Universidade Católica Portuguesa

Faculdade de Engenharia

Segurança em Sistemas de Informação

Migração e segurança em plataformas cloud computing

Roberto Carlos Gomes da Silva

Dissertação para obtenção do Grau de Mestre em

Segurança em Sistemas de Informação

Júri

Prof. Doutor Manuel José Martinho Barata Marques

Prof. Doutor Rui Jorge Correia Mendes Alves Pires

Prof. Doutor Tito Lívio dos Santos Silva

Junho de 2014

"*Computation may someday be organized as a public utility*."

John McCarthy, 1960

Agradecimentos *A todos os que acreditaram que seria possível cumprir este objectivo e me ajudaram nesse sentido, muito especialmente à minha mulher, pela paciência e suporte demonstrados.*
Uma especial nota de agradecimento ao meu orientador Prof. Doutor Tito Lívio dos Santos Silva.

Resumo

O paradigma *cloud computing* é cada vez mais uma tecnologia presente nas infraestruturas das organizações e vista por muitos como um marco no que respeita às tecnologias de informação. De facto, *cloud computing* representa mais uma mudança de paradigma na forma como os sistemas são implementados. Mas, de uma forma geral, *cloud computing* é também sinónimo de insegurança, que aos poucos se vai alterando. Ao migrar para um ambiente cloud, uma organização relega para o fornecedor do serviço o controlo sobre os seus dados e sistemas, fomentando um sentimento de insegurança pela perda de controlo inerente. As organizações têm que ter um nível muito elevado de confiança nos fornecedores cloud, antes de decidir confiar-lhes a sua informação confidencial ou regulada por normas ou leis. Neste trabalho propomos uma análise à segurança em ambientes cloud, riscos, vantagens e desvantagens, terminando com uma proposta de ferramenta de trabalho em migração para infraestruturas *cloud computing*, mantendo a segurança, privacidade e disponibilidade de sistemas, dados e informação.

Palavras-chave: *cloud computing*, SaaS, PaaS, IaaS, segurança, riscos, confidencialidade, privacidade, disponibilidade

Abstract

The cloud computing paradigm is becoming an existing technology at the organizations infrastructures and seen by many as a milestone in relation to Information Technology. In fact, cloud computing represents a paradigm shift in the way systems are implemented. But, in general, cloud computing is also synonymous with insecurity, which is gradually changing. When one organization migrate their data and systems to a cloud environment, it relegates to the service provider control over it, fostering a sense of insecurity for the loss of control inherent. Organizations have to have a very high level of trust in cloud providers before deciding to entrust them their confidential information or regulated by rules or laws. In this work we present a review of security in cloud environments, risks, advantages and disadvantages, ending with a proposal of a tool for migrating to an infrastructure of cloud computing, maintaining security, privacy and availability of systems, data and information.

Keywords: cloud computing, SaaS, PaaS, IaaS, risks, security, confidentiality, privacy, availability

Índice

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

ACL – Access Control List

AES - Advanced Encription Standard

API - Application Program Interface

DOS - Denial-Of-Service

DR - Disaster Recover

IDE - Integrated Development Environment

IDS - Intrusion Detection Systems

IP - Internet Protocol

IPD - Intrusion Prevention Detection

LAN – Large Area Network

MAC - Media Access Protocol

PII - Personal Identifiable Information

QoS – Quality of Service

RIP - Routing Information Protocol

SDLC - Software development lifecycle

SLA - Service Level Agreements

SOA - Service Oriented Architectures

SPI - Software Platform Infrastructure

SSL - Secure Sockets Layer

TI - Tecnologias de Informação

VM - Virtual Machine

1. Introdução

À medida que as empresas procuram novas formas para melhoria da eficiência e redução de custos a *cloud computing* emerge como uma nova plataforma que oferece ganhos financeiros nas suas necessidades de tecnologias de informação.

Embora a ideia de *cloud computing* seja uma tendência relativamente recente, as suas raízes remontam aos anos 60. Em 1961, John MaCarthy, Professor no MIT apresentou o conceito de computação fornecido como um bem de consumo, semelhante à electricidade. Mais tarde, em 1969, J. Licklider, pioneiro no projecto que desenvolveu as bases da ARPANET, precursor da Internet, apresentou a ideia de uma rede de escala: "*If such a network as I envisage nebulously could be brought into operation, we could have at least four large computers, perhaps six or eight small computers, and a great assortment of disc files and magnetic tape units—not to mention remote consoles and teletype stations—all churning away*.". Estes dois conceitos, em conjunto com a ubiquidade da internet, estão na base do que mais tarde viria a evoluir para uma infraestrutura de *cloud computing* (Krutz & Vines, 2010). De facto, o conceito de *cloud computing* não é mais que a evolução de conceitos de computação suportados por novas tecnologias e algumas já existentes, representando mais uma mudança de paradigma na forma como os serviços computacionais são desenvolvidos e acedidos pelos utilizadores (Sosinsky, 2011). Entre essas tecnologias podemos destacar, por exemplo, a capacidade de processamento, virtualização de recursos, a capacidade de armazenamento, largura de banda disponível, descida nos preços de *hardware*, etc. Tudo combinado torna a *cloud computing* uma infraestrutura apelativa e competitiva.

A inforworld num artigo de Junho de 2011 sobre os 10 piores apagões *cloud* (Raphael, 2011) vem salientar que os problemas de segurança existem, acontecendo mesmo onde menos se espera que ocorram, no fornecedor de serviços *cloud*. Mesmo fornecedores com elevada reputação como a Amazon, Google, Microsoft e Salesforce, para nomear apenas alguns dos citados no artigo, experimentaram distúrbios graves e prolongados no fornecimento dos seus serviços. Este facto vem salientar que os problemas de segurança em *cloud* são abrangentes e há que considerar todos os riscos e analisar as ameaças de todos os ângulos, num projecto de migração para a *cloud*.

Apesar da percepção de risco que o modelo *cloud* levanta, as organizações, seja em território nacional seja a nível internacional, ponderam cada vez mais a migração de alguns dos seus

serviços para a *cloud computing*. A IDC[1], empresa líder mundial na área de *market intelligence*, realizou um estudo em 2012 sobre as tendências de adopção destas tecnologias no território nacional. Nesse estudo analisou o grau de utilização deste tipo de serviços, assim como as perspectivas de utilização a curto prazo. Nele se conclui que com as alterações substanciais da conjuntura económica nacional nos últimos anos, a redução de custos de funcionamento e a melhoria da eficiência aparecem como as prioridades de negócio para a maioria das organizações inquiridas. Assim, Apesar das condições adversas da economia, as prioridades tecnológicas das organizações nacionais contemplam a consolidação da infraestrutura, a virtualização e a adopção de serviços de *cloud computing*. De facto, mais de um terço das organizações nacionais inquiridas consideram os serviços de *cloud computing* e apenas 20% ainda não tinham considerado uma aproximação ao modelo *cloud computing*.

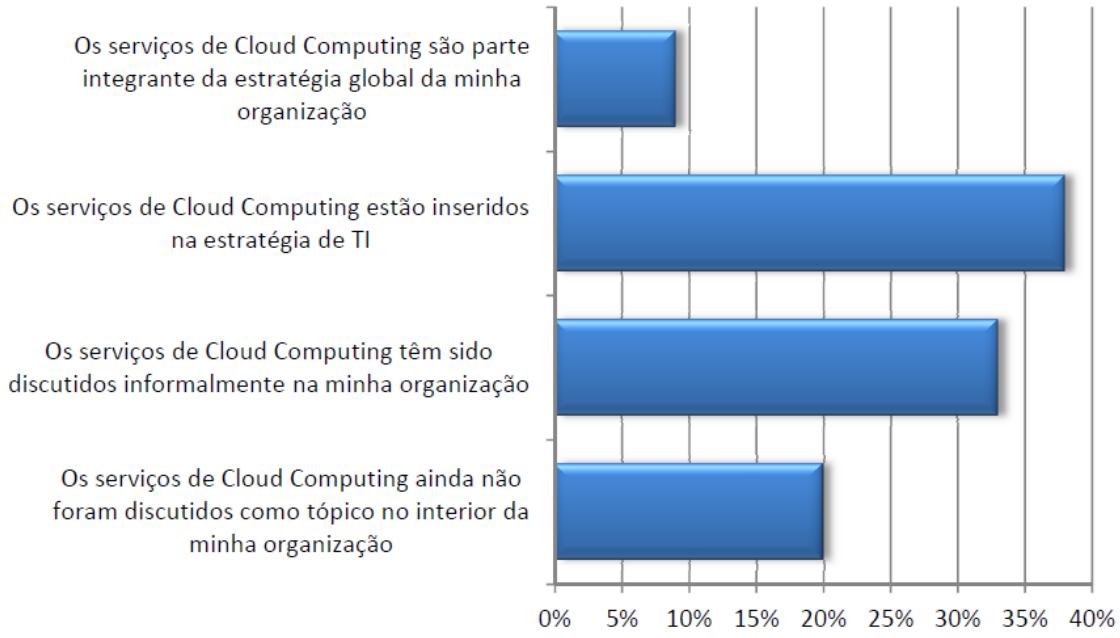

Figura 1: Maturidade do conceito *cloud computing* – (Portugal, 2012)

À semelhança de outros inquéritos levados a cabo a nível internacional, quando considerado a adopção dos serviços em *cloud computing*, as preocupações com a segurança, a privacidade e a confidencialidade surgem logo em primeiro plano. Num segundo plano, surgem em evidência as

[1] http://www.idc.pt/index.html

preocupações com contratos com os fornecedores, garantias e níveis de serviço dados pelos fornecedores e a dependência futura destes.

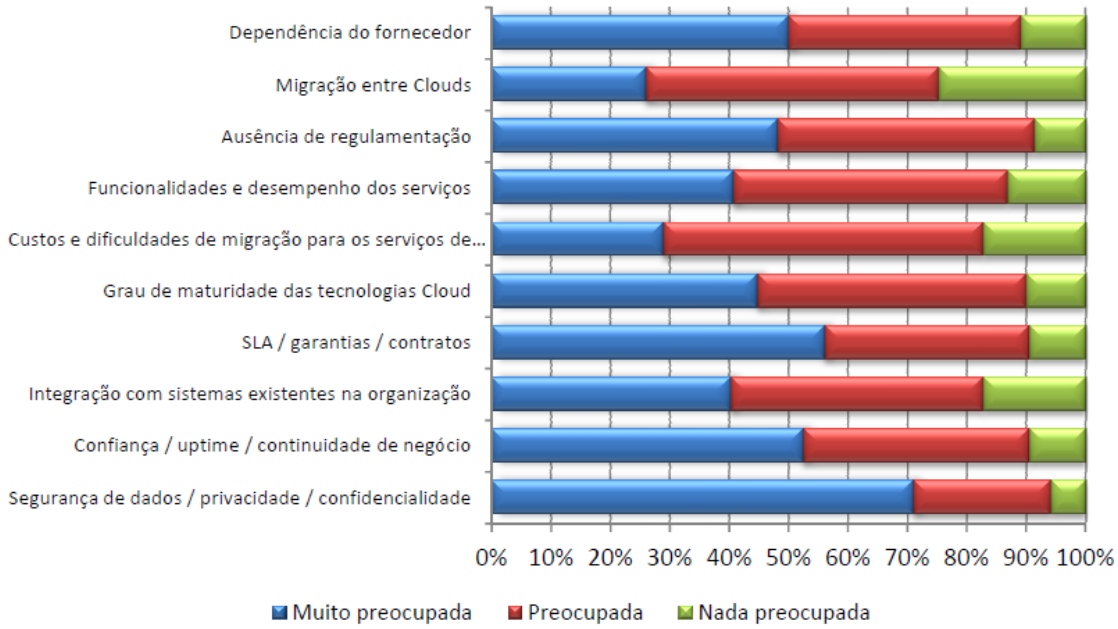

Figura 2: Obstáculos à adopção de *cloud computing* – (Portugal, 2012)

Factores como garantias de desempenho do serviço, suportados através da existência de *Service Level Agreements* (SLA), do preço competitivo das soluções e a existência de serviços profissionais são os critérios apontados pelas organizações nacionais como determinantes para a escolha do fornecedor de serviços de *cloud computing*.

1.1.Objectivos

Com este novo paradigma surgiram novas ameaças e receios que tornam a adopção de uma infraestrutura em *cloud computing* num projecto a ser pensado e analisado extensiva e cuidadosamente. Uma organização deve compreender os riscos e as vantagens, para uma decisão informada e consciente, mitigando os riscos e alavancando as vantagens do projecto. Assim, o objectivo principal desta dissertação é o de reunir informação sobre o conceito *cloud computing*, que permita uma decisão informada acerca da migração de sistemas para a *cloud*, com o foco na segurança e que permita a sua aplicação em casos de negócio.

1.2.Estrutura do Documento

Esta dissertação é composta, para além deste, por mais 4 capítulos e 2 Anexos

Capítulo 2: É efectuada uma abordagem ao modelo *cloud computing*, com descrição das principais características, modelos de serviço e de desenvolvimento, actores principais e infraestrutura de referência, terminado com uma análise à diferença entre arquitecturas, *cloud* e tradicional.

Capítulo 3: É analisada a arquitectura *cloud* de uma forma abrangente e pela óptica da segurança, são apontadas as suas vantagens, desvantagens e riscos antes de uma análise mais aprofundada sobre a segurança em ambientes *cloud*, com especial ênfase na *cloud* pública, que é a que mais preocupações de segurança levanta.

Capítulo 4: De vertente prática, apresenta-se uma ferramenta de trabalho (*framework*), que descreve um ciclo de migração para *cloud computing*, que se divide em 4 fases:

- Fase de definição, em que se identifica pessoas e equipas que irão ter um papel relevante no processo de migração, definição de um plano estratégico de migração e levantamento de necessidades de formação.

- Fase de análise, que compreende um levantamento de aplicações e sistemas a migrar, selecção do modelo de desenvolvimento e do modelo de serviço que melhor se adaptam à empresa e finalmente, a selecção do fornecedor *cloud*.

- Fase de segurança, com a informação suficiente já reunida nas duas fases anteriores, em que se propõem testes de migração, de implementação e gestão de *Service Level Agreements* (SLA) e definição dos controlos de segurança, necessários a um ambiente de segurança.

- Fase de operação, que completa o ciclo com o acompanhamento da operação numa óptica de melhoria continua.

Capítulo 5: Apresenta as conclusões do trabalho realizado e sugestões de trabalhos futuros.

Anexo A: Para uma comparação efectiva de fornecedores, é proposto o preenchimento das tabelas do Anexo.

Anexo B: Proposta de documento para caso de estudo de um projecto de migração para *cloud computing*.

2. Cloud Computing

De um ponto de vista bastante simplificado, *cloud computing* fornece serviços de Tecnologias de Informação (TI) através da *Internet* de tal forma que o utilizador final não precisa de se preocupar com a localização da infraestrutura, formas de armazenamento dos dados, tecnologia de suporte, etc. O utilizador recebe o serviço sem se preocupar com qualquer um dos detalhes tecnológicos. O serviço é fornecido de uma forma em tudo similar aos serviços tradicionais de água, gás, electricidade e telefone (Buyya, et al., 2009) pagando apenas pelo consumo e permitindo às empresas reduzir os custos, não pagando por equipamento não utilizado ou subutilizado (ISACA, 2011). Para o utilizador não há custos com a aquisição de *hardware*, licenças de *software*, gestão de actualizações, pessoal técnico ou de espaço para um centro de dados, havendo apenas custos medidos segundo a utilização. Sendo um cliente *cloud*, este está a partilhar com outros utilizadores a infraestrutura de suporte que fornece o serviço, não estando esta dedicada a nenhuma empresa ou utilizador em particular.

Existem muitas definições publicadas numa procura de melhor definir *cloud computing*. Roger Smith, na sua publicação de 2009 (Smith, 2009), oferece-nos um resumo de propostas para a sua definição, recorrendo a algumas instituições de renome das quais destacamos as seguintes:

- Berkeley University of California - "Ilusão de recursos infinitos de computação disponíveis a pedido, eliminando compromissos mais efectivos por parte dos utilizadores da *cloud*, possibilitando o pagamento pelo uso desses recursos de acordo com as necessidades de curto prazo."

- Gartner Group - Estilo de computação no qual recursos de TI, massivamente escaláveis são disponibilizados sob a forma de serviços, por meio da *Internet*, para múltiplos clientes *cloud* externos."

- Forrester Research - "Um conjunto de infraestruturas geridas, abstractas e altamente escaláveis, capazes de hospedar aplicações de clientes *cloud* finais, os quais pagam pelo consumo."

- International Business Machines (IBM) - "Plataforma que dinamicamente fornece, configura, reconfigura e liberta servidores de acordo com as necessidades, recorrendo a grandes centro de dados e potentes servidores, nos quais disponibiliza aplicações e serviços para serem utilizados via *Internet*."

(Vaquero, et al., 2009) No seu estudo "*A Break in the Clouds: Towards a Cloud Definition*" onde analisa mais de vinte definições propõe como definição completa de *cloud computing*: "Clouds

são uma larga gama de recursos virtualizados de fácil acesso e utilização (como *hardware*, plataformas de desenvolvimento e/ou serviços). Estes recursos podem ser reconfigurados dinamicamente para se ajustarem à carga de utilização (escala), permitindo também uma óptima utilização de recursos. Esta gama de recursos são tipicamente utilizados num modelo de pagamento por utilização, com garantias dadas pelo fornecedor da infraestrutura através de SLA's costumizados"[2]

Peter Mell e Timothy Grace, do National Institute of Standards and Technology (NIST) no documento intitulado "The NIST Definition of Cloud Computing", definem *Cloud Computing* como (Mell, Peter; Grance, Timothy; NIST, 2011): "…um modelo que viabiliza o acesso oportuno e a pedido a um pacote partilhável de recursos computacionais configuráveis (por exemplo, redes, servidores, áreas para armazenagem, aplicativos e serviços) que podem ser rapidamente aprovisionados e libertados com um mínimo esforço de gestão ou de interacção com o prestador de serviços."[3].

[2] "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs"

3 "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

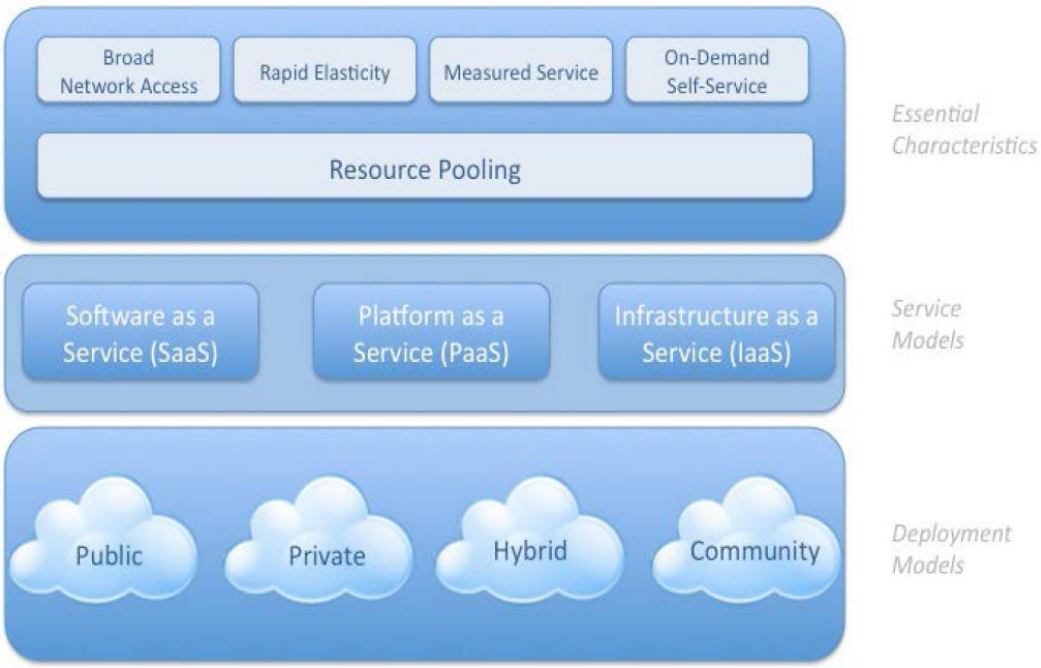

Figura 3: Modelo Visual da definição da NIST

Esta definição de Peter Mell e Timothy Grace, a mais aceite e a mais mencionada em todos os trabalhos e livros sobre o tema, aponta para a existência de três dimensões que caracterizam a *cloud computing* como um modelo e não uma tecnologia, baseado numa gama de serviços de rede, serviços de computação, capacidade de armazenamento e recursos aplicacionais (Williams, 2012). Essas dimensões são:

- Cinco características essenciais;
- Três modelos de serviço;
- Quatro modelos de desenvolvimento.

2.1.Visão Histórica

Analisando o passado, *cloud computing* pode ser considerado uma evolução de tecnologias existentes. Os seus fundamentos têm origens na década de 50, quando organizações e institutos de educação deram prioridade à eficácia e optimização dos seus grandes computadores centrais, permitindo o acesso a múltiplos utilizadores através de terminais, partilhando as suas capacidades de processamento. Desde daí, podemos identificar seis fases de desenvolvimento, cada uma muito relevante no seu tempo (Berger, 2009):

- Fase 1 – Nas décadas de 50, 60 e 70, os utilizadores ligavam-se a computadores centrais através de terminais. Estes computadores com grandes capacidades eram responsáveis por todo o processamento, exibindo os resultados aos utilizadores nesses terminais, que não dispunham de capacidades de processamento;

- Fase 2 – Já na década de 80, assistiu-se à democratização dos computadores pessoais. Estes ganharam capacidades de processamento e preços acessíveis, permitindo a sua expansão para o uso corrente dos utilizadores;

- Fase 3 – Ligação destes computadores pessoais e servidores a redes de comunicação locais, *Local Area Networks* (LAN);

- Fase 4 – Ligação destas redes locais entre si deu origem a uma rede global, a *Internet*, que permitiu a partilha de recursos entre computadores a nível global;

- Fase 5 – Computação em grelha, partilha da capacidade de computação e armazenamento por sistemas distribuídos;

- Fase 6 – Evolução da computação em grelha, melhora da partilha de recursos para uma forma mais simples e escalável, criando as condições necessárias para o início da *cloud computing*.

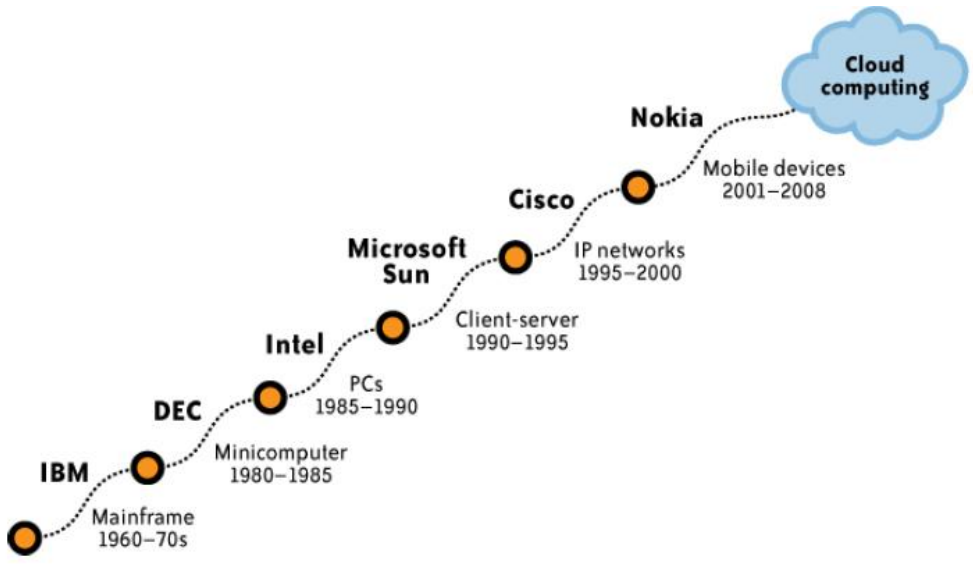

Figura 4: Evolução tecnológica (Mather, et al., 2009)

Daqui podemos concluir que desde a década de 60 se foi assistindo a um desenvolvimento tecnológico que viria a permitir a infraestrutura em *cloud* que temos actualmente. Com a *Web* 2.0

como a mais recente evolução. Alguns marcos históricos na evolução da *cloud computing* (Mohamed, 2009):

- 1999 – Salesforce.com foi pioneira na entrega de aplicações empresariais via web, funcionado como ponto de partida, para empresas de *software* fornecerem aplicações através da internet;

- 2002 – Amazon Web Services disponibilizam uma série de serviços *cloud*, que incluíam serviços de armazenamento, processamento e inteligência humana;

- 2006 – A Amazon lança a sua aplicação comercial, Elastic Compute Cloud (EC2), para o aluguer de computadores virtuais, que permitem aos clientes executar as suas aplicações;

- 2009 – Surge a Web 2.0, fomentando o aparecimento de outros intervenientes, como a Google com as suas aplicações empresariais via web, como as Google Apps.

2.1.Conceitos Similares

Existem alguns conceitos simulares e tecnologias que desempenharam um papel fundamental no aparecimento da *cloud computing*. Alguns conceitos estão mesmo na sua génese, como ficou demonstrado no parágrafo anterior:

- *Utility computing* – Recursos computacionais de processamento, de armazenamento e aplicações, disponibilizados aos clientes de uma forma similar a um serviço ou bem de consumo;

- Computação em grelha – Com origem nos anos 90, refere-se a computadores ligados em rede, partilhando capacidade de processamento, habitualmente para a resolução de problemas complexos;

- *Autonomic computing* – Funcionamento de um computador sem intervenção externa. Tem os seus fundamentos no funcionamento do sistema nervoso humano, que controla funções vitais em modo autónomo;

- Virtualização – Partição lógica de recursos computacionais físicos. Esta tecnologia é fundamental à *cloud computing*, pelo que será abordada mais em detalhe no parágrafo 2.7.2.2, Camada de Controlo e Abstracção de Recursos;

2.2.Características Principais da Cloud

De acordo com o NIST, as cinco características principais do modelo *cloud computing* são (Mell, Peter; Grance, Timothy; NIST, 2011):

- *Self-service* a pedido - Os clientes *cloud* podem, unilateralmente, provisionar capacidade computacional, à medida das necessidades e automaticamente, sem que seja necessária interacção humana com os fornecedores dos serviços;

- Ubiquidade – As capacidades estão disponíveis na rede e são acedidas por meio de mecanismos padronizados que possibilitam o uso através de distintas plataformas de *hardware*;

- *Pool* de recursos – Serviços acessíveis simultaneamente a múltiplos clientes *cloud*, com distintos recursos físicos e virtuais alocados e realocados dinamicamente de acordo com o solicitado, existindo um certo grau de independência e abstracção quanto à localização, na medida em que os clientes *cloud* não controlam ou têm conhecimento acerca dos locais exactos a partir dos quais acedem a esses recursos, mas ainda assim, podem especificar essa localização em alto nível (por exemplo, país, região ou até mesmo centro de dados);

- Rápida elasticidade – Recursos adicionais devem ser, rápida e eficazmente aprovisionadas e libertados, em alguns casos até de forma automática, permitindo aumentar e reduzir dinamicamente as quantidades de serviços contratados. Para um cliente *cloud*, as capacidades disponíveis para aprovisionamento apresentam-se como praticamente ilimitadas e podem ser requisitadas em qualquer quantidade e a qualquer momento;

- Serviços mensuráveis - Sistemas em *Cloud* automaticamente controlam e optimizam o uso dos recursos, por meio de mecanismos de medida inseridos em níveis apropriados para cada tipo de serviço (Armazenamento, Processamento, largura de banda utilizada e contas activas). Assim, o uso dos recursos pode ser controlado e reportado com transparência para ambos, consumidor e fornecedor de serviços.

A Cloud Security Alliance (CSA), na sua publicação de "*security guidance for critical areas of focus in cloud computing*" defende ainda a inclusão de mais uma característica essencial no modelo, *multi-tenancy* (CSA, 2011):

- *Multi-tenancy* – Na sua forma mais simples, implica o acesso por vários utilizadores a recursos ou aplicações de forma partilhada, podendo estes pertencer ou não à mesma organização, tornando fundamental o reforço de politicas de segurança, segmentação, isolamento, governança, níveis de serviço e facturação de custos para as diferentes organizações.

Esta característica pode ter diferentes implicações dependendo do modelo de serviço a que se refere, sendo mais importante em modelos de desenvolvimento de *cloud* pública, embora em *cloud* privadas também se possa aplicar, caso uma organização deseje uma forma de segregação inter-departamental, por exemplo.

2.3. Outras Características da Cloud

Para além das características principais do modelo de *cloud computing* existem outras que podem ser apontadas como essenciais ou relevantes, consoante o modelo de serviço e desenvolvimento escolhidos:

- Fiabilidade - Transversal a todos os modelos *cloud*, denota a capacidade de assegurar a operação constante de um sistema, sem interrupções e perda de informação. Tipicamente é conseguida recorrendo a recursos e sistemas redundantes (Lutz Schubert, s.d.);

- Interoperabilidade – Capacidade dos sistemas para comunicarem, em que a informação enviada é perfeitamente entendida (Ahronovitz, et al., 2010) ;

- *Cloud Bursting* – Técnica usada numa *cloud* híbrida para fornecer recursos adicionais a uma *cloud* privada conforme necessário. Caso uma *cloud* privada tenha recursos disponíveis para a carga em curso, a *cloud* pública não é usada. Quando os recursos atingem um pico na *cloud* privada, recursos adicionais da *cloud* publica são disponibilizados (Ahronovitz, et al., 2010);

- Manutenção e actualizações – Manutenção e actualização de *software* estão muito facilitados pela centralização dos sistemas (Sosinsky, 2011).

Posteriormente será feita uma análise mais exaustiva, mas numa primeira abordagem, estas características fomentam duas vantagens significativas na adopção do modelo cloud *computing* (Lutz Schubert, s.d.):

- Redução de custos – A capacidade de adicionar recursos dinamicamente, como computadores virtuais, espaço de armazenamento, equipamento de rede, entre outros, permitindo que os clientes *cloud* possam gerir as necessidades de recursos ou serviços com base em cargas de trabalho consideradas normais, em vez de apontar para picos de carga ocasionais, proporcionando redução de custos em *hardware*, equipamento de rede, *software*, consumo energético e com pessoal técnico.

- Mais capacidade de resposta – O planeamento, aprovação e compra de novo equipamento ou *software* pode levar dias ou mesmo semanas em qualquer empresa. No modelo *cloud computing*, a aquisição e posterior libertação do recurso acontece de acordo com as necessidades do momento, podendo ainda dispensar qualquer intervenção humana no processo.

2.4.Modelos de Serviço

Os serviços de *cloud computing*, também referidos como *Software Platform Infrastructure* (SPI) (CSA, 2011), dividem-se em três modelos universalmente aceites (Sosinsky, 2011) de acordo com o nível de abstracção das capacidades fornecidas e com o modelo de serviço dos fornecedores (Mell, Peter; Grance, Timothy; NIST, 2011) (Vaquero, et al., 2009):

- *Software-as-a-service* (SaaS);

- *Platform-as-a-service* (PaaS);

- *Infrastructure-as-a-service* (IaaS).

Estes modelos podem ser vistos como uma arquitectura em camadas, onde os serviços de uma camada mais elevada incluem os serviços das camadas inferiores.

Cada modelo de serviço disponibiliza uma funcionalidade única de acordo com o utilizador e com o controlo sobre o ambiente de trabalho aumentando à medida que descemos na infraestrutura, sendo menor no modelo *Software-as-a-Service* e maior no modelo *Infrastructure-as-a-Service* (CIO Council , s.d.).

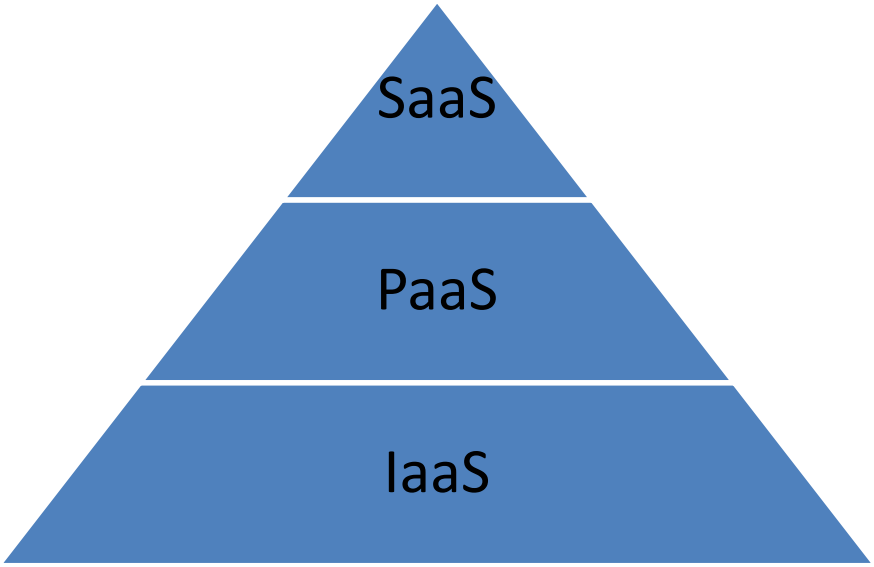

Figura 5: Modelos de Serviço

2.4.1. Software as a Service (SaaS).

Software-as-a-Service é um modelo de distribuição de *software* e talvez o modelo de *cloud* mais comum e conhecido. O cliente não compra o *software*, aluga-o através de uma subscrição ou paga consoante a utilização (Mather, et al., 2009). Os serviços disponibilizados ao cliente *cloud* utilizam aplicações do fornecedor e são executados numa infraestrutura em *cloud* e acedidas através de dispositivos vários via um *browser* (*thin client*) ou o interface de um programa (*heavy client*). Os clientes *cloud* não gerem ou controlam a infraestrutura subjacente, sejam redes, servidores, sistemas operativos, áreas de armazenamento ou mesmo funcionalidades específicas dos aplicativos, com uma possível excepção na definição de determinados parâmetros de configuração (Mell, Peter; Grance, Timothy; NIST, 2011).

Vantagens deste modelo (Mather, et al., 2009):

- Permite a uma organização transferir a gestão, a instalação e a manutenção de uma aplicação para terceiros, reduzindo custos de licenciamento, servidores e outra infraestrutura, assim como com pessoal necessário para a gerir, instalar e manter internamente;

- Permite controlar, limitar a utilização do *software* por parte do fornecedor, permitindo um apertado controlo sobre as versões instaladas. Esta forma de centralização facilita ainda a optimização de custos ao tornar desnecessário a instalação do *software* em todos os dispositivos cliente;

- A distribuição de *software* neste modelo usa o modo *one-to-many*, com a *internet* como infraestrutura subjacente, permitindo ao utilizador final aceder à aplicação através de um *browser*. Alguns fornecedores recorrem a um interface próprio desenhado para dar suporte a algumas características únicas das suas aplicações;

- Uma aplicação típica deste modelo não requer um equipamento específico para ser executado, necessitando apenas de acesso através da infraestrutura existente com acesso à *internet*. Pede ser necessário proceder a alterações da *firewall* corporativa para que a aplicação seja executada sem problemas;

- Do ponto de vista do utilizador, a gestão da aplicação é suportada pelo fornecedor, podendo ser configurada recorrendo a uma API, mas, ainda assim, uma aplicação neste modelo não permite um elevado nível de customização.

2.4.2. Platform as a Service (PaaS).

Este modelo pode ser descrito como um ambiente de trabalho para programadores de aplicações para a *cloud* (Youseff, et al., 2008), instalado na infraestrutura do fornecedor, tornando desnecessária qualquer instalação de *software* de desenvolvimento localmente (Mather, et al., 2009). Os serviços disponibilizados permitem executar numa infraestrutura em *cloud* aplicações desenvolvidas ou adquiridas pelos clientes *cloud*, usando linguagens de programação, ferramentas, livrarias e serviços suportadas pelo fornecedor. O cliente *cloud* não gere ou controla a infraestrutura subjacente, incluindo redes, servidores, sistemas operativos ou áreas de armazenamento, mas controla as aplicações desenvolvidas e eventualmente configurações do ambiente de trabalho do sistema de desenvolvimento (Mell, Peter; Grance, Timothy; NIST, 2011).

Este modelo deve incluir as seguintes características (Mather, et al., 2009):

- Acesso via *browser* às ferramentas de programação;

- Providenciar um ambiente de elevada produtividade, *Integrated Development Environment* (IDE), a ser executado na mesma plataforma de produção a que se destina, facilitando cenários de testes e depuração;

- Fornecer integração com serviços web externos e base de dados;

- Capacidade de monitorização da aplicação e actividade do utilizador, permitindo aos programadores entender melhor as aplicações e efeitos das melhorias;

- Escalabilidade, fiabilidade e segurança devem estar incluídas no modelo sem necessidade de desenvolvimentos adicionais, configuração ou custos acrescentados;

- Suporte, formalmente ou a pedido, de colaboração transversal a todo o ciclo de vida de *software*, desenvolvimento, teste, documentação e operação mantendo a segurança do código fonte e propriedade intelectual associada;

- Incluir suporte de custos consoante a utilização.

2.4.3. Infrastructure as a Service (IaaS).

Disponibiliza ao cliente *cloud* recursos de infraestrutura e serviços como capacidade de processamento, áreas de armazenamento, redes e outros recursos computacionais de modo a possibilitar a execução de aplicações e sistemas operativos. Os clientes *cloud* não gerem a infraestrutura subjacente, mas podem controlar os sistemas operativos, áreas de armazenamento e aplicações desenvolvidas e possivelmente configurar componentes de rede, por exemplo, *firewalls, routers,* etc (Mell, Peter; Grance, Timothy; NIST, 2011). Assim, um cliente *cloud* tem privilégios de desligar e ligar os servidores e equipamentos de rede, adicionar discos virtuais, configurar permissões de acesso, etc (Buyya, et al., 2011).

Os custos para o cliente *cloud* em relação aos sistemas TI tradicionais são bastante inferiores, uma vez que este não tem que adquirir servidores, equipamento de rede, custos com espaço de instalação, pessoal técnico de suporte, etc. Assim, o acesso a recursos de infraestrutura é feito por aluguer e pago consoante os recursos efectivamente consumidos.

Os serviços disponibilizados neste modelo de desenvolvimento podem ser categorizados em (Youseff, et al., 2008):

- Recursos Computacionais – O mais comum neste modelo é a disponibilização de computadores virtuais (*virtual machines*), proporcionando completa flexibilidade aos utilizadores com acesso total aos sistemas operativos;

- Armazenamento de dados – Permite aos clientes *cloud* armazenar dados numa infraestrutura remota, acessíveis de qualquer lugar e a qualquer hora, facilitando o crescimento das aplicações *cloud* para além dos servidores onde estão instaladas;

- Comunicações – *Cloud computing* elevou as necessidades de um serviço garantido de comunicações, tornando-se numa componente vital. Consequentemente, os

fornecedores *cloud* estão obrigados a providenciar comunicações que sejam, orientadas ao serviço, configuráveis, passíveis de agendamento, previsíveis e fiáveis.

2.5.Modelos de Desenvolvimento

Embora o termo *cloud computing* tenha emergido principalmente do modelo público, mais conhecido como *Public Cloud*, existem outros modelos desenvolvimento, consoante a localização física da infraestrutura de suporte e modo de distribuição que sejam adoptados. O NIST (Mell, Peter; Grance, Timothy; NIST, 2011) propõe quatro modelos de desenvolvimento:

- *Public cloud* (*Cloud* Pública);
- *Private cloud* (*Cloud* Privada);
- *Community cloud* (*Cloud* Comunitária);
- *Hibryid cloud* (*Cloud* híbrida).

Cloud pública e a *cloud* privada são subcategorias da internet que se definem pela sua relação com a empresa ou com o cliente *cloud*, podendo ainda ser referidas como internas ou externas, (Mather, et al., 2009) onde a diferenciação é baseada na relação da *cloud* com a empresa.

2.5.1. Cloud Pública

A *cloud* pública é o modelo de desenvolvimento mais conhecido e que se encontra disponível a qualquer indivíduo ou organização, bastando para tal um acesso à *internet*, e pode ser acedida de forma quase imediata. O NIST (Mell, Peter; Grance, Timothy; NIST, 2011) define este modelo como uma infraestrutura localizada dentro da propriedade do fornecedor que é aprovisionada para uso aberto ao público em geral, podendo a propriedade, a gestão e a operação ser efectuada por organizações de âmbito empresarial, académico ou governamental.

Neste modelo, a gestão da segurança e operações diárias são relegadas para o lado do fornecedor, que é responsável pela oferta do serviço, deixando pouco ou nenhum controlo ou conhecimento acerca da segurança física e lógica da infraestrutura subjacente aos clientes (Mather, et al., 2009).

2.5.2. Cloud Privada

No modelo de *cloud* privada a infraestrutura subjacente é desenvolvida e gerida exclusivamente para um cliente *cloud* específico, podendo o fornecedor pertencer à mesma organização. Já a localização desta pode ser no seio da infraestrutura da organização ou hospedada exteriormente numa infraestrutura gerida por terceiros. Uma *cloud* privada oferece ao cliente *cloud* mais controlo sobre a infraestrutura, recursos computacionais e clientes *cloud* (Jansen & Grance, 2011) que o modelo anterior. O NIST (Mell, Peter; Grance, Timothy; NIST, 2011) define este modelo como uma infraestrutura em que a operação é direccionada apenas para um cliente *cloud*, com a gestão efectuada pelo próprio ou por uma terceira entidade, e que, normalmente, a infraestrutura de suporte se encontra dentro da propriedade do cliente.

Uma vez que a organização tem que adquirir, instalar e gerir toda a infraestrutura, não beneficia da redução de custos de outros modelos, e mais vincadamente em comparação com o anterior, *cloud* publica. É ainda responsável pela gestão da segurança e operações diárias, podendo essas responsabilidades ser delegadas a uma terceira entidade por *outsourcing* reguladas por SLA's.

2.5.3. Cloud Comunitária

Conceptualmente, este modelo situa-se entre o modelo de *cloud* pública e o modelo de *cloud* privada. Recorrendo mais uma vez à definição do NIST (Mell, Peter; Grance, Timothy; NIST, 2011) para este Modelo, uma *cloud* comunitária é uma infraestrutura partilhada por várias organizações, pertencendo a uma comunidade específica e partilhando objectivos comuns, como a missão, os requisitos de segurança e as políticas e considerações de conformidade. A gestão pode ser efectuada pelas organizações ou por terceiros e a sua localização ser interna ou externa.

2.5.4. Cloud Híbrida

Uma *cloud* híbrida junta dois ou mais dos modelos referidos anteriormente. Esta abordagem pode trazer benefícios ao cliente *cloud* uma vez que permite o uso de *cloud* privada ou mesmo comunitária, para aplicações ou informação de características mais sensíveis e *cloud* pública, para aplicações ou informação de carácter não sensível para a organização. Permite ainda, quando necessário, recorrer ao *cloud bursting*, isto é, para fazer face a um pico de necessidade computacional, a organização requisita, temporariamente, a capacidade extra a um fornecedor de *cloud*, (Buyya, et al., 2011). O NIST (Mell, Peter; Grance, Timothy; NIST, 2011) define este modelo com uma

combinação de dois ou dos três modelos (Pública, Privada e Comunitária), os quais continuam a existir isoladamente, mas são integrados por meio de tecnologia proprietária ou aberta, que viabiliza a portabilidade e mobilidade da informação e aplicações.

2.6.Modelos de Desenvolvimento Alternativos

Para além do Modelo proposto pelo NIST e globalmente aceite, existem dois modelos de desenvolvimento alternativos. O primeiro apresenta uma visão diferente de *cloud computing* e foi proposto pelo Jericho Forum[4], e outro que complementa o modelo do NIST, proposto por David Linthicum, no SYS-CON's *Virtualization Journal*[5] e posteriormente no seu livro, *Cloud Computing* and SOA *Convergence in Your Enterprise, a Step-by-Step Approach*.

2.6.1. O Modelo de Linthicum

Numa tentativa de melhor descrever *cloud computing*, David Linthicum propõe uma pilha (s*tack*), onde considera cada componente lógica da infraestrutura de *cloud computing* e como os seus componentes interagem, interligando SOA e *cloud computing*. Este modelo, ainda que possa parecer mais complexo, não é necessariamente assim. Na verdade e analisando para além disso, este modelo aporta um valor acrescentado, afirma. Assim propõe onze categorias para a tecnologia de *cloud computing* (Linthicum, 2009):

[4] www.jerichoforum.org

[5] http://virtualization.sys-con.com/

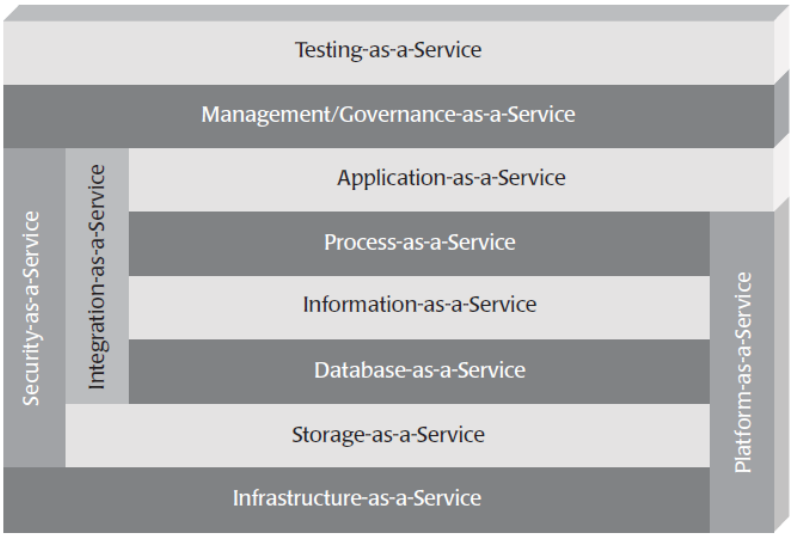

Figura 6: Componentes e categorias de *cloud computing* (Linthicum, 2009)

- *Storage-as-a-service* (Espaço de disco a pedido) - Capacidade de disponibilizar espaço físico de armazenamento num local remoto, mas tratado localmente para qualquer aplicação que dele necessite. Esta é a forma mais primitiva de *cloud computing* e é uma componente com influência em todas as restantes;

- *Database-as-a-service* (DaaS) – Disponibiliza a capacidade de usar uma base de dados remota, partilhando-a com outros utilizadores e funcionando logicamente como localmente;

- *Information-as-a-service* – Capacidade de consumir qualquer tipo de informação, localizada remotamente, recorrendo a um interface, por exemplo uma API;

- *Process-as-a-service* – Recurso remoto com capacidade de vincular múltiplos recursos juntando-os, sejam serviços ou informação, localizados no mesmo recurso de *cloud computing* ou remoto, criando um processo de negócio;

- *Application-as-a-service* (AaaS) – Também conhecido como *Software-as-a-service* (SaaS), é qualquer aplicação entregue via internet ao utilizador final, tipicamente recorrendo a uma aplicação *browser*. Comum ao modelo proposto pelo NIST, referido no parágrafo 2.4.1;

- *Platform-as-a-service* (PaaS) – Trata-se de uma plataforma completa, incluindo ferramentas de desenvolvimento, armazenamento, teste, etc, entregues através de uma plataforma remota aos utilizadores. Baseia-se no modelo de partilha de recursos. Comum ao modelo proposto pelo NIST, referido no parágrafo 2.4.2;

- *Integration-as-a-service* – Capacidade de entrega de uma *stack* completa de integração da *cloud*, incluindo interface com as aplicações, mediação semântica, controlo de fluxo, desenho de integração, etc. Essencialmente, *Integration-as-a-Service* inclui a maioria das capacidades e funções encontradas numa tecnologia tradicional de *Entreprise Application Integration* (EIA), entregue como um serviço;

- Security-as-a-service – capacidade de disponibilizar remotamente serviços de segurança através da internet;

- Management/governance-as-a-service (MaaS e GaaS) – Qualquer serviço a pedido que forneça capacidades de gestão de um ou mais serviços de *cloud*. Tipicamente os serviços mais simples, como topologia, utilização de recursos, virtualização. Sistemas de governança também vão sendo disponibilizados, oferecendo, por exemplo, capacidade para aplicar políticas definidas para informação e serviços;

- Testing-as-a-service – Capacidade de testar localmente ou sistemas entregues em plataforma *cloud* recorrendo a *software* de teste e serviços remotos.

  Infrastructure-as-a-service (IaaS) – Também referido como *data-center-as-a-service.* Capacidade para remotamente aceder a recursos computacionais. Comum ao modelo proposto pelo NIST, referido no parágrafo 2.4.3.

2.6.2. Modelo de Desenvolvimento Jericho Cloud Cube

O Jericho Forum, vinculado ao The Open Group[6], criado em 2004, composto por profissionais da área de segurança nas tecnologias de informação, governamentais, empresariais e académicas, propõe em Abril de 2009 no documento *Jericho Forum* Cloud *Model* um modelo estruturado a partir de quatro dimensões, ao qual denominam *Cloud Cube Model* (Jericho Forum, 2009). Este documento tem como finalidade (Krutz & Vines, 2010):

- Apontar que nem todos os serviços de informação funcionam melhor na *cloud*, sendo mesmo preferível mantê-los nos sistemas tradicionais;

- Explicar o seu entendimento dos modelos *cloud computing* propostos;

[6] http://www.opengroup.org/

- Descrever as características chave, riscos e benefícios de cada modelo;

- Disponibilizar uma *framework* para explorar com mais detalhe a natureza diferente de cada modelo, identificando problemas que necessitam respostas com o objectivo de os tornar mais seguros.

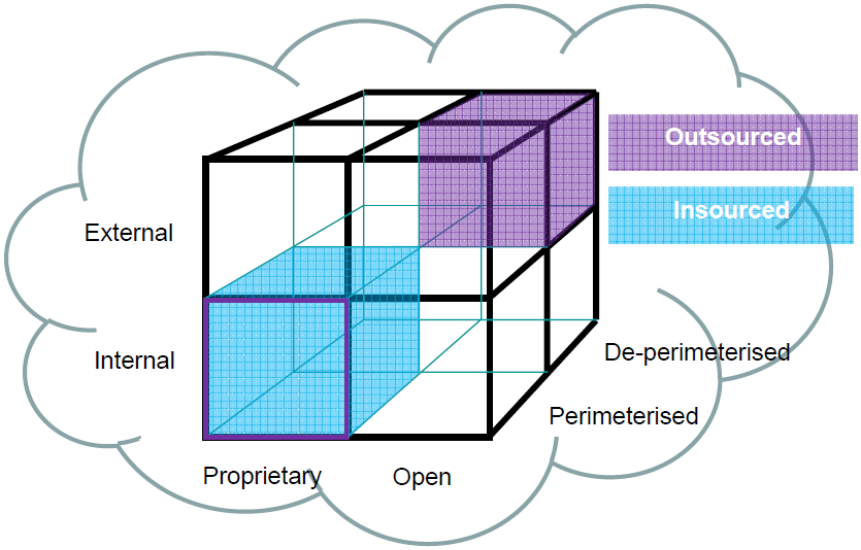

Figura 7: Representação Gráfica do Cubo da *Cloud* – Fonte: Jericho Forum

As quatros dimensões propostas de forma resumida (Sosinsky, 2011):

- Localização física da informação: Determina as fronteiras de uma organização, Interna (I) ou Externa (E);

- Direito de Propriedade: Medida que não se aplica apenas ao direito de propriedade, mas também de interoperabilidade, facilidade de transferência da informação e grau de dependência aplicacional do fornecedor (*vendor aplication lock-in*), *Proprietary* (P) ou *Open* (O);

- Fronteiras de segurança: Unidade de medida aplicável para apurar se a operação se localiza dentro ou fora desta fronteira de segurança, *Perimeterised* (Per) / *De-perimiterised* (D-p);

- Origem: *Insourced* or *Outsourced* refere se o serviço é fornecido pelo cliente ou pelo fornecedor.

Estas quatro dimensões correspondem a dois diferentes estados, nos oito modelos de *cloud* possíveis: Per (IP, IO, EP, EO) and D-p (IP, IO, EP, EO). A dimensão Origem

aponta a entrega do serviço. O *Cloud Cube Model* demonstra que a fronteira de segurança, habitualmente a *firewall* corporativa, não se aplica a *cloud computing*.

2.7.Infraestrutura de Referência de Cloud Computing

Um modelo de referência de *cloud computing* é uma abstracção dos conceitos e relações que podem ser usados para auxiliar as organizações a criar normas e directivas para a sua aplicação. Estes modelos têm como atributos chave a abstracção, entidades, relações entre elas e desprovimento de factores tecnológicos, esclarecendo contextualmente os aspectos do modelo.

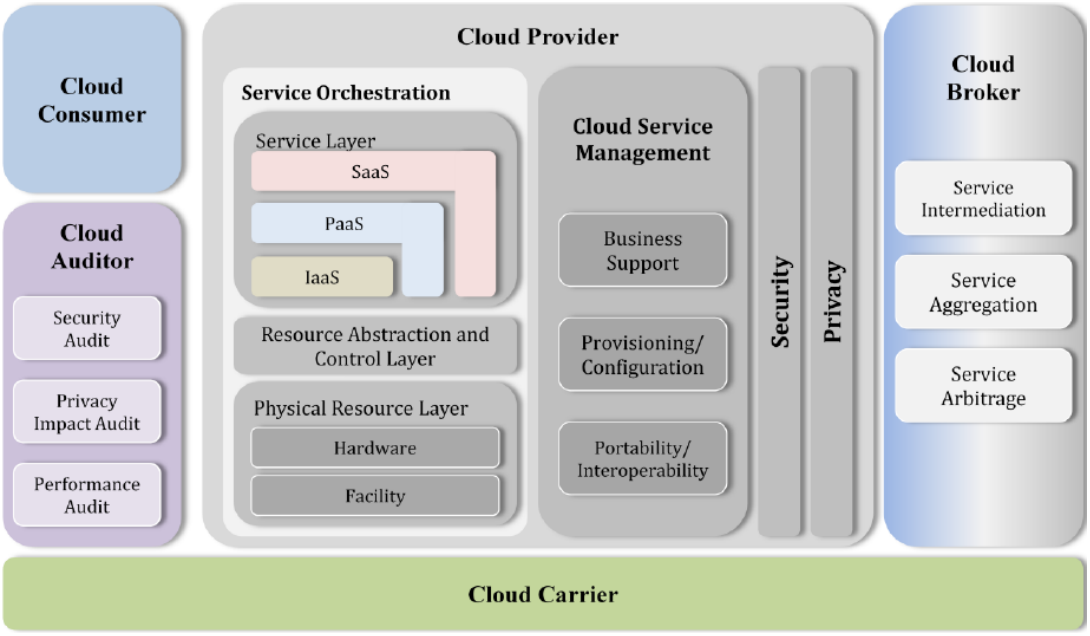

Figura 8: O modelo de referência conceptual (Liu, et al., 2011)

A infraestrutura de referência de *cloud computing* proposta pelo NIST é um modelo conceptual de alto nível que define os actores, actividades e funções usadas no processo de desenvolvimento de arquitecturas de *cloud computing* e é apresentado em duas partes (Hogan, et al., 2011):

- Uma primeira parte em que são definidos os actores ou entidades do modelo *cloud computing*, que participam em transacções ou processos
    - Cliente *cloud*;
    - Fornecedor *cloud*;

- Auditor *cloud*;
- Intermediário *cloud*[7];
- Fornecedor de serviços de internet *cloud*[8].

- Uma segunda parte, que inclui as mais importantes componentes da arquitectura *cloud computing* para a gestão e fornecimento de serviços:
  - Orquestração de serviços,
  - Gestão de serviços,
  - Segurança
  - Privacidade.

2.7.1. Actores do Modelo Cloud Computing

Numa análise ao modelo e num primeiro nível, temos os actores principais da arquitectura. Assim, os cinco actores do modelo *cloud computing* podem ser caracterizados da seguinte forma (Liu, et al., 2011):

- Cliente *Cloud* – Pessoa ou organização ou entidade que mantém uma relação comercial com um ou mais fornecedores de serviços *cloud*;
- Fornecedor *Cloud* – Pessoa, organização ou entidade responsável por disponibilizar serviços *cloud* às partes interessadas, clientes e agregadores *cloud*;
- Auditor *Cloud* – Pessoa, organização ou entidade responsável pelo exame cuidadoso e sistemático aos serviços, operações, execução e segurança em cloud *computing*;
- Intermediário *Cloud* – Pessoa, organização ou entidade que faz a gestão do uso, execução e entrega de serviços *cloud*, funcionando como intermediário entre fornecedores e clientes;

[7] Cloud Broker

[8] Cloud Carrier

- Fornecedor de serviços de internet *Cloud* – Entidade ou organização que fornece serviços de comunicação a fornecedores e clientes *cloud*.

2.7.2. Orquestração de Serviços

Orquestração de serviços é a organização dos componentes de serviço para suporte aos fornecedores de *cloud computing* na configuração, coordenação e gestão de recursos para o fornecimento de serviços aos clientes *cloud* (Liu, et al., 2011). Neste modelo são propostas três camadas de componentes que os fornecedores *cloud* necessitam para entregarem os seus serviços:

- Camada de serviço;
- Camada de controlo e abstracção de recursos;
- Camada de recursos físicos.

2.7.2.1. Camada de Serviço

Nesta camada os fornecedores *cloud* definem os interfaces que permitem aos clientes *cloud* aceder aos serviços de *cloud computing*. O modelo de serviço SPI representa um aumento da abstracção da complexa infraestrutura subjacente (Winkler, 2011). Assim, cada modelo de desenvolvimento, SaaS, PaaS e IaaS, implicam diferentes riscos e benefícios, pelo que deve ser dada atenção às especificidades de cada modelo. A partilha de responsabilidades entre o cliente e o fornecedor difere de acordo com o modelo de *cloud computing*. Dum ponto de vista do fornecedor, as suas responsabilidades vão aumento à medida se sobe na infraestrutura, isto é, tem menos responsabilidade no modelo IaaS em que apenas controla a infraestrutura de suporte subjacente, até ao modelo SaaS, em que toda a parte de *software* de suporte e software aplicacional é da a sua responsabilidade. Verifica-se o inverso sob o ponto de vista do cliente em que a responsabilidade aumenta à medida que se desce na infraestrutura.

2.7.2.2. Camada de Controlo e Abstracção de Recursos

Camada composta pelos componentes de abstracção, que permite aos fornecedores de *cloud computing* gerir e fornecer acesso às camadas físicas aos clientes. A gestão nesta camada recorre a componentes de *software* que são responsáveis por controlo de acessos, alocação de recursos e monitorização da utilização dos serviços contratados. Esses componentes de *software* são conhecidos como *hypervisores* (supervisores), máquinas virtuais, dispositivos de armazenamento e outros métodos de abstracção, separando a parte física da infraestrutura da parte computacional.

A virtualização é um elemento chave na tecnologia de *cloud computing* (Amies, et al., 2012) e permite que servidores, dispositivos de armazenamento e outros componentes de rede sejam tratadas como um conjunto de recursos, podendo ser alocadas quando solicitadas (CSA, 2011).

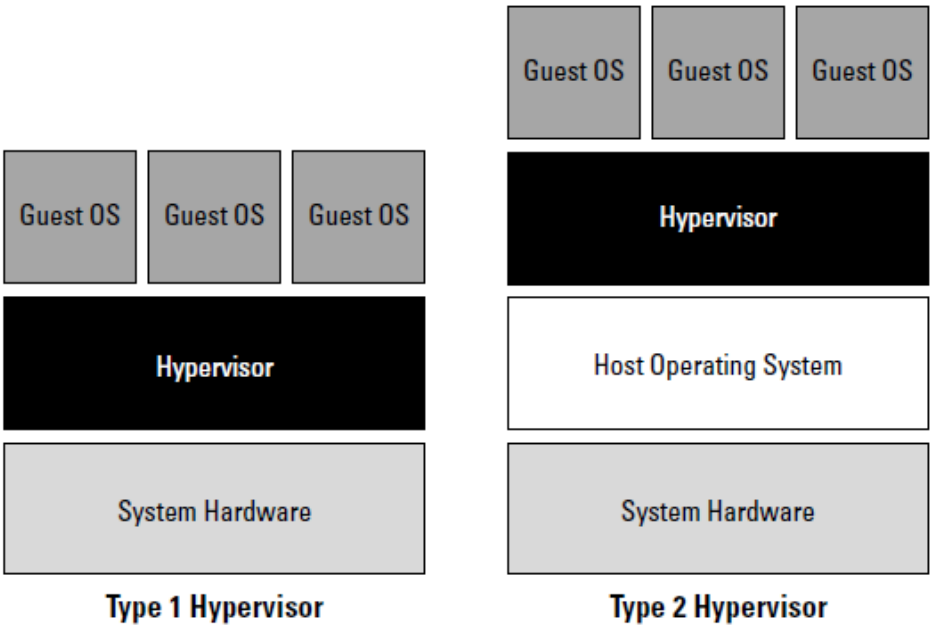

Figura 9: Arquitecturas de virtualização

Existem dois tipos de arquitecturas de virtualização. A virtualização do tipo I, em que o supervisor é instalado logo acima do *hardware*, sem qualquer outro sistema operativo ou software intermediário, e comunica directamente com o *hardware*. A virtualização de tipo II o supervisor é executado sobre o sistema operativo anfitrião e este é responsável pela comunicação com o *hardware*.

O supervisor é a componente da máquina virtual que permite a partilha de recursos e o isolamento desta com o *hardware* do sistema anfitrião. Esta funcionalidade de isolamento do supervisor determina a capacidade de resistência e segurança da máquina virtual e a sua exposição ao risco.

Outras formas de virtualização usadas em *cloud computing* são a para-virtualização, que permite que um único servidor seja utilizado como se de vários servidores se tratasse e o *clustering*, que permite que vários servidores sejam utilizados como apenas um.

Os benefícios da virtualização incluem a *multi-tenancy*, isto é, a melhor utilização dos servidores e a consolidação dos centros de dados. Estes permitem aos fornecedores de serviços *cloud* alcançarem mais densidade de clientes *cloud* num mesmo servidor, que se

traduz em melhores taxas de utilização de *hardware*, aportando ganhos financeiros em despesas com equipamentos e eficiência operacional. Todavia, a virtualização também traz consigo preocupações de segurança, como sistemas operativos a serem executados no topo de outro sistema operativo e problemas de segurança ao nível do supervisor.

A virtualização tem as seguintes características (Ghosh & Hughes, 2011):

- Isolamento – Um equipamento virtual encontra-se isolado dos restantes e, dessa forma, problemas e falhas com um não tem efeito nos restantes;
- Independentes do *hardware* – Máquinas virtuais que são independentes do *hardware*, o que permite a sua movimentação entre diferentes plataformas;
- Encapsulamento – Máquinas virtuais são encapsuladas em formato de ficheiro. Esta característica permite que a sua movimentação entre servidores de suporte seja uma tarefa simples, tornando possível a rápida automatização e eficácia para a disponibilização de recursos adicionais, tarefa que seria muito demorada e de difícil implementação com instalações de raiz;
- Compatibilidade – Os sistemas operativos e aplicações podem ser executados sem alterações em ambientes virtuais.

Algumas formas de virtualização que podem ser apontadas:

- Virtualização de servidores;
- Virtualização de dispositivos de armazenamento;
- Virtualização de dispositivos de rede;
- Virtualização de serviços;

Actualmente e de uma forma geral, a virtualização encontra-se em quase todas as infraestruturas, tradicionais ou de *cloud*. A razão para isso são os benefícios que os ambientes virtuais proporcionam e que podem ser resumidos (Josyula, et al., 2012)

- Acesso a pedido a recursos de rede, de armazenamento ou computacionais;
- Custos energéticos mais reduzidos, com os benefícios inerentes;
- Redução do espaço ocupado pela infraestrutura;

- Redução de custos iniciais e operacionais em equipamento.

2.7.2.3. Camada de Recursos Físicos

A terceira e última camada inclui recursos físicos de *hardware*, tais como computadores, *routers, firewalls, switches*, componentes de armazenamento e outras componentes da infraestrutura. Inclui ainda todo o equipamento de suporte, como equipamento de refrigeração e ventilação, equipamento redundante de energia, fontes de alimentação, comunicações e espaço físico. A Cloud Security Aliance define a segurança nesta camada de forma similar à segurança actualmente existente nas infrestruturas tradicionais (CSA, 2011). Assim a segurança pode ser vista de dois prismas (Krishnan, 2010):

- Segurança física – Um centro de dados tem diversas camadas de segurança, acumulando controlos em cada perímetro. O acesso às zonas de gestão a partir das quais é feita a gestão, o acesso à informação e às aplicações dos clientes *cloud*, é restrito e apenas autorizado ao pessoal estritamente necessário. O acesso físico aos equipamentos de suporte da infraestrutura também deve ser controlado. Para impedir o acesso a possíveis atacantes que possam comprometer a informação e detectar possíveis intrusões, são usados controlos de segurança, como, por exemplo câmaras, leitores biométricos, leitores de cartões, detectores de movimento, etc. Devem ainda existir detectores para os riscos de fogo, inundação, calor extremo e controlo de níveis de humidade;

- Segurança de rede – A segurança de rede é garantida recorrendo a uma variedade de dispositivos como balanceadores de rede, *firewalls*, sistemas de detecção de intrusão, etc. As aplicações e serviços são segmentados em áreas virtuais, garantindo que o tráfego de rede não passa para além do perímetro necessário ao funcionamento aplicacional.

Com o objectivo de redução das vulnerabilidades para um nível tolerável e de minimizar os efeitos de um ataque, são utilizados diversos controlos de segurança que podem ser categorizados nas seguintes áreas (Krutz & Vines, 2010):

- Restritivos – Visam reduzir a probabilidade de um ataque;

- Preventivos – Proteger as possíveis vulnerabilidades tornando um ataque impossível ou reduzindo o seu impacto. Também desencorajam tentativas de violação das políticas de segurança;

- Correctivos – Tem como objectivo reduzir os efeitos de um ataque;

- Detectivos – Detectar ataques e desencadear controlos preventivos ou correctivos. Estes controlos informam sobre violações ou tentativas de violação das políticas de segurança e incluem controlos como *Intrusion Detection Systems* (IDS), políticas organizacionais, câmaras e detectores de movimentos.

Já na perspectiva dos clientes *cloud computing*, as preocupações de segurança centram-se no armazenamento e processamento de informação sensível em modelos de *cloud* públicas, híbridas e comunitárias, ainda que um pouco menos neste último modelo de desenvolvimento (Winkler, 2011). Estas preocupações focam-se em duas áreas:

- Perda de controlo sobre a informação quando a gestão desta passa a ser efectuada dentro do perímetro de rede informática do fornecedor de serviços *cloud*;

- Preocupações sobre a sua informação residir em sistemas partilhados, com os riscos daí inerentes para informação sensível.

2.7.3. Serviços de Gestão na Cloud

Esta camada inclui todas as funções necessárias para a gestão e operação dos serviços requisitados pelos clientes de *cloud computing* (Liu, et al., 2011) e divide-se em três áreas:

- Suporte ao negócio;

- Aprovisionamento e configuração;

- Portabilidade e interoperabilidade.

2.7.3.1. Suporte ao Negócio

Para o suporte ao negócio estão todos os processos que permitem ao cliente gerir os custos com a *cloud*, efectuar pagamentos e a troca de informação entre cliente e fornecedor acordada contratualmente, como por exemplo informação sobre incidentes, tentativas de intrusão, etc. Também deve ser permitido ao cliente *cloud* prever necessidades futuras para que, caso se mostre necessário, rever as condições contratuais com o fornecedor.

2.7.3.2. Aprovisionamento e Configuração

Para o aprovisionamento e configuração os fornecedores devem disponibilizar aos seus clientes ferramentas que lhes permitam uma gestão automática e facilitada dos seus recursos. As API's são uma dessas ferramentas que actuam como facilitador e que permitem aos clientes o aprovisionamento de recursos adicionais e a pedido, com menor

ou maior capacidade disponível para a configuração desses mesmos recursos (Scruggs, et al., 2011). Estas API's permitem retirar dos ambientes *cloud* todas as suas capacidades e vantagens, mascarando a complexidade dos sistemas subjacentes da arquitectura.

Um dos problemas actuais e que deve ser analisado com atenção é a proliferação de diferentes API's de cada fornecedor, dificultando a portabilidade e a interoperabilidade entre fornecedores e infraestruturas. A Unified Communications Interoperability Forum (UCI)[9], organização sem fins lucrativos, visa definir normas que facilitem a unificação e interoperabilidade entre sistemas de hardware, *software*, fornecedores de serviços *cloud* e consumidores *cloud*. Existem outras organizações que estudam este problema, que será abordado mais à frente.

2.7.3.3. Portabilidade e Interoperabilidade

Os fornecedores devem disponibilizar aos seus clientes ferramentas que facilitem e permitam a fácil mobilidade da informação e comunicação entre os seus sistemas e os sistemas do cliente ou de outros fornecedores. A portabilidade a interoperabilidade são dos aspectos que levantam preocupações aos potenciais clientes do modelo de *cloud computing*. De facto, muitos fornecedores têm um modelo de infraestrutura de suporte e API's proprietárias que, após a migração das aplicações e informação de um cliente para a sua infraestrutura *cloud*, a sua portabilidade e interoperabilidade com outros sistemas, pode tornar-se difícil e complexa pelas diferenças entre o suporte aplicacional e de compatibilidade.

2.8. Diferença entre Arquitectura Cloud e Arquitectura Tradicional

Numa primeira análise podemos encontrar semelhanças entre estas duas arquitecturas, a infraestrutura *cloud* e a infraestrutrura tradicional, porque normalmente ambas são compostas de três camadas. Na arquitectura tradicional a primeira camada, a infraestrutura, compreende todo o equipamento de rede, tais como servidores, *switches*, balanceadores, *routers*, equipamentos de protecção, rede física, etc, em tudo similar com à camada IaaS do modelo *cloud*. A segunda camada é composta pelo *middleware*, onde se encontram os sistemas operativos, as plataformas de desenvolvimento e o diverso

[9] http://www.ucif.org/Home.aspx

software de suporte à camada seguinte, que podemos mapear para PaaS no modelo *cloud*. Na camada de topo temos todo o *software* aplicacional em tudo idêntico ao SaaS no modelo *cloud computing*.

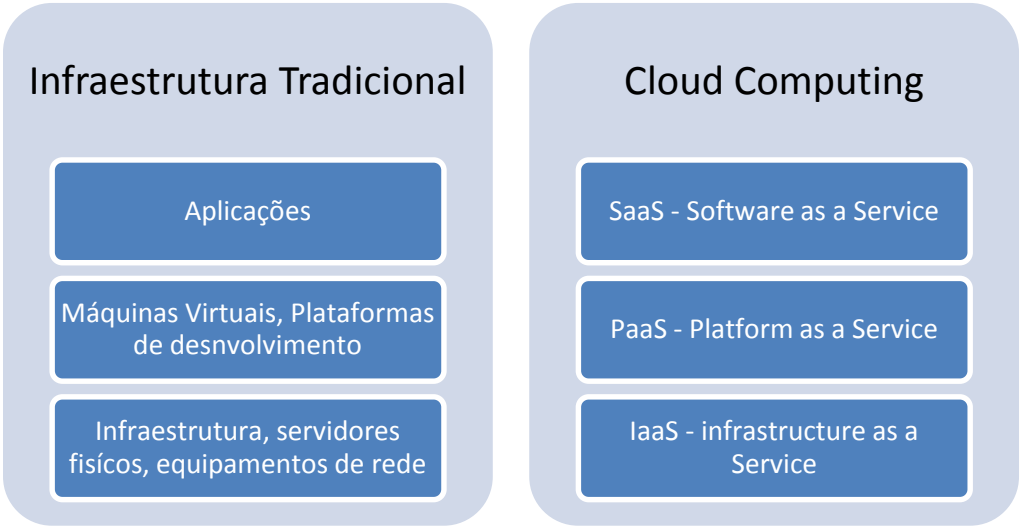

Figura 10: Infraestrutura tradicional versus *Cloud Computing*

Apesar de existirem semelhanças entre as duas arquitecturas, *cloud* e tradicional, estas têm diferenças fundamentais (Ghosh & Hughes, 2011):

- Tempo de Implementação - Uma vez efectuadas as configurações iniciais na arquitectura *cloud*, o acesso é muito mais rápido que numa arquitectura tradicional, que necessita de tempo de instalação e configuração. Numa arquitectura *cloud* o tempo de implementação pode ser de minutos ou horas, já numa arquitectura tradicional esse tempo pode ascender a dias ou mesmo semanas;

- Custo de implementação - A arquitectura *cloud* reduz ou elimina os elevados custos iniciais na aquisição de equipamento, de *software* e na instalação que se verificam numa arquitectura tradicional em que esse valor é fixo e inicial. Numa arquitectura *cloud*, o custo é variável consoante os serviços contratados;

- Economia de escala - Uma das vantagens da arquitectura *cloud* é que as boas práticas de segurança que os fornecedores devem observar na configuração dos sistemas favorecem todos os clientes. Numa arquitectura tradicional essas configurações têm que ser implementadas em cada infraestrutura instalada e, dado o seu custo operacional, por vezes essas boas práticas de segurança apenas se encontram em empresas de maior dimensão e maior capacidade financeira;

- *Multi-tenacy* – Quando aplicado correctamente numa arquitectura *cloud* permite aos fornecedores terem vários clientes suportados pelos seus sistemas partilhados. Numa arquitectura tradicional apenas encontramos esta característica em certas aplicações de *hosting*;

- Escalabilidade – Permite que os recursos numa arquitectura *cloud* possam ser aumentados ou reduzidos de forma automática e sem intervenção humana no processo. Já numa arquitectura tradicional essa intervenção é sempre necessária;

- Virtualização – As arquitecturas *cloud* são habitualmente virtualizadas ao passo que nos sistemas tradicionais predominam os sistemas físicos, ainda que ocasionalmente possam existir sistemas virtualizados.

“*Out of intense complexities intense simplicities emerge.*”

Winston Churchill

3. Análise à Arquitectura Cloud Computing

O paradigma de *cloud computing* possui propriedades únicas que o tornam muito apetecido nos dias de hoje. Algumas dessas propriedades levantam preocupações, como por exemplo, de segurança, perda de controlo sobre a informação, de disponibilidade dos serviços migrados para a *cloud*, de performance no acesso aos serviços, de custos, etc. Um inquérito levado a cabo pela Internacional Data Corporation[10] (IDC), no 3º trimestre de 2009 a 263 executivos de tecnologias de informação, ao pedido para hieraquizar a preocupações do modelo *cloud computing* obteve como resultados que as três principais preocupações eram nas áreas de segurança, disponibilidade e performance.

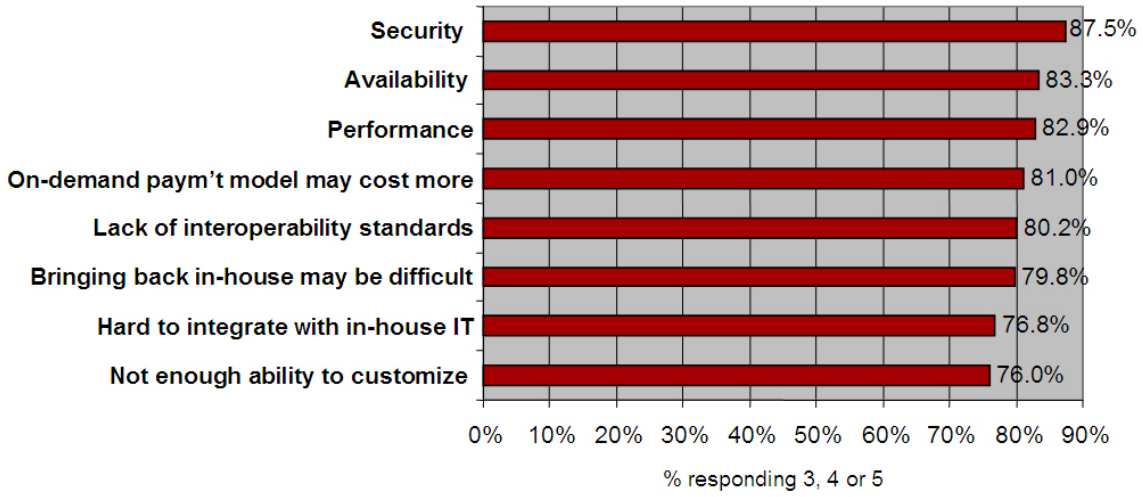

Figura 11: Principais preocupações na cloud (Gens, 2009)

Os fornecedores de serviços *cloud*, tendo consciência dessas preocupações e receios desenvolveram técnicas e ferramentas de protecção para as minimizarem e tornarem a *cloud computing* segura (Sosinsky, 2011). Para que os sistemas em *cloud computing* possam atingir todo o potencial prometido pela tecnologia, devem oferecer aos seus clientes e utilizadores uma segurança, privacidade e desempenho efectivos.

A grande concentração de informação e sistemas de vários fornecedores numa infraestrutura em *cloud* apresentam-se como alvos preferenciais a ataques informáticos, por outro lado, sistemas *cloud* podem apresentar defesas mais robustas, escaláveis e com um custo efectivo (Perilli, et al., 2009). A confiança na utilização da *cloud* depende dos mecanismos de segurança, controlo

[10] http://www.idc.com/about/about.jsp

efectivo de acessos, gestão robusta de identidades, meios seguros de comunicação e controlos de segurança devidamente implementados e auditados.

De acordo com outros inquéritos levados a cabo por outras entidades, as seguintes preocupações parecem estar na mente de muitos clientes *cloud computing* (Josyula, et al., 2012):

- Como irá a *cloud* manter a informação segura e disponível;
- Como gerir os riscos de segurança e gestão de risco, actuais e futuros;
- Que tipos de serviços de segurança estão disponíveis através da *cloud*;
- Como efectuar auditorias externas e internas à segurança na *cloud*;
- Como automatizar o aprovisionamento de serviços de rede, computacionais e de armazenamento;
- Como fazer aprovisionamento a pedido e em tempo real recorrendo a um portal que suporte todos os dispositivos de infraestrutura necessários;
- Como promover a interacção de todas as novas ferramentas de *cloud* com as ferramentas actuais.

Os responsáveis pela segurança de uma organização devem estar aptos a determinar os controlos preventivos e detectivos de segurança existentes, para que possam definir a postura de segurança da organização (Krutz & Vines, 2010). Para uma melhor análise e decisão de um processo de migração para *cloud computing*, um conhecimento aprofundado da sua infraestrutura, das suas vantagens e desvantagens e das questões de segurança, é necessário e pode marcar o sucesso ou insucesso na adopção de um modelo de *cloud computing* no seio de uma organização. Nos parágrafos seguintes analisaremos o modelo de *cloud computing*, tendo como base a infraestrutura de referência proposta pelo NIST e globalmente mais aceite, definindo claramente as fronteiras de responsabilidade do fornecedor e do cliente, vantagens e desvantagens, riscos e questões de segurança inerentes ao ambiente de *cloud computing*, assim como várias ferramentas de controlo e monitorização existentes.

3.1. Vantagens Cloud Computing

Para além das cinco vantagens essenciais definidas pelo NIST e já abordadas no capítulo 2.2, *self-service* a pedido, ubiquidade, pool de recursos, rápida elasticidade e serviços mensuráveis, outras vantagens podem ser apontadas ao modelo *cloud computing*:

- Redução de custos;
- Escalabilidade;
- Actualizações automáticas;
- Facilidade de acesso;
- Fiabilidade;
- Rápido desenvolvimento e implementação;
- Acesso a melhores recursos tecnológicos.

3.1.1. Redução de Custos

Os motivos mais importantes para a introdução de uma infraestrutura *cloud* numa organização são os factores financeiros. O ganho financeiro pode ser significativo, dependendo do modelo de desenvolvimento *cloud* seleccionado, sendo mais elevado num ambiente de *cloud* pública e mais reduzido ou nulo num modelo de *cloud* privada. De facto, a *cloud* pública não requer investimento em *hardware*, *software* ou equipamento de rede (Mather, et al., 2009). De uma forma geral, uma infraestrutura *cloud computing* reduz os custos de gestão, manutenção e instalação de um centro de dados próprio com melhorias de eficiência nas infraestruturas TI, minimizando os custos e melhorando de forma significativa a agilidade na instalação e disponibilização de novos serviços e recursos. Dependendo do modelo escolhido, por vezes é afirmado (SUN, 2011) que, para os utilizadores, o ambiente de *cloud computing* significa que não existem necessidades de aquisição de equipamento, gestão de licenças, gestão de *software* e actualizações, contratação de pessoal técnico ou consultores e a compra ou arrendamento do espaço necessário.

Outro factor de grande relevância no modelo de *cloud computing* é a capacidade de gerir picos de utilização, eliminando a necessidade de ter recursos subutilizados apenas para provir essa procura ocasional.

Para que as razões económicas sejam consideradas, os modelos *cloud computing* devem ser facilitadores dos seguintes aspectos (Lutz Schubert, s.d.):

- Redução de custos – É um dos primeiros objectivos para avançar para uma infraestrutura de *cloud computing*, adaptável às necessidades dos utilizadores e oferecendo redução de custos na sua manutenção e aquisição. As características da *cloud* que favorecem a redução de custos são a escalabilidade e pagamento por utilização (*pay per use*);

- Custo por utilização – Uma característica fundamental do modelo *cloud computing* é relacionar os custos com a efectiva utilização dos recursos. O pagamento por utilização está intimamente relacionado com a qualidade do serviço suportado, onde os requisitos e as características solicitadas para o sistema com um determinado custo inerente, podem ser requisitados. Esta mudança estrutural no fornecimento de serviços é peça fundamental no interesse actual no paradigma da *cloud computing*, deslocalizando o investimento inicial para custos operacionais, beneficiando assim o desenvolvimento de pequenas empresas e negócios, pela facilidade na adopção de tecnologias e soluções inovadoras;

- Melhor *time to market* – Característica essencial para pequenas empresas e negócios que desejam colocar os seus serviços e bens no mercado, sem necessidade de adquirir e instalar uma infraestrutura informática, melhorando assim a capacidade competitiva com empresas instaladas e de maior dimensão, que até são compelidas a disponibilizar os seus serviços de forma mais rápida para se manterem competitivas. *Cloud computing*, com a sua capacidade de fornecer fácil e rapidamente uma infraestrutura adaptada a cada negócio reduz o *time to market*;

- Retorno de Investimento (ROI)[11] – Factor essencial para todos os investidores mesmo que nem sempre seja garantido. Um sistema de *cloud computing* deve permitir que os custos e esforço no seu investimento tenham retorno para ser comercialmente viável, directamente, trazendo mais clientes para o negócio, ou indirectamente, em benefícios por publicidade;

[11] Return of Investiment

- Alterar despesas de Capital (CAPEX)[12] em despesas operacionais (OPEX) [13] - Despesas de capital são sempre necessárias para instalar uma infraestrutura local. Com a deslocalização em regime de *outsourcing* dos recursos computacionais para *cloud computing*, uma organização está, actualmente, a ter despesas operacionais para garantir os recursos necessários, uma vez que os irá adquirir segundo as necessidades operacionais;

- "Amigo de Ambiente"[14] – Relevante não apenas para reduzir os custos energéticos mas também a "pegada ecológica". A emissão de carbono pelo *hardware* pode ser estimado e deve ser levado em conta e *cloud computing* permite a redução do consumo energético.

3.1.2. Escalabilidade

O modelo *cloud computing* oferece aos seus clientes uma elevada escalabilidade, disponibilizando recursos em picos de utilização imprevistos, sejam temporários ou mais definitivos (Rountree & Castrillo, 2014), permitindo que a necessidade de capacidade adicional possa ser muito rapidamente respondida, em vez de terem que adquirir e configurar novo equipamento. Caso esses picos de utilização já não se verifiquem, esses recursos podem ser desligados da infraestrutura, não deixando para trás parque informático desnecessário.

A escalabilidade permite ainda responder às necessidades de curto prazo ou projectos de curta duração. Um cliente *cloud computing* tem flexibilidade para a instalação de novos recursos sempre que tal se mostre necessário.

3.1.3. Actualizações Automáticas

Os clientes de *cloud computing* têm sempre ao seu dispor a versão de *software* mais recente e actualizada, reduzindo o tempo necessário que os seus empregados TI dedicam a essa tarefa,

[12] CAPEX - Capital expenditure, designa o montante de dinheiro dispendido na aquisição (ou introdução de melhorias) de bens de capital de uma determinada empresa, nomeadamente em equipamentos e instalações.

[13] OPEX - Operacional expenditure, designa o montante de dinheiro utilizado para manter em operação os bens de capital de uma determinada empresa, nomeadamente em equipamentos e instalações.

[14] "Going green"

libertando-os assim para outras mais importantes e focadas nas necessidades e objectivos da empresa (Scruggs, et al., 2011).

3.1.4. Facilidade de Acesso

Empregados, clientes e parceiros de negócio de uma empresa cliente do modelo *cloud computing*, podem com facilidade aceder à informação necessária, seja para consulta ou actualização. Esta facilidade de acesso proporciona uma melhoria na colaboração entre elementos de uma equipa geograficamente dispersa (Scruggs, et al., 2011).

Outra razão na facilidade de acesso deve-se ao aumento dos dispositivos com capacidade de acesso a serviços *cloud*, permitindo a utilização de qualquer computador, pessoal ou empresarial, dispositivos móveis, *tablets* ou *smart phones* (Mather, et al., 2009). Desde que tenham acesso à internet são potenciais clientes de *cloud computing*, pois permitem um acesso ubíquo. Esta facilidade é um factor importante na tomada de decisão para clientes *cloud computing*.

3.1.5. Fiabilidade

O fornecedor *cloud*, sendo este o seu negócio principal e face aos acordos assinados com os clientes e escala, têm as capacidades técnicas, pessoal especializado e sistemas para manter um serviço com qualidade e fiabilidade, seja a nível de equipamentos, de comunicações e de segurança, proporcionando boa fiabilidade dos serviços que disponibiliza aos seus clientes.

3.1.6. Rápido Desenvolvimento e Implementação

Duas das cinco características principais de *cloud computing* que apontam para um rápido desenvolvimento e implementação são self-service a pedido e rápida elasticidade. Uma empresa em vez de adquirir instalar e configurar sistemas e computadores, despendendo todo o tempo necessário para essa tarefa, pode recorrer a um fornecedor *cloud* e ter ao seu dispor os sistemas necessários, instalados e configurados. Caso já tenha um contrato com um fornecedor e dependendo das suas cláusulas, o tempo necessário será de poucos minutos.

3.1.7. Acesso a Melhores Recursos Tecnológicos

Algumas empresas, especialmente as de pequena dimensão, podem ter dificuldade no acesso a melhores recursos tecnológicos e na contratação de colaboradores com os conhecimentos necessários à sua implementação e manutenção. Movendo os seus serviços e informação para o modelo *cloud*, podem ter acesso aos mesmos recursos tecnológicos que uma empresa de maior dimensão ou com mais recursos financeiros (Scruggs, et al., 2011). Permite ainda

acesso uma a infraestrutura bem desenhada e dimensionada para as necessidades específicas uma vez que o negócio central de fornecedor de serviços *cloud* é em sistemas de tecnologias de informação (Ghosh & Hughes, 2011)

3.1.Desvantagens da Cloud Computing

A *cloud* apresenta também algumas desvantagens, que são geralmente referidas como barreiras à adopção do modelo e a mais mencionada por todos é a segurança, que, dada a sua importância, será abordada mais à frente, no parágrafo 3.2. As desvantagens que podem ser apontadas ao modelo são:

- Maturidade – Sendo uma tecnologia ainda recente, o mercado de fornecedores é emergente, com muitas e variadas ofertas, em que cada um reclama serem as mais inovadoras, quer em termos técnicos quer em termos financeiros. O que se verifica é que muitas dessas empresas emergentes são mais tarde adquiridas por empresas maiores e já estabelecidas (Ghosh & Hughes, 2011). Este aspecto levanta um sério problema aos clientes *cloud* porque a empresa adquirente passa a ser o fornecedor e pode não garantir o mesmo serviço acordado, assim como assegurar a interoperabilidade com os sistemas, dados e informação com a infraestrutura *cloud* desse fornecedor;

- SLA's – A oferta de SLA´s ainda é díspar entre fornecedores e alguns, de pequena dimensão, não dispondo mesmo desses acordos (Linthicum, 2009). Este problema dificulta a comparação entre fornecedores ou torna essa comparação mesmo impossível perante um leque de ofertas tão diferenciado. A normalização de SLA's que permite aos fornecedores a adaptação a um público-alvo mais alargado também é uma desvantagem, porque impede aos clientes de acederem a SLA's negociados ou se negociados o sejam a custos mais elevados;

- Definição dos componentes – A definição das componentes *cloud* ainda não é clara, dificultando a selecção por comparação de um fornecedor *cloud* (Ghosh & Hughes, 2011);

- Monitorização – Os fornecedores *cloud* nem sempre disponibilizam ferramentas de monitorização ou a sua funcionalidade é restricta (Sosinsky, 2011), limitando a visibilidade dos clientes *cloud*, no que respeita a incidentes ou tentativas de intrusão na infraestrutura do fornecedor;

- Comunicações – Se as comunicações não forem bem dimensionadas para picos de transferências, mover grandes quantidades de informação para a *cloud* pode originar paragens prolongadas para os utilizadores.

3.2.Riscos de Segurança

Para uma migração para o modelo *cloud* torna-se imperativo um perfeito conhecimento dos riscos de segurança inerentes. Existe uma multiplicidade de formas de analisar os riscos de segurança do modelo *cloud computing*, mas estes podem ser divididos em três classes distintas (Chow, et al., 2009):

- Ameaças de segurança tradicionais – referem-se aos riscos de qualquer sistema de informação ligado à internet acrescido de ameaças inerentes do modelo *cloud*. O impacto das ameaças tradicionais é claramente amplificado devido, quer aos múltiplos recursos passíveis de serem afectados, quer ao número de entidades que podem ser afectadas. A área nebulosa sobre as responsabilidades, entre clientes e fornecedores, para a identificação da causa de determinado incidente, acrescenta preocupações de segurança ao modelo. As ameaças tradicionais começam na infraestrutura do cliente, devendo este aplicar os meios de segurança necessários aos sistemas que o liguem aos serviços *cloud*, tarefa por vezes complicada quando parte da infraestrutura se encontra no exterior à sua *firewall*;

- Ameaças de segurança à disponibilidade dos sistemas – Falhas de acesso a serviços e informação de forma grave e prolongada. Estas podem ocorrer por catástrofes naturais, falhas de sistemas, cortes de energia, falha de comunicações ou mesmo por ataques aos sistemas do fornecedor. Medidas de segurança que mitiguem estas ameaças devem existir e estarem implementadas pelo fornecedor.

- Ameaças de terceiros – O controlo por terceiros de informação sensível ou confidencial levantam preocupações nos clientes. De facto existem várias ameaças dentro da própria infraestrutura do fornecedor, como a coexistência de vários clientes, que podem ser concorrentes de negócio potenciando o perigo de exposição ou fuga de informação. O acesso à informação e sistemas por funcionários da empresa fornecedora de serviços também levanta sérias preocupações de segurança aos clientes.

Para uma melhor avaliação do risco, devem ser efectuadas as seguintes análises (Sosinsky, 2011):

- Determinar claramente quais os recursos de dados, serviços ou aplicações a migrar para *cloud computing*;
- Determinar a exposição dos recursos ao risco;
- Determinar quais os riscos associados a um determinado modelo de serviço *cloud*;
- Avaliar o sistema do fornecedor ou fornecedores de serviços *cloud* escolhidos, compreender como a informação irá ser transferida, onde irá ser armazenada e avaliar as comunicações entre a organização e o fornecedor.

Apesar de parte do controlo em modelos *cloud* passarem para a esfera do fornecedor de serviços, ainda assim, o cliente *cloud* deve ter em conta a sua responsabilidade pelo uso dos serviços, mantendo um conhecimento dos riscos envolvidos, ponderar alternativas, estabelecer prioridades e possíveis alterações ao nível da segurança e privacidade, na sua organização.

Os riscos mais comuns associados à *cloud computing* a ter em consideração por qualquer organização que pretende adoptar o paradigma de *cloud computing* são (Perilli, et al., 2009):

- Perda de governança – Ao optar por modelos *cloud*, o cliente necessariamente cede o controlo da sua informação, dados e sistemas ao fornecedor de serviços. *Os* SLA´s entre ambas as partes podem não comprometer suficientemente o fornecedor a disponibilizar serviços ou controlos de segurança que reduzam ou eliminem as preocupações dos clientes, aumentado o seu sentimento de insegurança face ao modelo;
- Fornecedor *Lock-In* – Dependência dos serviços proprietários de um determinado fornecedor de serviços *cloud*, origina a que um cliente tenha grande dificuldade na migração para outro fornecedor. Serviços que não suportem a portabilidade de informação e serviços para outro fornecedor, aumentam o risco de indisponibilidade.
- Fornecedor *Lock-Out* – Similar ao abordado no ponto anterior, mas nesta situação o cliente é impedido de aceder à informação, seja por falência do fornecedor ou por outras causas. Este risco pode tornar a informação e recursos vitais para o negócio do cliente indisponíveis;

- *Compliance* e riscos legais – Investimentos feitos pelas empresas cliente para obter certificações podem ser postos em causa, caso o fornecedor de serviços *cloud* não possa fazer evidência que também as possui ou que não permita uma auditoria por parte do cliente à sua infraestrutura. É da responsabilidade do cliente certificar-se que o fornecedor detém as certificações necessárias e ainda, ter conhecimento da partilha de responsabilidades de segurança entre o fornecedor e o cliente;

- Vulnerabilidades na gestão dos interfaces – Estes interfaces são normalmente utilizados pelo cliente com acesso através da *internet* e permitem acesso a mais informação e recursos que os fornecedores de recursos tradicionais, aumentado o risco, especialmente se usados em conjunto com acesso remoto e existam vulnerabilidades no *browser* ou nas comunicações utilizadas;

- Protecção de Informação – *Cloud computing* coloca vários riscos a clientes e fornecedores. O mais relevante é a exposição ou fuga de informação sensível, mas também a sua perda ou indisponibilidade. Para o cliente pode ser difícil avaliar as práticas e políticas no tratamento e manuseamento da informação pelo fornecedor. Este problema aumenta quando se utilizam transferências de informação entre diversos modelos de *cloud*;

- Eliminação de informação de forma insegura ou incompleta – Pedidos do cliente *cloud* ao fornecedor para eliminar recursos ou informação, por exemplo, no fim do contrato ou por mudança de fornecedor, pode não ser efectuada da forma mais apropriada para elimina-la de forma completa e eficaz. Em *cloud computing*, a eliminação da informação pode por vezes ser difícil pela redundância inerente ao modelo, ou porque os dispositivos onde essa informação reside também são usados por outros clientes, dificultando a efectiva eliminação da informação;

- Comportamento malicioso de funcionários – Danos causados intencionalmente por funcionários do fornecedor, que podem ser extensos, pelas permissões de acesso e autorizações inerentes às suas funções. Este risco é abrangente ao modelo *cloud computing*, uma vez que tanto pode ocorrer dentro da organização do cliente, como na organização do fornecedor;

- Tratamento de incidentes – A detecção, informação e subsequente gestão de falhas de segurança é uma preocupação para os clientes, que depositam a sua confiança nos fornecedores para o seu correcto tratamento;

- Ambiguidade de responsabilidades – Uma vez que os serviços de *cloud computing* abrangem ambas as organizações, cliente e fornecedor, a responsabilidade nas áreas de segurança também são transversais às duas, potenciando que áreas de defesa sejam deixadas sem supervisão caso não sejam claramente definidas as responsabilidades sobre todas a áreas. Esta partilha de responsabilidades é diferenciada consoante o modelo *cloud* adoptado;

- Falha de isolamento – *Multi-tenancy* e partilha de recursos da *cloud*, são características mais abrangentes no modelo de desenvolvimento de *cloud* pública. Uma falha nos mecanismos de separação e isolamento de recursos e informação dos diversos clientes *cloud*[15] pode levar à perda de informação ou à sua exposição indevida;

- Indisponibilidade do serviço – Esta indisponibilidade pode ser causada por uma multiplicidade de razões, deste a falha de equipamento, *software* ou comunicações entre o cliente e fornecedor, etc.

3.3. Responsabilidade em cada Modelo de Serviço

As responsabilidades sobre os riscos e segurança em *cloud computing*, estão sempre intimamente ligados com o modelo de serviço escolhido, SaaS, PaaS ou IaaS, aumentando o grau de responsabilidades do cliente na gestão da segurança e riscos associados à medida que este se move do modelo SaaS para PaaS e deste para IaaS.

[15] tenants

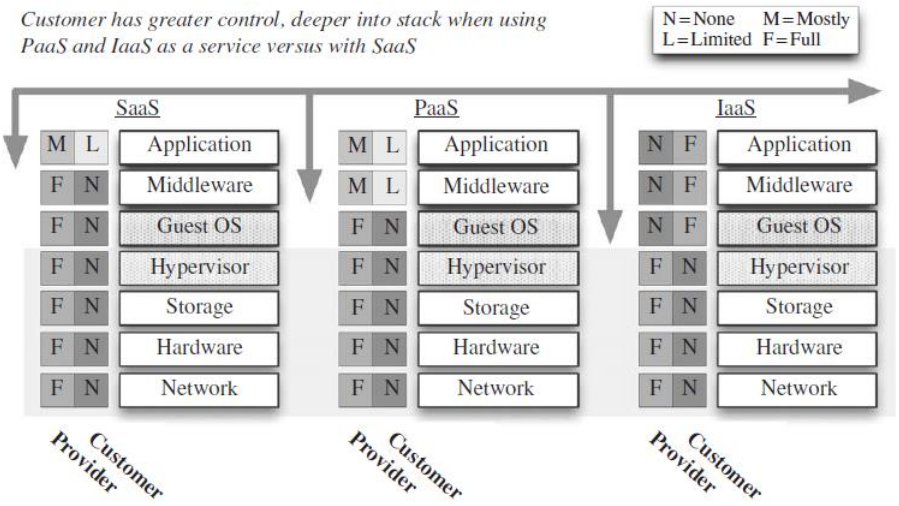

Figura 12: Controle sobre a segurança em SaaS, PaaS e IaaS (Winkler, 2011)

As responsabilidades entre os fornecedores e clientes variam de acordo com o modelo serviço. Nas tabelas seguintes sumarizam-se as responsabilidades de cada em cada modelo.

Tabela 1: Responsabilidades no Modelo SaaS

Cliente *Cloud*	Fornecedor *Cloud*
• Manutenção dos sistemas de gestão de identidades; • Gestão dos sistemas de identidades; • Gestão da plataforma de autenticação.	• Infraestrutura fisíca de suporte, desde as instalações aos equipamentos de suporte; • Equipamentos da infraestrutura, servidores, equipamento de rede, etc.; • Gestão das actualizações e procedimentos de segurança; • Configuração dos sistemas de segurança; • Sistemas de monitorização; • Manutenção das plataformas de segurança; • Registo de eventos e monitorização de segurança.

Tabela 2: Responsabilidades no Modelo PaaS

Cliente *Cloud*	Fornecedor *Cloud*
• Assegurar *compliance* na protecção de dados e informação, tratados e processados; • Manutenção dos sistemas de gestão de identidades; • Gestão dos sistemas de identidades; • Gestão da plataforma de autenticação.	• Infraestrutura fisíca de suporte, desde as instalações aos equipamentos de suporte; • Equipamentos da infraestrutura, servidores, equipamento de rede, etc.; • Gestão das actualizações e procedimentos de segurança; • Configuração dos sistemas de segurança; • Sistemas de monitorização; • Manutenção das plataformas de segurança; • Registo de eventos e monitorização de segurança.

Tabela 3: Responsabilidades no Modelo IaaS

Cliente *Cloud*	Fornecedor *Cloud*
• Manutenção dos sistemas de gestão de identidades; • Gestão dos sistemas de identidades; • Gestão da plataforma de autenticação; • Gestão do SO virtual, actualizações e configurações de segurança; • Configuração dos sistemas de segurança; • Monitorização dos SO virtuais; • Manutenção das plataformas de segurança; • Registo de eventos e monitorização de segurança.	• Infraestrutura fisíca de suporte, desde as instalações aos equipamentos de suporte; • Equipamentos da infraestrutura, servidores, equipamento de rede, etc.; • Equipamentos de gestão

3.4.Risco

Para uma análise de segurança, o conceito de risco surge em primeira linha. Numa definição muito redutora, risco[16] é a possibilidade de um acontecimento futuro e incerto; perigo. O risco alia-se à incerteza, que define o nosso conhecimento sobre eventos futuros e o seu desfecho (M.Talabis, et al., 2013). Por outro lado, risco pode ser definido pela quantificação ou medida da incerteza permitindo dessa forma classificar o risco, ou seja, fazer uma avaliação do risco. Para a definição de risco ser completa, o risco envolve as seguintes componentes:

Evento - Acaso ou situação que é possível mas não é certa e que no contexto da avaliação de risco é sempre no futuro e ocorre por acção ou inacção. Em termos de segurança a sua ocorrência tem sempre uma conotação negativa.

- Activos – São os alvos da ocorrência, directa ou indirecta;
- Resultado – É o impacto do evento sobre os activos da organização;
- Probabilidade – É a quantificação de determinado evento acontecer.

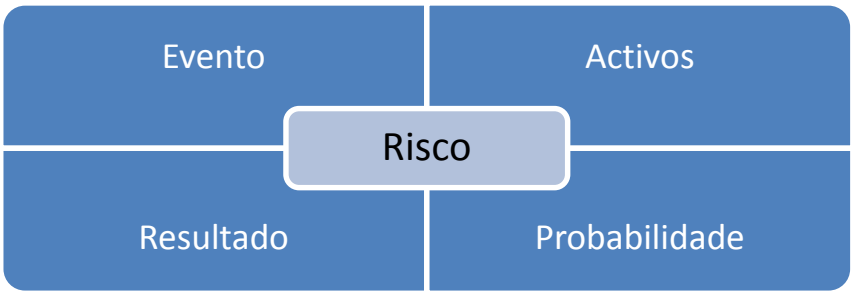

Figura 13: Componentes do Risco

3.4.1. Avaliação do Risco

A avaliação do risco é definido pela probabilidade da concretização de uma ameaça e determinando o resultado desse evento medindo o impacto negativo sobre os sistemas, dados ou informação. A Tabela 4 mostra como a correlação entre a probabilidade e o impacto pode ser efectuada.

[16] http://www.infopedia.pt/lingua-portuguesa/risco

Tabela 4: Análise de Risco. Adaptado de ISO/IEC 27005:2008

		Probabilidade				
		Muito Baixa	Baixa	Média	Elevada	Muito Elevada
Impacto	Muito Baixo	**0**	**1**	**2**	**3**	**4**
	Baixo	**1**	**2**	**3**	**4**	**5**
	Médio	**2**	**3**	**4**	**5**	**6**
	Elevado	**3**	**4**	**5**	**6**	**7**
	Muito elevado	**4**	**5**	**6**	**7**	**8**

A Avaliação do risco envolve a identificação e a quantificação dos riscos de perda de confidencialidade, de integridade e de disponibilidade (M.Talabis, et al., 2013) e deve ser efectuada para cada processo, informação e sistemas que se encontrem em consideração num projecto de migração para a *cloud*.

3.5.Segurança em Ambientes Cloud

A segurança em ambientes *cloud* deve alinhar fornecedores e clientes com um objectivo comum, salientando a capacidades e requisitos para um padrão que assegure a interoperabilidade, a facilidade de integração e a portabilidade. A relação entre estes factores deve ser tratada de forma a criar controlos de segurança e minimizar as preocupações na utilização de serviços *cloud*. As organizações com pretensões na migração dos seus serviços e informação para a *cloud* devem ter, desde do início, noção dos seguintes conceitos (CSA, 2011):

- Completa noção de como os serviços *cloud* são desenvolvidos e de que são frequentemente disponibilizados de locais muito diferenciados, originando confusões sobre a localização da informação e serviços;

- A forma como os serviços *cloud* são acedidos é muitas vezes descrito em relação ao perímetro de segurança de uma organização, habitualmente bem definido por algum equipamento de segurança, como por exemplo uma *firewall*. Enquanto contínua a ser da maior importância compreender a localização das fronteiras de segurança em

cloud computing, esta noção não e por vezes bem compreendida ou tratada correctamente por muitas organizações;

- A deslocalização e erosão das fronteiras de segurança já ocorrem nos dias de hoje, mesmo sem uma infraestrutura *cloud computing*, no entanto, esta veio acentuar e acelerar esse problema. Os controlos de segurança anteriores usados não estão adequados com à ubiquidade no acesso à informação e serviços proporcionada pela infraestrutura *cloud computing*, tornando necessário aplicar novos controlos que se adequem ao conceito *cloud*;

Os controlos de segurança em *cloud computing* não diferem muito dos controlos de segurança nas infraestruturas mais tradicionais, contudo, devido aos modelos de serviço, modelos operacionais e às tecnologias empregadas, este pode apresentar diferentes riscos para uma organização, quando comparado com os modelos tradicionais (CSA, 2011). Como referido anteriormente, a segurança é uma das principais preocupações das organizações e clientes quando ponderam o uso de modelos *cloud*. De facto, muitas análises e inquéritos de mercado revelam que a segurança é um dos maiores obstáculos à adopção do modelo (Anon., 2012) (Mather, et al., 2009), tornando-se imperativo ser correctamente tratado para criar um ambiente de confiança que facilite a migração para uma infraestrutura de *cloud computing*. À medida que novos clientes aderem ao paradigma e movem as suas aplicações e informação para um fornecedor de serviços *cloud*, o nível de percepção de segurança deve ser igual ou superior ao que tinham na arquitectura tradicional, mesmo quando a informação é acedida através de redes inseguras como internet e com reduzido controlo onde a mesma é guardada.

A postura de segurança de uma organização é sempre caracterizada pela efectidade, pela maturidade e pela complitude dos riscos ajustados aos controlos de segurança e à sua implementação. Estes controlos devem abranger todas as camadas, desde a segurança fisica das instalações, à segurança da infraestrtura e dos sistemas passando pelas aplicações neles instaladas, assim como às pessoas e aos processos que com eles operam e interagem, com separação de responsabilidades, de acessos e de processos de autenticação. Os objectivos de segurança são factores chave na decisão para a migração de serviços e informação para uma plataforma *cloud computing*, pelo que as organizações devem proceder a uma análise de risco na avaliação às opções de segurança e privacidade disponibilizadas pelo fornecedor de serviços (Jansen & Grance, 2011).

Para minimizar os custos e maximizar a efectividade, as organizações devem considerar a segurança e a privacidade durante todo a ciclo do processo, com início logo na fase de planeamento. *Frameworks* de controlo ainda não se encontram completamente adoptadas em

ambientes *cloud*, ainda que os existentes, como COBIT, ITIL e ISO 27001 e ISO 27002 sejam considerados sufucientes e um bom ponto de partida (Halpert, 2011). A ISO encontra-se actualmente a desenvlover novas normas, nomeadamente a norma ISO/IEC 27018[17], para a protecção da *Personal Identifiable Information* (PII) em *clouds* públicas pelos fornecedores de serviços e a norma ISO/IEC 27002[18], com recomendações para a segurança da informação e controlos de segurança em *cloud computing*. Existem ainda organizações que estudam e emitem relatórios com recomendações e programas de *compliance* e de segurança em *cloud computing* como a CSA, NIST, ISACA e ENISA.

Com o objectivo de mitigar e reduzir o risco, os clientes devem avaliar e gerir a segurança e privacidade do ambiente *cloud*. Para o atingir devem recorrer à implementação de controlos em todos os serviços e a processos que assegurem a observância e cumprimento das boas regras e postura de segurança de todos os intevenientes. Assim as organizações na adopção do modelo devem observar os seguintes passos:

- Processos de governança, risco e *compliance*;
- Auditar os processos de negócio e operacionais;
- Gestão de pessoas, processos e identidades;
- Assegurar a protecção da informação;
- Aplicar políticas de privacidade;
- Avaliar as disposições de segurança para as aplicações em *cloud*;
- Assegurar que a infraestrutura e ligações de rede são seguras;
- Avaliar os controlos de segurança da infraestrutura e estrutura;
- Gerir controlos de segurança nos contratos com o fornecedor;
- Revogar os serviços com um fornecedor.

[17] http://www.iso27001security.com/html/27018.html

[18] http://www.iso27001security.com/html/27017.html

3.5.1. Processos de Governança, Gestão de Risco e Compliance

A maior parte das organizações têm establecidas políticas de segurança e *compliance* para a protecção do seu sistema de informação e dos dados nele armazenados, tratados e processados. Estas políticas e procedimentos são criados com base numa análise de risco efectuada na organização, após considerado o impacto no caso dos seus sistemas de informação serem comprometidos. Uma *framework* de controlos e procedimentos é criada e posta em prática servindo de referência à execução e validação da *compliance* existente numa organização. Estes princípios, políticas, plano de segurança e processos de melhoria contínua representam para uma organização a governança da segurança, gestão do risco e modelo de *compliance*.

Para mitigar os desafios de segurança no modelo, para além do já referido, o cliente deve solicitar ao fornecedor de serviços provas de que estes também aderem aos controlos de segurança. Isso pode ser demonstrado através de certificações por entidades independentes. Existe um número de certificações que são úteis em serviços *cloud computing*, dependendo do modelo de serviço fornecido e da localização do fornecedor.

3.5.1.1. Compliance

Compliance é a responsabilidade de uma organização em operar de acordo com as leis, regulamentos, especificações e padrões do meio onde se insere. Cada país tem as suas leis e regulamentos a nível de segurança e privacidade, tornando potencialmente difícil uma organização ser *compliant* dentro do seu espaço de acção quando opta por uma solução em *cloud computing* (Jansen & Grance, 2011). Quando uma organização migra os seus sistemas para a *cloud* há uma incerteza sobre a localização exacta onde a sua informação será armazenada ou onde os seus processos são efectivamente executados. Por outro lado, uma das características do modelo *cloud* é a redundância e assim replicando a informação por vários servidores e centro de dados onde os fornecedores operem. Esta informação nem sempre é disponibilizada aos clientes, devendo, no entanto, o fornecedor facultar toda a cooperação com o cliente sobre os requisitos deste acerca da localização da sua informação e sistemas (Krutz & Vines, 2010).

3.5.1.2. Governança

Governança é o controlo e fiscalização de uma organização sobre as politícas, procedimentos e normas para o desenvolvimento de aplicações e aquizição de serviços de sistemas de informação, assim como o desenho, implementação, teste, utilização e monitorização dos serviços contratados. Apesar de *cloud computing* simplificar a aquisição de novos serviços,

não significa obrigatoriamente menor necessidade de governança (Jansen & Grance, 2011). A facilidade de aquisição de novos serviços e sistemas em *cloud computing* pode fomentar que certas áreas de uma organização não observem as regras e politícas de segurança. Para mitigar este risco, devem ser disponibilizados mecanismos de auditoria e ferramentas de verificação para validar os serviços e reforçar a observância das políticas de segurança da organização. Existem muitos modelos de governança, no entanto todos eles obedecem a cinco princípios básicos (CSA, 2011):

- Auditar os fornecedores de serviços;
- Equipa responsável pela gestão de processos;
- Responsabilidade corporativa e *compliance*;
- Transparência financeira e divulgação de informação;
- Estrutura de propriedade da informação e controlo de acessos.

A governança numa organização tem como objectivos principais (NIST, 2011):

- Estabelecer uma direcção estratégica;
- Assegurar que os objectivos organizacionais e de negócio são atingidos;
- Confirmar que os riscos são geridos apropriadamente;
- Verificar se os recursos são usados correctamente.

3.5.1.3. Gestão do Risco

Até há alguns anos, *firewalls* e *software* de antivírus era tudo o que a esmagadora maioria das organizações necessitavam para mitigar o risco. Nos anos mais recentes, o panorama das ameaças mudou consideravelmente (Davis, et al., 2011). As ameaças, nos dias de hoje são bastante mais vastas. Desde ameaças internas numa organização, novos vírus e *malware* que surgem mais frequentemente, piratas informáticos com motivos politícos ou apenas para mostrarem as suas capacidades, passando por novas normas e legislação governamental. Tudo combinado torna imperativo a existência de uma *framework* de gestão de risco.

Numa organização, a gestão do risco requer um conhecimento abrangente dos processos de negócio, das ameças potenciais e das vulnerabilidades que possam ser exploradas junto com

uma avaliação da probabilidade da ameaça e seu impacto, caso esta se concretize (Josyula, et al., 2012).

Gestão de risco é um procedimento para identificar e avaliar o risco dos processos, dos activos e pessoas na sua interacção com os diversos sistemas operacionais, tomando as medidas necessárias para o reduzir para um valor aceitável.

Uma *framework* de gestão de risco numa organização inclui os métodos e processos para gestão de riscos e aproveitamento de oportunidades, mantendo o foco no négocio. Em ambientes *cloud computing* a gestão escolhe uma resposta estratégica aos riscos identificados e analizados que podem passar por (CSA, 2011):

- Evitar – Passa por abandonar as actividades sujeitas ao risco;
- Reduzir – Tomar medidas que reduzam a probabilidade do risco ocorrer ou minimizar o seu impacto;
- Transferir ou segurar – Transferência, total ou parcialmente do risco, assegurando compensações monetárias caso este aconteça;
- Aceitar – Não são tomadas medidas e o risco é aceite mediante uma decisão de custo/benefício.

Como na generalidade das metedologias, a gestão do risco, quando aplicada de forma apropriada, ganha caracteristicas de ciclo, proporcionando uma melhoria contínua e ajustável às alterações dos processos. A gestão de risco é composta por cinco fases (Davis, et al., 2011):

Figura 14: *Framework* de gestão do risco. Adaptado (Davis, et al., 2011)

Cada fase é compreendida por:

- Fase 1 - Identificar os activos dos sistemas de informação:
    - Criar uma base de controlo de risco;
    - Reavaliar o risco.
- Fase 2 - Quantificar e qualificar as ameaças:
    - Definir valores de criticidade da informação;
    - Identificar as funções de negócio;
    - Mapear processos de informação;

    - Identificar activos do sistema de informação;
    - Atribuir valores de criticidade aos activos.
- Fase 3 - Avaliar as vulnerabilidades:
    - Avaliar as ameaças ao negócio;
    - Identificar ameaças técnicas físicas e administrativas;
    - Quantificar a probabilidade de impacto da ameaça;
    - Procurar fraquezas nos fluxos dos processos;
    - Identificar ameaças nas componentes dos processos;
- Fase 4 - Corrigir falhas de controlo:
    - Identificar os controlos existentes em relação às ameaças;
    - Determinar lacunas nas componentes do processo;
    - Alterar as falhas dos controlos em processos e posteriormente em funções de negócio;
    - Categorizar falhas nos controlos por severidade;
    - Atribuir classificações de risco;
- Fase 5 - Gerir o risco residual:
    - Selecção de controlos;
    - Implementar Controlos;
    - Validar novos controlos;
    - Recalcular classificações de risco;

3.5.2. Auditar os Processos de Negócio e Operacionais

As organizações compreendem a importância em auditar a conformidade dos seus sistemas e se estes se encontram alinhados com as políticas da organização, as leis, nacionais ou internacionais, regulamentos, especificações e padrões. Com os desafios colocados com a migração de serviços e informação para ambientes *cloud computing*, os clientes devem solicitar aos fornecedores relatórios de auditoria realizados por entidades independentes, que certifiquem que eles se encontram em *compliace* com essas directivas e regulamentos. Antes da escolha recair sobre determinado fornecedor, um cliente deve ter toda a informação sobre os centros de dados e práticas de segurança deste (Scruggs, et al., 2011). O acesso pleno à informação de auditoria é essencial para determinar os termos dos contratos e SLA's.

Alinhamento com a segurança é um elemento significativo de qualquer *compliance framework*. Existem três áreas onde metedologias de segurança devem ser observadas em ambientes *cloud* e que são de particular interesse para clientes e auditores:

- Compreender o ambiente interno de controlo de um fornecedor, incluindo riscos, controlos de segurança e aspectos de governança, sempre que o ambiente do cliente interagir com serviços *cloud*;
- Acesso ao processo de auditoria, incluindo fluxo e autorização quando esse processo abrange os serviços *cloud*;
- Acesso a ferramentas de gestão e controlo dos serviços *cloud*, disponibilizados pelos fornecedores aos clientes e informação sobre a segurança das mesmas.

3.5.2.1. Compreender o Ambiente Interno de um Fornecedor Cloud

A utilização de serviços em ambientes *cloud* levanta a necessidade de auditoria às actividades dos empregados do fornecedor, de forma a verificar que os controlos de segurança vão de encontro às necessidades do cliente. Devem ser aplicados controlos que permitam:

- Assegurar o isolamento das aplicações e informação do cliente nos ambientes partilhados entre múltiplos clientes;
- Promover a protecção dos activos de acesso não autorizado por pessoas da organização do fornecedor.

3.5.2.2. Acesso ao Processo de Auditoria

Os clientes de serviços *cloud* têm a expectativa legítima de que os seus serviços e informação irão manter a integridade e serão devidamente protegidos (Winkler, 2011). Uma auditoria à segurança de um fornecedor de serviços é um aspecto essencial nas considerações de segurança do cliente quando pretende migrar serviços e informação para a infraestrutura do fornecedor. As auditorias devem ser afectuadas por pessoas ou entidades independentes e com conhecimento especializado. É da responsabilidade do cliente afectuar auditorias regulares, durante o período de vigência do acordo entre ambos e, dessa forma, certificar que os serviços continuam a ser prestados dentro dos parâmetros acordados (Scruggs, et al., 2011).

As políticas de segurança de um fornecedor de serviços, certamente incluem a proibição de fornecer informação sobre certas áreas da sua infraestrutura, nomeadamente, detalhes técnicos de segurança, processos ou alguma informação que coloque em risco dados e privacidade dos seus clientes. Ainda assim, devem fornecer informação suficiente a um cliente que permita que estes tomem decisões informadas no processo de escolha de um fornecedor, ou para implementar medidas de segurança adicionais, caso se mostre necessário. Estas informações devem incluir (Winkler, 2011):

- Políticas de segurança – Facultar detalhes suficientes das normas e políticas de segurança, que permitam aos clientes formar uma expectativa de segurança e adequar o seu comportamento na utilização dos serviços;

- Implementação de segurança e procedimentos – Um fornecedor deve detalhar suficientemente as implementações de segurança e procedimentos, de modo a permitir ao cliente formar uma opinião de confiança sobre a segurança da sua informação e serviços prestados e processados na infraestrutura do fornecedor. Esta informação não deve ser de teor puramente técnico, mas sim tão abrangente que permita ao cliente aferir que o fornecedor compreende a necessidade de segurança, se está de facto implementada e se este possui a capacidade de a manter em todos os aspectos de operação;

- Comunicações de serviço – Comunicações de segurança e disponibilidade de serviços devem ser fornecidas aos clientes para que estes tomem as medidas necessárias e elaborem planos de contingência.

3.5.2.3. Acesso a Ferramentas de Gestão e Controlo

Para além dos controlos aplicáveis aos serviços *cloud*, os fornecedores devem também facultar aos clientes ferramentas de gestão e de monitorização das suas aplicações e informação. Essas ferramentas incluem:

- Catálogos de serviços;
- Serviços de subscrição;
- Processos de pagamento;
- Registos de eventos operacionais;
- Informação actualizada sobre utilização de serviços;
- Ferramentas de configuração de serviços e gestão de utilizadores.

3.5.3. Gestão de Pessoas, Processos e Identidades

As organizações têm habitualmente que criar e gerir muitos colaboradores, cada um com a sua função que acedem a recursos, a serviços e a aplicações. Os fornecedores devem permitir aos seus clientes assignar e gerir níveis de acesso diferenciado, de acordo com as suas políticas de segurança. Estas funções e permissões de acesso são aplicadas a cada recurso, serviço ou aplicações. Os clientes, por seu lado, devem assegurar, que o fornecedor de serviços tem processos e funcionalidades de controlo de acesso às aplicações e informação residentes na sua infraestrutura.

A gestão de identidades é um mecanismo fundamental no controlo de acessos em ambientes *cloud*, prevenindo o acesso não autorizado na manutenção das funções dos utilizadores. A implementação de um sistema de gestão de identidades deve incluir (Krutz & Vines, 2010):

- Estabelecer uma base de dados de identidades e credenciais;
- Gerir os direitos de acesso dos utilizadores;
- Cumprimento das políticas de segurança;
- Desenvolvimento da capacidade de criar, modificar e apagar contas de acesso;

- Configurar e monitorizar os acessos aos recursos;
- Criar um procedimento para remover direitos de acesso;
- Dar acções de formação sobre a correcta utilização dos procedimentos.

Este sistema de gestão de identidades deve permitir um acesso simples e robusto para serviços e utilizadores, proporcionando o aprovisionamento e gestão de identidades únicas para cada utilizador ou serviço. Um problema recorrente para as organizações que utilizem serviços *cloud* é a dificuldade em prolongar a identificação e autenticação da sua estrutura para a estrutura *cloud* do fornecedor. Em alternativa, a utilização de dois sistemas de identificação e autenticação, uma para os sistemas internos e outra para os sistemas *cloud* externos, é fonte de complicações e dificuldades de gestão no decurso do tempo. A *Identity Federation* (federação de identidade), popularizada com a introdução do *Service Oriented Architectures* (SOA), é uma solução (Jansen & Grance, 2011).

Federação de identidade proporciona a uma organização cliente de serviços *cloud* e a uma organização fornecedora de serviços *cloud*, confiar e partilhar identidades e respectivos atributos transversalmente às duas infraestruturas. Um factor importante numa organização para efectivamente gerir identidades e controlo de acessos em ambientes *cloud computing* é a presença de um sistema de gestão de federação de identidades (Mather, et al., 2009). Esta capacidade é da maior importância para permitir a um cliente *cloud* recorrer ao *single sign-on* nos seus sistemas, internos e externos. Genéricamente os fornecedores *cloud* devem ainda suporte:

- Gestão de federação de identidade e gestão de identidades externa - Organizações que consumam recursos em ambientes *cloud* e que, na maioria dos casos, já dispõem de uma base de dados de utilizadores nos seus sistemas, que irão pretender utilizar sem necessidade de as recriar quando recorram a serviços de terceiros;
- Aprovisionamento de identidades e delegação – Um fornecedor de serviços *cloud*, deve delegar aos seus clientes a gestão e administração de utilizadores;
- *Single Sign-On* e *Single Sign-Off* – Um cliente *cloud* pode recorrer à federação de identidades para todas a aplicações, internas de externas, que permitam o *single sign-on* e *single sign-off*, assegurando que as sessões de utilizador terminem graciosa e apropriadamente;

- Identidade e Auditoria de acessos – Deve ser permitido aos clientes *cloud* auditarem os registos de acessos a serviços e aplicações, para sua segurança e *compliance* com políticas, leis, normas e regulamentos;

- Processos de autenticação robustos – Para acesso a informação sensível, um fornecedor *cloud* deve suportar autenticação robusta, multi-factor ou mesmo biométrica;

- Funções, permissões de acesso e gestão de políticas – Os clientes *cloud* devem descrever e fazer cumprir as suas políticas de segurança, funções de utilizadores, grupos e permissões de acesso às suas aplicações e informação, respeitando os requisitos legais, nacionais ou internacionais.

3.5.4. Protecção de Dados e Informação

Para todas as organizações os dados são uma das priopridades do ponto de vista da segurança. Face ao modelo distribuido e redundante dos ambientes *cloud computing* e às responsabilidades partilhadas, entre cliente e fornecedor, esta realidade ganha ainda mais importância, para todos os modelos em *cloud computing*. A *data life cycle* (ciclo de dados), em ambientes *cloud* é composto por seis fases:

Figura 15: Ciclo de dados

Nos modelos de *cloud computing* existem essencialmente duas formas de dados (Scruggs, et al., 2011):

- Dados em repouso – Dados gravados em qualquer meio de suporte magnético ou outro que se encontrem na infraestrutura do fornecedor de serviços;
- Dados em trânsito – Dados manuseados ou transferidos entre dois pontos, dentro da infraestrutura do fornecedor ou entre este e a infraestrutura do cliente.

Essencialmente, as questões relacionadas com o risco de dados ou informação, em ambientes *cloud* têm origem em:

- Risco de roubo ou divulgação de informação;
- Risco de alteração maliciosa de dados (*tampering*) ou acesso não autorizado à informação;
- Risco de perda ou indisponibilidade da informação

A norma ISO/IEC 27001:2013 - *Information technology - Security techniques - Information security management systems - Requirements*, classifica a informação de acordo com categorias de importância e sensibilidade, conforme a tabela seguinte:

Tabela 5: ISO/IEC 27001:2013 - Information technology

Categoria dos dados	Descrição
Não classificados e públicos	• Os dados não são confidenciais e podem ser tornados públicos sem implicações para a empresa. • Perda de disponibilidade por inacessibilidade dos sistemas é um risco aceitável. • A integridade é importante mas não vital.
Proprietária	• A informação é restrita a acessos internos sujeitos a aprovação e protegida de acessos externos. • Acesso não autorizado comprometendo a eficácia operacional e causar perdas financeiras consideráveis, ganhos à entidades concorrênciais ou causar perda de confiança. • A integridade dos dados é um factor fundamental.

Categoria dos dados	Descrição
Dados confidenciais de clientes	• A dados recebidos de clientes em qualquer suporte para processamento em produção pela empresa. A cópia original desses dados não pode ser alterada sem a expressa autorização do cliente. • Níveis mais elevados de integridade, confidencialidade e o acesso restrito é fundamental.
Dados confidenciais da empresa	• Dados recolhidos e utilizados pela empresa nos processos de negócio, para empregar colaboradores, para realizar pedidos de clientes e gerir todos os aspectos financeiros. • O acesso a estes dados é muito restrito no seio da empresa. • Níveis muito elevados de integridade, confidencialidade e acesso restrito.

3.5.5. Controlos de Segurança de Dados em Ambientes Cloud

Como já referido anteriormente os controlos de segurança dependem sempre, do modelo de serviço a que se aplicam. Num modelo de serviço IaaS, a responsabilidade dos controlos de segurança estão mais no lado dos consumidores *cloud* por exemplo a responsabilidade da encriptação da informação, já num modelo de serviço SaaS, a responsabilidade está do lado do fornecedor *cloud*, uma vez que, quer os dados quer as aplicações não são visíveis ou controláveis pelo consumidor *cloud*.

3.5.5.1. Aplicar Confidencialidade, Integridade e Disponibilidade

Os princípios da confidencialidade, integridadede e disponibilidade, são aplicáveis ao manuseamento de dados, através da aplicação de políticas e procedimentos que reflitam a classificação dos dados.

Os dados confidenciais devem ser encriptados, seja quando em trânsito ou em repouso. A encriptação dos dados é aplicado em três áreas distintas ou estados (Davis, et al., 2011):

- Dados em trânsito através da rede, encriptados por protocolos seguros, por exemplo, *Secure Sockets Layer* (SSL);
- Dados em repouso, encriptados através de algoritmos, por exemplo, *Advanced Encription Standard* (AES);

- Dados em utilização, que descreve o processamento dos dados pelas aplicações. Em ambientes *cloud* devem ser utilizadas formas seguras de programação das aplicações. A *Open Security Architecture* [19](OSA), disponibiliza modelos de *frameworks* de programação segura.

A integridade dos dados deve ser validada através do uso de *digests* ou algoritmos de *secure hash*, aliados à duplicação de dados, técnicas de redundância e cópias de segurança (Mell, Peter; Grance, Timothy; NIST, 2011).

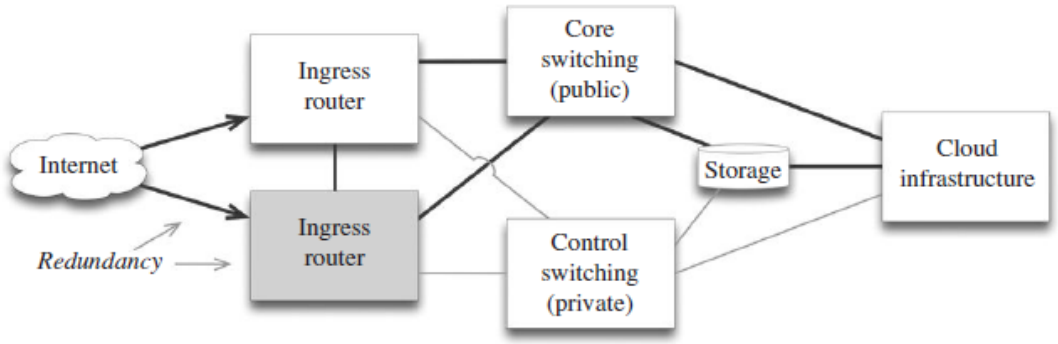

Figura 16: Redundância e disponibilidade (Winkler, 2011)

Para providenciar disponibilidade da informação e sistemas, devem ser utilizadas cópias de segurança e sistemas redundantes e resilientes, assim como técnicas para mitigar formas de ataques informáticos, como, por exemplo *Denial-Of-Service* (DoS).

3.5.5.2. Considerar Todas a Formas de Dados

As empresas estão a aumentar a quantidade de dados não estruturados, isto é, dados heterogénios e variáveis sob os mais variados formatos, incluindo texto, documentos, imagem, video, etc (Intel Corporation, 2012). Esta informação pode ter um teor confidencial necessitando de tratamento específico, como como por exemplo mascarar assinaturas e informação pessoal.

Para protecção da informação, os dados estruturados em ambientes *cloud* e que se encontrem armazenados em base de dados com informação classificada como confidencial, devem ser segmentados em tabelas separadas com os dados encriptados,

[19] http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloudcomputing

acesso controlado e restrito. As base de dados podem conter a informação mais sensível de uma empresa (Davis, et al., 2011).

3.5.5.3. Catálogo de Activos

Um aspecto chave na segurança da informação é a implementação de um catálogo de activos de dados que é utilizado para guardar informação acerca de todos os activos de dados e informação de uma empresa (DHS, 2010).

Todos os activos de uma empresa devem ser identificados e classicados em termos de sensibiliade para o negócio, especificando o *owner* (dono) e responsável desses activos, assim como a localização, a sua utilização e finalidade. As relações existentes entre estes activos devem também ser documentadas.

3.5.5.4. Requisitos de Privacidade

A privacidade está geralmente abrangida por leis e regulamentos relacionados com a recolha, guarda e utilização de informação pessoal, *Personal Identifiable Information* (PII), o que implica limitações de uso e acesso, com os requisitos associados de etiquetação, salvaguarda segura da informação e acesso apenas quando autorizado. Em ambientes *cloud*, devem ser estabelecidos controlos apropriados para protecção desta informação.

A norma ISO/IEC 27018 - *Information technology - Security techniques - Code of Practice for PII Protection in Public Clouds Acting as PII Processors*, providência aos fornecedores *cloud* orientação para os controlos de segurança necessários na protecção da privacidade da PII dos seus clientes.

3.5.5.5. Controlo de Identidades e Gestão de Acessos

Para além do sistema de gestão de identidades, deve ser estabelecido um controlo de identidades e gestão de acessos que deve ser acompanhada com autorização apropriada para todos os utilizadores no acesso a informação confidencial. Juntamente com esta necessidade, surge a gravação de eventos relacionados com segurança e acessos a informação confidencial, permitindo posteriormente a investigação, caso ocorram acessos não autorizados ou para recolha de informação para apresentar quando requisitada nas auditorias ao sistema informático .

3.5.6. Políticas de Privacidade

A privacidade tem vindo cada vez mais a ganhar relevância nos sistemas de TI. Como abordado anteriormente, a privacidade está abrangida por leis, regulamentos e normas, relacionados com a recolha, guarda e utilização de informação pessoal. A PII pode incluir dados como (McCallister, et al., 2010):

- Nome próprio, apelido e nome de familiares;
- Número do bilhete de identidade, da segurança social, do passaporte, de contribuinte, do cartão de crédito, etc;
- Características pessoais como a fotografia, impressões digitais, escrita ou outros dados biométricos;
- Informação de morada, *e-mail*, contactos telefónicos de emprego ou pessoais e quaisquer outros contactos;
- Informação sobre propriedade pessoal como terrenos, automóvel, habitação, etc;
- Informação sobre equipamentos como o *Internet Protocol* (IP), *Media Access Protocol* (MAC) ou outra informação específica sobre os equipamentos pessoais;
- Informação sobre uma pessoa que se encontre associada ou possa ser associada com qualquer uma das já referidas, data de nascimento, emprego, informação médica, dados financeiros, etc.

Em muitos países as leis e regulamentos e outras normas legais obrigam a que as organizações, públicas ou privadas, protejam a privacidade da informação pessoal e a segurança dos sistemas informáticos usados no seu tratamento e armazenamento. Portugal encontra-se abrangido por lei comunitárias, como a directiva 95 / 46 / EC[20] do Parlamento Europeu e do Conselho de Outubro de 1995, na protecção de pessoas, na recolha e tratamento de PII e movimentação dessa informação. Esta directiva estabelece que (Parlamento Europeu e do Conselho, 1995):

[20] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

- Os Estados membros, de uma forma geral, devem proteger os direitos e liberdades fundamentais dos seus cidadãos, em particular garantir o seu direito à privacidade no que respeita ao processamento de informação pessoal;

- Os Estados Membros não devem restringir ou proibir a livre circulação de informação pessoal entre Estados Membros, por motivos ligados à protecção nos termos do ponto anterior.

Esta directiva define a confidencialidade durante o processamento da informação por qualquer pessoa a actuar sob a autoridade do cliente[21] ou do fornecedor[22], incluíndo o próprio fornecedor, que tenha acesso a dados pessoais do cliente, não os devendo processar, exepto com instruções expressas do cliente ou quando requisitado por motivos legais.

É da máxima importância que os dados críticos e PII sejam tratados adequadamente nos contratos entre fornecedores e clientes, assim como nos SLA's acordados entre ambos. As empresas são responsáveis por definir as políticas de segurança, criar uma consciência sobre a necessidade da segurança no seio da empresa e certificar-se que os fornecedores também aderem a esta necessidade. É da responsabilidade dos clientes auditar os fornecedores para garantir que as políticas de segurança são observadas.

A privacidade é um aspecto importante de um negócio, focado em assegurar que os dados pessoais sejam protegidos, desde a recolha e utilização indevida até ao roubo e divulgação desta informação. De uma forma geral, a protecção de dados pessoais obedece aos seguintes pontos (Rittinghouse & Ransome, 2010):

- Recolha – Deve existir uma razão válida de negócio para o desenvolvimento de um programa e implementação de um sistema de informação que recolha, processe e divulgue dados pessoais;

- Notificação – O dono da informação deve ser notificado da intenção de recolha, qual a finalidade, tempo de retenção, divulgação e a protecção existente durante a retenção desses dados;

[21] Data Controller, na terminologia Europeia
[22] Processor usando a terminologia Europeia

- Opção e consentimento – O dono da informação deve expressamente e sem ambiguidade, consentir a recolha, definir a finalidade autorizada, tempo de retenção, sua divulgação e protecção;

- Utilização – Uma vez recolhida a informação, esta deve apenas servir o propósito que levou à sua obtenção, incluindo divulgação a terceiros, de acordo com o estabelecido na notificação;

- Segurança – Devem ser implementadas medidas de segurança apropriadas que assegurem a confidencialidade, a integridade e autenticidade dos dados durante a transferência, guarda e manuseamento;

- Acesso – Deve existir um processo à disponibilidade do dono para revisão e actualização da informação. Esse processo deve garantir que o acesso aos dados pessoais deve ser restrito e apenas quando autorizado;

- Retenção – Deve ser implementado um processo que assegure que a retenção da informação pessoal seja apenas pelo período de tempo necessário, para a finalidade que levou à sua recolha ou pelo tempo determinado pelos requisitos legais;

- Eliminação – A informação pessoal deve ser eliminada de forma definitiva e segura.

3.5.7. Segurança nas Aplicações Cloud

As organizações devem proteger as suas aplicações críticas para o negócio de ameaças externas e internas durante todo o ciclo, desde o desenho até à implementação em produção e garantir que estas cumpram as políticas de segurança em vigor na organização. Aplicações seguras, métodos de programação seguros, formação, ferramentas de programação e teste fazem parte de um processo de colaboração entre as equipas de segurança e de desenvolvimento (Rittinghouse & Ransome, 2010). As equipas de desenvolvimento têm o seu foco na camada aplicacional e na sua interacção com as camadas da infraestrutura.

Para uma melhor resposta às ameaças, internas e externas, o processo de desenvolvimento deve respeitar a metedologia de *Secure - Software Development Lifecycle* (S-SDLC) e a segurança deve integrar um lugar central em todo o processo. As organizações devem aplicar as mesmas políticas de segurança no desenvolvimento de *software* que aplicam na protecção da sua infraestrutura. Uma aplicação comprometida pode ser uma porta de entrada e comprometer os restantes sistemas.

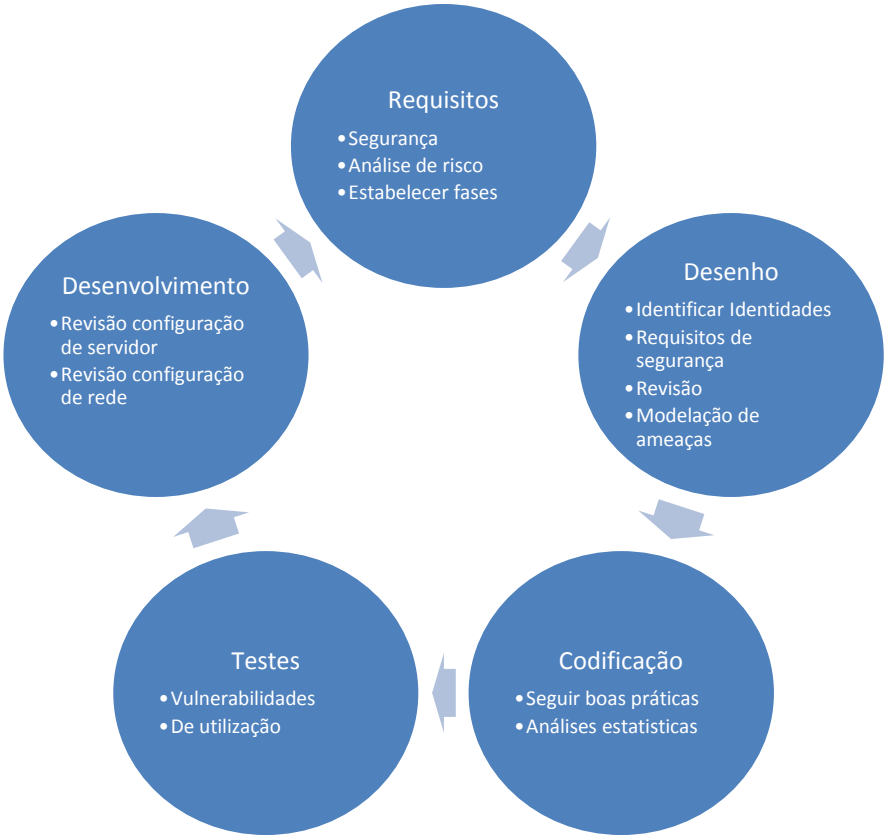

Figura 17: Secure Software Development Life Cycle. Adaptado (arD3n7, 2013)

Em ambientes *cloud*, o desenvolvimento de *software* deve considerar o modelo a que as aplicações se destinam. As considerações de segurança são diferenciadas para os três modelos, SaaS, PaaS e IasS, conforme resumido na Tabela 6.

Tabela 6: Responsabilidade sobre as aplicações nos modelos s *cloud*

Modelo	Descrição
Software-as-a-Service	• O consumidor apenas tem acesso a alterar alguns parâmetros da aplicação, pelo que as politícas de segurança encontram-se, sobretudo do lado do fornecedor e dependentes do acordado no contrato e respectivos SLA's. • O consumidor deve ter conhecimento dos procedimentos sobre o acesso administrativo à informação pelo fornecedor. A informação acerca da sua localização, habitualmente não é disponibilizada ao consumidor. • O consumidor deve conhecer as políticas de actualização de *software* e quando estas ocorrem, e os controlos existentes.

Modelo	Descrição
Platform-as-a-Service	• O consumidor é responsável pela camada aplicacional o seu desenvolvimento e instalação. É da sua responsabilidade as políticas de segurança, de controlo de acessos e gestão de identidades. • O consumidor é responsável pelas camadas da infraestrutura, sistema operativo e qualquer *software* intermediário.
Infrastructure-as-a-Service	• O consumidor é responsável por todo o software, desde o sistema operativo até à camada aplicacional, logo responsável por todas as políticas de segurança. • O consumidor deve aplicar as mesmas políticas de segurança que aplica na infraestrutura interna da sua organização.

3.5.8. Segurança da Infraestrutura e Ligações de Rede

Um fornecedor de serviços *cloud* deve garantir que a sua infraestrutura é segura, quer de ameaças externas, quer de ameaças internas. Relativamente às ameaças externas, a infraestrutura do fornecedor deve ter meios de protecção que permitam apenas as comunicações legitimas e impeçam todas as que sejam uma ameaça para os sistemas ou para a informação sob sua custódia. O mesmo se aplica às ameaças internas, sejam de colaboradores do fornecedor ou de ataques bem sucedidos em que o atacante se encontre já nos sistemas internos do cliente ou em sistemas de outros clientes. Outro factor da maior importância é a separação fisíca dos recursos da infraestrutura de gestão interna do fornecedor dos restantes recursos reservados aos clientes. Destes recursos fazem parte os *switches* e routers usados para ligar todos os restantes dispositivos, virtuais e físicos.

3.5.8.1. Controlos Externos

O cliente *cloud* devem avaliar os controlos externos de segurança do fornecedor nas seguintes àreas:

- Análise ao trafego de entrada - Um atacante procura, primeiramente, por dispositivos de rede mal configurados para explorar e tentar a entrada nos sistemas. As vulnerabilidades mais comuns incluem configurações fracas de instalação, controlos de acesso totalmente abertos e dispositivos sem

actualizações. Existe também tráfego de rede destinado a portas bem conhecidas que o fornecedor deve bloquear.

Tabela 7: Procedimentos de segurança em *routers* (Microsoft, 2003)

Router	Caracteristicas
- Pacotes correctivos e actualizações	• O *routers* devem ter a última versão de *software* e instalados os *patchs* de correcção a vulnerabilidades;
- Protocolos	• Bloquear protocolos não utilizados • Implementar Filtragem *Ingress and egress* • Tráfego ICMP é verificado (*screened*) da rede interna • *TTL expired messages with values 1 or 0* são bloqueadas • *Screened* pacotes de *Ping requests* com grande dimensão • Pacotes de *Routing Information Protocol* (RIP), se utilizado, deve ser bloqueado no router exterior
- Acesso Administrativo	• Desabilitar portas de gestão não utilizadas nos *routers* • Usar rotas estáticas • Desabilitar administração suportada por *web browser*
- Serviços	• Desabilitar serviços não utilizados
- Auditar e registar eventos (*logs*)	• Manter registo de todo o tráfego não autorizado • Os registos são revistos com frequência para permitir uma análise rápida • Todos os equipamentos de rede estão sincronizados com uma fonte horária comum

Os procedimentos de segurança dos *routers*, apresentados na Tabela 7, devem ser complementados com outros meios de análise tráfego de rede, sobre os quais o cliente deve obter informação sobre as suas funcionalidades:

- *traffic screening* – O cliente deve solicitar ao fornecedor uma lista de bloqueios (*block list*) das *firewals* e certificar-se que vão ao encontro das suas necessidades de segurança e ainda fornecer informação sobre o tráfego permitido. Deve

certificar-se de estas podem impedir um ataque de *Distributed Denial of Service* (DDOS), tornando inacessível toda a sua informação e sistemas na *cloud*;

- Intrusão, prevenção e detecção – Ainda que algum tráfego possa parecer legítimo, uma análise aprofundada descobre ataques conhecidos, virús ou *malware*. Para isso, o fornecedor deve ter instalado sistemas de *Intrusion Detection Systems* (IDS) e/ou *Intrusion Prevention Systems* (IPS). Enquanto os primeiros recolhem informação para posterior análise, os últimos tomam decisões com base em padrões, detectando actividade suspeita que possa denotar a existência de um ataque em progresso.

- Notificação - Ainda que o fornecedor não divulgue informação que possa comprometer a sua segurança, seja da infraestrutura de gestão ou de informação relativa a outros clientes, para que um cliente compreenda a efectividade da segurança, o fornecedor deve facultar informação sobre incidentes e ataques bloqueados, áreas atingidas na infraestrutura do cliente, assim como políticas de retenção de registos, estatisticas de ataques e polítcas de notificação.

3.5.8.1. Controlos Internos

Os controlos internos de segurança diferem dos controlos externos de segurança. Se uma quebra de segurança acontecer a partir do interior, significa que o atacante já passou pelos dispositivos de segurança de rede externos ou porque teve acesso físico à infraestrutura interna, com ou sem autorização válida.

Num ambiente com múltiplos utilizadores, como é uma infraestrutura *cloud* e mais vincadamente uma *cloud* pública, é da reponsabilidade do fornecedor a separação das infraestuturas de cada cliente, assim como a separação da sua infraestrutura de gestão dos demais. Os clientes devem solicitar os controlos de segurança da infraesturura interna ou certificação independente da sua conformidade com os regulamentos e normas e *compliance*.

Algumas das tecnologias que podem ser utilizadas são:

- *Local Area Network* (LAN) dedicadas e *Virtual LANs* (VLAN) – Em ambientes *cloud*, é frequente a utilização de *VLANs*, separação lógica de *LANs* no mesmo *switch*. As *VLANs* não foram inicialmente criadas com pensamento na segurança (McClure, et al., 2009), pelo que a sua utilização para fins de segurança na infraestrutura, coloca um risco acrescido para os clientes *cloud* . Um *switch* ou

VLAN não configurada correctamente representa um risco de segurança. Os clientes devem certificar-se que o fornecedor aplica os controlos adequados nos seus equipamentos de rede. Na Tabela 8 e Tabela 9 apresentamos algumas recomendações para os *switchs* e outros equipamentos de rede.

Tabela 8: Procedimentos de segurança em *switchs* (Microsoft, 2003)

Switch	Características
- Pacotes de correcções e actualizações	• Os *Switchs* devem ter a última versão de *software* e instalados os pacotes de correcção de vulnerabilidades;
- *VLANs*	• Assegurar que as *VLANs* não estão sobre utilizadas ou com excesso de permissões
- Configurações base	• Palavras passe de fábrica nos equipamentos alteradas • Activar apenas as portas de gestão necessárias
- Serviços	• Serviços não utilizados estão desactivados
- Encriptação	• Encriptar tráfego *switched*

Tabela 9: Procedimentos de segurança em outros equipamentos (Microsoft, 2003)

Outros equipamentos	Características
- Sincronização de *logs*	• Sincronizar todos os relógios em dispositivos com capacidades de manter logs
- Acesso Administrativo	• Usar autenticação segura em todos os acessos administrativos
- *Access control List* (ACL) de rede	• ACL's devem ser configurados nos equipamentos e redes

- Isolamento da infraestrutura do fornecedor – O tráfego das redes públicas deve ser segregado das redes de controlo e gestão internas da infraestrutura, para melhor isolamento (Winkler, 2011).

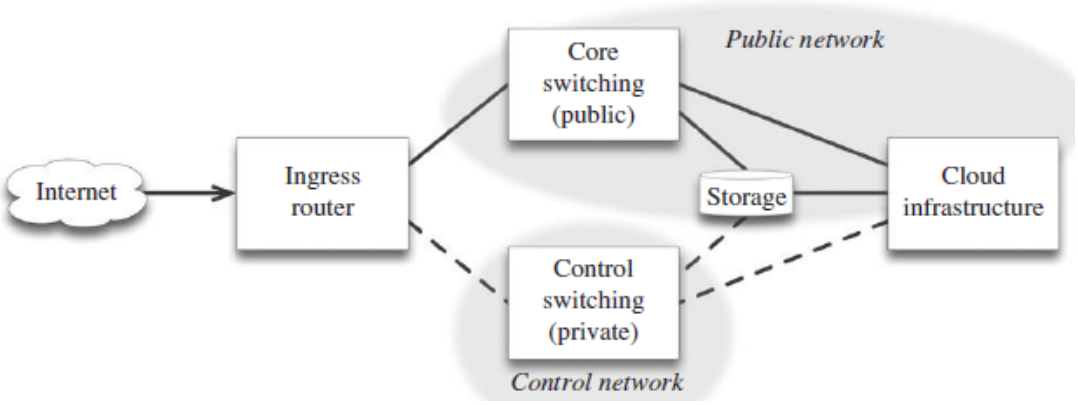

Figura 18: Isolamento de tráfego de controlo e público (Winkler, 2011)

3.5.9. Controlos de Segurança da Infraestrutura

Com a migração para um ambiente *cloud*, os consumidores perdem o controlo sobre a segurança física dos servidores e sistemas, dado que esses servidores se encontram em qualquer local onde o fornecedor tenha a suas operações (Rittinghouse & Ransome, 2010). Assim, a responsabilidade da segurança física sobre o centro de dados é então do fornecedor, cabendo ao cliente pedir comprovativos de que os processos e controlos de segurança existem, estão implementados e são cumpridos. Esses comprovativos podem ser obtidos através de uma certificação fornecida por uma entidade independente que demonstre que o fornecedor aplica os controlos de segurança que afirma ter.

A norma ISO/IEC 27002:2013 - *Information technology - Security techniques - Code of practice for information security controls*, da International Organization for Standardization (ISO), contêm recomendações sobre as melhores práticas e objectivos de controlo que garantam a confidencialidade, a intergridade e a disponibilidade da informação e sistemas. No que respeita à segurança de um centro de dados, esta norma aborda a segurança das áreas circundantes, segurança de equipamentos e sistemas, mitigação de riscos ambientais ou de outra ordem às infraestruturas, controlo de pessoas que operem equipamentos e sistemas e visitas ocasionais às instalações (ISO, 2013):

- Manter um perímetro físico de segurança nas áreas adjacentes para prevenir acessos não autorizados, com controlos físicos que assegurem que apenas pessoas autorizadas acedem às áreas sensíveis da infraestrutura. A segurança física deve extender-se aos locais que suportem os serviços do centro de dados;

- Controlos de segurança sobre os equipamentos para prevenir a perda, furto ou dano, acidental ou propositado;

- Controlo das pessoas que operem nas àreas de segurança para prevenir intensões maliciosas sobre a infraestrutura;

- Proteções que mitiguem ameaças ambientais, externas ou internas, como cheias, incêndios, terramotos ou acidentes que comprometam a segurança dos dados ou informação guardada nos sistemas;

- Sistemas redundantes de abastecimento de gás, água, sistemas de comunicações e electricidade. Particularmente para abastecimento eléctrico e de comunicações, devem existir planos de segurança, continuidade de serviço e de actuação para uma eventual ocorrência de uma interrupção ou anomalia grave;

- Devem existir planos detalhados de manutenção dos equipamentos de suporte ao centro de dados;

- Devem ser planeados processos de *disaster recover* (DR), *backup* da informação e continuidade de serviços, para falhas graves dos sistemas;

- Manter controlos de segurança apertados para todos os acessos ao edifício, incluindo visitas ocasionais;

- Deve existir controlo para abate de equipamentos, com destruição de qualquer informação que estes ainda possam ter.

3.5.10. Gestão de Controlos de Segurança nos Contratos

Uma das formas que um cliente tem disponível para assegurar que as suas aplicações e informação migradas para a *cloud*, se encontram seguras e de acordo com as suas políticas de segurança e normas de *compliance* é o contrato entre ambos, cliente e fornecedor, e os respectivos *service levels agreements* (SLA) nele acordados. Este acordo pode tomar duas formas, uma forma padrão, geralmente quando a capacidade negocial do cliente *cloud* é menor, ou uma forma negociada, apenas ao alcançe de organizações de maior dimensão e com maior capacidade negocial. Uma vez que o fornecedor apenas está obrigado a entregar as funcionalidades acordadas nos SLA's (Anon., 2012), o cliente deve certificar-se que estes têm todos os requisitos em termos de segurança, confidencialidade, integridade e disponibilidade da sua informação e recursos e que estes vão de encontro às suas necessidades e expectativas.

Quando se negoceia um SLA para ambientes *cloud*, certos tópicos, do ponto de vista da governança, devem ser claramente identificados, discutidos e negociados, de forma a garantir a protecção da informação e das funções de negócio. Os pontos mais importantes num acordo SLA são (Halpert, 2011):

- Suporte para interrupções de serviço;
- Garantias de segurança da informação, serviços e sistemas;
- Procedimentos para resposta a incidentes;
- Auditabilidade à segurança implementada;
- Pagamento de compensações por perdas;
- Certificação de confiança.

Os elementos chave que devem constar num acordo SLA, são (Buyya, et al., 2011):

- Parâmetros dos serviços - Descreve uma propriedade observável e mensurável de um determinado serviço;
- Métricas – Define os valores das propriedades dos serviços, medidos através de um sistema ou tratados informaticamente a partir de outras métricas ou constantes. As métricas são um instrumento fundamental para descrever o que significam os parâmetros do SLA, especificando como devem ser tratados e quantificados;
- Função – Especifica como calcular o valor de uma métrica a partir dos valores de outras métricas e constantes. As funções são fundamentais na descrição exacta de como os parâmetros SLA são calculados a partir de métricas de recursos;
- Directivas métricas - Especificam como quantificar e avaliar uma métrica.

3.5.11. Revogar os Serviços com um Fornecedor.

Um dos cenários que uma organização deve planear à partida e antes de tomar a decisão de migrar serviços ou sistemas para ambientes *cloud* é a revogação do contrato com o fornecedor. Para além de poder ser difícil, demorado e dispendioso para a organização, por vezes a ligação e dependência do fornecedor é tão forte que se pode tornar mesmo impossível (Petri, 2014). Uma das razões para a ocorrência deste problema são as plataformas proprietárias de muitos fornecedores. Mudar de uma plataforma para outra completamente diferente, é demorado,

oneroso e requer muito tempo. Duas das razões que podem despoletar a revogação do contrato entre fornecedor e cliente são:

- *Lock-in* – Como já referido, pode ocorrer porque o contrato entre fornecedor e cliente terminou, mas também porque o cliente deseja migrar para outro fornecedor, com melhor oferta de serviços ou de preço;

- *Lock-out* – Quando o fornecedor entra em falência e encerra as suas operações. Nesta situação o cliente pode perder o acesso aos seus sistemas e informação.

Toda a informação do cliente migrada, criada ou processada pelos sistemas *cloud*, é propriedade deste, não tendo o fornecedor qualquer direito sobre a mesma. O cliente, ao estabelecer o acordo com o fornecedor, deve especificar as formas de recuperação da informação migrada para os sistemas do forneceder (Scruggs, et al., 2011):

- Processo – Detalhar, passo a passo, o processo de retirada da informação;

- Janela temporal – Determinar o tempo necessário para a remoção da informação;

- Formato – Especificar claramente o formato no qual a informação será devolvida;

- Destruição – Caso faça parte do acordo, o fornecedor destruir a informação, estabelecer os termos em que essa operação será realizada e se o cliente é autorizado a auditar o processo.

Para reduzir esta ameaça dos ambientes *cloud*, muitos fornecedores disponibilizam ferramentas que permitem a exportação, não apenas dos dados mas também da metadata gerada pelos seus clientes (Winkler, 2011). Também existem, actualmente, empresas dedicadas a este problema e que disponibilizam ferramentas e processos para migrar a informação de um fornecedor para outro. A Advancing Storage and Information Technology - SNIA[23] e a Backupify[24] são apenas dois exemplos.

[23] http://www.snia.org/

[24] https://www.backupify.com/

4. Migração para Cloud Computing

A crescente oferta de serviços de *cloud computing* está a mudar a forma como as empresas olham para a implementação dos seus sistemas TI. De facto, as vantagens apontadas ao modelo, como a maior flexibilidade e o menor tempo de implementação enquanto reduz custos e complexidade, torna sedutivo para as empresas a migração das suas infraestuturas, sistemas e informação para ambientes *cloud computing*. No entanto, é de salientar que nem todas as infraestuturas, sistemas e informação se adaptam bem a ambientes *cloud* ou são isentas à exposição a riscos acrescidos e a novas ameaças, caso sejam deslocados para uma infraestrutura *cloud*. Assim, antes de uma empresa abraçar um projecto de migração, de parte ou da totalidade dos seus sistemas, este deve ser bem ponderado, analisado e planeado de forma a garantir o seu sucesso.

A adopção de *cloud computing* deve ter uma abordagem de ciclo, proporcionado uma melhoria contínua. Walter Andrew Shewhart (1891 - 1967) propôs nos anos 30 uma metodologia de melhoria contínua em quatro fases, planeamento (*Plan*), executar (*Do*), verificar (*Check*), actuar (*Act*). Nos anos 50, Edward Deming recuperou esta metodologia quando propôs que os processos de negócio e sistemas deviam ser monitorizados, medidos e analisados de forma contínua, identificando falhas e aplicando medidas correctivas de melhoria. Esta metodologia ficou assim conhecida por ciclo Demings *Plan–Do–Check–Act* (PDCA) (Best & Neuhauser, 2006):

- *Plan* – Identificar o que pode ser melhorado e que alterações são necessárias;
- *Do* – Implementar as alterações;
- *Check* – Medir e analisar o processo ou os seus resultados;
- *Act* – Se os resultados não foram os esperados.

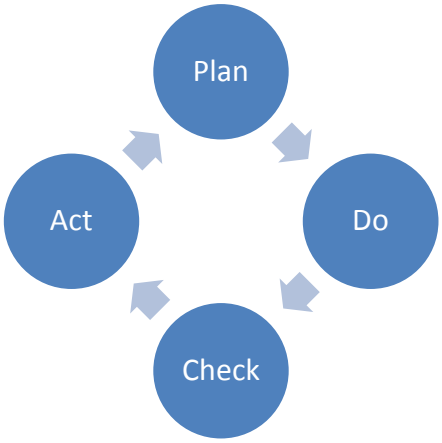

Figura 19: Ciclo PDCA de Deming

Para além da metodologia de Deming, existem muitos factores a ponderar num projecto de migração para *cloud computing*. Entre eles podemos salientar, factores económicos, de negócio e de segurança. Não obstante a importância de qualquer um dos factores, pretende-se aqui explorar mais exaustivamente a questão da segurança, apresentando uma metodologia de migração para a *cloud*, com análise de riscos e ameaças e como reduzir esses riscos e mitigar as ameaças para níveis aceitáveis. Durante esse processo, uma organização deve recolher infomação suficiente para o preenchimento do documento proposto no anexo B. Os passos que propomos para a migração de sistemas e informação para a *cloud computing* devem ser definidos como um processo de governança que seja abrangente e é compreendido por quatro fases distintas:

- Definir – Identificar e estabelecer as pessoas, entidades ou equipas responsáveis para cada fase, a estratégia, os objectivos da organização e identificar as necessidades internas para o projecto de migração;

- Analisar – Analisar os modelos de desenvolvimento e os modelos de serviço *cloud*, comparar fornecedores *cloud* e desenvolver e planear um projecto piloto e respectivos testes;

- Segurar – Integrar serviços, informação e sistemas com os existentes na organização, gerir e desenvolver os contratos, SLA's, políticas e controlos de segurança, executar testes de performance, operação e migração antes de prosseguir com a migração de informação e de sistemas para a *cloud*;

- Gerir – Processos de monitorização e melhoria. Devem ser estabelecidos meios claros de facturação de serviços criando processos de acompanhamento.

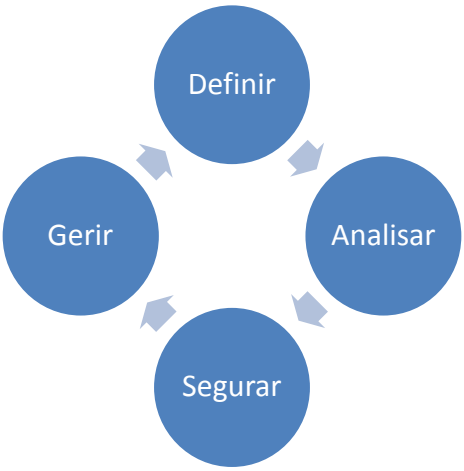

Figura 20: Ciclo de Migração para *Cloud Computing*

4.1.Fase de Definição

Esta fase é uma das mais importantes de todo o projecto. Deve promover o envolvimento de todas pessoas em cada fase de implementação, traçar os objectivos e métodos de intervenção e desenvolver e aprovar um plano estratégico e de implementação. Os objectivos devem ficar absolutamente claros para todos desde o início do projecto. A organização deve também, nesta fase, identificar conhecimentos técnicos existentes na organização e fazer um levantamento das eventuais necessidades de formação, ou decidir por recorrer a serviços externos para suprir as necessidades identificadas.

4.1.1. Identificação de Pessoas e Equipas

Os recursos humanos necessários para o projecto de migração para uma infraestrutura *cloud computing* divide-se por três áreas de intervenção:

- A estratégica – Envolvendo a direcção e órgãos de gestão de topo da organização que definem a visão, as directrizes e os objectivos que levaram à opção de migração;
- A táctica – Deve incluir órgãos de gestão das áreas abrangidas. Compreende a análise técnica e a análise de negócio necessárias ao projecto;
- A operacional – Transversal à organização, envolvendo todas as áreas da organização, na aquisição de equipamentos, implementação de serviços e operação.

A tabela seguinte sumariza as necessidades em cada uma dessas áreas de intervenção.

Tabela 10: Identificação de Pessoas e Equipas por Área de actuação

Área	Características	Descrição
Estratégica	- Direcção - Administração - Gestores - Directores	Definir uma visão global para a adopção *cloud* e passar essa visão para os níveis abaixo, particularmente para os níveis executivos, que devem adoptar o conceito e a visão, alinhado com os objectivos da organização, postura de segurança a adoptar e procupações de segurança, privacidade e disponibilidade.
Táctica	- Sistemas TI - Área Legal - Gestores	Análise técnica e de négocio, para verificação dos requisitos legais e estabelecer objectivos de curto e longo prazo, técnicos e de negócio, definindo modelo e serviço a adoptar.
Operacional	- Sitemas TI - Gestores - Área Legal - Funcionários	Fase mais abrangente com três vectores: Negociação – Acordo com o fornecedor seleccionado, deve incluir todos os intervenientes anteriormente referenciados. Implementação – Desenvolvimento, costumização e configuração dos serviços. Técnicos especializados, desde programadores equipas de teste aos sistemas implementados. Operação – Abrange todos os que irão interagir com os novos serviços, seja na capacidade de operação ou administração dos sistemas *cloud*.

4.1.2. Plano Estratégico de Migração

Para assegurar uma migração segura e que contribua de forma significativa para os objectivos de uma organização, deve ser delineado um plano estratégico abrangente a todas as áreas de intervenção. Quando terminado, deve proporcionar um conhecimento mais abrangente das infraestruturas *cloud* e determinar o grau de preparação face ao paradigma *cloud computing*. O plano estratégico deve:

- Incluir um levantamento e identificação dos riscos e ameaças à implementação de uma infraestrutura *cloud*;
- Incluir um primeiro levantamento e identificação das aplicações e sistemas que beneficiem com a migração para *cloud*;

- Ter objectivos bem definidos com métricas que permitam avaliar o sucesso ou insucesso do plano. Estas métricas devem ser acordadas com quem tiver que tomar a decisão final. Devem ser definidas marcas de referência (*Benchmarks*) para os serviços a migrar, que permitam medir o impacto após a migração;

- Ter em linha de conta a infraestrutura e tecnologias existentes em que os novos serviços se vão integrar e interagir, assim como, garantir que a estratégia de migração continue a observar os padrões existentes;

- Abranger o curto prazo, identificando processos de migração de informação e serviços para a *cloud* e o longo prazo, com o planeamento para migração para outros fornecedores, caso se mostre necessário, minimizando os riscos de fornecedor *lock-in* ou *lock-out*. Implementação de normas, interoperabilidade e portabilidade devem ser cuidadosamente analisados;

- Incluir análise de *compliance* com as normas e leis, nacionais e internacionais, por exemplo, PII, localização física dos dados e informação, destruição de dados, disponibilidade de serviços, propriedade intelectual, etc;

- Incluir mapeamento dos benefícios de *cloud computing* em oposição com os problemas de negócio que pretende resolver;

- Fornecer informação suficiente para ajudar à tomada de decisão final, migrar ou não migrar (*Go/No Go*). Com base neste plano estratégico, todas as métricas definidas, informação recolhida, levantamento de necessidades, deve proporcionar a uma organização ter informação que permita responder a questões como:

    - Deve o projecto de migração ser abandonado, reduzido ou adiado?

    - É o modelo *cloud computing* apropriado para o negócio?

    - Deve a análise ser retomada e ser mais aprofundada?

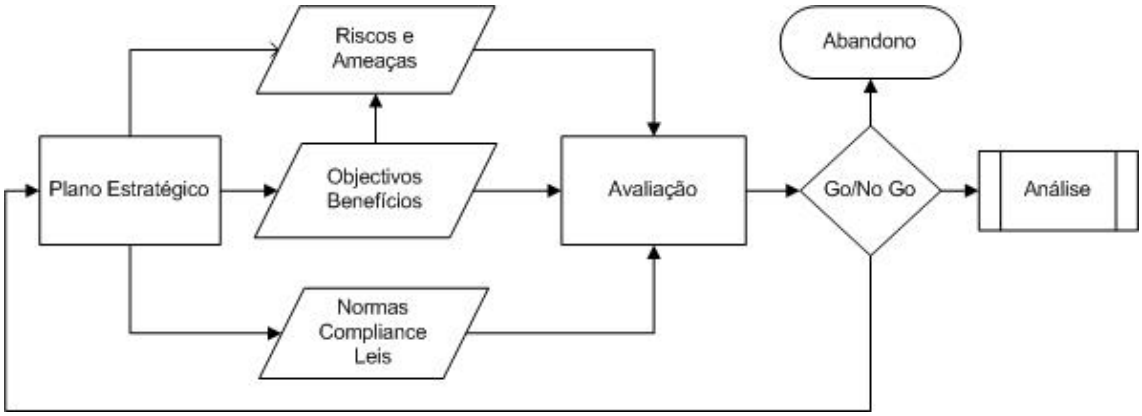

Figura 21: Plano Estratégico

4.1.1. Conhecimento e Formação Necessários

O plano estratégico de migração deve permitir um levantamento completo sobre as necessidades de conhecimentos técnicos, que permita a elaboração de planos de formação ou tomar a decisão de recorrer a serviços externos, para complementar a lacunas identificadas na organização. O levantamento de conhecimentos deve ser extensivo a todas a áreas, garantindo que o projecto pode ser realizado e que promova que todos partilhem uma definição comum de *cloud computing*.

4.2.Fase de Análise

Nesta fase é definido quais as aplicações e sistemas que reúnem as condições para migrar para a *cloud* e que controlos aplicar para manter ou melhorar a segurança, a confidencialidade, a disponibilidade e a integridade. Após esta análise, uma organização deve efectuar uma análise aos modelos de desenvolvimento e decidir quais adoptar, numa perspectiva de benefícios económicos, eficiência, agilidade e inovação que possam trazer para a organização, mantendo a necessária segurança. Finalmente, decidir que modelos de serviço *cloud* adoptar, após o levantamento das aplicações e sistemas analisados, e confirmação de qual é a mais-valia para organização a sua migração para a *cloud*.

4.2.1. Aplicações e Sistemas

Para uma selecção informada de aplicações, sistemas ou informação a migrar para a *cloud*, deve ser efectuada uma análise cuidada e definir claramente quais os critérios de avaliação para cada. Estes podem mudar de organização para organização consoante as suas necessidades, a informação a migrar, as leis e regulamentos que devem observar, a segurança, etc. Esta avaliação é da maior importância, quer para decidir pelo modelo *cloud* a implementar, quer para avaliar os possíveis fornecedores *cloud*. Os critérios de

avaliação devem ser analisados segundo as necessidades de segurança e as características das aplicações dos sistemas e da informação.

Características das aplicações e sistemas a avaliar e classificar:

- Disponibilidade – Identificar os quais os requisitos de disponibilidade para sistemas e informação. Devem ainda ser identificados quais os dispositivos, *software* ou *hardware* utilizados para sistemas de elevada disponibilidade;

- Latência – Identificar os requisitos mínimos de latência permitidos por determinada aplicação ou acesso a informação. Uma latência muito elevada pode tornar uma aplicação difícil ou mesmo impossível de utilizar;

- Integração – Avaliar a integração com outros sistemas de rede ou aplicações. Uma aplicação *stand-Alone* facilita uma possível migração para a *cloud*, enquanto uma aplicação ou informação integrada, torna a migração tecnicamente mais complicada de executar;

- Portabilidade – Avaliar as capacidades de exportação dos dados, quer para a infraestrutura do fornecedor, quer da infraestrutura de um fornecedor para outro fornecedor. As aplicações ou dados que mostrem ser de elevada dificuldade de migração podem não ser bons candidatos para a *cloud*;

- Estabelecimentos de estado – Identificar as necessidade de manter os estados das aplicações. As aplicações que obriguem a manter o estado (*stateful*), as comunicações devem ser garantidas, ao passo que as aplicações sem estado (*stateless*) facilitam a migração.

Critérios de segurança a avaliar:

- Segurança – Quais os requisitos de segurança dos dados, consoante a classificação da informação e quais as opções de sistemas de encriptação disponíveis, para dados em trânsito ou em repouso. Deve também ser avaliado se são utilizados sistemas de encriptação próprios ou de terceiros;

- Privacidade e confidencialidade – Os requisitos de segurança que permitam aplicar controlos que garantam a privacidade, confidencialidade e disponibilidade da informação;

- Integridade – Os requisitos necessários para garantir a integridade da informação, por meio de redundância da informação, cópias de segurança ou permissões que permitam alteração dos dados;

- *Compliance* – Aplicações com informação sensível e sujeita a leis e regulamentos, nacionais ou internacionais, que devem ser observados quando são consideradas para migração.

4.2.2. Modelo de Desenvolvimento

Na escolha do modelo de desenvolvimento existem muitos factores que devem ser ponderados cuidadosamente pelas organizações. Entre esses factores, os económicos e de segurança surgem de imediato no topo das considerações. Grandes empresas, com um nível elevado de maturidade de serviços TI podem ter mais inclinação por um modelo de *cloud* privada, com os benefícios de segurança inerentes, deixando para mais tarde a consideração sobre a migração para *cloud* pública dos serviços ou aplicações de baixa criticidade. Já numa empresa de pequena ou média dimensão a sua escolha pode tender para um modelo de *cloud* pública, beneficiando dos factores financeiros que esta proporciona e de tecnologias mais recentes, que de outra forma seriam de mais difícil acesso. Para análise, vamos comparar estes dois modelos na Tabela 11 abaixo.

Tabela 11: Analise aos modelos *cloud* pública e *cloud* privada

Factor	*Cloud* Pública	*Cloud* Privada
Custos	Custos baixos, pagando apenas pelos serviços utilizados. A infraestrutura está a cargo do fornecedor *cloud*.	Custos elevados, com a instalação, configuração e manutenção dos serviços internamente. Uma empresa pode recorrer ao *hardware* já existe.
Segurança	Indicada para informação ou serviços que não sejam critícos para a organização ou tenham informação classificada de sensível. Implementar controlos de segurança apertados para a migração desses serviços e informação.	Indicada para Informação ou serviços classificados de críticos para uma organização. Uma empresa pode considerar implementar uma *cloud* privada, implementar controlos e procedimentos de segurança, para mais tarde considerar a migração para uma *cloud* pública.

Factor	*Cloud* Pública	*Cloud* Privada
Ameaças	Visibilidade e controlo limitados uma vez que a infraestrutura está a cargo do fornecedor. Requer boas políticas de segurança, asseguradas por SLA's entre cliente e fornecedor. Riscos acrescidos pela partilha da infraestrutura com outros clientes.	Podem ser implentados controlos internos de segurança para protecção sobre as ameaças à informação e sistemas. Maior facilidade de protecção, uma vez que a infraestrutura não é partilhada com terceiros.
Elasticidade	Elevada, virtualmente infinita, apenas limitada pelos contratos entre fornecedor e cliente.	Baixa, limitada à infraestrutura existente num centro de dados. Aumentar a elasticidade acarreta um aumento de custos.

No entanto, outras opções podem ser consideradas. A Gartner, no seu relatório de 2013 - *Top 10 Strategic Technology Trends for* 2014 em que identifica as dez tendências nas técnologias de informação para o ano seguinte (Gartner, 2013), aponta para um crescimento na utilização da *cloud* híbrida. Uma organização pode optar por este modelo, dispersando os serviços e informação pelos dois modelos, como por exemplo, uma *cloud* pública e outra privada, deixando a *cloud* pública reservada para informação ou serviços que não sejam critícos para a organização ou tenham informação classificada de sensível, migrando os restantes para a *cloud* privada, tirando daí os benefícios de segurança inerentes.

4.2.3. Modelos de Serviço

Na escolha do modelo de serviço, Iaas, PaaS ou SaaS, há que ter em consideração os requisitos de negócio da organização e a que suporte de sistemas ou informação se destina. Como referido anteriormente, quando for adoptada a *cloud* pública para sistemas ou informação de carácter sensível, há que considerar a implementação de políticas e controlos segurança apertados e sistemas de encriptação de dados com gestão própria.

4.2.3.1. Considerações de Migração para SaaS

Com este modelo de serviço, as opções de segurança que um cliente *cloud* pode controlar estão restritas ao nível aplicacional, ficando o controlo dos níveis inferiores a cargo do

fornecedor *cloud*. Numa *cloud* pública, este facto leva a que a escolha do fornecedor seja da maior importância, daí a necessidade do cliente aceder aos controlos e normas de segurança aplicados pelo fornecedor nessa área. Abordaremos este tema mais adiante na selecção do fornecedor *cloud* e nas tabelas do Anexo A.

O modelo SaaS é indicado de uma forma abrangente, para aplicações de colaboração, *E-Mail*, produtividade, *Customer Relationship Management* (CRM), *Human Capital Management* (HCM), ou para sectores específicos, como logística ou *Supply Chain Management* (SCM).

Os controlos de segurança incidem sobre os acessos à informação e na sua forma de implementação. Como o acesso é efectuado por *browser* ou uma API específica, os controlos de segurança também se tornam necessários no *software* instalado nos dispositivos do cliente. Deve existir um processo de teste, avaliação e instalação de pacotes correctivos e actualizações críticas aos *browsers* e API's. Como as comunicações com as aplicações passam pela *internet*, uma rede pública e insegura, deve ser considerada a utilização de sistemas de encriptação, próprios ou de outras entidades. Para informação classificada como crítica, deve ser não apenas considerado a utilização de sistemas de encriptação próprios, como também a encriptação dos dados armazenados na infraestrutura do fornecedor. Outros controlos a considerar podem passar por autorizar ou não a cópia e envio da informação e se esta pode ficar residente nos dispositivos de acesso do cliente, principalmente se o acesso à infraestrutura é autorizado a partir de dispositivos públicos.

4.2.3.2. Considerações de Migração para PaaS

A oferta de PaaS reside sobretudo num ambiente completo de desenvolvimento, onde os programadores podem desenvolver, testar e gerir as suas aplicações. Com base em normas e automatização de topologias, este modelo proporciona elasticidade e eficiência.

O modelo PaaS é indicado para aplicações próprias ou costumizadas, serviços de base dados, *Identity Mangement Services* (IMS), serviços de segurança, etc.

As considerações de segurança abrangem o controlo de acessos e autorizações, operação em ambientes partilhados, informação e dados, tanto dados em circulação como dados em repouso. Este modelo opera sobre um ambiente partilhado, logo é essencial uma *framework* de autenticação forte e efectiva que assegure que o acesso à informação e dados é apenas autorizada a quem tem as devidas permissões. Um cliente *cloud* deve optar por formas de autenticação fortes, como *two-factor authentication* e considerar quais as

normas que o fornecedor *cloud* implementa, como a complexidade das palavras-chave, qual o tempo decorrente para forçar a mudança da palavra-chave, quais os procedimentos de protecção às palavras-chave, etc.

4.2.3.3. Considerações de Migração para IaaS

Com o modelo IaaS, um fornecedor disponibiliza uma infraestrutura completa aos seus clientes, onde estes podem instalar e disponibilizar serviços e recursos aos seus utilizadores, internos e externos. Esta infraestrutura é implementada de forma a dar aos clientes uma sensação de recursos infinitos, com transparência e agilidade no aprovisionamento de novos recursos, acompanhado o crescimento do negócio.

Quando considerando IaaS em *cloud* privada, podem-se apontar os seguintes benefícios:

- Consolidar e virtualizar uma infraestrutura existente, traduzindo-se numa mais-valia financeira pela melhor utilização dos recursos existentes;
- Incentivar a utilização de imagens virtuais na organização;
- Melhor gestão das imagens virtuais.

O modelo IaaS aplica-se primordialmente a espaço em disco (*storage*), computação, armazenamento, publicação de páginas *web* e sistemas de *backup* e *disaster recovery*.

A segurança necessária neste modelo é transversal a toda a infraestrutura porque, como é partilhada com outros clientes, os problemas de segurança são mais vincados. O cliente deve solicitar ao fornecedor evidências dos controlos de segurança que tem implementados e observados, que garantam a efectiva separação e segurança dos equipamentos virtuais, da utilização de memória, dos recursos de rede e de armazenamento. À semelhança dos modelos anteriores, devem ser considerados métodos de encriptação, quer para dados em trânsito quer para dados em repouso.

4.2.4. Avaliação e Selecção do Fornecedor

A avaliação e selecção do fornecedor de serviços é um processo complexo, que deve observar normas comparativas, de tal forma que permita uma real comparação entre os vários potenciais fornecedores de serviços. No anexo A, apresentamos uma abordagem comparativa mais exaustiva, mas numa primeira abordagem, esta deve avaliar os seguintes tópicos:

- Integração de serviços, dados e aplicações – Analisar as características de integração da infraestrutura existente na organização com os serviços disponibilizados pelo fornecedor *cloud*;

- Protecção de dados e informação – Análise à *framework* para segregação de dados e informação entre clientes que utilizem a mesma infraestrutura. Que sistemas de encriptação são utilizados pelo fornecedor, seja para dados em trânsito ou dados em repouso;

- *Performance* – Na escolha de um fornecedor, é da maior importância efectuar testes de acesso e este providenciar tanta informação quanto a necessária para uma avaliação correcta;

- Negociações contratuais – A negociação contratual com um fornecedor deve ser bem analisada, confirmando cenários importantes como por exemplo, a portabilidade da informação e sistemas, a facilidade na mudança de fornecedor, as negociações de SLA's e as condições contratuais para alteração de serviços;

- *Compliance* – Quais as *frameworks* e as normas a que o fornecedor adere e que certificações ou auditorias este pode demonstrar ter efectuado;

- Segurança física – Verificação das normas de segurança física para instalações que o fornecedor tenha implementas e que evidências pode fornecer;

- Suporte técnico – Confirmar o que está incluído no suporte técnico e quais os custos adicionais para fornecimento de serviços de suporte. Verificar qual o horário em que este se encontra disponível e qual a formação e certificações da equipa de suporte técnico;

- Referências – Solicitar ao fornecedor uma lista de clientes actualizada e procurar informações sobre a sua organização, quer na sua página da *internet* quer em análises efectuadas por revistas da especialidade. Grupos ou fóruns de discussão podem também providenciar informação complementar.

4.3.Fase de Segurança

Nesta fase, a segurança deve ter um papel central, onde são definidos controlos que atestem que a segurança é efectiva e observada. Devem também ser planeados, testados e executados

testes de migração e operação que permitam decidir como e quando a migração das aplicações, dados e informação deve ser efectuada. Estes testes devem permitir determinar se a aproximação à migração será efectuada de forma faseada ou na totalidade, aferindo as necessidades de manter serviços ou aplicações em paralelo e durante quanto tempo. Devem ainda ser definidas as políticas de governanca, de segurança e quais os SLA's e controlos necessários para garantir, controlar e melhorar a entrega dos serviços contratados ao fornecedor *cloud*. Esta fase termina com a migração para a *cloud* dos sistemas, aplicações e informação analisados.

4.3.1. Testes de Migração e Operação

Um dos passos finais antes da decisão de migração é o planeamento e execução de testes e operação. Dependendo do tipo de aplicação e dos requisitos de disponibilidade necessários para o seu normal funcionamento, o planeamento e execução da migração pode variar. Se a aplicação for classificada como imprescindível ou a sua paragem implicar perdas significativas para o negócio, a migração para a *cloud* deve ser planeada por fases, podendo mesmo coexistir ambas as infraestruturas, interna e *cloud*, até à migração total. A informação recolhida nos passos anteriores deve ser utilizada para a criação de testes, simulando todos os tipos de dados, de informação e de carga. Um plano de testes bem desenvolvido e aplicado é garante do sucesso dum projecto de migração para a *cloud*. Nestes testes devem ser analisadas as seguintes funcionalidades e actividades:

- Garantir a correcta execução e performance das aplicações em ambientes virtuais;
- Verificar que em ambientes *cloud* as aplicações a migrar mantêm todas as funcionalidades anteriores à migração;
- Utilizadores seleccionados devem executar transacções com a aplicação, confirmando a integridade dos dados;
- Definir e confirmar planos de recuperação e resposta a desastres;
- Definir métricas de qualidade de serviço (QoS) e controlos de segurança necessários;
- Verificar necessidades acrescidas ao plano de formação necessário, para utilizadores regulares da aplicação ou com responsabilidades de gestão da aplicação. Deve também ser planeada formação a quem tenha que responder às questões ou problemas dos utilizadores (*helpdesk*);

- Definir um plano de retorno, caso se verifiquem problemas não previstos anteriormente, quando a aplicação já se encontre em ambiente produtivo.

4.3.2. Implementar e Gerir SLA's

Os SLA´s são da maior importância num ambiente *cloud computing*, uma vez que são estes que definem claramente quais as expectativas de serviço que um fornecedor *cloud* deve disponibilizar aos seus clientes. Um acordo SLA deve estabelecer quais os níveis de serviço a ser fornecidos e definir claramente quando não é da responsabilidade do fornecedor o não cumprimento do estabelecido nos contratos entre ambos, seja por degradação ou interrupção dos serviços. Estes acordos devem ter em linha de conta a criticidade de cada serviço fornecido. Um plano bem implementado e de gestão de SLA's deve:

- Designar uma equipa responsável, que deve integrar membros de todos os sectores da empresa e com intervenção no projecto e ainda incluir utilizadores chave, designados consonte a área de responsabilidade. O departamento legal deve também ter representatividade, para definir e analisar a legalidade do estabelecido nos contratos;

- Compreender na íntegra as expectativas da organização com a migração para a *cloud*, das aplicações, da informação e dos dados, conforme definido anteriormente;

- Identificar e definir os elementos críticos para a protecção das aplicações, da informação e dos dados a migrar, que devem contemplar:

    - Planos de migração para outro fornecedor ou retorno da informação para a infraestrutura interna da organização;

    - A observância das leis, normas e regulamentos, nacionais e internacionais aplicáveis ao contexto onde a empresa se insere;

    - Ferramentas que garantam a segurança, a privacidade e a disponibilidade da informação mais sensível;

    - Definir claramente as métricas mínimas que atestem a disponibilidade e performance dos sistemas;

    - Processos de recuperação da informação em casos de incidentes graves e que levem à paragem dos serviços por períodos superiores ao acordado;

- Prever indemnizações devidas em casos de incumprimento pelo fornecedor dos serviços acordados;

- Estabelecer com o fornecedor um ponto único de contacto para questões e preocupações com o serviço fornecido;

- Estabelecer a periocidade de relatórios de serviço que inclua indicadores que atestem a qualidade de serviço e incidentes verificados;

- Definir níveis de escalamento para incidentes graves, seja no lado do fornecedor, seja no lado do cliente, que facilitem a rápida tomada de decisões e que promovam a necessária agilidade na sua resolução;

- Definir processos internos que assegurem a resolução da entrega de serviço fora do estabelecido nos SLA's. Caso sejam atingidos níveis serviço inaceitáveis, devem existir formas que permitam a revogação do contrato com o fornecedor e as respectivas indemnizações, se aplicável;

- Agendar com o fornecedor revisões periódicas dos SLA's estabelecidos;

- Estabelecer canais internos de comunicação atempada de problemas verificados com o serviço em ambiente *cloud*;

Os SLA's devem ser um processo contínuo de monitorização, de avaliação e de modificação, certificando que continuam a responder aos objectivos iniciais.

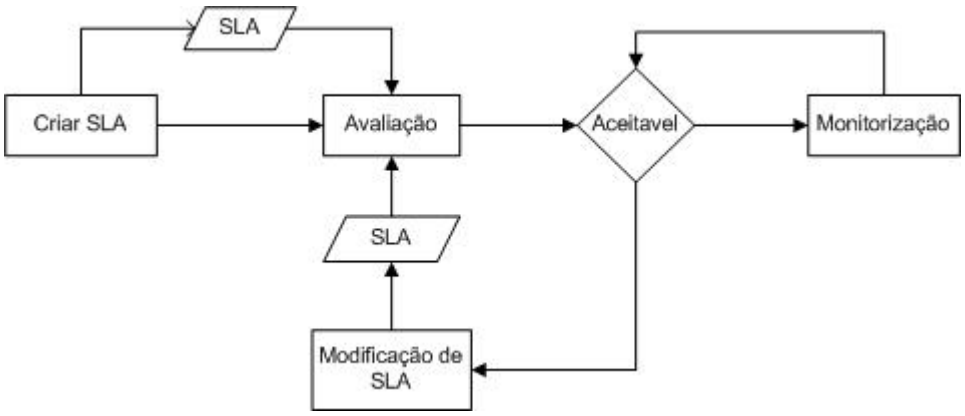

Figura 22: Ciclo de um SLA

- Para um SLA ser considerado aceitável deve incluir:

- Responsabilidades claras e bem definidas entre consumidores e clientes;
- Lista completa de serviços a que se refere;
- Métricas que permitam uma avaliação e monitorização que atestem que o fornecedor cumpre com acordado;
- Quais as alterações permitidas a um SLA em vigor;
- Quais as penalidades devidas por incumprimento.

4.3.3. Definir Políticas e Controlos de Segurança

A introdução dos serviços de *cloud* computing numa organização levanta muitos e novos desafios de segurança. A postura de segurança de uma organização é caracterizada pela maturidade, pela eficácia e pela completude da política de segurança implementada e ajustada à exposição ao risco (CSA, 2011). Esta é a fundação para uma efectiva e bem estruturada implementação e gestão de segurança e deve incluir as normas, os métodos e os procedimentos para preservar os três pilares da segurança em TI, a confidencialidade, a integridade e a disponibilidade. Deve estar bem definida e documentada e ser do conhecimento de todos os utilizadores que fazem uso da informação.

4.3.3.1. Política de Segurança

A política de segurança deve ter a devida aprovação da direcção e ser a fundação da qual, deriva toda a postura de segurança de uma organização. Deve também incluir todos os aspectos e requisitos de segurança, sem detalhes técnicos, que mudam com frequência, de uma infraestrutura *cloud*. Uma política de segurança deve (Winkler, 2011):

- Identificar todos os recursos e sistemas que se pretende proteger;
- Identificar todas a vulnerabilidades e ameaças e exposição às ameaças;
- Decidir as medidas de protecção dos recursos, avaliar os controlos de segurança e estimar custos de implementação do ponto de vista de custo benefício;
- Comunicar os resultados às partes interessadas;
- Monitorizar e rever de forma contínua o processo e procurar melhorias.

Entidades independentes têm trabalhos publicados sobre as políticas e controlos de segurança, que consideramos de maior importância a sua consulta na definição de controlos de segurança num projecto de migração para a *cloud*.

Council on CyberSecurity[25], organização independente sem fins lucrativos que visa a segurança e uma internet aberta. Tem vários documentos sobre controlos de segurança e sua implementação, ferramentas de automatização de controlos críticos e informação detalhada sobre segurança. De entre eles destacamos:

- *Critical Controls for Effective Cyber Defense* Ver 4.1 de Março de 2013
- *The Critical Security Controls for Effective Cyber Defense*, Ver 5.0 de Fevereiro de 2014

NIST[26] – Tem várias publicações na área de controlos de segurança, entre os quais destacamos:

- NIST Special Publication 800-53 - S*ecurity and Privacy Controls for Federal Information Systems and Organizations*, Ver 4 de 30 de Abril de 2013.
- Documento *Security Controls Assessment Form* que visa:
    - A normalização na verificação de resultados dos processos de controlos de segurança;
    - A preparação de auditorias a programas e sistemas;
    - O suporte a programas de avaliação para certificação;
    - Fornecer métricas de avaliação de segurança.

[25] http://www.counciloncybersecurity.org

[26] http://csrc.nist.gov/

4.3.3.2. Controlos de Segurança

Os controlos de segurança são medidas administrativas, técnicas ou físicas, que atestam que as políticas de segurança são observadas e seguidas. Estes garantem ou minimizam a perda ou alteração indevida da informação, a indisponibilidade dos sistemas, a degradação de serviços e a perda de acesso aos sistemas ou seja, tudo o que possa colocar em risco a normal operação de uma organização. Como referido anteriormente no parágrafo 2.7.2.3, os controlos podem ser restritivos, preventivos, detectivos ou correctivos e dividem-se em três categorias:

- Controlos físicos – Implementação de controlos de segurança que impeçam o acesso não autorizado a instalações, equipamentos ou sistemas ou para prevenção de incidentes, tais como, cameras de vigilância, leitores biométricos, sensores de movimento, detectores de incêndio e inundação, etc.

- Controlos técnicos – Implementação de tecnologias de controlo de acessos a informação armazenada em sistemas de TI, como por exemplo, encriptação de dados, ACL's. *software* de auditoria da intergridade *software*, autenticação de rede, cartões de acesso, etc.

- Controlos administrativos – Implementação de controlos administrativos de segurança que previnam o acesso à informação, intencionalmente ou não, como por exemplo, acções de formação e de informação, registo de pessoas, planos de emergência, etc.

Para identificar correctamente os controlos necessários deve-se analisar os processos e os sistemas para identificar a que ameaças eles estão sujeitos, quais as vulnerabilidades que têm e quais as probabilidades das ameaças se concretizarem. Existem ferramentas disponíveis para verificação dos sistemas, que geram relatórios com as vulnerabilidades conhecidas encontradas nos sistemas. Neste processo, devem também ser avaliados os riscos físicos, como o roubo de documentos com informação sensível ou em qualquer outro suporte. Com a lista das ameaças identificadas, avaliar os controlos de segurança necessários para eliminar a ameaça, considerando o custo, a redução do risco, a probabilidade da ameaça ocorrer e o valor do processo ou sistema.

O NIST na publicação 800-53 *Revision* 4, *Recommended Security Controls for Federal Information Systems and Organizations*, apresenta uma lista de controlos que se dividem em três classes principais, técnica, operacional e de gestão. Embora o documento tenha como objectivo as agências federais Americanas, os controlos nele definidos também

servem as necessidades de clientes e fornecedores em ambientes *cloud computing*, nomeadamente os controlos técnicos, organizados em 18 famílias. Cada controlo encontra-se bem definido com (NIST, 2013):

- Identificador – Com o nome da família e número;
- Declaração inicial – Descrição das actividades e acções que devem ser desenvolvidas;
- Guia suplementar – Contém informação adicional que deve ser aplicada conforme necessário;
- Melhoramentos – Informação para melhorar a funcionalidade e a robustez do controlo;
- Referências – Identificação das normas, das leis e demais informação considerada relevante para o controlo;
- Prioridade e sequência – Permite sequenciar e priorizar a aplicação do controlo.

O SANS *Institute*[27]estabelecido desde 1989 na pesquisa e educação. Tem publicado um trabalho *Critical Security Controls for Effective Cyber Defense* onde identifica os controlos críticos para uma efectiva segurança de uma infraestrutura IT. Estes controlos abrangem as ameaças mais recentes, pelo que recomendamos a sua implementação em qualquer organização com ou sem infraestrutura *cloud*. Os controlos propostos abrangem (Institute, 2013):

- Inventário dos equipamentos autorizados e não autorizados;
- Inventário de software autorizado e não autorizado;
- Configuração segura de equipamentos e *software* em dispositivos móveis, computadores portáteis, estações de trabalho e servidores;
- Avaliação contínua de vulnerabilidades e remediação;

[27] http://www.sans.org/

- Defesas contra *software* malicioso;
- Aplicar segurança ao *software*;
- Controlo dos acessos *wireless*;
- Capacidade de recuperação de dados;
- Avaliação das capacidades técnicas e treino apropriado para preencher as lacunas;
- Configuração segura em dispositivos de rede, como *firewalls*, *routers* e *switches*;
- Limitar e controlar as portas de rede, protocolos e serviços;
- Uso controlado dos privilégios administrativo;
- Defesa do perímetro;
- Manter, monitorizar e analisar os registos de auditoria;
- Acesso controlado com base em necessidade;
- Monitorização e controlo de contas;
- Protecção da informação;
- Gestão e resposta a incidentes;
- Engenharia de rede segura;
- Testes de protecção e exercícios *red team*.

4.4.Fase de Operação

Esta fase decorre após a migração da informação e sistemas para a infraestrutura *cloud* e consiste em uma avaliação estratégica a intervalos regulares, que certifiquem que os serviços contratados estão dentro dos objectivos definidos. Devem ser estabelecidos processos de análise de métricas, de controlo de cumprimento dos SLA's acordados com o fornecedor e funcionamento operacional, procurando medidas de melhoria que importem mais-valias para o negócio. Esses processos devem:

- Promover entrevistas e recolha de informação internamente, que permitam uma análise qualitativa e quantitativa e que apontem problemas e fragilidades que devam ser resolvidos;

- Atestar a segurança, a privacidade e a *compliance* com as normas e leis em vigor, determinadas nas análises e acordos com o fornecedor;

- Monitorizar os SLA's, garantindo que estes são cumpridos pelo fornecedor. Neste processo, o cliente deve ter procedimentos para solicitar alterações aos SLA's, conforme estabelecido no próprio acordo;

- Analisar as métricas que atestem o bom funcionamento de aplicações e sistemas, antecipando possíveis problemas e criando alertas automáticos, caso a performance e operação desçam para valores inaceitáveis;

- Analisar, a intervalos regulares, os serviços similares de outros fornecedores, comparando os seus serviços e condições com os actualmente contratados;

- Solicitar a intervalos regulares, certificados, inspecções e auditorias ao fornecedor para garantir que estes mantêm os processos, controlos de segurança e *compliance* inicialmente observados e acordados;

- Estabelecer processos de monitorização da facturação dos serviços contratados e efectivamente consumidos.

“*Institutions will try to preserve the problem to which they are the solution.*”

Clay Shirky

5. Conclusão

Actualmente, num mundo empresarial altamente concorrencial, cada empresa procura avidamente formas de aumentar a competitividade e de melhorar os seus resultados financeiros, fazendo emergir o conceito de *cloud computing* pelos benefícios que actualmente lhe são reconhecidos, nomeadamente financeiros. No entanto, desenvolver e implementar uma estratégia correcta, é um processo complexo e encontrar a solução que mais se adeque a cada empresa, pode demonstrar-se uma tarefa complexa e difícil, com barreiras a cada passo, mais vincadamente para empresas que não disponham de quadros técnicos com os conhecimentos adequados. De facto, para a migração de sistemas e informação para *cloud computing* é imperativo uma análise cuidada e abrangente, que não realce apenas as vantagens e benefícios, mas também que observe o modelo sob uma perspectiva de segurança e riscos que este acarreta.

Assim, nesta dissertação de mestrado tivemos como objectivo fazer um estudo sobre infraestruturas *cloud computing* e propor um método estruturado e centrado na segurança, para a migração para o modelo. A abordagem para a sua realização dividiu-se em duas fases. A primeira fase, de investigação, passou pela leitura de trabalhos, relatórios e livros sobre o tema, reunindo toda a informação considerada relevante, conceitos, ideias e opiniões sobre as tecnologias de uma infraestrutura em *cloud computing*, formando uma visão analítica e crítica. A segunda fase passou pela elaboração do documento com o que mais relevante se nos apresentou da fase anterior, que permita um conhecimento completo do modelo, vantagens, desvantagens, segurança e riscos de um processo de migração para uma infraestrutura em *cloud computing* levando à proposta do método.

A migração de sistemas e informação para uma infraestrutura em *cloud computing*, ainda levanta muitos receios e desconforto no seio da comunidade empresarial. Preocupações com perdas de privacidade, de segurança e de fiabilidade saltam para a ordem do dia quando a opção é considerada. Contudo, acreditamos que a migração para a *cloud* é possível e ainda assim manter os níveis de segurança equivalentes aos existentes nos sistemas tradicionais. Porém e antes de mais, é imperativo que todas as partes envolvidas, principalmente quem tem a responsabilidade de decisão, conheçam bem o modelo, as tecnologias envolvidas, as suas vantagens e desvantagens. Com esse propósito, dedicamos o 2º capítulo deste trabalho com informação que proporcione esse conhecimento fundamental. Nele apresentamos uma pequena resenha histórica e conceitos similares que estão na génese do surgimento do paradigma, antes de aprofundar o modelo *cloud computig*, com as principais características, descrição dos modelos de serviço (SaaS, PaaS e IaaS) e modelos de desenvolvimento (Público, Privado, Hibrido e Comunitário), terminando o capítulo com uma análise completa à infraestrutura de referência, que descreve todo

o conceito de uma forma abstracta e aponta os actores, as actividades, as funções e as relações entre eles.

Com um conhecimento, que esperamos seja mais claro e abrangente do que é o paradigma *cloud computing*, salientamos no capítulo seguinte as vantagens desvantagens, riscos e o que deve incluir, do ponto de vista da segurança, uma infraestrutura *cloud*, nomeadamente, processos de governança, *compliance* e gestão de risco. Conforme é claramente apontado, estes processos devem permitir uma correcta gestão da segurança em ambientes *cloud* e garantir a privacidade, segurança, fiabilidade. Para que essa segurança seja efectiva e permanente, auditorias regulares devem ser efectuadas, quer aos sistemas internos quer aos sistemas do fornecedor, certificando que os controlos foram correctamente desenvolvidos e implementados. Outro factor da maior importância em ambiente *cloud* é a relação com o fornecedor, esta deve ser assegurada por SLA's completos e que garantam uma correcta entrega dos serviços contratados.

A realização mais prática deste trabalho culmina no 4º capítulo com a apresentação de uma proposta de *framework* para migração, de sistemas e informação, para uma infraestrutura em *cloud*, numa perspectiva de segurança. Esse processo deve ser contínuo, mantendo um controlo sobre as operações e procurando melhorias constantes com um perfeito controlo sobre as operações diárias. Para isso, tomamos por base o ciclo Demings (PDCA), definindo quatro fases distintas, definição, análise, segurança e gestão. Este processo de governança deve ser abrangente a todo o plano de migração e gestão de operações, com processos de monitorização e melhoria contínua.

O futuro revela-se promissor para ambientes *cloud computing*, no entanto, questões de segurança continuam na ordem do dia, quando o tema é abordado. Com a realização desta dissertação, esperamos dar o nosso contributo para uma desmistificação da ideia que, segurança e *cloud computing* são dois conceitos que não podem coexistir na infraestrutura de uma organização. Com processos bem implementados e geridos, é possível garantir a privacidade, a segurança e a fiabilidade numa infraestrutura em *cloud computing*. Como apontámos no início do 3º capítulo, a confiança na utilização da *cloud* depende dos mecanismos de segurança, controlo efectivo de acessos, gestão robusta de identidades, ambiente seguro e meios seguros de comunicação.

5.1.Trabalho futuro

O tema abordado é certamente muito vasto, proporcionando os mais variados temas para trabalho futuro. Após a realização deste trabalho, ficou claro que ficou em falta uma análise financeira do modelo *cloud*, com vantagens e desvantagens financeiras, para uma organização

que adopte o modelo *cloud computing*. Propomos ainda, estudos mais detalhados, para organizações que pretendam implementar um plano de recuperação de sistemas e resposta ao desastre, recorrendo a serviços em *cloud*.

“*Any life truly lived is a risky business, and if one puts up too many fences against the risks one ends by shutting out life itself”*

Kenneth S. Davis

Bibliografia

Ahronovitz, M., Amrhein, D. & Anderson, P., 2010. *Cloud Computing Use Cases,* s.l.: Cloud Computing Use Cases Discussion Group.

Amies, A., Sluiman, H., Tong, Q. G. & Liu, G. N., 2012. *Developing and Hosting Applications on the Cloud.* s.l.:IBM Press Program.

Anon., 2012. *Security Recommendations for Cloud Computing Providers,* s.l.: Federal Office for Information Security.

arD3n7, 2013. *Introduction to Secure Software Development Life Cycle.* [Online]
Available at: http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/
[Acedido em 07 04 2014].

Berger, I. W., 2009. *Cloud - the Emergence of a New Model of Computing.* [Online]
Available at: http://blog.irvingwb.com/blog/2009/04/cloud-the-emergence-of-a-new-model-of-computing.html
[Acedido em 15 05 2014].

Best, M. & Neuhauser, D., 2006. *Walter A Shewhart, 1924, and the Hawthorne factory.* [Online]
Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2464836/
[Acedido em 25 04 2014].

Buyya, R., Broberg, J. & Goscinski, A., 2011. *Cloud computing : principles and paradigms.* s.l.:John Wiley & Sons, Inc..

Buyya, R. et al., 2009. *Future Generation Computer Systems,* s.l.: Elsevier.

Chow, R. et al., 2009. *Controlling data on the cloud - Outsourcing computations without outsourcing control.* s.l.:ACM - Digital Library.

CIO Council , s.d. *Creating Effective Cloud Computing Contracts for the Federal Government,* s.l.: Federal Cloud Compliance Committee.

CSA, 2011. *Security Guidance for Critical Areas od Focus in Cloud Computing,* s.l.: Cloud Security Aliance.

Davis, C., Schiller, M. & Wheeler, K., 2011. *IT Auditing: Using Controls to Protect Information Assets.* Second Edition ed. s.l.:McGraw-Hill.

DHS, 2010. *Open Government Plan Version,* s.l.: DHS - Department of Homeland Security.

Gartner, 2013. *Gartner Identifies the Top 10 Strategic Technology Trends for 2014.* [Online]
Available at: http://www.gartner.com/newsroom/id/2603623
[Acedido em 05 02 2014].

Gens, F., 2009. *New IDC IT Cloud Services Survey: Top Benefits and Challenges.* [Online]
Available at: http://blogs.idc.com/ie/?p=730
[Acedido em 02 04 2013].

Ghosh, S. & Hughes, G., 2011. *Cloud Computing Explained,* s.l.: Open Group.

Halpert, B., 2011. *Auditing Cloud Computing - A Security and Privacy Guide.* s.l.:John Wiley & Sons, Inc..

Hogan, M., Liu, F., Sokol, A. & Tong, J., 2011. *NIST Cloud Computing Standards Roadmap,* s.l.: NIST - National Institute of Standards and Technology.

Institute, S., 2013. *Critical Security Controls - Version 5,* s.l.: s.n.

Intel Corporation, 2012. *Big Data 101: Unstructured Data Analytics,* s.l.: Intel Corporation.

ISACA, 2011. *IT Control Objectives for Cloud Computing.* s.l.:ISACA.

ISO, 2013. *ISO/IEC 27002.* [Online]
Available at: http://www.iso27001security.com/html/27002.html#Section11
[Acedido em 28 04 2014].

Jansen, W. & Grance, T., 2011. *Guidelines on Security and Privacy in Public Cloud Computing,* s.l.: NIST - National Institute of Standards and Technology.

Jericho Forum, 2009. *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration.* [Online]
Available at: https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
[Acedido em 06 10 2013].

Josyula, V., Orr, M. & Page, G., 2012. *Cloud Computing: Automating the Virtualized Data Center.* s.l.:Cisco Press.

Krishnan, S., 2010. *Programming Windows Azure.* s.l.:O'Reilly.

Krutz, R. L. & Vines, R. D., 2010. *Cloud Security - A Comprehensive Guide to Secure Cloud Computing.* s.l.:Wiley Publishing, Inc.

Linthicum, D. S., 2009. *Cloud Computing and SOA Convergence in Your Enterprise.* s.l.:Addison Wesley.

Liu, F. et al., 2011. *NIST Cloud Computing Reference Architecture,* s.l.: NIST.

Lutz Schubert, s.d. *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010,* s.l.: Eropean Commission.

M.Talabis, M. R., Martin, J. L. & Wheeler, E., 2013. *Information Security Risk Assessment Toolkit.* s.l.:Syngress.

Mather, T., Kumaraswamy, S. & Latif, S., 2009. *Cloud Security and Privacy.* s.l.:O'Reilly.

McCallister, E., Grance, T. & Scarfone, K., 2010. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* s.l.: NIST - National Institute of Standards and Technology.

McClure, S., Scambray, J. & Kurtz, G., 2009. *Hacking Exposed 6: Network Security, Secrets & Solutions.* s.l.:s.n.

Mell, Peter; Grance, Timothy; NIST, 2011. *The NIST Definition of Cloud Computing,* s.l.: National Institute of Standards and Technology.

Microsoft, 2003. *Securing Your Network.* [Online]
Available at: http://msdn.microsoft.com/en-us/library/ff648651.aspx#c15618429_010
[Acedido em 04 05 2014].

Mohamed, A., 2009. *A history of cloud computing.* [Online]
Available at: http://www.computerweekly.com/feature/A-history-of-cloud-computing
[Acedido em 16 05 2014].

NIST, 2011. *Managing Information Security Risk,* s.l.: NIST - National Institute of Standards and Technology.

NIST, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations,* s.l.: s.n.

Parlamento Europeu e do Conselho, 1995. *Eur-Lex.* [Online]
Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046
[Acedido em 08 04 2014].

Perilli, A., Manieri, A., Algom, A. & Balding, C., 2009. *Cloud Computing - Benefits, risks and recommendations for information security,* s.l.: ENISA - European Network and Information Security Agency.

Petri, G., 2014. *Tune into the Cloud: Locked out of Heaven.* [Online]
Available at: http://blogs.gartner.com/gregor-petri/2014/04/05/tune-into-the-cloud-locked-out-of-heaven/?fnl=search
[Acedido em 10 05 2014].

Portugal, I., 2012. *Situação Actual e Tendências de Adopção de Serviços Cloud Computing em Portugal,* s.l.: s.n.

Raphael, J., 2011. *The 10 worst cloud outages (and what we can learn from them).* [Online]
Available at: http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902?page=0,0
[Acedido em 04 10 2013].

Rittinghouse, J. W. & Ransome, J. F., 2010. *Cloud Computing - Implementation, Management, and Security.* s.l.:CRC Press.

Rountree, D. & Castrillo, I., 2014. *The Basics of Cloud Computing.* s.l.:Syngress.

Scruggs, R., Trappler, T. & Philpott, D., 2011. *Contracting for Cloud Services.* s.l.:Government Training Inc.™.

Smith, R., 2009. *Computing in the Cloud,* s.l.: Research-Technology Management.

Sosinsky, B., 2011. *Cloud Computing Bible.* s.l.:Wiley Publishing, Inc..

SUN, 2011. *Take Your Business to a Higher Level,* s.l.: SUN.

Vaquero, L. M., Rodero-Merino, L., Caceres, J. & Lindner, M., 2009. *A Break in the Clouds: Towards a Cloud Definition.* s.l.:Telefonica Investigacion y Desarrollo and SAP Research.

Williams, B., 2012. *The Economics of Cloud Computing.* s.l.:Cisco Press.

Winkler, V. (., 2011. *Securing the Cloud - Cloud Computer Security Techniques and Tactics.* s.l.:Syngress.

Youseff, L., Butrico, M. & Silva, D. D., 2008. *Toward a Unified Ontology of Cloud Computing*, s.l.: University of California.

Anexo A

1. Avaliação de fornecedores

Uma avaliação correcta dos vários fornecedores *cloud* só é possível se for uniforme. As tabelas deste anexo permitem manter a uniformidade necessária nessa avaliação. Estas tabelas foram construídas a partir de normas publicadas por entidades independentes, como:

ENISA - European Union Agency for Network and Information Security, publicação *Cloud Computing* Information Assurance Framework (CCIAF)[28];

CSA – Cloud security Alliance, publicação Cloud Security Alliance Cloud Controls Matrix (CCM)[29];

NIST - National Institute of Standards and Technology, publicação NIST Special Publication 800-53[30] Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

As tabelas dividem-se em três áreas distintas e fundamentais para uma boa segurança de informação e sistemas:

- Segurança fundamental;
- Integridade de sistemas;
- Segurança operacional.

1.1. Segurança Fundamental

A base para uma infraestrutura de segurança tem início nos procedimentos, políticas de segurança e avaliação constante da sua actualidade. Um cliente *cloud* deve ter informação sobre como os fornecedores implementam as normas de segurança, não só nas suas instalações mas também com as entidades externas, com quem mantém contacto. Outro factor é o pessoal técnico e de manutenção ao serviço do fornecedor e como são garantidos os acessos destes à infraestrutura do fornecedor.

[28] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

[29] https://cloudsecurityalliance.org/research/ccm/

[30] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Segurança fundamental	*Observações*	*Fornecedor*		
		1	*2*	*3*
Segurança com pessoal				
O fornecedor tem em prática procedimentos e politicas para contratação de empregados				
São efectuados levantamento de passado para empregados com privilégios e acessos especiais				
Existem planos de formação em segurança para empregados				
São feitas revisões para determinar se empregado com privilégios e acessos especiais. Com que periocidade esses são efectuados				
Empregados com privilégios e acessos especiais são certificados em segurança				
Os privilégios de acesso são aplicados em todos os sistemas do fornecedor				
O acesso físico às instalações é verificado				
Terceiros				
Existem serviços fornecidos por entidades externas ao fornecedor				
As políticas de segurança e governança e normas são extensíveis às entidades externas				
São efectuadas auditorias de *compliance* e segurança às entidades externas				
Continuidade de negócio				
O fornecedor tem *sites* secundários para resposta ao desastre				
O fornecedor tem um processo de contingência documentado para a continuidade do negócio				
Qual o recovery point objective (RPO) e recovery time objective (RTO) do fornecedor				
O fornecedor comunica interrupção de serviços aos seus clientes				
Conceitos legais				
Em que jurisdição são os dados mantidos				
O fornecedor recorre a serviços externos fora da sua área de jurisdição				
O fornecedor tem procedimentos escritos para resposta a questões legais				
O fornecedor tem seguro de incidentes que permitam indemnizar possíveis incidentes graves com perda de informação ou exposição de informação de clientes				
Políticas e normas				
O fornecedor tem políticas de segurança e normas bem documentadas, aprovadas, envolvendo todas as partes da organização				
Foram as políticas de segurança revistas em termos legais				
As políticas de segurança e privacidade estão de acordo com as normas da indústria e normas reconhecidas internacionalmente				

Segurança fundamental	*Observações*	*Fornecedor*		
		1	*2*	*3*
As entidades externas também se encontram abrangidas por essas normas				
Transparência do fornecedor				
O fornecedor fornece aos clientes cópias das políticas de governança e das normas em vigor na sua organização				
O fornecedor Informa os seus clientes de alterações às políticas e às normas em vigor na sua organização				
O fornecedor providencia informação sobre auditorias à sua organização				
O fornecedor providência informação sobre testes de penetração efectuadas à sua infraestrutura				
O fornecedor exibe prova documental das auditorias efectuadas às entidades externas ao seu serviço				
O fornecedor permite aos seus clientes a destruição de dados e informação destes, existente na sua infraestrutura				
Provisão de recursos				
Que controlos e procedimentos o fornecedor tem estabelecido para evitar a exaustão de recursos				
O fornecedor limita a subscrição de serviços, protegendo os SLA's existentes				
O fornecedor permite aos seus clientes ferramentas de planeamento de utilização				

1.2. Integridade de Sistemas

Um aspecto de segurança reside na integridade dos sistemas. Uma correcta gestão de acessos a sistemas, dados e informação, permite uma melhor segurança e detecção de acessos indevidos ou não autorizados. Sendo a virtualização uma tecnologia central para infraestruturas em *cloud computing*, a sua segurança também ganha uma importância acrescida. Na tabela seguinte apresentamos algumas questões que podem ser feitas a potenciais candidatos *cloud*.

Integridade de sistemas	*Observações*	*Fornecedor*		
		1	*2*	*3*
Gestão de Acessos e Identidades				
O fornecedor utiliza mecanismos de autenticação robustos				
É possível usar métodos de autenticação de dois ou mais factores				
Existem meios técnicos de implementar Single sign-on				
Existem procedimentos de revogação de contas comprometidas				
Os sistemas IDS/IPS detectam utilização anormal de contas de utilizadores				

Integridade de sistemas	*Observações*	*Fornecedor*		
		1	*2*	*3*
É o sistema de validação passível de interagir com outros sistemas – Federation ID				
Existem controlos para contas com acesso privilegiado				
É a separação de funções efectiva e observada				
O Fornecedor recorre a dupla validação. Para que operações				
O fornecedor efectua validação de identidades na abertura de contas				
Como é feita a eliminação de contas de acesso. Que controlos existem				
Encriptação e gestão de chaves de encriptação				
Que controlos de segurança estão estabelecidos para protecção de chaves de encriptação				
Quem tem acesso às chaves de encriptação				
Como é assegurada a protecção das chaves de encriptação				
Que procedimentos existem para recuperação de chaves de encriptação comprometidas				
Que procedimentos existem para a revogação de chaves de encriptação				
Para que operações a encriptação é usada				
As políticas definem claramente o que deve ser encriptado				
Sistemas de encriptação de terceiros são adequadamente validados				
Segurança de rede				
O fornecedor procede a testes periódicos de penetração e que características técnicas têm				
Que políticas e processos tem o fornecedor implementados para identificação de vulnerabilidades				
O fornecedor comunica as vulnerabilidades aos seus clientes, assim como as medidas tomadas para as eliminar				
O fornecedor permite testes de penetração aos sistemas do cliente				
Que normas e boas práticas tem o fornecedor implementadas nas infraestruturas virtuais				
Que protecções usa o fornecedor contra ataques de MAC *spoofing*, ARP *poisoning*, *denial of service*, etc.				
Que meios usa o fornecedor para isolar redes administrativas da infraestrutura das redes de clientes				
Como são isoladas os sistemas virtuais dos clientes e o supervisor				
Quais os controlos e segurança usados contra ataques externos				
Segurança de Software e Sistemas Operativos				

Integridade de sistemas	*Observações*	*Fornecedor*		
		1	*2*	*3*
Que controlos tem o fornecedor implementados para protecção e integridade de aplicações, actualizações de *firmware*, sistemas operativos, e outro *software*				
Quais as normas e boas práticas são observadas pelo fornecedor				
O fornecedor efectua testes de vulnerabilidades antes de cada instalação de novo *software*, *updates* ou pacotes correctivos				
Que procedimentos toma o fornecedor quando identifica vulnerabilidades				
Que controlos e boas práticas tem o fornecedor implementadas para alteração de ficheiros de configuração				
Segurança de máquinas virtuais e equipamentos				
O fornecedor procede ao *update* e actualização das máquinas virtuais antes de a disponibilizar aos seus clientes				
Qual a frequência de actualização de actualização às máquinas virtuais após serem disponibilizadas aos clientes				
As máquinas virtuais são encriptadas quando se encontram em estado de paragem				
O fornecedor permite aos clientes o fornecimento das suas próprias máquinas virtuais				
O fornecedor providenciar máquinas virtuais com segurança reforçada, que implementações de segurança têm estas máquinas virtuais				
Que procedimentos tem o fornecedor implementados para certificar a segurança efectiva das máquinas virtuais				
Como é assegurada e mantida a separação entre máquinas virtuais de diferentes clientes dentro do mesmo servidor físico				
Como é implementada a comunicação entre máquinas virtuais do mesmo cliente				
Como é a segurança efectuada entre na interacção entre sistemas na infraestrutura do fornecedor e fora desta infraestrutura				
Que políticas de segurança existem implementados para dados em movimento entre sistemas				
Que políticas de segurança existem para dados em parados em disco ou sistemas de suporte				

1.3. Segurança operacional.

Muitos dos problemas de segurança em ambientes *cloud*, tem a sua origem na infraestrutura do fornecedor, onde os clientes não têm abrangência para protecção e onde uma quebra de segurança pode afectar um número elevado de clientes. Uma correcta avaliação nesta vertente a cada candidato a fornecedor é da máxima importância, para um ambiente seguro, para dados, sistemas e infraestrutura.

Segurança Operacional	*Observações*	*Fornecedor*		
		1	*2*	*3*
Gestão de incidentes				
Que informação é retida pelo fornecedor nos eventos de rede e sistemas e qual o seu período de retenção				
Quem tem acesso aos registos de eventos e com que frequência estes são analisados				
Que políticas de protecções estão implementas para controlo de acessos aos registos de eventos				
As componentes da infraestrutura do fornecedor encontra-se sincronizada com uma fonte de tempo, *single time source* (NTP)				
O fornecedor tem implementado processos de identificação e resposta a incidentes				
O fornecedor efectua testes aos processos de identificação e resposta a incidentes. Com que frequência esses testes são efectuados				
A informação de incidentes é mantida permitindo análise futura a ataques bem sucedidos				
Quais os procedimentos de resposta a incidentes				
O fornecedor disponibiliza relatórios de incidentes na sua infraestrutura aos clientes				
O fornecedor disponibiliza um ponto único de contacto aos seus clientes para tratamento de incidentes				
Existe, por parte do fornecedor, uma estrutura de reclamação para incidentes não resolvidos em tempo útil ou fora do acordado nos SLA's				
O fornecedor aceita a integração dos registos de incidentes dos clientes nos seus registos				
Gestão de equipamentos				
O fornecedor mantém um registo completo de todo o equipamento existente na sua infraestrutura				
Que ferramentas são usadas para manter esse inventário actualizado e completo				
O fornecedor mantém um registo dos equipamentos utilizados por um determinado cliente ou que tenha sido utilizado para armazenamento de dados				
O fornecedor permite a segregação de equipamentos com diferentes níveis de segurança				
Que ferramentas são utilizadas para garantir a segregação de equipamentos com diferentes níveis de segurança				
Segurança física de instalações				
Que procedimentos tem o fornecedor em prática para o acesso às suas instalações				
Permite pessoas estranhas à organização acesso às instalações. Que controlos de segurança estão implementados				
As instalações do fornecedor encontram-se seccionadas por níveis de segurança				
Que formas de autenticação de acessos se encontram instalados				

Segurança Operacional	*Observações*	*Fornecedor*		
		1	*2*	*3*
O fornecedor mantém registos de todos os acessos às suas instalações				
Existem alarmes e detectores de acessos não autorizados às instalações				
Com que frequência são efectuados testes aos sistemas de alarme				
Os sistemas de suporte às instalações encontram-se de acordo com as normas				
Existem sistemas alternativos de alimentação eléctrica, comunicações, fornecimento de água, etc.				
Práticas operacionais				
O fornecedor tem implementado um processo de controlo de alterações				
As alterações são precedidas de uma análise de risco antes de implementadas				
O fornecedor tem ambientes distintos para desenvolvimento, testes e produção				
As alterações são claramente documentadas				
Que controlos de segurança estão implementados para assegurar as boas práticas de desenvolvimento de *software*				
O fornecedor garante a eliminação da informação do cliente quando este termina o contrato				
Pode o cliente assistir à eliminação dos dados e auditar essa eliminação				
Que procedimentos tem o fornecedor em prática para eliminar os dados dos sistemas de segurança e cópia de segurança				

Anexo B

Formulário de proposta para preenchimento do caso de estudo em migração de sistemas para a *Cloud computing*

1. Identificação do caso de estudo

Nome	

1.1. Identificação dos participantes

Participantes	Unidade de Negócio / Departamento	Localização

1.2. Identificação do autor do documento

Criado por	
Data	____/____/_____
Versão	

1.3. Identificação de alterações ao documento

Actualização Realizada Por	Data	Versão
	____/____/_____	
	____/____/_____	

1.4. Identificação dos modelos de serviço e desenvolvimento a que o caso de estudo se aplica

Modelos de Desenvolvimento *Cloud*	Modelos de Serviço *Cloud*		
	SaaS	PaaS	IaaS
Privada			
Pública			
Híbrida			
Comunitária			

2. Descrição

Descrição detalhado do objectivo do caso de estudo

3. Termos e definições

Definições e termos usados no caso de estudo que necessitem de explicação detalhada

4. Conceitos de operação

4.1. Sistema actual

Breve descrição do funcionamento do sistema e sua interacção com os restantes sistemas. Por Exemplo:

- Integração dos vários sistemas entre eles;
- Requisitos de segurança;
- Requisitos de comunicações para cada sistema.

4.2. Implementação futura na *cloud*

Descrever a implementação desejada e quais a capacidades existentes actualmente na empresa. Por exemplo:

- Necessidades de formação para técnicos e utilizadores;
- Melhoria das comunicações.

5. Actores primários

Identificação dos actores primários com descrição completa de funções

Nome	Funções	Descrição
Actor n		
Actor n+1		

6. Objectivos de negócio

Descrição do esperado com a implementação do sistema ou serviço em ambiente *cloud computing*, com vantagens e desvantagens para os actores identificados no ponto anterior.

7. Modelo de serviço

Justificar a opção pelo modelo de serviço seleccionado, indicando as vantagens e desvantagens dessa opção.

8. Modelo de desenvolvimento

Justificar a opção pelo modelo de desenvolvimento seleccionado, indicando as vantagens e desvantagens dessa opção.

9. Condições de implementação

Identificar as condições que devem ser observadas após a implementação da solução

Condições		Classificação		
		Baixa	Média	Elevada
Confidencialidade	*Organização*			
	Pessoal			
Integridade	*Autorização*			
	Não repúdio			
Disponibilidade	*Acessibilidade*			
	Recuperação			
Gorvernaça	*Visibilidade*			
	Controlo			
	Organizacional			
Gestão do Risco	*Incerto*			
	Exposição			
Compliance	*Leis*			
	Normas			
	SLA's			
Condição n				
Condição n + 1				

10. Características

Descrever em como a implementação vai de encontro às principais características da *cloud*.

Característica	Descrição
Self-service a pedido	
Ubiquidade	
Pool de recursos	
Rápida elasticidade	
Serviços mensuráveis	
Multi-tenacy	

11. Tarefas

Descrição de cada tarefa do sistema e resposta esperada em condições normais. Na tabela abaixo, 5 corresponde a uma boa resposta, 1 a uma má resposta

Nome da tarefa	Descrição	Classificação				
		1	2	3	4	5
Tarefa n						
Tarefa n+1						

12. Requisitos

Identificar requisitos adicionais identificados.

Requisito	Descrição
Requisito n	
Requisito n+1	

13. Riscos

Identificação de riscos

Riscos	Data	Probabilidade			Severidade			Medidas de mitigação	Estado
		B	M	A	B	M	A		
Risco n									
Risco n+1									

- Riscos – Nome do risco identificado
- Data – Quando foi o risco identificado
- Probabilidade e Severidade – B (Baixa), M (Média), A (Alta)
- Medidas de mitigação - Acções tomadas para eliminar, reduzir ou transferir o risco
- Estado – Indicação se o risco foi resolvido ou ainda se encontra activo

14. Comentários

Notas e observações sobre este caso de estudo que seja pertinente referir