é., quanto ao modelo de serviço e quanto ao modelo de implementação e na respetiva mitigação, que reside grande parte do sucesso do modelo de *Cloud Computing* que nos propomos validar e detalhar num próximo artigo.

6. Bibliography

CANNON, David L. 2011. *CISA Certified Systems Auditor Study Guide.* 3nd. Indianopolis : John Wiley & Sons, Inc., 2011.

CISA. 2014. *CISA Review Manual.* USA : ISACA, 2014.

CLOUD COMPUTING. 2012. *Security Considerations for Cloud Computing.* 2012.

CLOUD GOVERNANCE. 2013. *Cloud Governance: Questions Boards Of Directors Need to Ask.* 2013.

CMMI Product Team-Carnegie Mellon University. 2010. *CMMI® for Development, Version 1.3.* s.l. : SEI publications, 2010.

COBIT5 Assurance. 2014. *COBIT 5 for Assurance.* Rolling Meadows, IL 60008 USA : ISACA, 2014.

COBIT5 Framework. 2012. *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows USA : ISACA, 2012.

COBIT5 Security. 2012. *COBIT 5 - For Information Security.* 2012.

COBIT5 Vendor Management. 2014. *Vendor Management: Using COBIT 5.* Rolling Meadows, IL 60008 USA : ISACA, 2014.

CSA. 2012. *Security Guidance for Critical Areas of Focus in Cloud Computing.* 2012.

HARDING, Chris. 2011. *Cloud Computing for Business.* Amersfoort, NL : Van Haren, 2011.

IBM DeveloperWorks. 2012. *Delivering Business Process as a Service (BPaaS).* s.l. : IBM, 2012.

ISACA. 2009. *ISACA Serving IT Governance Professionals.* 15 de Out de 2009.

ISACA Journal - BIG DATA. **ISACA. 2014.** Selecting the right Cloud operating model - Privacy and Data Security in the Cloud, Rolling Meadows, Illinois, USA : ISACA, 2014, Vol. 3, p. 32.

ISO/IEC. 2004. *ISO/IEC-15504 Information technology* . Switzerland : ISO/IEC, 2004.

ISO/IEC-27002:2013. 2013. *Information techonology - security techniques - ISO/IEC 27002:2013.* Geneva : ISO/IEC, 2013.

ITGI - IT Governance Institute®. 2008. *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit.* EUA : ITGI, ISACA, OGC and TSO, 2008.

Mike Kavis, Esmeralda Swartz, Liz McMillan, Dana Gardner, Andreas Grabner. 2013. Cloud BPM : Enabling the Emerging BPaaS Market. *Cloud Computing Journal.* [Online] 2013.

NIST. 2012. *Definition of Cloud Computing.* 2012.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks.* Paris : OECD, 2002.

OGC CSI. 2007. *ITIL Continual Service Improvement v3.* London : TSO, 2007.

OGC SD. 2007. *ITIL Service Design v3.* London : TSO, 2007.

OGC SO. 2007. *ITIL Service Operation v3.* London : TSO, 2007.

OGC SS. 2007. *ITIL Service Strategy v3.* London : TSO, 2007.

OGC ST. 2007. *ITIL Service Transition v3.* London : TSO, 2007.

Thor Olavsrud, Dan Muse. 2012. How Secure Is the Cloud - IT Pros Speak Up. *CIO Review.* 2012.

Vaz, Johann, et al. 2013. *Securing the cloud: important steps to protect sensitive information as data storage involves.* 2013.

VMWARE CIO. 2014. Delivering IT as a Service. *white paper | itaas.* 2014.