Análise de risco para Computação em Nuvem

Luis Manuel Marques Paiva

Tese de

Mestrado em Informação e Sistemas Empresariais

2016

Esta página foi intencionalmente deixada em branco

Análise de risco para Computação em Nuvem

Luis Manuel Marques Paiva

Tese de

Mestrado em Informação e Sistemas Empresariais

Tese orientada pelo: Professor Doutor José Borbinha, IST

2016

Esta página foi intencionalmente deixada em branco

“If you don’t invest in risk management, it doesn’t matter what business you’re in, it’s a risky business.” Gary Cohn.

Esta página foi intencionalmente deixada em branco

RESUMO

Têm-se notado nos últimos anos um crescimento na adoção de tecnologias de computação em nuvem, com uma adesão inicial por parte de particulares e pequenas empresas, e mais recentemente por grandes organizações.

Esta tecnologia tem servido de base ao aparecimento de um conjunto de novas tendências, como a Internet das Coisas ligando os nossos equipamentos pessoais e *wearables* às redes sociais, processos de *big data* que permitem tipificar comportamentos de clientes ou ainda facilitar a vida ao cidadão com serviços de atendimento integrados.

No entanto, tal como em todas as novas tendências disruptivas, que trazem consigo um conjunto de oportunidades, trazem também um conjunto de novos riscos que são necessários de serem equacionados.

Embora este caminho praticamente se torne inevitável para uma grande parte de empresas e entidades governamentais, a sua adoção como funcionamento deve ser alvo de uma permanente avaliação e monitorização entre as vantagens e riscos associados.

Para tal, é fundamental que as organizações se dotem de uma eficiente gestão do risco, de modo que possam tipificar os riscos (identificar, analisar e quantificar) e orientar-se de uma forma segura e metódica para este novo paradigma. Caso não o façam, os riscos ficam evidenciados, desde uma possível perda de competitividade face às suas congéneres, falta de confiança dos clientes, dos parceiros de negócio e podendo culminar numa total inatividade do negócio.

Com esta tese de mestrado desenvolve-se uma análise genérica de risco tendo como base a Norma ISO 31000:2009 e a elaboração de uma proposta de registo de risco, que possa servir de auxiliar em processos de tomada de decisão na contratação e manutenção de serviços de Computação em Nuvem por responsáveis de organizações privadas ou estatais.

Palavras-chave: Computação em Nuvem, Risco, Segurança, Gestão do Risco.

Esta página foi intencionalmente deixada em branco

ABSTRACT

In recent years, we assisted an increase in the adoption of Cloud Computing technologies, with an initial membership by individuals and small businesses, and more recently by large organizations.

This technology has been the basis for the emergence of a set of new technologies, such as the Internet of Things, connecting our personal equipment and wearables to social networks, Big Data processes to easily typify behaviors and adapt products to potential customers or make life easier for citizens with integrated care services.

However, as with all disruptive trends, which bring with them a number of opportunities, they also bring a set of new risks that need to be addressed.

Although the adoption of Cloud Computing becomes almost inevitable for a large part of companies and government entities, its adoption as operation must be subjected to an ongoing evaluation and monitoring between advantages and risks involved.

To this end, it is essential that the organizations have an efficient risk management, so that typification of risks (identify, analyze and quantify) serve as a guide to the new paradigm. If they do not, the risks are evident, from a possible loss of competitiveness compared to their congeners, lack of trust of customers, business partners or even to a total downtime of business.

This Master Thesis aims to develop a generic risk analysis based on NP ISO 31000:2009 with a proposal risk register, which can serve to assist in decision-making processes by organizations leaders when hiring Cloud services for private enterprises or Public Sector.

Key words: Cloud computing, Risk Register, Security, Risk Management.

Esta página foi intencionalmente deixada em branco

AGRADECIMENTOS

Em primeiro lugar, gostaria de expressar a minha gratidão ao Prof. Dr. José Borbinha pela sua valiosa orientação e aconselhamento para a construção da minha tese de Mestrado. O seu apoio, disponibilidade e suporte para a finalização da mesma foi fundamental.

Também estou grato ao Prof. Dr. Mira da Silva e Prof. Dr. Henrique Mamede pela direção do mestrado, passagem de conhecimentos ao longo do mesmo e motivação.

Uma palavra de apreço ao Ricardo Vieira do IST/INESC pela sua ajuda em alguns aspetos técnicos da tese.

Agradecer à Direção Geral do Orçamento por nos permitir realizar o estudo e caso prático utilizado nesta tese.

Finalmente, gostaria de agradecer à minha família, especialmente à minha esposa Suzana, e aos meus filhos Eduardo e Sofia, pelo apoio e paciência nestes últimos meses pela minha maior ausência, de modo que mais facilmente pudesse completar esta etapa.

A minha gratidão a todos.

Esta página foi intencionalmente deixada em branco

ÍNDICE

LISTA de TABELAS

Esta página foi intencionalmente deixada em branco

LISTA de FIGURAS

Esta página foi intencionalmente deixada em branco

ACRÓNIMOS

AP	Administração Pública
API	Application Programmable Interface
BaaS	Backup as a Service
CN	Computação em Nuvem (Cloud Computing)
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organization of the Treadway Commission
CRM	Customer relationship management
CSA	Cloud Security Alliance
ENISA	European Union Agency for Network and Information Security
ESPAP	Entidade de Serviços Partilhados da Administração Pública
EUA	Estados Unidos da América
FERMA	Federation European Risk Management
GR	Gestão do Risco
IaaS	Infrastructure as a Service
IDC	International Data Corporation
IPQ	Instituto Português de Qualidade
ISO	International Organization for Standardization
IT	Information Technology (Tecnologias de Informação)
NIST	National Institute of Standards and Technology
NP	Norma Portuguesa
OWAP	Open Web Application Security Project

Paas	Plataform as a Service
SaaS	Software as a Service
SI	Sistemas de Informação
SLA	Service Level Agreement ou Acordo do Nível de Serviço
STAKEHOLDER	Parte Interessada
SWOT	Strenghts, Weaknesses, Opportunities,Threats
UE	União Europeia
UML	Unified Modeling Language

1
INTRODUÇÃO

Atualmente os fornecedores de serviços de Computação em Nuvem oferecem capacidade de alocação de recursos (processamento, armazenamento), escalabilidade e disponibilidade que não está ao alcance de centros de IT de pequena ou média dimensão. Além disso, pela sua dimensão global e capacidade, conseguem praticar preços de utilização bastante baixos com uma diversidade de serviços e de segurança são uma opção a ter em consideração por parte das empresas ou organizações governamentais.

A IDC indicou que "Um terço de todos os gastos mundiais em infraestrutura dizem respeito à Nuvem, estes deverão crescer 26,4 por cento este ano (2015), para os 33,4 biliões de dólares. De realçar que os investimentos em infraestrutura tradicional, sem ser Cloud, deverão manter-se estagnados nos 67 mil milhões de dólares". [1] (Itchannel.com, 2015)

Também a "Goldman Sachs estimou que os gastos em infraestrutura de computação em nuvem e plataformas crescerá a um ritmo de 30% a partir de 2013 até 2018 em comparação com 5% de crescimento em infraestruturas empresariais tradicionais".[2] (Forbes.com, 2015)

Mesmo em Portugal, e após alguns anos de reajustamento económico com o respetivo reflexo de desinvestimento em TI, os estudos de mercado apontam para que 2016 seja um ano de viragem nesta tendência: a Computação em Nuvem será uma das áreas de maior investimento e aposta por parte dos decisores de TI, onde os estudos apontam para um

[1] Traduzido de http://www.itchannel.pt/article.php?a=14142 obtido em Ago/2015

[2] Tradução livre do autor. Original: *"A Goldman Sachs study published this month projects that spending on cloud computing infrastructure and platforms will grow at a 30% CAGR from 2013 through 2018 compared with 5% growth for the overall enterprise IT."*

crescimento elevado, acima dos dois dígitos anualmente com a respetiva diminuição de infraestruturas de IT tradicionais (ver fig.1).

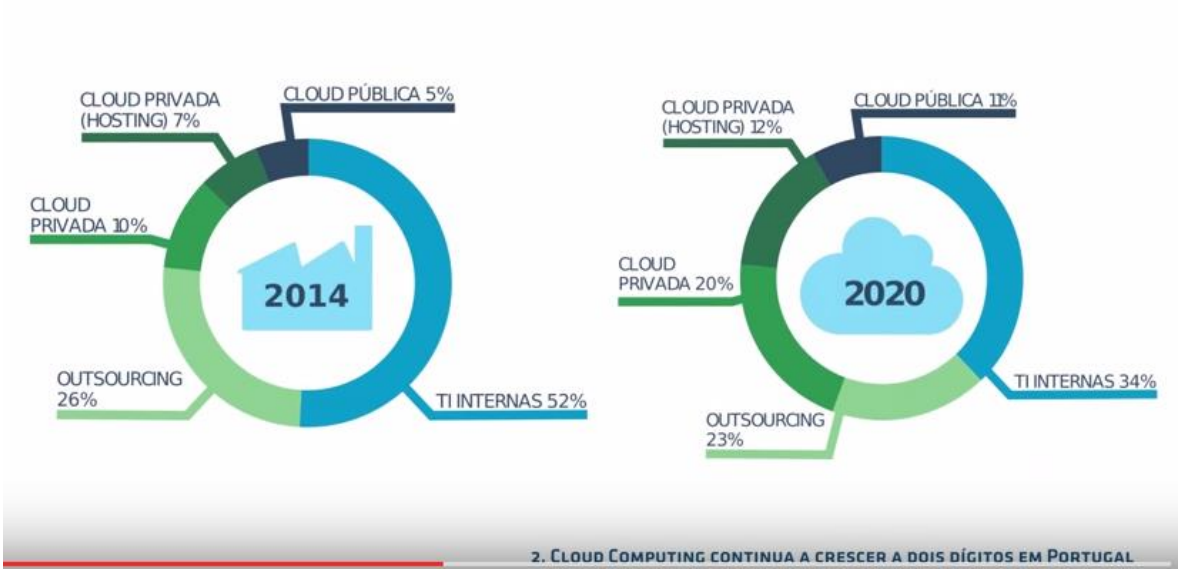


Figura 1 - Crescimento de serviços de Computação em Nuvem versus IT Tradicional (IDC Predictions 2015 - Portugal - Youtube.com, s.d.) [3]

Tal como em todas as tendências, as tecnologias de Computação em Nuvem continuam no sentido de maturação até que surja uma nova tecnologia disruptiva. No entanto e no entretanto interessa-nos perceber como melhor potenciar a sua utilização. Para tal devem-se aprofundar duas vertentes, maximização das suas potencialidades e minimização de riscos (de falhas, não adequação, etc).

Se por um lado a segurança de dados, confidencialidade, privacidade, disponibilidade e interoperabilidade são campos em que a Computação em Nuvem permite melhorar relativamente às Infraestrutura de IT tradicionais, é também evidente que esta mudança apresenta um conjunto de novos riscos que deverão ser tidos em conta.

Acrescido, do fato que os gestores de TI's são normalmente confrontados com a necessidade de num curto prazo de tempo de implementação de soluções de Computação em Nuvem,

[3] http://www.youtube.com/watch?v=Za39DN5JFT0

quer por imposições de competitividade de negócio, quer por motivos de racionalidade financeira, verificamos que existem muitas razões que podem potenciar o incremento de riscos que decorrem de tal mudança.

1.1 - Objetivo da tese

A gestão do risco deve ser realizada numa perspetiva de análise de risco de forma integrada, sistematizada numa transversalidade de todas as suas componentes como a confidencialidade e segurança, de modo que se minimize a incerteza nos objetivos definidos para as organizações na mudança de paradigma de TI.

Assumindo que o cliente destas tecnologias de certa forma já tem conhecimento dos serviços e potencialidade da Computação em Nuvem, esta **tese pretende focar-se na segunda vertente: a minimização dos riscos na adoção de tecnologias de Computação em Nuvem, e de uma forma estruturada e sistematizada, com base num modelo e ferramenta de gestão do risco seguindo a Norma NP ISO 31000:2009** (ISO.org, 2013). Assim, permitirá que os gestores de IT de uma organização, de uma forma ativa e alicerçada em dados, possam equacionar os riscos de mudança para a Nuvem (e/ou sua manutenção), de modo a ganhar uma vantagem competitiva perante outras organizações congéneres e garantir a permanência de funcionamento do negócio.

Esta tese está estrutura da seguinte forma:

1.2 - Esquema da tese

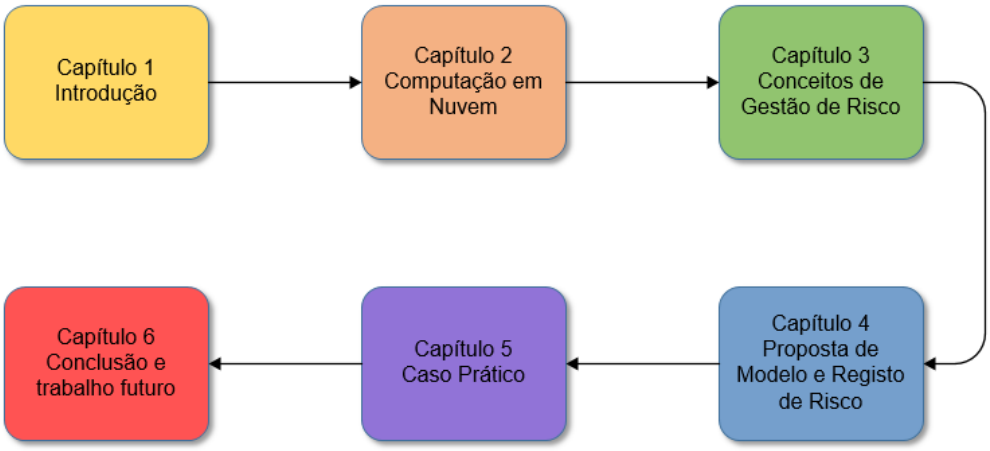


Figura 2 - Esquema da tese

Capítulo 1: neste capítulo contextualiza-se o trabalho a realizar, o que se pretende atingir com a elaboração desta tese e a metodologia utilizada.

Capítulo 2: são apresentados os conceitos de Computação na Nuvem, a sua evolução, características, modelos de serviços e tipos de implementação. Estes conceitos são fundamentais para quem pretende iniciar uma análise de gestão do risco nesta área de forma a aperceber-se das suas vantagens e riscos associados a cada opção. Nesse sentido, faz-se uma primeira abordagem aos tipos de riscos associados a cada modelo de Computação na Nuvem e tipo de implementação. No final indicam-se as principais empresas que operam neste setor e a sua história.

Capítulo 3: são apresentados os principais conceitos de gestão do risco e métodos de cálculo. Existindo inúmeras estruturas de gestão do risco, fala-se um pouco das caraterísticas e o porquê da adoção para a elaboração deste trabalho da Norma ISO 31000:2009.

Capítulo 4: é apresentado uma proposta de modelo de domínio de gestão do risco para cenários de Computação em Nuvem e Registo de Risco, tendo por base a Norma 31000:2009. É também importante de se perceber a razão de uso de modelos de domínio, assim como conceitos de registo de risco e a sua importância.

Capítulo 5: aplicação em caso prático tendo em conta a metodologia e modelo proposto no capítulo 4 de forma a verificar a sua eficácia numa situação real.

Capítulo 6: neste capítulo apresentam-se as principais conclusões do trabalho desenvolvido, assim como caminhos para trabalho futuro e seus desafios.

1.3 – Métodos de investigação

Utilizou-se o seguinte método de investigação:

Pesquisa Bibliográfica: recolha de informação, triagem de informação relevante, análise e interpretação de dados das diversas fontes ligadas à temática.

A pesquisa bibliográfica foi suporte de desenvolvimento da tese em todas as suas fases, auxiliando a definir e circunscrever o problema, focalizar o objetivo, elaborar hipóteses e finalmente, a extrair conclusões.

A investigação teve como pontos de abordagem o estudo:

1. Modelos e tecnologias de computação em nuvem.
2. Referência ISO 31000:2009 e seus conceitos de Gestão do Risco
3. Organizações que tenham emitido informações sobre práticas de Gestão do Risco em adoção de tecnologias de Computação em Nuvem.

Os pontos 1 e 2 permitem-nos conhecer melhor a tecnologia e adequar processos de gestão do risco.

O ponto 3 permite-nos conhecer a realidade do que já está a ser feito de modo que possa servir de base para o trabalho que se foi desenvolvendo na tese tendo em conta entidades dedicadas a normas de GR ou empresas privadas com interesses nesta área.

Estudo de Caso: Através da aplicação prática numa organização e vertendo os resultando para a elaboração da tese.

2

COMPUTAÇÃO em NUVEM

Neste capítulo iremos abordar a evolução da computação em nuvem ao longo dos últimos anos. Iremos focar os vários tipos de implementação, modelos de serviços de computação em nuvem e os riscos inerentes a cada tipo de abordagem

2.1 – Conceitos de Computação em Nuvem

O conceito de Computação em Nuvem (em inglês, Cloud Computing) tem como princípio a utilização de recursos informáticos a partir de qualquer ponto do mundo [4]. Atualmente tem-se assistido a um aumento de serviços e empresas neste setor que disponibilizam os mais variados tipos de recursos, como espaço de armazenamento, aplicações, serviços, capacidade de processamento e muitos outros serviços que mais à frente serão analisados em pormenor.

Embora seja uma tendência tecnológica relativamente recente, verifica-se que a sua génese remonta aos anos 50, onde se colocaram em rede os primeiros *mainframes* e passaram a ser acedidos a partir de locais remotos. Mas foi a partir do início dos anos 2000 que esta tecnologia se tem afirmado, devido à maturidade de um conjunto de outras tecnologias, nomeadamente a capacidade de aumento de débito nas redes de comunicações, tecnologias de virtualização, redução de custos em armazenamento de dados, constante capacidade de aumento de processamento e redução de espaço físico ocupado pelos centros de dados.

Foi a empresa Amazon que popularizou o conceito através do seu serviço de *Cloud – Elastic Compute Cloud,* sendo ainda hoje um dos maiores *players* em tecnologias de Computação em Nuvem.

[4] http://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem obtido em Out/2015

Podemos hoje considerar a CN como a combinação de virtualização, automatização de processos e resposta dinâmica às necessidades. Cada uma destas condições individualmente não significa mais que uma extensão do funcionamento do IT tradicional, no entanto a sua combinação muda o paradigma e indica-nos a função que a Computação em Nuvem tem nos dias de hoje. (Jared Carstensen, 2012).

Segundo a organização National Institute of Standards and Technology (NIST) Computação em Nuvem é:

"Um modelo que permite, de uma forma simples e conveniente, através da rede de comunicações, acesso a um conjunto de recursos computacionais (e.g., comunicações, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente disponibilizados e libertados através de uma consola de gestão ou através de pedido ao fornecedor de Nuvem ".[5] (Mell, 2011)

2.2 - Modelos de serviços de Computação em Nuvem

Os serviços de computação em nuvem são normalmente classificados em três tipos, Infraestrutura como Serviço (IaaS), Software como Serviço (SaaS) e Plataforma como Serviço (PaaS). No entanto, recentemente tem aparecido novos serviços que procuram encontrar novos mercados e necessidades das organizações.

De seguida fazemos uma breve apresentação dos tipos de serviços em nuvem existentes, já que é importante conhecer as várias tecnologias e modelos de modo a também poder-se realizar, de uma forma mais alicerçada, uma Gestão do Risco nesta área:

- **IaaS (Infrastruture as a Service)** - é um modelo onde fornecedor Cloud disponibiliza equipamento de infraestrutura, normalmente espaço de armazenamento, servidores, equipamentos de comunicações. O fornecedor detém o equipamento e é responsável pela sua manutenção, onde o cliente paga a sua utilização. Os principais fornecedores nesta área são: Amazon, Google, Microsoft, IBM.

[5] Tradução livre do autor. Original: *"Cloud Computing is 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"*

- **SaaS (Software as a service)** - este modelo permite que o fornecedor disponibilize software parametrizado ao cliente. A gestão de toda a infraestrutura é da responsabilidade do fornecedor de software (servidores, comunicações, etc) e o cliente paga o que usa ou através de um valor fixo mensal. Atualmente as implementações deste modelo são usualmente realizadas via browser ou em sistemas de instalações locais ligadas à nuvem, como software de antivírus, de backups remotos, aplicações financeiras/administrativas ou gestão de parque informático.
- **PaaS (Platform as a Service)** - Plataforma como Serviço é uma solução mais abrangente do modelo de computação em nuvem do que o SaaS. Relativamente a este apresenta várias vantagens, como permite a parametrização do sistema operativo às necessidades do cliente e partilha de recursos por organizações cujos seus colaboradores utilizam primordialmente equipamentos portáteis. Este serviço, está também adequado a equipas de desenvolvimento, que necessitam que o sistema operativo seja parametrizado especificamente consoante os diversos tipos de testes, ou que permita acesso rápido/pontual a vários tipos de sistemas operativos ou plataforma, minimizando assim os custos de aquisição de equipamento e tempos de instalação.

É importante notar que, que estes três de modelos de CN não são estanques e têm nos últimos anos surgido no mercado soluções híbridas, como por exemplo modelos de IaaS com serviços aplicacionais adicionais, ficando já mais próximos de uma solução de PaaS.

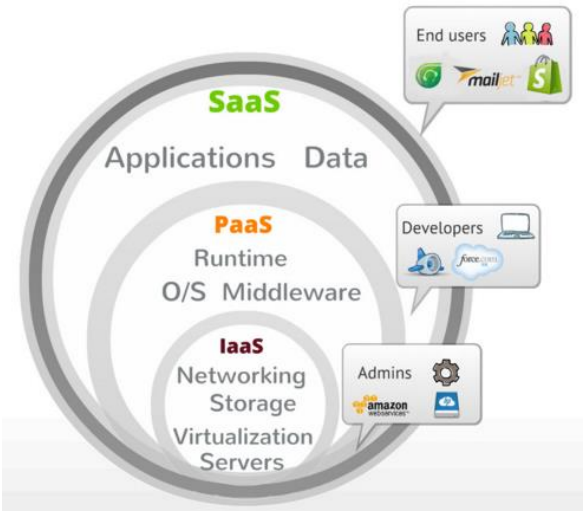


Figura 3 - Modelos de serviços de Computação em Nuvem *(Herrera, 2014)*

As organizações têm apostado essencialmente em modelos de serviços de IaaS e SaaS. As razões inerentes a esta situação prende-se que o modelo de serviço IaaS permite uma implementação faseada não disruptiva entre a IT tradicional e a computação em nuvem (com soluções híbridas). O modelo SaaS, também tem tido uma adoção célere pelas suas caraterísticas de fácil implementação, permitindo à organização acesso a um conjunto de aplicações transversais e sem grande necessidade de especificidade ao negócio, como por exemplo Email, CRM e aplicações financeiras.

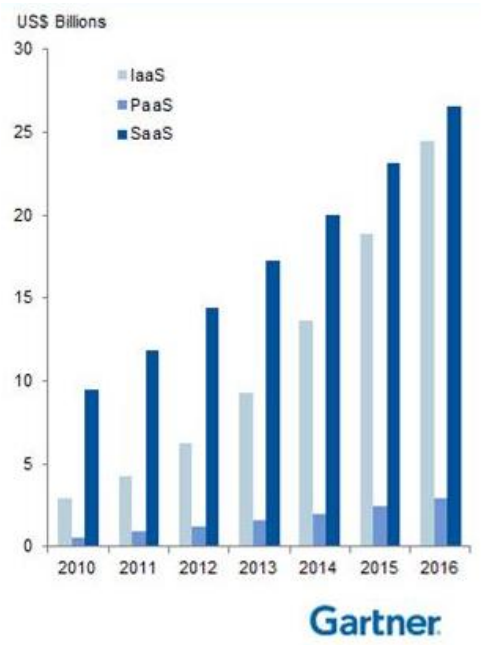


Figura 4 - Crescimento de modelos de serviços de Computação em Nuvem (Source: Gartner)

Encontramos também um conjunto de serviços de computação em nuvem mais específicos, embora com algum crescimento nos últimos tempos:

- **StoraaS (Storage As A Service)** - o StoraaS é um modelo de negócio em que os fornecedores de Computação em Nuvem, alugam espaço de armazenamento para os seus clientes. Prevê-se que este tipo de serviço continue em grande crescimento, sendo um dos seus principais foci, backup de infraestruturas **(BaaS)**, por ser de simples implementação e refletindo baixos custos para o cliente final.
- **DBaaS (Data Base as a Service)** - é um modelo de serviço em nuvem gerido por um operador, que oferece acesso aos seus clientes suporte a serviços de bases de dados. Tal como é sabido, os custos de gestão e manutenção de base de dados são elevados

(por necessidade de pessoal especializado, manutenção, aquisição, etc.) permitindo que as empresas tenham acesso a serviços de base de dados muito fiáveis e com custos reduzidos.

- **CaaS (Communication as a Service)** - solução de serviços de comunicações em nuvem onde os clientes podem ter serviços de comunicações, como por exemplo voz sobre IP (VoIP ou telefonia via Internet), mensagens instantâneas (IM), colaboração e videoconferência em aplicações ou dispositivos fixos e móveis.
- **EaaS/XaaS (Everything as a Service ou Tudo como Serviço em português)** - teve origem no modelo software como serviço (SaaS) e desde então tem-se expandido para incluir serviços de infraestrutura e outros, como StoraaS, Disaster recovery-as-a-service e, até mesmo, modelos recentes como o desktop como um serviço.

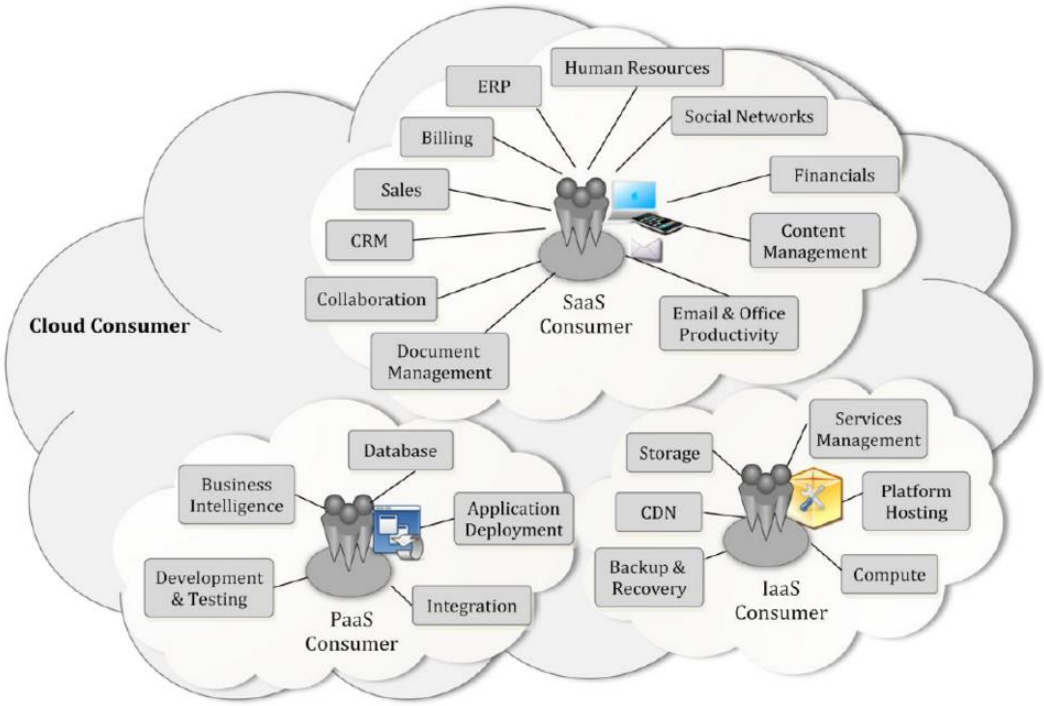


Figura 5 - Modelos de serviços de Computação em Nuvem (Source NIST)

2.3 - Modelos de implementação de Computação em Nuvem

O modelo a implementar deve também ter em conta o que se pretende a nível de serviço de computação em nuvem e a segurança de informação, descrevem-se abaixo os diferentes tipos de implementação:

- **Nuvem privada (Private cloud)** - Normalmente este tipo de serviço é realizado para estender a capacidade de processamento do cliente, sendo instalado num misto de serviço assegurado pelo IT internas e estendido para o fornecedor de serviço. Para implementação, este tipo de serviço obriga a um nível de capacidade técnica elevada, de modo a virtualizar a infraestrutura e a colocar o seu funcionamento no exterior. Uma nuvem privada permite assegurar um maior nível de segurança e manter o conhecimento interno dos processos tecnológicos que podem ser diferenciadores do negócio. Por sua vez, o fato de manter as duas infraestruturas aumenta os custos de manutenção e de pessoal qualificado. (Mell, 2011).
- **Nuvem pública (Public Cloud)** - define-se uma nuvem pública quando os serviços contratados se encontram disponíveis para o público/clientes. Normalmente este tipo de serviços tem um modo de utilização de pagamento por utilização e/ou através de um valor mensal fixo. Embora tecnicamente não existam grandes diferenças entre uma nuvem pública e uma nuvem privada, a última tem normalmente associado um nível de segurança superior e mais serviços que obviamente têm reflexo nos custos. (Mell, 2011).
- **Nuvem híbrida (Hybrid Cloud)** - o modelo de nuvem híbrida consiste na agregação de duas ou mais tecnologias de nuvem (nuvem privada, comunitária ou pública) interligadas permitindo aos clientes o melhor das soluções consoante as necessidades - segurança por um lado e redução de custos e escalabilidade por outro. (Mell, 2011). Existem várias tipologias de implementação de nuvens híbrida, como por exemplo uma organização armazena dados sensíveis na sua nuvem privada, mas com ligações a nuvens públicas para disponibilização de serviços de aplicações web ou em alturas de maior pico de negócio rapidamente aumentar a capacidade de processamento disponível no fornecedor.
- **Nuvem comunitária (Community Cloud)** - este modelo assenta numa partilha de infraestrutura Cloud em que várias organizações, tendo as mesmas necessidades, criam ou adquirem serviços Cloud. A grande vantagem deste sistema é a redução de custos em detrimento de uma menor segurança relativamente a uma nuvem privada.
- **Internuvem (Intercloud)** - é um modelo baseado na ligação global de tecnologias Cloud, ou seja, uma Cloud de Clouds. O que se pretende é que os fornecedores de serviço Cloud permitam que as suas infraestruturas e serviços tenham processos e protocolos abertos de comunicação. Este poderá ser um passo decisivo para reduzir valores de aluguer de espaço, competitividade e que as organizações possam ganhar

a autonomia a nível da sua informação. Podemos fazer uma comparação de internuvem como uma Cloud de Clouds em analogia com a internet, uma rede de redes.

- **Multinuvem (Multicloud)** - é uso de múltiplas Clouds e serviços de computação heterógenos de modo a criar uma menor dependência a um só fornecedor e ganhar-se em escolha. Permite que se escolha o fornecedor que melhor serviço ou custo apresenta. Permite também salvaguardar a informação, já que os dados podem estar em vários locais, e precaver situações de desastre. Este modelo distingue-se de uma nuvem híbrida porque abrange serviços de múltiplos fornecedores. Por exemplo, uma empresa pode usar simultaneamente diferentes fornecedores de computação em nuvem para (IaaS) e (SaaS) ou usar vários fornecedores de Cloud para infraestrutura (IaaS).

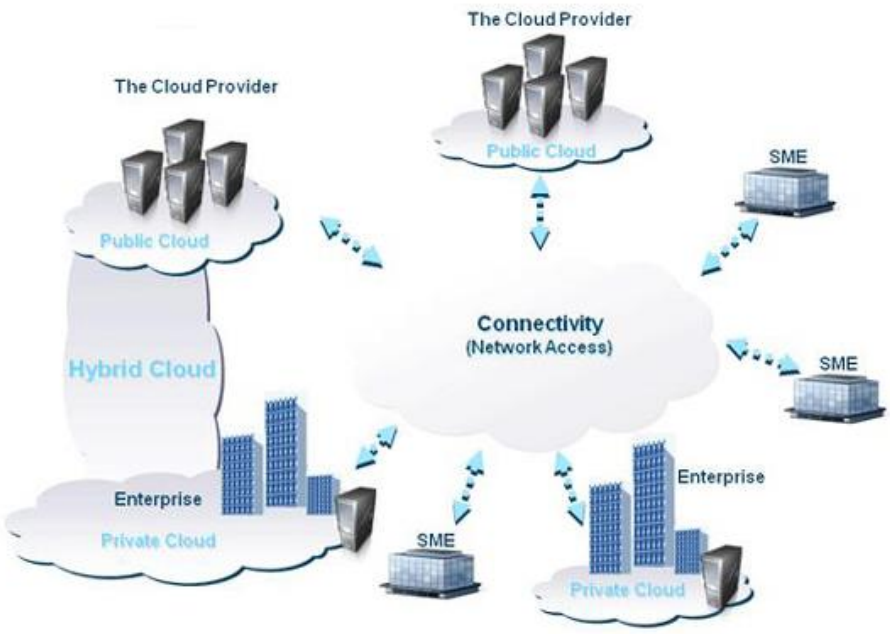


Figura 6 - Tipos de implementação de serviços de Computação em Nuvem *(Dieder, 2011)*

2.4 – Análise de risco de cada modelo

Verificamos que ao longo da última década os riscos que os ativos de IT estão expostos tem aumentado. Tal deve-se a uma mudança de paradigma em que inicialmente o IT servia a gestão interna e funcionamento da empresa, ou seja, “virado para dentro”. Com a explosão da internet e a necessidade de as empresas comunicarem entre si e prestarem serviços aos

clientes, os ativos de IT passaram a ser configurados para o exterior, aumentando a sua exposição e claro os riscos.

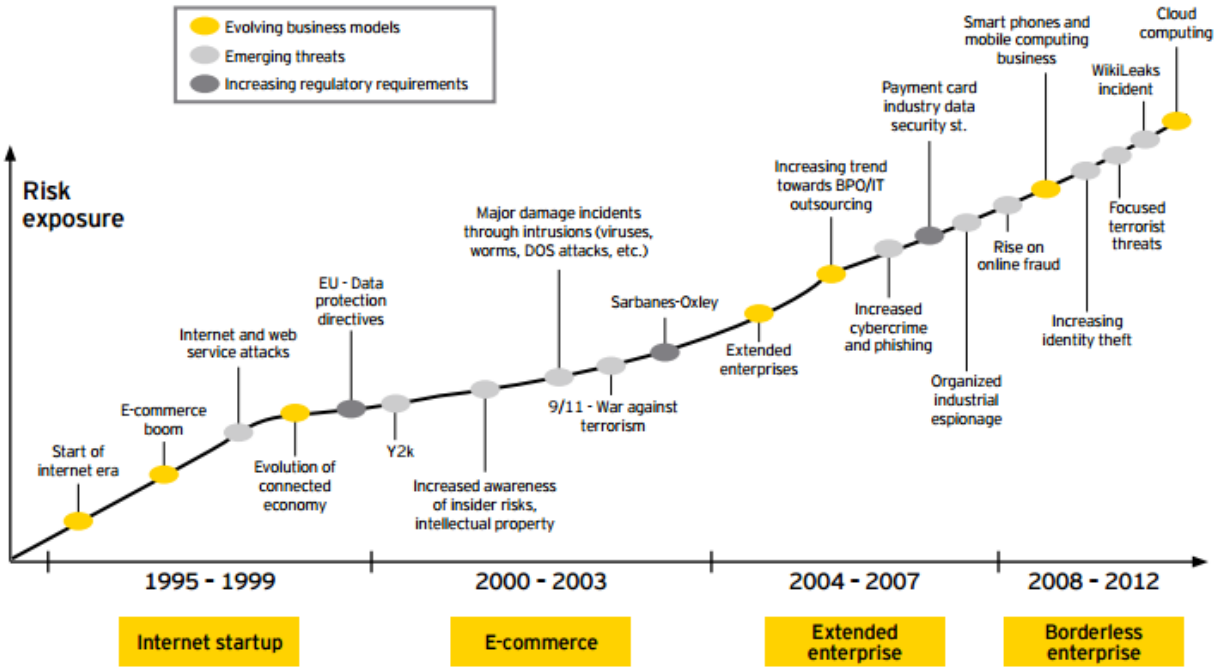


Figura 7 - Aumento da exposição de risco em IT *(Young, 2011)*

Tendo em conta as especificidades dos vários modelos de serviços de CN, verificamos que o modelo que apresenta menor risco é o IaaS. No extremo oposto, temos o modelo de serviço SaaS, que exige por parte do fornecedor e da equipa de segurança em IT, um maior rigor na sua implementação. Devera-se aplicar regras de segurança mais restritas, como por exemplo encriptação nas comunicações entre o fornecedor de CN e a organização (ex: VPN).

Relativamente aos modelos de implementação de serviços de CN, estes também apresentam níveis de risco diferenciados. Um modelo de Nuvem Privado é o que menor risco apresenta de perda de dados ou ataques informáticos, e o modelo de Nuvem Pública é o que merece um maior cuidado na sua implementação relativamente a proteção de dados.

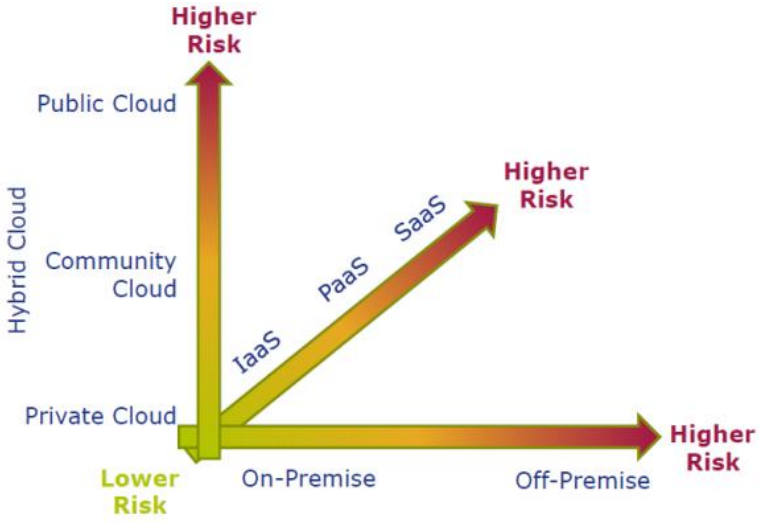


Figura 8 - Risco versus Tipo de Infraestrutura/Serviço *(Stokes, 2013)*

Verificamos que o tipo de *Cloud* e serviço a implementar deve ser bem equacionado, tendo em conta os tipos de riscos que a organização está disposta a "correr".

Se, por um lado, modelos de Internuvem ou Multinuvem permitem reduzir os riscos de *lock-in* a um fornecedor, perda de dados ou manter o funcionamento da organização, relativamente a modelos mais simples, como nuvem pública, por outro lado, aumentam os custos informáticos.

Para identificar as principais ameaças ou problemas, CSA realizou uma pesquisa/inquérito a um conjunto de especialistas da indústria, de modo que pudessem dar uma opinião profissional sobre as maiores vulnerabilidades que, no seu entendimento, existem na computação em nuvem (Alliance, 2013) [6]:

- Violação de Dados
- Perda de Dados
- Ataque e uso de contas de utilizadores
- APIs inseguras
- Denial of Service
- Ataques internos maliciosos

6 https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf obtido em Out/2015

- Abuso de Serviços em Nuvem
- Insuficiente e célere resolução de problemas
- Partilha de recursos tecnológicos

Nos diversos questionários realizados a responsáveis de IT, constata-se que as principais preocupações na adoção de computação em nuvem situam-se na área de segurança e governação dos dados.

É comum existirem preocupações de:

- Como sei onde estão guardados os dados da minha empresa?
- O que me garante que um empregado do fornecedor computação em nuvem não rouba os dados?
- O que me garante que o serviço é redundante, e têm aplicadas as boas normas de segurança?
- Onde fica delimitada a responsabilidade caso algo não corra bem?

Embora as áreas em evidência coloquem alguma dificuldade na delimitação de responsabilidades entre o fornecedor de serviço CN e a organização, a tabela abaixo permite-nos delinear responsabilidades de segurança consoante o tipo de modelo de prestação serviço *Cloud* implementado, tendo em conta as 3 áreas de chave de responsabilidade: Infraestrutura, Sistema Operativo/*Middleware* e serviços aplicacionais.

Tabela 1 - Delimitação de responsabilidades

		IaaS	**PaaS**	**SaaS**
Aplicação	Responsabilidade	Organização	Organização	Fornecedor
	Ação	Boas práticas e Certificação	Boas práticas e Certificação	Atualização e certificação
OS/ Middleware	Responsabilidade	Organização	Fornecedor	Fornecedor
	Ação	Boas práticas e Certificação	Atualização e certificação	Atualização e certificação
Infraestrutura	Responsabilidade	Fornecedor	Fornecedor	Fornecedor
	Ação	Atualização e certificação	Atualização e certificação	Atualização e certificação

A linha mais escura delimita a responsabilidade entre a organização e o fornecedor de serviço *Cloud* consoante o tipo de serviço implementado. Ou seja, na implementação da responsabilidade do fornecedor de serviços a organização assume uma atitude passiva e vice-versa. (Jared Carstensen, 2012)

No entanto a lista de riscos que uma organização enfrenta na sua mudança tecnológica para a computação em nuvem é muito mais ampla e que se discrimina em mais pormenor:

A nível de segurança de informação:

- **Confidencialidade:** confidencialidade é definida como a garantia de que a informação é acessível somente a pessoas autorizadas.
- **Integridade:** garantir que a informação não foi alterada sem a devida permissão ou não se encontra corrompida (Whitman and Mattord 2008).
- **Disponibilidade:** assegurar que os utilizadores autorizados tenham acesso à informação e a equipamentos quando necessário.
- **Responsabilidade:** é o estado de ser capaz de rastrear inequivocamente uma ação de uma entidade no sistema de Informação (NIST 2002).

2.5 - Principais fornecedores de serviços de Computação em Nuvem

Tem-se assistido a crescimento de empresas que exploram comercialmente a tecnologia de computação em nuvem. Estas diferenciam-se pelos tipos de infraestruturas, serviços e segurança.
Grande parte dos fornecedores de CN estão sediados nos EUA, país onde se tem desenvolvido mais a investigação e implementação desta tecnologia.

Fornecedores de Computação em Nuvem líderes a nível mundial

- IBM Softlayer: um dos principais fornecedores de mercado CN tem serviços de IaaS, PaaS e SaaS, como também capacidade de implementações de Nuvem Híbrida. Dado o seu elevado conhecimento e leque de clientes no setor bancário e financeiro tem tido um crescimento assinável.

- Salesforce.com: uma das tecnológicas pioneiras de sistemas de CN, começou a disponibilizar a sua aplicação de CRM através do sistema SaaS, tem no entanto diversificado os seus produtos para modelos PaaS permitindo que programadores possam desenvolver aplicações que executam nativamente na plataforma Salesforce com linguagem Apex.
- Amazon Web Services (AWS): um dos primeiros fornecedores de Computação em Nuvem, tendo iniciado as suas operações em 1996. Atualmente líder de mercado apresenta um dos mais completos leques de serviços, aliado a uma capacidade de investimento muito elevada e política agressiva de preços. Nele encontramos grandes empresas como a Twitter.
- Microsoft Azure: uns dos líderes do mercado CN, a Microsoft têm-se posicionado como fornecedor global, sendo um dos poucos fornecedores a ter aprovação governamental europeia para colocação de dados institucionais. Conta com serviços de IaaS/PaaS e modelos de implementação de Nuvem pública. Apresenta uma solução que permite facilmente a migração de infraestruturas Windows para os seus servidores e que os programadores possam usar linguagem .Net.
- Oracle (Cloud IaaS): empresa que se notabilizou em aplicações de bases de dados, conta com serviços de nuvem em IaaS, PaaS, SaaS sendo o seu forte soluções de Data as a Service (DaaS) e de Business Intelligence as a Service (BIaaS).
- SAP, AG: empresa alemã líder em serviços ERP tendo-se lançado em serviços Computação em Nuvem mais recentemente. Foca-se principalmente em disponibilizar o serviço de SaaS das suas aplicações, mas também serviços de IaaS.
- Google (Cloud/Enterprise): fornecedor americano de serviços Computação em Nuvem com serviços de IaaS, SaaS, PaaS, StoraaS. Os serviços de nuvem do Google surgiram inicialmente para o consumidor final tendo depois passado para a área empresarial. Atualmente é um dos líderes em serviços CN pela sua capacidade financeira e inovação.
- Rackspace: empresa iniciou atividade em 2006. Vocacionada para um modelo de nuvem em IaaS e com vários modelos de implementação (privada, pública, híbrida) é hoje um dos maiores fornecedores deste tipo de tecnologia.
- Opennebula: empresa que pretende divulgar e fornecer serviços de nuvem em protocolos abertos e standard. Utiliza servidores Linux, com virtualização Vmware e permite ligação a vários fornecedores da nuvem como a Amazon. No modelo IaaS tem como base a plataforma aberta Openstack.

Fornecedores de Computação em Nuvem portugueses:

- PT/MEO Cloud: empresa líder em Portugal de serviços de nuvem criou um centro de dados na Covilhã especificamente para o efeito de disponibilização de infraestruturas serviços Computação em Nuvem.
- Oni Cloud: empresa fundada em 2000, hoje tendo um leque alargado de serviços de Computação em Nuvem, desde a disponibilização de infraestrutura a serviços/aplicações disponíveis em modo SaaS.

Fornecedores de Computação em Nuvem Europeus:

- Aepona: empresa Irlandesa que fornece produtos e serviços de nuvem. É uma start-up que tem tido um dos maiores crescimentos neste setor.
- Amplidata: empresa belga com elevado grau de especialização em serviços de nuvem. Grande parte dos seus fundadores e pessoal técnico foi recrutado de outras grandes empresas da Computação em Nuvem.
- Cloudmore: iniciou atividade em 2004, empresa sueca conseguiu estabelecer-se como um dos principais fornecedores de serviços em nuvem na Europa em menos de uma década.

2.6 - Tecnologia de código aberto para Computação em Nuvem

Um dos mais recentes avanços nas tecnologias de Computação em Nuvem, vem por parte de projetos *Cloud Open Source*, sendo um conceito apoiado pelas grandes empresas de software open *source*.

Estas plataformas têm como princípio orientador que os clientes tenham possibilidade de ter acesso a infraestruturas compatíveis e com total interoperabilidade entre si, resultando que a diferença entre fornecedores de Computação em Nuvem se faça pelo valor de custo de utilização da plataforma ou dos níveis dos seus serviços/aplicações.

A interoperabilidade e a capacidade de o fornecedor estar conforme as especificações da ***Cloud Open Source*****, permitem assegurar aos clientes a possibilidade de mais facilmente poderem mudar de fornecedor de serviço cloud, reduzindo assim um dos fatores de risco que a contratação destas infraestruturas implica**. É deveras importante

que se tenham em atenção estas caraterísticas no ato de adjudicação de um serviço, principalmente se o fornecedor de serviço é uma empresa menos conhecida no mercado.

É interessante de se verificar que a tendência de mercado tem indicado que as empresas têm desinvestido na aquisição de equipamento e *software open source* em detrimento de soluções *Cloud Open Source* e OWAP devido a uma maior estabilidade e maturidade desta tecnologia, como ainda a uma redução de custos.

No gráfico abaixo, tendo em conta um estudo realizado pela Forrsights (Forrsights, 2013) verificamos que as soluções de Nuvem privadas tradicionais se mantêm na liderança. No entanto, começa-se a verificar o crescimento na adoção de plataformas *Cloud Open Source* em particular, a plataforma Openstack, sendo expetável que esta diferença se reduza.

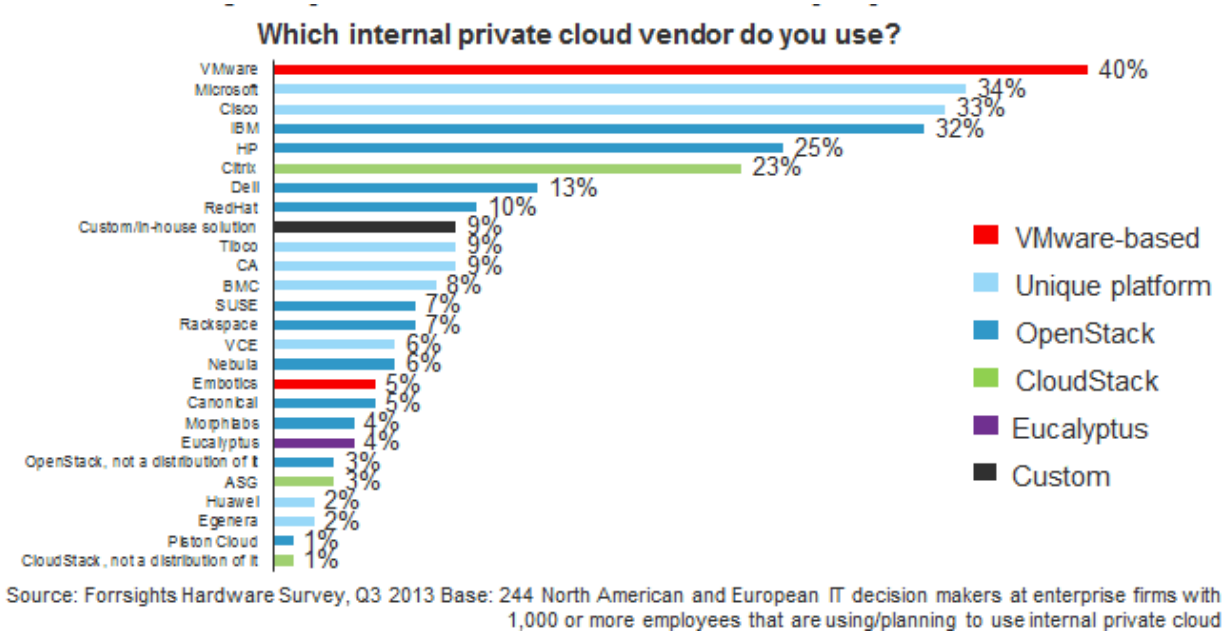


Figura 9 - Adoção de plataformas de Computação na Nuvem por tipo de tecnologia e fornecedor *(Forrsights, s.d.)*

Plataformas *Open Source Cloud* (em sistema IaaS):

Openstack - projeto iniciado em 2010, desenvolvido inicialmente pela Rackspace e NASA. Hoje tem o apoio de grandes empresas fornecedoras de equipamento como a HP. É hoje uma das plataformas de maior crescimento com uma lista de clientes de renome, como a Sony Entertainment, Lenovo, Netflix, Yahoo.

Esta plataforma é constituída por vários componentes nomeando-se os mais importantes:

- Infraestrutura de Armazenamento (Swift).
- Infraestrutura Computacional (Nova).
- Infraestrutura de Gestão de identidades (Keystone).

Eucalyptus - este projeto aparece como resultado de uma investigação na universidade de Santa Barbara nos EUA, fazendo em 2009 o seu *spin-off* para empresa. Como empresas de apoio ao projeto temos a Dell e a Amazon Web Services. Tem uma extensa lista de clientes que a usam como plataforma, como a Nokia, Puma, Sharp, etc.

Ganeti - projeto que surgiu dos laboratórios de investigação da Google e usado atualmente como sua infraestrutura de servidores de *back-office*. Tem como principais vantagens o foco na capacidade de tolerância a falhas e estar preparada para usar equipamento de baixo custo.

Conclusão de capítulo: neste capítulo apresentaram-se os principais conceitos de computação na nuvem, modelos de serviços e tipos de implementação.

Verificamos, através de estudos já realizados por outras entidades, que existe uma relação entre o aumento de risco e a externalização do IT. Este fato confirma-se em soluções de nuvem privada versus nuvem pública, em implementações de IT tradicional versus Computação na Nuvem e, dentro desta última, com um aumento progressivo de risco à medida que caminhamos de soluções assentes em IaaS a soluções SaaS.

Verificamos também que a computação em nuvem apresenta um conjunto de valências relativamente às implementações de infraestruturas tradicionais:

- **Escalabilidade e elasticidade** por alocação rápida de recursos (processamento, armazenamento, etc.), tendo em conta a elevada capacidade financeira dos grandes service providers.
- **Redução de custos** para o cliente final, principalmente para pequenas **organizações** que se deixam de preocupar com contratação de pessoal especializado, formação, aquisição ou manutenção de instalações físicas e equipamentos, eletricidade, serviços de segurança, auditorias, etc.

- **Segurança de informação**, podendo os fornecedores contratar serviços e pessoal especializado com maior facilidade.
- **Potenciar a mobilidade e acessibilidade à informação** (ex: Teletrabalho), já que a informação se encontra normalmente acessível a partir da internet.
- **Interfaces padrão** permitindo aos técnicos maior facilidade de gestão e na contratação dos mesmos. (ENISA, 2009)

Mas também um conjunto de riscos que devem ser objeto de estudo e no qual esta tese apresenta uma metodologia:

- **Dificuldade, dependência e custos elevados** para migração dos serviços ou infraestrutura para a Nuvem ou entre fornecedores, ou mesmo de novo para próprio centro de dados.
- **Maior exposição a ataques informáticos** com eventual perda de dados ou roubo de informação (tal como as recentemente reveladas em 2013 no caso Snowden ou o caso Ashley Madison em 2015).
- Maior dependência do bom funcionamento da infraestrutura de comunicações.
- **Dificuldade de monitorizar e aplicar os termos contratuais dos SLA's** em caso de quebras de serviço, como ainda poder resolver o problema ou mesmo melhorar os serviços apresentados.
- **Aumento de custos à medida que o número de serviços** contratados aumenta, o que no longo prazo pode não ser sustentável e, principalmente, menos atrativo para grandes empresas.
- **Pouca capacidade negocial**, principalmente por parte das pequenas e médias empresas.
- **Regulamentação legislativa muito restrita** para colocação de dados pessoais ou governamentais na nuvem - principalmente na Europa pode ser um entrave à adoção da Nuvem.
- **Desconhecimento das reais capacidades do fornecedor de serviço** – desconhecimento das instalações, procedimentos de funcionamento, de segurança, de política de backups e disaster recover, testes, capacidade do pessoal especializado, etc.

- **Dificuldade de Governação** por falta de responsabilização direta sobre os dados, backups, e procedimentos, quer também por ser um novo paradigma de IT, cujos os técnicos e gestores podem não estar preparados**.**
- **Não isolamento de serviços e aplicações** potenciando que uma aplicação coloque em risco todas as restantes (por erro de programação).

Verifica-se que, existem várias formas de mitigar os riscos, como por exemplo, a implementação de CN assente em sistemas abertos, permitindo assim, assegurar uma maior facilidade de mudança de fornecedor de serviço, redução de custos pela necessidade de competitividade dos fornecedores e um maior potencial de crescimento da infraestrutura à medida das necessidades da organização. Ou então ainda, através de um fornecedor CN de grande dimensão, permitindo uma capacidade de redundância de *datacenter* ou de recursos humanos com elevado conhecimento técnico.

No entanto, a mitigação de riscos passo a passo numa solução de CN, sem uma metodologia de gestão do risco, com certeza estará destinada ao fracasso, como iremos ver no capítulo seguinte, em que tal deve ser abordada como um todo.

3

CONCEITOS de GESTÃO DO RISCO

Neste capítulo apresentamos os principais conceitos de gestão do risco. Abordaremos as várias referências de gestão do risco e, particularmente a Norma ISO 31000:2009 (ISO.org, 2013). Desde 2012 que esta norma se encontra traduzida para português, tendo tido a sua revisão em 2013 (NP ISO 31000:2013 – Gestão do Risco) e onde a partir daqui iremos referir simplesmente como norma NP ISO 31000.

3.1 – Gestão do Risco

Toda atividade humana envolve algum tipo de risco e, se realizássemos uma pergunta a vários gestores de IT sobre uma definição do que consideram como risco ou gestão do risco (GR), seria normal obtermos tantas respostas diferentes quanto o número de participantes, dado as perspetivas, as vivências de cada um e especificidade do negócio em que estão inseridos. [7] (Bjelland , 2012) .

Como definição mais abstrata de risco, podemos designar como a probabilidade de ocorrência de um determinado evento futuro aleatório [8] (Aven, 2008) e, prevísseis impactos (positivos ou negativos) num projeto, equipamento ou organização.

É normal associarmos riscos a consequências negativas, como perda de informação ou inoperacionalidade de negócio. No entanto, mais recentemente começou-se a associar que os riscos podem também assumir resultados positivos. Tomemos como exemplo, o risco de um determinado projeto terminar antes de tempo e por consequência, redução de custos. Ou

[7] Tradução livre do autor. Original*: "What is risk? If you interview ten different risk management professionals, you might end up with ten answers where some are fundamentally different from one another while others just has some small discrepancies between them."*

[8] Tradução livre do autor. Original: *"By risk we understand the combination of events and the consequences of these events, and the associated uncertainties."*

ainda, uma organização sofrer um ataque informático, nomeando-se uma equipa responsável para a situação, criando mais tarde uma área de negócio e serviços para outras organizações. Podemos assim, considerar que o risco é também uma alavanca de processos de negócio

A norma NP ISO 31000 (ISO.org, 2013) define risco como:

- "O efeito que determinada incerteza tem nos objetivos de uma organização". Onde esses efeitos podem ser de fatores ou influências internos ou externos.
- "O risco é frequentemente expresso como a combinação das consequências de um dado evento (incluindo alteração de circunstâncias) e respetiva probabilidade de ocorrência".

Em vários estudos, é usual encontrarmos exemplos de formas de cálculo de risco, como:

(i) Nível de Risco = Verosimilhança de evento * Impacto da consequência

Onde

- Verosimilhança: possibilidade de acontecer o evento de risco
- Impacto: grandeza dos danos provocados

No entanto, tal como também a Norma ISO indica, cabe à organização/equipa de gestão do risco encontrar a fórmula de cálculo de risco que melhor se adequa à sua realidade, definindo graus de probabilidade e impacto dos eventos e consequências.

Nas últimas três décadas tem havido uma modificação do conceito de gestão do risco e sua abordagem. Durante os anos 1960 e 1970, as equipas de projeto antecipavam os riscos listando os seus impactos. Entre os anos 1980 e 1990, as equipas de projeto começaram a identificar as oportunidades que surgem num projeto, em simultâneo com os seus riscos, sabendo-se que nunca se podem limitar os mesmos na sua totalidade. Isto mostra um claro ênfase no uso de oportunidades dos imprevistos ou riscos, em oposição a uma ideia em que estes somente representavam uma ameaça para a gestão de projetos.[9] (Forsberg, 2005)

[9] Tradução livre do autor. Original*: "In the last three decades, there has been a steady concept modification in risk management. During the 1960s and 1970s, project teams often forestalled risks by downgrading their impacts. Subsequently, in the 1980s and 1990s, project teams started tacking opportunities alongside risks. This shows a*

Quais os objetivos de uma eficiente política de gestão do risco?

- Proteção da organização e transmitir confiança para clientes/parceiros de negócio;
- Maior eficácia para alcançar os objetivos do negócio;
- Priorização de alocação de recursos e ações nas áreas internas/negócio para o bom e contínuo funcionamento da organização;
- Redução de perdas e aumento da capacidade para tirar benefício das oportunidades que surgem.

Os principais desafios para uma eficiente gestão do risco:

- Uma clara identificação do risco;
- Definição de uma estratégia (para gestão do risco);
- Consciencializar a organização da importância de criação de documentação e processos de gestão do risco.

Embora seja normal cada profissional seguir os seus processos internos para gestão do risco, mediante a sua visão do que é necessário e experiência. Este caminho é perigoso, já que não aborda o problema de uma forma sistematizada e é normalmente falível, já que o conhecimento pessoal é sempre menor do que o conhecimento coletivo.

De forma a colmatar o evidenciado atrás, convém que a grande variedade de riscos que uma empresa se encontra exposta e o seu IT, sejam vistos à luz de uma política de gestão do risco bem delineada e mais global. A GR é vista como uma pedra angular de uma boa governação corporativa e, portanto, resulta numa melhor prestação de serviços, utilização mais eficiente e eficaz dos escassos recursos, melhor gestão e controlo de projetos [10] (Collier, 2007).

De acordo com Dorfman, a gestão do risco é o desenvolvimento lógico e implementação de um plano para lidar com potenciais perdas. É importante que uma organização implemente programas de GR, de modo a gerir a sua exposição aos riscos, bem como proteger os seus

[10] Tradução livre do autor. Original: *"Risk management is viewed as a corner stone of good corporate governance and therefore results in better service delivery, more efficient and effective use of scarce resources and better project management."*

ativos. Dorfman afirma que a gestão do risco é uma estratégia de gestão pré-perda para recursos pré-perda [11] (Dorfman, 2007).

Sendo difícil de gerir todos os riscos envolvidos numa empresa, é fundamental a aplicação de métodos e processos para a mitigação dos mesmos, ou seja, a utilização de *framework* de gestão de risco.

Podemos assim, definir *Framework* de Gestão do Risco como um conjunto de diretivas, com regras de identificação de riscos, sua avaliação, controlo, monitorização e responsabilização direta de resolução dos mesmos. Cria também uma linguagem universal de entendimento entre todos os interessados [12] (COSO.ORG).

Em 2003, foi introduzida por Chapman and Ward (Wiley, Chapman C. and Ward S., 2003) a *framework* 6Ws. Esta tem como mais valias ser simples e de fácil aplicação à gestão do risco. Esta é contruída à base de um conjunto de questões base permitindo construir-se um conhecimento do que fazer, quem, quando, etc.

Tabela 2 - Estrutura 6Ws

W's	Questões	Tradução
Who	Quem vai estar envolvido	Quem está interessado
Why	Porque é que se pretende atingir aquele objetivo	Motivo
What	No que se pretende	O quê
Whichway	Que decisões serão tomadas	Decisões e atividades
Wherewithal	Que recursos necessários alocar	Recursos
When (quando)	Até quando tem de ser implementado	Quando

[11] Tradução livre do autor. Original:" Risk *management is the logical development and implementation of a plan to deal with potential losses. It is important for an organization to put in place risk management programmes so as to manage its exposure to risks as well as protect its assets."*

[12] http://www.coso.org/documents/ERM-FAQs.pdf

Até aos dias de hoje, têm sido inúmeras as organizações que se têm dedicado à criação de normas de GR. Iremos à frente referir algumas das mais importantes.

3.2 – Referências ISO em Gestão do Risco

ISO 31000 (ISO.org, 2013) - um passo em direção ao consenso no seio das *frameworks* de gestão de risco foi realizado pela International Organization for Standardization (ISO). A Norma NP ISO 31000 foi elaborada por um grupo de trabalho que incluía 18 peritos de países diferentes. Ao longo de vários anos, este grupo reviu a norma de gestão do risco da Austrália/Nova Zelândia AS/NZS 4360:2004 (Australian/New Zealand Standard, 2004), criando uma nova norma, que pode ser usado por qualquer organização, independente do país, nos mais diversos setores empresariais e independentemente da sua dimensão.

A Norma NP ISO 31000 (ISO.org, 2013), tendo em conta a sua transversalidade e simplicidade é hoje uma das principais *frameworks* de gestão do risco e a qual esta tese tem como referência. Esta Norma estabelece os princípios de gestão do risco, permitindo que com maior facilidade as empresas criem processos de identificação de riscos e elaborem processos de controlo dos mesmos. Agregada a esta norma temos um conjunto de diretivas.

ISO Guide 73 (ISO, ISO Guide 73 - Risk management - Vocabulary, 2009) – Fornece as definições de termos genéricos relacionados com a gestão do risco.

Os termos tratados estão agrupados da seguinte forma:

- Termos relativos ao risco;
- Termos relativos à gestão do risco;
- Termos relativos ao processo de gestão do risco;
- Termos relativos a comunicação e consulta;
- Termos relativos ao contexto;
- Termos relativo à avaliação de risco;
- Termos relativos a identificação do risco;
- Termos relativos à análise do risco;
- Termos relativos a avaliação do risco;
- Termos relativos ao tratamento do risco;
- Termos relativos à monitorização e medição.

Este Guia destina-se a incentivar a compreensão mútua e consistente entre os vários *stakeholders*:

- Técnicos envolvidos na gestão do risco;
- Responsáveis envolvidos em atividades de ISO;
- Responsáveis pelo desenvolvimento de Normas, manuais, procedimentos e códigos de práticas nacionais ou sectoriais relacionadas com a gestão do risco.

ISO/IEC 31010 (ISO, ISO 31010 - Risk management - Risk assessment techniques, 2009) – Auxilia as organizações na implementação dos princípios e diretrizes da Norma ISO 31000. Contém um conjunto de técnicas de avaliação do risco, onde se faz a identificação de riscos, suas ocorrências, probabilidades e como mitigar os mesmos.

ISO 31004 (ISO, ISO 31004 - Risk management - Guidance for the implementation of ISO 31000, 2013) – Esta diretiva fornece linhas orientadoras para que às organizações consigam implementar de uma forma eficaz a Norma ISO 31000 e seus mecanismos de gestão do risco.

Outras Normas também importantes para uma gestão do risco de Computação em Nuvem temos a **Norma ISO 27001** (ISO, ISO 27001 - Information security management, 2013)**,** referência mundial para a identificação de riscos de segurança da informação e implementação de controlos

A **Norma ISO/IEC 27018:2014** (ISO, Information technology - Security techniques - Code of practice for protection of personally identifiable information in public clouds, 2014) é mais recente e foi criada especificamente para a Computação em Nuvem. Sendo menos abrangente que a Norma ISO 31000, permite que os fornecedores de serviço possam identificar e avaliar riscos como ainda implementação de controlos para a proteção dos dados pessoais armazenados na nuvem.

3.3 – Técnicas em análise de risco

De acordo com a ISO 31010 (ISO, ISO 31010 - Risk management - Risk assessment techniques, 2009), para identificação de riscos e seu grau de impacto existem métodos qualitativos e quantitativos.

- **Técnicas qualitativas de análise de riscos** são relevantes para "[...] priorização dos riscos para posterior análise ou ação adicional, através da avaliação e combinação de sua probabilidade de ocorrência e o seu impacto". [13] (PMBOK, 2004)
- **Técnicas quantitativas de análise de riscos** são relevantes para "[...] analisar numericamente o efeito dos riscos identificados sobre os objetivos gerais". [14] (PMBOK, 2004). Os impactos serão calculados perante dados recolhidos e posteriormente será gerado um ranking total dos riscos, seus impactos e probabilidades.

Técnicas qualitativas

- Recolha documental: recolha de informação em revistas, livros, artigos académicos sobre riscos;
- Brainstorming: reunião multidisciplinar de um conjunto de especialistas debatendo e gerando ideias sobre os riscos e como mitigar os mesmos. Aconselha-se que a reunião seja realizada com um número de elementos entre os 10 e os 15. A duração não deve exceder as 2 horas por reunião e pode ser alicerçada com mais do que um encontro;
- Técnica Delphi: distribuição de um questionário a um conjunto de especialistas na matéria. As respostas devem ser anónimas. Esta técnica tem algumas semelhanças com a técnica brainstorming, no entanto, apresenta a vantagem de ser utilizada quando os participantes se encontram dispersos geograficamente. Além disso, permite que não exista um elemento que domine a discussão, tal como pode acontecer na técnica de Brainstorming;
- Crawford slip: é usado para recolher ideias de um número elevado de pessoas (grupos de 50 a 200 pessoas). Cada indivíduo escreve ou desenha a sua opinião num post-it para que outros comentem a sua relevância. As perguntas podem ser várias vezes repetidas de modo a obrigar os participantes a pensarem em diversas soluções. Como vantagem: desbloqueia pensamento coletivo e a opinião de cada membro da equipa;
- Entrevistas a especialistas: identificação de riscos através das experiencias dos participantes.

---

[13] Tradução livre do autor. Original: *"prioritizing risks for further analysis or further action by assessing and combining their probability of occurrence and their impact."*

[14] Tradução livre do autor. Original: *"numerically analyzing the effect of identified risks on overall project objectives"*

- Analogia: ter em conta projetos semelhantes de outras organizações semelhantes a nível de caraterísticas;
- SWOT Analysis – análise através de uma descrição das forças, fraquezas, oportunidades e ameaças;
- Técnicas de diagramas: os diagramas de causa e efeito ou diagramas de fluxo de processos são também uma das ferramentas utilizadas para a identificação de riscos;
- Matriz de impacto e probabilidades: tem como finalidade comunicar aos vários stakeholders, de uma forma visual e simples a severidade dos riscos e quais devem ser prioritários de resolução. Esta tabela é construída através de uma combinação de valores de probabilidade e impacto;
- Técnica nominal de grupo: reunião com menos de 10 pessoas, que escrevem individualmente as suas ideias. O moderador recolhe a informação e coloca-a exposta, sem identificar a sua origem. Este método tem a vantagem de ultrapassar alguma inibição ou dificuldade de participação de algumas pessoas.

Técnicas quantitativas

- Registo de risco (Risk Register): lista de riscos identificados pela organização, seus impactos e probabilidades. Podem ainda ser identificado políticas de minimização de riscos e controlos;
- Análise de sensibilidade – ajuda a determinar qual o risco que tem um maior impacto no objetivo do projeto, examinando o impacto que de cada elemento e o seu resultado no âmbito do projeto;
- Método de caminho critico (Critical Path Method): determinação de qual o caminho que menos riscos apresenta;
- Análise do valor monetário esperado (Expected monetary value EMV) – é um conceito estatístico que calcula a média do resultado. O EMV é um resultado ponderado pela probabilidade de ocorrência. EMV de oportunidades são atribuídos valores positivos, aos EMV de riscos são atribuídos valores negativos;
- Árvore de decisão: consiste na representação através de diagramas de uma determinada situação, em que cada uma das opções ou cenários possíveis é representado como um ramo do diagrama, sendo calculado o respetivo custo e

probabilidade de ocorrência. A quantificação final da árvore de decisão permite atribuir valores aos diferentes cenários para comparação;

- Análise Monte Carlo - é uma técnica que envolve utilização de números aleatórios e probabilidade para a resolução de problemas. A simulação Monte Carlo é um método de avaliação interativa. A sua grande vantagem é a de determinar como uma variação aleatória conhecida, ou como o erro, afetam o desempenho ou a viabilidade do sistema que está a ser analisado.

Principais caraterísticas da NP ISO 31000 (ISO.org, 2013)

- De fácil entendimento e implementação;
- Abordagem pró-ativa, em vez de uma abordagem de conformidade;
- Implementação top-down;
- Cria uma relação entre riscos e estratégia da empresa;
- Endereça ambos os lados do risco (negativos e positivos);
- Fornece uma abordagem consistente, que pode ser adaptada a qualquer tipo de setor empresarial;
- Permite uma fácil comunicação entre os vários stakeholders, usando termos conhecidos na GR;
- Permite que através de uma checklist se minimize situações de falha de algum elemento;
- Não tem certificação associada.

O que esta Norma potencia para a organização:

- Ações de gestão pró-activa ao invés de ações reactivas;
- Melhorar a governação e gestão da organização;
- Melhorar operacionalização de gestão de incidentes;
- Melhorar a identificação de oportunidades e riscos;
- Alinhamento com diretivas internacionais;
- Melhorar a alocação de recursos para o tratamento de riscos;
- Melhorar a confiança dos Stakeholders.
- Potenciar a implementação de controlos de minimização de riscos.

Princípios de Gestão do Risco NP ISO 31000 (ISO.org, 2013)

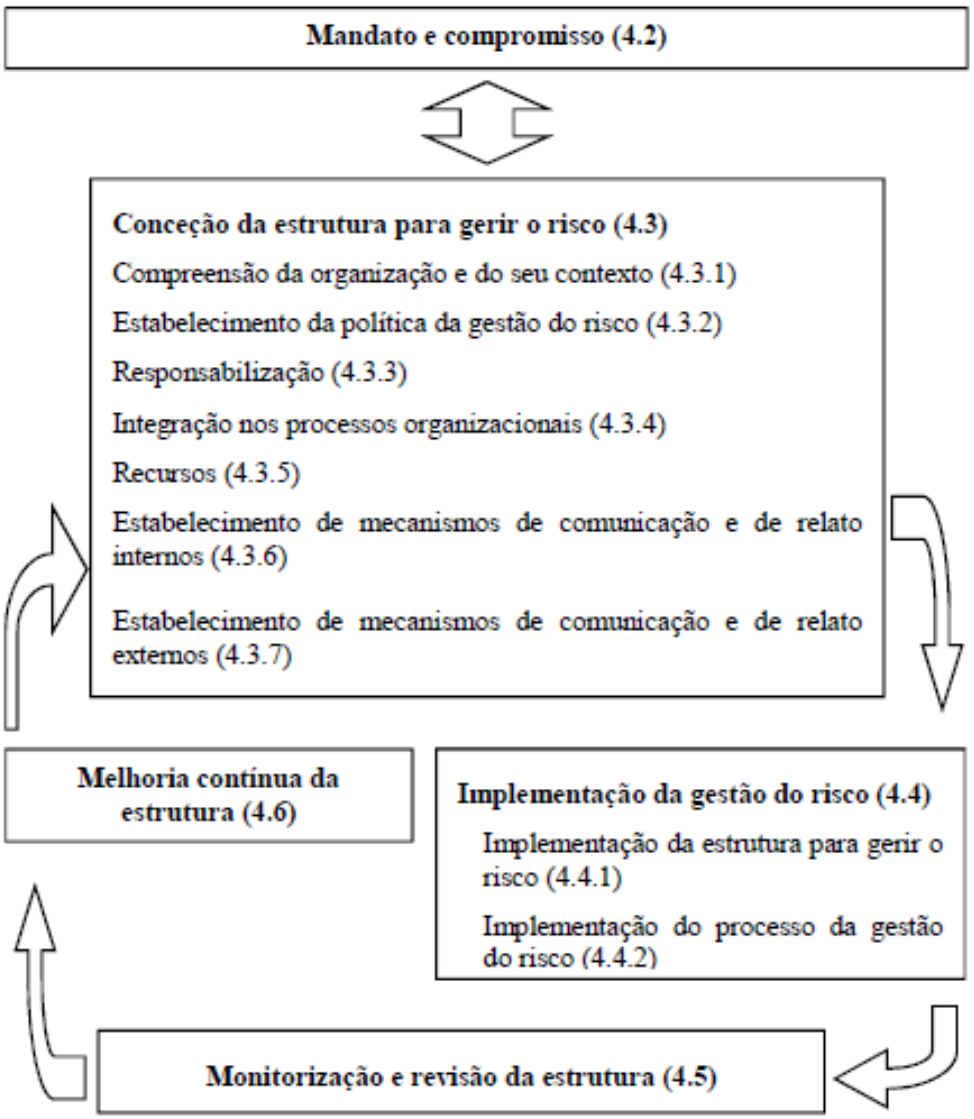


Figura 10 - Dependência e interligação entre os vários componentes da Estrutura Gestão do Risco *(ISO.org, 2013).*

Figura 11 - Processo de Gestão do Risco *(ISO.org, 2013)*

De seguida e de uma forma resumida, explicam-se as fases mencionadas pelas figuras atrás - diagrama de processos de gestão do risco NP ISO 31000 e interligação de componentes (ISO.org, 2013), essenciais para uma que a informação sobre riscos seja adequadamente reportada e utilizada como base para a tomada de decisões (ISO.org, 2013).

Mandato e compromisso (4.2) – Esta etapa é uma das mais importantes na gestão do risco. É imperativo que exista um compromisso entre todos os *stakeholders* da organização, em particular a gestão de topo. Só desta forma se poderá atingir os objetivos de mitigar riscos que determinada organização enfrenta. Idealmente, a equipa que ficar responsável pela gestão do risco, deverá reportar diretamente à gestão de topo da organização, de forma que não fique dependente de outras áreas que poderão estar focadas noutros objetivos. A gestão de topo deve demonstrar a toda a organização o seu total empenho nesta matéria, disponibilizando todos os recursos humanos e financeiros possíveis para o objetivo estipulado.

Fica patente num estudo realizado pela KPMG (KPMG-IPQ, 2013) (ver fig. 14), que o principal fator-chave para o sucesso de uma GR, é existir o apoio e o compromisso por parte da gestão de topo.

Figura 12 - Principais fatores-chave para o desenvolvimento da prática de gestão do risco das empresas (%) *(KPMG-IPQ, 2013)*

Além disso, nesta etapa devem-se definir indicadores de desempenho da gestão do risco, alinhar objetivos com os objetivos da organização, atribuir responsabilidades e assegurar recursos necessários.

Conceção de estrutura para gerir o risco (4.3), processo constituído pelas seguintes etapas:

- Perceber o que é a organização e a sua envolvência;
- Políticas de gestão do risco;
- Responsabilização;
- Integração da gestão nos processos organizacionais;
- Prestar contas e comunicação;
- Recursos.

Implementação da gestão do risco (4.4) é constituído pelas seguintes fases:

- Implementação de uma estrutura para gerir o risco;
- Implementação de processo da gestão do risco.

Monitorização e revisão da estrutura (Framework) (4.5): entende-se como verificar continuamente e observar de forma crítica os controlos aplicados e se os novos resultados estão dentro dos níveis que se pretendem atingir. Devem-se definir as periodicidades (que nunca devem ser superiores a um ano), e meios técnicos e humanos para a boa concretização deste processo.

Assim, esta etapa deve:

- Medir o desempenho da gestão do risco;
- Medir periodicamente o progresso e os desvios em relação ao plano da gestão do risco;
- Rever periodicamente se a estrutura, política e o plano da gestão do risco continuam atualizados;
- Elaborar relatórios sobre o risco;
- Rever a eficácia da estrutura da gestão do risco.

Melhoria contínua da Estrutura (4.6): a gestão do risco deve ser encarada numa perspetiva de melhoria. Iniciando-se com o passo de *design* da estrutura, implementação de GR, monitorização, melhorias à solução e de novo para a primeira etapa. De forma macro Plan - Do – Check – Act (Planear – Fazer – Verificar – Agir).

Comunicação e consulta (5.2): processos iterativos que uma organização realiza para partilhar e obter informação com as partes interessadas (*stakeholders*) sobre os desenvolvimentos da gestão do risco.

Nesta componente deve ficar assegurado:

- Estabelecer o contexto de forma apropriada;
- Os interesses de todos os stakeholders;
- Os riscos são identificados de forma clara;
- Reunir especialistas para análise dos riscos;
- Apoio ao plano de tratamento do risco;
- Desenvolver um plano de comunicação aos stakeholders.

Estabelecimento de contexto (5.3): definição dos parâmetros externos e internos a serem tidos em conta na gestão do risco, através de uma definição de âmbito e critério de risco [15] (ISO.org, 2013)

Contexto interno - ambiente interno no qual a organização pretende atingir os seus objetivos e onde resumidamente deverá ter em conta:

- Políticas e estratégias;
- Capacidade e conhecimento da organização (recursos humanos, tecnologia, capital financeiro, etc.);
- Cultura da organização;
- Sistemas de informação, sua disponibilidade, penetração nos processos.

Contexto externo - ambiente externo no qual a organização pretende atingir os seus objetivos e onde resumidamente deverá ter em conta:

- Como a organização se integra num ambiente social e cultural, político, legal, regulamentar, financeiro, tecnológico, económico, etc.;
- Tendências que podem ter impacto nos objetivos;

[15] Tradução livre do autor. Original: *"defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (3.3.1.3) for the risk **management policy** (2.1.2)"*

- Stakeholders, suas inter-relações e valores.

Apreciação do Risco (5.4): processo usado para entender a natureza ou eventos dos riscos identificados e para estimar a sua severidade. É também utilizado para estudar as consequências e controlos a implementar.

> **Identificação do Risco (5.4.2)**: a primeira fase é a identificação dos riscos que possam interromper ou prejudicar o desenvolvimento do negócio [16] (Napp, Master Thesys - Financial Risk Management in SME, 2011). Também inclui a identificação das potenciais consequências. Para esta identificação é normal usarem-se processos de recolha de dados na organização e fora dela, análise teórica, opiniões, inquéritos, conselhos de especialistas e as partes interessadas.
>
> **Análise do risco (5.4.3):** o objetivo da avaliação de risco é determinar o grau de severidade do risco e quantificar o seu impacto na organização e verosimilhanças de acontecerem. No entanto, uma quantificação do impacto é na maioria dos casos impossível, já que os resultados futuros são incertos, por isso normalmente recorrem-se a estimativas. Ambos os métodos quantitativos e qualitativos podem ser utilizados para estas estimativas. Ao utilizarem-se métodos qualitativos, a frequência e o impacto dos riscos são avaliados com base na experiência e avaliação dos gestores da empresa e funcionários. (Napp, Master Thesys - Financial Risk Management in SME, 2011, p. 10)
>
> **Avaliação do risco (5.4.4):** o objetivo da avaliação de risco serve de apoio à tomada de decisão após os resultados da análise de risco. Nesta fase, deve ser feita a análise do nível de risco identificado com os critérios definidos inicialmente.

A Organização deve definir:

- Nível de aceitação de risco: até que ponto uma organização aceita o risco. Por vezes, sabendo-se da existência de um risco, o mesmo pode não ter efeitos importantes na manutenção do negócio e por isso aceita-se que o mesmo possa ocorrer;

[16] Tradução livre do autor. Original: *"The aim of this phase to identify all risks, which could interrupt or damage the business development"*

- Redução de exposição: se os novos controlos permitem diminuir a exposição à vulnerabilidade ou risco;
- Transferência do risco: estratégias para gerir riscos tipicamente incluem transferência do risco para outra entidade mais avalizada para o tratamento do mesmo.

Tratamento do Risco (5.5): implementação de políticas e controlos no intuito de diminuição de riscos que a organização e o IT estão expostos Ações estas, que podem passar por simplesmente terminar ou mudar a atividade (ou origem) que implica o risco, partilha de risco com outras entidades, aumentar o risco que possa potenciar oportunidades, simplesmente identificá-lo, mudar a sua ocorrência ou probabilidade. (ISO.org, 2013).

Monitorização e revisão do risco (5.6): na última fase do processo de gestão do risco deve-se ir avaliando controlos implementados e se estes estão a atingir as metas estipuladas. Nesta fase devem já estar perfeitamente definidas as responsabilidades pela monitorização e revisão.

Nesta fase tem-se como objetivos:

- Assegurar que os controlos são eficazes e eficientes;
- Identificar riscos emergentes;
- Detetar alterações de contexto, incluídos critérios de risco;
- Alicerçar conhecimento sobre os vários eventos e consequências.

Registo do processo da gestão do risco (5.7): Através do registo de todos os acontecimentos relativos à gestão do risco permite que no futuro se possam melhorar e adequar com mais precisão os métodos e ferramentas.

Conclusão de capítulo: resultante de uma pesquisa bibliográfica do assunto e estudos de diversas organizações apresentaram-se os principais conceitos e *frameworks* de gestão do risco.

Explicamos a escolha da norma NP ISO 31000 (ISO.org, 2013) para o trabalho a desenvolver nos próximos capítulos:

- Genérica, com linhas de orientação gerais para gestão do risco;
- Pode ser aplicada em qualquer tipo de organização;
- Pode ser aplicada em qualquer tipo de setor;
- Pode ser aplicada em qualquer tipo de risco (positivo ou negativo);
- De fácil entendimento e implementação;
- Abordagem pró-ativa, em vez de uma abordagem de conformidade;
- Implementação top-down;
- Cria uma relação entre riscos e estratégia da empresa;
- Endereça ambos os lados do risco (negativos e positivos);
- Fornece uma abordagem consistente que pode ser adaptada a qualquer tipo de setor empresarial;
- Permite uma fácil comunicação entre os vários stakeholders, usando termos conhecidos na GR;
- Permite que através de checklist se minimize situações de falha de algum elemento.

A norma NP ISO 31000 (ISO.org, 2013) permite aos responsáveis pela gestão do risco, poderem responder de uma forma eficaz e eficiente aos riscos que uma organização se encontra exposta.

Aborda-se ainda os conceitos de modelos de domínio de gestão do risco e registo de risco. Descreve-se sumariamente o que o registo de risco deve contemplar, tendo em conta a Norma ISO.

4

PROPOSTA de MODELO

de REGISTO DE RISCO

Este capítulo é constituído por quatro secções. Na primeira, apresentamos conceitos de Modelos de Domínio e na segunda secção, uma proposta de modelo de domínio de gestão do risco para cenários de computação em nuvem. A terceira secção, exploramos conceitos de Registo de Risco tendo como base a Norma NP 31000 (ISO.org, 2013).

4.1 - Conceitos do Modelo de Domínio

À medida que a complexidade dos sistemas tende a ser elevada, um Modelo facilita a decomposição dos cenários em partes menores, i.e., cenários menores que podem ser geridos e tratados mais facilmente. (Ackermann, 2012, p. 86) [17].

O uso de modelos tem um conjunto de benefícios:

- Facilitador de decisão, aumentando a eficiência pelo fato de reduzir tempo de análise;
- A decisão torna-se mais objetiva, já que se parte do princípio que os resultados serão iguais perante as mesmas circunstâncias;
- Permitir sintetizar problemas complexos. (Management Solutions, 2014).

É, no entanto,

- Necessário ter em atenção que podem surgir problemas pelo uso de modelos não adequados ao problema em estudo. (Management Solutions, 2014)

17 http://www.asecib.ase.ro/cc/carti/IT%20Security%20Risk%20Management%20in%20the%20Context%20of%20Cloud%20Computing%20[2013].pdf obtido em Out/2015

Um modelo de domínio de gestão de risco deve permitir-nos, de uma forma simples e concisa, mostrar aos vários *stakeholders* os componentes de interação, e ativos que se querem proteger ou objetivos a atingir.[18]

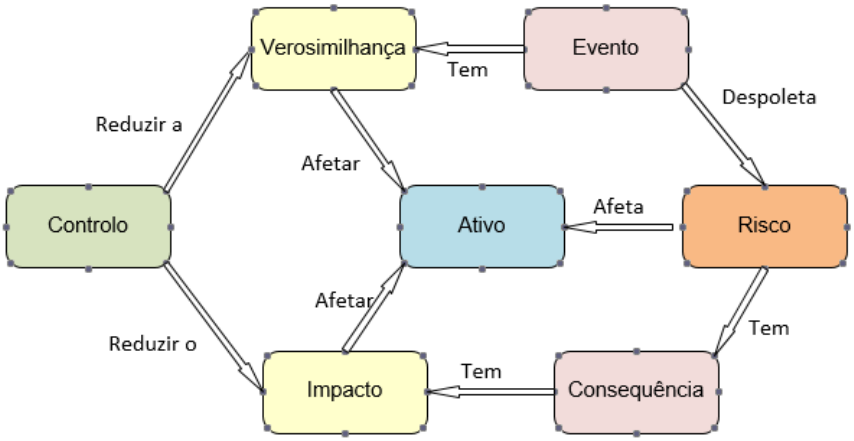


Figura 13 - Conceitos de risco gerais e sua interligação

Para melhor entendimento, tal processo deve ser acompanhado da descrição de conceitos, e no nosso caso específico de gestão do risco, estes são expostos abaixo:

Ativo – Entidade ou equipamento com um determinado valor (qualitativo ou quantitativo) que se pretende proteger no contexto de uma GR. Os ativos de uma organização estão sujeitos a eventos, gerando na maioria das vezes consequências que deverão ser minimizadas ou mesmo eliminadas. O **Ativo** pode ter um valor tangível (quantitativo - valor financeiro) ou intangível (qualitativo - imagem de marca, confiança).

Evento (ou Causa): de acordo com a Norma NP ISO 31000 (ISO.org, 2013), um evento pode ser uma ocorrência, várias ocorrências, ou mesmo uma não ocorrência (quando algo que devia acontecer e não ocorreu). Também podemos considerar que um evento pode ser uma alteração das circunstâncias. Os eventos são por vezes referidos como causas, incidentes ou acidentes que despoletam uma consequência.

18 http://www.asecib.ase.ro/cc/carti/IT%20Security%20Risk%20Management%20in%20the%20Context%20of%20Cloud%20Computing%20[2013].pdf obtido em Out/2015.

Risco: encontra-se presente em todos os níveis de operação de uma organização, podendo-se tipificar normalmente em duas grandes áreas – de negócio ou operacional. (Ashenden, 2005)

De acordo com a Norma NP ISO 31000 (ISO.org, 2013), o risco é o "efeito da incerteza sobre os objetivos definidos". Esse efeito pode ter desvios positivos, negativos ou por vezes ambas as situações.

Controlo: um controlo é qualquer medida ou ação que modifique o risco. Destes podemos incluir qualquer política, procedimentos, práticas, processos, tecnologia, técnica, método ou dispositivo que modifique ou faça gestão do risco.

Redução de verosimilhança de evento (Controlo) – Medidas que podem minimizar ou eliminar nos ativos os efeitos dos eventos de risco.

Consequência (Efeito ou impacto): uma consequência é o resultado que um evento tem sobre os ativos ou objetivos da organização. Um único evento pode gerar um ou uma série de consequências, que por sua vez podem ter efeitos positivos e negativos sobre os objetivos e a que se podem associar valores tangíveis ou intangíveis.

As consequências iniciais podem gerar por efeito de arrastamento um conjunto de outras consequências. (ISO.org, 2013). O impacto pode ser delineado numa escala linear ou em termos exponenciais, considerando-se esta última abordagem a mais realista e aconselhada.

Redução de impacto de uma consequência (Controlo): Medidas que podem minimizar o impacto que determinados riscos causaram.

Os controlos devem ser monitorizados por auditores, sendo aconselhável que se crie uma área autónoma e dependente somente da direção máxima da organização.

Vulnerabilidade: falha que expõe o Ativo a eventos de risco. O objetivo de todas as normas de gestão do risco é de criar processos de modo a minimizar os níveis de vulnerabilidade de um determinado sistema, de modo a mais facilmente se atingirem os objetivos da organização.

Verosimilhança (ou Probabilidade): é a possibilidade que algo possa acontecer. Pode ser medida de forma objetiva ou subjetiva e expressa de modo qualitativo (por exemplo por escalas – baixa, média, alta) ou quantitativo através de fórmulas matemáticas (NP ISO 31000).

O termo correto de uso é verosimilhança já que é o termo português mais próximo do inglês "*likelihood*"

Qual o **Objetivo:** o que se pretende proteger ou atingir. Normalmente está associado à visão e missão de uma organização. Por exemplo, manter a empresa como uma referência de credibilidade e valor para com os seus clientes. Para isso, deverão controlar-se os riscos de perda de informação e manutenção do negócio.

4.2 - Modelo de domínio Gestão do Risco em Computação em Nuvem.

Com cada vez mais organizações a adotarem a tecnologia Computação em Nuvem, o número elevado de fornecedores e serviços com diferentes abordagens de implementação colocam em evidência incertezas e riscos que é necessário equacionar por parte dos seus clientes.

No caso em concreto, sugere-se um modelo com base na Norma NP ISO 31000 (ISO.org, 2013), mais geral e de fácil entendimento, que permite às organizações determinar potenciais riscos da implementação de soluções CN, com identificação de eventos, ativos, consequências e possíveis controlos.

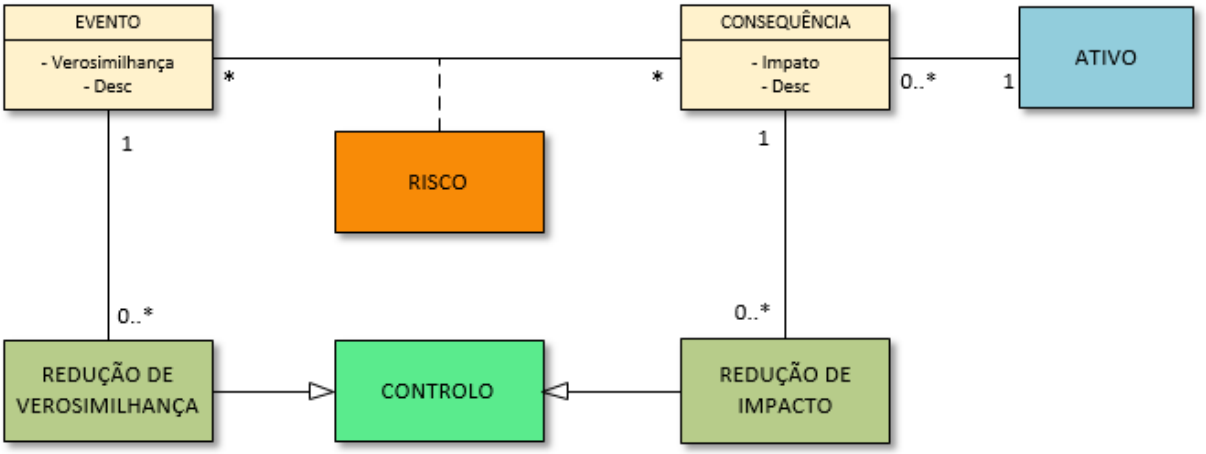


Figura 14 - Modelo de domínio Gestão do Risco em Computação em Nuvem

O modelo proposto permite contextualizar na maioria das situações, os problemas e riscos de adoção de Computação em Nuvem, encontramos os seguintes conceitos:

- Ativo;
- Evento;
- Consequência;

- Risco;
- Controlo de verosimilhança;
- Controlo de Impacto.

Sendo o foco desta tese, o processo de análise do risco em CN, interessa-nos “desenvolver a compreensão do risco” (ISO.org, 2013). Para tal, temos de entender as fontes do risco (eventos), suas consequências para a organização e como estas afetam os ativos e objetivos. Também referido na Norma “A análise de risco pode também fornecer uma entrada para tomada de decisões” (ISO.org, 2013) ou seja, perante a análise de risco a organização fica mais documentada do que a pode afetar, de como mitigar risco, permitindo a todos os *stakeholders* proactivamente criar as condições para melhor atingirem os objetivos.

Segundo a (ISO.org, 2013) “as consequências e a sua verosimilhança podem ser determinadas pela modelação dos resultados de um evento ou conjunto de eventos...”, onde para tal se torna essencial esquematizar essa inter-relação.

No caso particular do nosso estudo, podemos descrever o modelo exposto na figura 14 (tendo em conta a ótica de adoção de serviços Computação em Nuvem) que determinados **Ativos** da organização pelas suas **Vulnerabilidades**, ficam expostos à **verosimilhança** (**probabilidade)** de existirem **eventos (causas)** passiveis de causar **Riscos**. Como resultado dos Riscos, o Ativo sofre um conjunto de **Consequências** que poderão ser quantificáveis em níveis de **impacto**.

Um Ativo, no caso particular de um contexto Computação em Nuvem, está normalmente **exposto a vários eventos** (ex: ataques informáticos, mudanças legislativas de privacidade de dados, etc.). Verificamos que **um evento**, normalmente **despoleta uma consequência** (ex: inatividade da organização, inconsistência de dados, etc.).

Os controlos (Redução de verosimilhança de eventos de riscos e Redução de impacto de consequência) vão permitir **minimizar a probabilidade** ou **impacto dos eventos**, resultando num conjunto de ações de controlo, monitorização e melhoria. Os controlos fazem parte do processo de tratamento do risco (Norma NP ISO 31000 – 5.5) e que não iremos aprofundar nesta tese, sendo que nos remetemos essencialmente ao aspeto de análise do risco.

4.3 – Conceitos de Registo de Risco

Registo de risco (em inglês *Risk Register*) é uma atividade fundamental para documentar todos os tipos de risco e suas implicações. Permite além de gestão do risco, o armazenamento e comunicação de informações entre partes interessadas (*stackholders*) de uma forma concisa e consistente [19] (Kohout, 2013)

Devemos considerar um Registo de Risco, como uma base de dados, tendo informação pertinente e detalhada para cada tipo de risco que uma organização pode enfrentar.

É normalmente caraterizada:

- Informação do responsável pelo tratamento do risco;
- Informação e detalhes do cenário de risco;
- Informação do resultado da análise de risco;
- Informação de tratamento do risco e seu estado;
- Informação de controlos aplicados ou políticas (caso aplicável) (Meadows, 2009).

Um registo de risco deve ter em conta os seguintes princípios:

- Útil: deverá conter só informação relevante para os stakeholders na descrição dos riscos.
- Conciso: a informação não deverá conter termos técnicos ou ambíguos.
- Simples: de fácil entendimento para as partes interessadas na organização.
- Em tempo: deverá estar ao dispor dos stakeholders de modo que estes possam tomar as ações corretivas a tempo.
- Disponível: deverá estar sempre acessível às partes interessadas a qualquer instante.
- Audiência: deverá ter em conta o conhecimento das partes interessadas (gestores) e os técnicos que vão implementar os procedimentos.

[19] Tradução livre do autor. Original*: "Risk register is a key part of documenting any risk analysis e effort and one of the most important supporting tools of risk management, enabling storage and communication of information in a relevant, consistent and concise manner."*

No seguimento das diretivas da Norma NP ISO 31000 (ISO.org, 2013), e de uma forma generalista é necessário (Barateiro, 2012) o registo de identificação de riscos e ações que se descrevem abaixo:

Tabela 3 - Atividade; Descrição de conceitos de domínio

Atividade	**Descrição dos conceitos de domínio**
Identificação de Risco (5.4.2)	Identificação de Ativos, Vulnerabilidade, Eventos de risco (eventos) e riscos (por combinação dos fatores anteriores)
Análise de risco (5.4.3)	Identificação dos valores: dos ativos; da exposição das vulnerabilidades, verosimilhança dos eventos e impactos das consequências
Avaliação do risco (5.4.4)	Comparação da severidade do risco de acordo com os critérios estabelecidos
Tratamento do Risco (5.5)	Medidas ou controlos possíveis para redução dos riscos (verosimilhança e impactos)

- Numa **Análise de Risco (5.4.3**) é normal associar os seguintes domínios de valores tendo em conta uma escala de análise qualitativa normalmente retirada de conjunto de questões realizada a peritos na matéria (ex: Método Delphi - Questionário).
- É normal associar-se a valores de impactos a escala exponencial de modo a melhor refletir a realidade e a necessidade de maior visibilidade para situações críticas que necessitam de maior atenção.

Tabela 4 - Exemplo de valores

Tipo	**Valor**
Valor Ativo	1 - muito baixo, 2 - baixo, 3 - médio, 4 alto, 5 - muito alto
Verosimilhança de evento de risco	Valor 0 (mín) a 1 (max)
Impacto da consequência	Valor de 1 (mín) a 40 (max)

Na aplicação prática de um registo de risco é usual uma abordagem de métodos qualitativos e quantitativos, sendo, no entanto, sempre que possível a utilização preferencial deste último de forma a diminuir a subjetividade de resultados.

4.4 - Aplicação de Registo de Risco

Tal como referido pela Norma NP ISO 31000 (ISO.org, 2013) “todas as atividades de gestão de riscos deverão ser rastreáveis”. Assim, em cada etapa devera-se registar-se toda a informação importante para uma eficaz gestão de risco em computação em nuvem.

No caso, em estudo seguiremos os seguintes passos:

1. Definição do contexto (5.3): definição dos parâmetros externos e internos da organização.
    a. O ambiente externo e interno da organização (políticas, cultura, etc)
    b. Estratégia TI: modelo de serviço de Computação em Nuvem (IaaS, SaaS, etc.); Escolha do modelo de implementação (Nuvem privada, pública, etc.).
    c. Capacidade e conhecimento dos recursos internos da organização e do fornecedor de serviço CN.
    d. Identificação dos Ativos da organização:
        1. Identificação do Ativo (ex: dados, recursos humanos, etc)
        2. Descrição
2. Apreciação do Risco (5.4)
    a. Identificação dos Riscos (5.4.2) que esses ativos estão expostos numa mudança para Cloud.
        i. Identificação dos eventos ou causas que poderão provocar os riscos nos ativos referidos (ex: ataque informático, etc.)
            1. Evento
            2. Descrição
        ii. Identificação das consequências de cada risco (ex: perda de informação, etc).
            1. Consequência
            2. Descrição
        iii. Identificação dos riscos:

1. Risco
2. Descrição

b. Análise do Risco (5.4.3)
    i. Cálculo do valor do ativo (ex: dados informáticos - valor alto).
    ii. Identificação da probabilidade do evento (ex: baixa, média, etc).
    iii. Identificação do Impacto da consequência (ex: baixa, média, etc).
    iv. Cálculo do nível de risco (ex: Impacto*Verosimilhança).
c. Avaliação do Risco (5.4.4)
    i. Comparação dos resultados da análise do risco com os critérios do risco para determinar se o risco e/ou a respetiva magnitude é aceitável

3. Comunicação e consulta (5.2)
    a. A inserção dos dados em excel ou numa na aplicação de gestão do risco (ex: das diversas existentes no mercado), poderão gerar relatórios fundamentais para uma efetiva comunicação.
    b. Análise dos resultados e sua comunicação.
4. Tratamento do Risco (5.5)
    a. Identificação dos controlos para minimizar a probabilidade da ocorrência desses eventos.
    b. Identificação dos controlos para minimizar o Impacto dos riscos.
    c. Identificação do responsável para tratamento do risco
5. Monitorização e revisão (5.6) indicando-se a periodicidade, responsáveis e meios.

Como vemos, o processo de registo de risco e de criação de um repositório, é um processo transversal a toda a gestão do risco, e onde no processo de análise de risco se dá um principal foco no registo de eventos, consequências e riscos. Existem no mercado diversas aplicações vocacionadas este efeito, cada uma com a sua valência e adequada a cada tipo de registo de GR e setor. Neste trabalho de tese, pretendemos que o mesmo fosse independente do tipo de plataforma escolhido e que se pudesse adequar a qualquer solução de software. No nosso trabalho usamos folhas de cálculo (excel), mas que rapidamente podem ser adaptadas a outras soluções de software.

Para os processos de Identificação dos Riscos (5.4.2) e da Análise de Riscos (5.4.3), a organização deverá nomear uma equipa dedicada e multidisciplinar para o estudo de gestão do risco. Cabe a esta equipa, obter o maior número de dados e verificar a integridade dos

mesmos, aplicando as técnicas (quantitativas e qualitativas) perante o maior número de fontes de informação possíveis (*stakeholders*, técnicos, artigos de especialidade).

Ainda na definição de o contexto, a equipa de gestão de risco, inicia o levantamento dos ativos da organização. Estes ativos são os que estão expostos (ou não) a eventos.

Tabela 5 - Ativos e Exposição/Vulnerabilidade

ATIVOS			
ID	**NOME**	**DESCRIÇÃO**	**Exposição Vulnerabilidade**
A#	Ativo	Descrição Ativo	Exposição
…	…	….	…

Seguir-se-á o processo **Identificação dos Riscos (5.4.2)**, onde será necessário identificar os eventos de risco que podem afetar os ativos da organização. Existem muitos estudos sobre os eventos de risco (ex: ENISA, CSA, etc.) em computação em nuvem que deverão ser tidos em conta neste levantamento. Além disso, será sempre importante uma análise do que já existe nesta matéria em organizações similares (negócio, tecnologia, etc).

Processo similar deve ser realizado para o levantamento das consequências sobre os ativos.

A etapa seguinte, será a identificação e criação de uma lista de riscos, perante o levantamento de eventos e consequências. Estes riscos colocam em perigo o atingir dos objetivos da organização. A fonte do risco pode estar sob o controlo da organização ou não. Também será conveniente tipificar os riscos em grandes áreas para melhor entendimento dos *stakeholders.*

Tabela 6 - Registo do risco

RISCOS		
ID	**NOME**	**DESCRIÇÂO**
R#	Risco	Descrição
…	….	…..

Segue-se a etapa de **Análise de Risco (5.4.3)**: aqui, pretende-se desenvolver uma compreensão de risco (ISO.org, 2013). O risco é analisado, determinando as verosimilhanças e impactos dos riscos. A análise pode ser qualitativa, semi-quantitativa ou quantitativa e as variáveis calculadas a partir de dados experimentais, de informação bibliográfica e com peritos da área.

Para cálculo da verosimilhança de um evento acontecer é usual escalas que definam níveis entre valores de 0 a 1 (ex: 0,25; 0,50, e onde um evento impossível de acontecer teria um valor de zero e onde a verosimilhança de acontecer de certeza teria um valor de 1). No entanto as classificações variam consoante o tipo de empresa ou setor de atividade. O número de níveis é também variável, embora seja usual encontrarem-se 5 níveis. A frequência deve estar adequada ao seu propósito (ex: pode estar referida ao número de ocorrências possíveis num mês ou a número de ataques informáticos). Tal como já referido na Norma NP ISO 31000, cabe à equipa de gestão do risco verificar qual a escala mais adequada e que permita aos *stakeholders* uma melhor perceção dos riscos e sua grandeza:

Tabela 7 - Registo de eventos

EVENTOS - VEROSIMILHANÇA			
ID	**NOME**	**DESCRIÇÃO**	**VEROSIMILHANÇA**
ER#	Evento de Risco	Desc	Verosimilhança
…	….	….	…

Situação similar deve ser realizada para registo do impacto de consequência. No entanto aconselha-se que os valores de impacto tenham uma escala não linear. Consequências de maior impacto tenham valores mais elevados e bastante diferenciados (usando escalas não lineares) de forma a demonstrar aos *stakeholders* pontos de maior atenção e para uma melhor alocação de recursos.

Tabela 8 - Registo de Consequências

CONSEQUÊNCIAS - IMPACTO			
ID	**NOME**	**DESCRIÇÃO**	**IMPACTO**
C#	Consequência	Desc.	Impacto
..	….	….	….

Finalmente, chegamos à construção da tabela Eventos-Consequências-Riscos que será um resumo geral de identificação de eventos, riscos, consequências, verosimilhança, impactos e nível (severidade) de riscos. O cálculo do nível do risco permitirá à equipa de gestão do risco e restantes *stakeholders,* separar os riscos menores que possam ser aceitáveis, dos grandes riscos que devem ser tidos em conta de maior atenção no imediato.

Tabela 9 - Eventos/Riscos/Consequências/Severidade risco

EVENTOS-RISCOS-CONSEQUÊNCIAS										
ID Evento	**NOME EVENTO**	**PROB.**	**Valor**	**ID Risco**	**NOME RISCO**	**ID Conseq**	**NOME CONSEQUÊNCIA**	**IMPACTO**	**Valor**	**Severidade Risco**
ER#	Descrição de evento risco			RO#	Descriçao de risco	C0#	Descrição de consequência			
…	…	..	..	..	…	…	…	…	….	…

Como exemplo, a Severidade do risco pode calculada:

Severidade do risco = verosimilhança de evento * impacto da consequência

Segundo a Norma NP ISO 31000 (ISO.org, 2013) um dos pontos importantes é a **Comunicação e consulta (5.2), que deve ser clara para todos os *stakeholders*,** sendo aconselhado que os resultados sejam apresentados usando gráficos ou tabelas que permitam um fácil entendimento das severidades dos riscos. A matriz de risco permite-nos de uma forma simples e visual atingir o objetivo. A sua construção é realizada tendo em conta os eixos de impacto e verosimilhança, e depois o posicionamento dos riscos consoante os valores de níveis de severidade.

Tabela 10 – Matriz do Risco

Verosimilhança-> **Impacto**	Valor 1	Valor 2	Valor 3	Valor 4	Valor 5
Valor 5					Risco3
Valor 4		Risco1			
Valor 3	Risco2		Risco4	Risco5	
Valor 2					
Valor 1					Risco6

Onde podemos definir os níveis de risco como:

Risco Baixo	Risco Médio	Risco Elevado

Sendo a **Avaliação do Risco (5.4.4):** Segundo a norma NP ISO 31000 (ISO.org, 2013) a avaliação do risco permite apoiar a tomada de decisões tendo em conta os critérios de riscos estabelecidos pela organmização. As decisões devem ser tomadas de acordo com as exigências legais e enquadramento de funcional da organização.

Chegamos á etapa de **Tratamento do Risco (5.5),** de forma a se poder controlar os efeitos dos riscos sobre os ativos e objetivos da organização. O plano de tratamento deverá identificar claramente o evento ou consequência que vai tratar, responsável e datas de intervenção.

Finalmente, chegamos à etapa de **Monitorização e revisão (5.6)**, onde deverá associar-se numa tabela, a cada evento de risco o controlo a aplicar e o responsável pela sua monitorização e resultado. Este passo é crucial para definir responsabilidades que obviamente deverão estar ligados aos objetivos a atingir. É necessário que na definição de responsabilidade, que a gestão de topo da organização forneça os meios necessários para se atingirem os objetivos pretendidos. Cabe à equipa de gestão do risco de servir de veículo

de verificação que estão reunidas as condições e foram tidas em conta todas as especificidades.

Conclusão de capítulo: neste capítulo, apresentamos uma proposta de modelo de domínio de gestão do risco para cenários de Computação em Nuvem, tendo por base a Norma 31000:2009.

Modelo apresentado permite contextualizar na maioria das situações os problemas e riscos de adoção de Computação em Nuvem, como também evidenciar os controlos a aplicar.

Ele é constituído pelas classes:

- Evento
- Risco
- Consequência
- Redução de probabilidade
- Redução de impacto
- Ativo

Fizemos uma descrição de cada uma das classes e sua interligação de forma a melhorar a comprensão do modelo em causa.

Exploramos conceitos subjacentes ao registo de risco, em que este processo deve documentar toda a informação pertinente e detalhada da gestão de risco, no nosso caso particular de computação nuvem.

Além disso, delineou-se um processo de registo de risco, tendo em conta os pontos-chave da Norma NP ISO 31000 (ISO.org, 2013), descrevendo-se o que se deve registar, forma de comunicação de modo a permitir uma melhor compreensão dos *stakeholders* e das severidades dos riscos que uma organização está exposta.

Devem ficar registados os processos de definição de contexto, identificação de riscos, análise de riscos, tratamento e monitorização.

5

CASO PRÁTICO

Neste capítulo, pretende-se criar um caso prático que permita demonstrar a aplicação do modelo e método de registo de risco evidenciado no capítulo anterior. Para tal, decidiu-se ver a sua aplicabilidade numa organização da Administração Pública (AP) que tem estado a implementar alterações na sua infraestrutura de sistemas de computação em nuvem.

Este caso prático produzirá um registo de risco e informação que irá ajudar os diversos *stakeholde*rs a melhor focar os seus esforços num processo de migração e manutenção de serviços de computação em nuvem e garantir o seu bom funcionamento.

Para o caso específico escolheu-se o organismo Direcção-Geral do Orçamento (DGO), já que a sua infraestrutura de informática iniciou um projeto de alterações dos seus sistemas para uma nova realidade de Computação em Nuvem e, de certa forma, tem uma infraestrutura algo complexa.

5.1 – Definição de Contexto

A DGO é um organismo da administração Pública, integrado no Ministério das Finanças.

A sua missão é:

- Regular e controlar o processo orçamental das finanças públicas,
- Avaliar a evolução das contas públicas,
- Propor medidas que garantam o cumprimento dos objetivos orçamentais,
- Participar na preparação da programação financeira plurianual da UE.

Com isso, diariamente são processados e trocadas informações com centenas de organismos nacionais e internacionais, sendo um organismo com uma grande responsabilidade para o bom funcionamento da AP no seu geral.

A nível da estrutura funcional, atualmente o organismo tem cerca de 200 colaboradores, distribuídos nas mais diversas áreas, como orçamental, contabilidade, administrativa/apoio ao funcionamento, edição gráfica/comunicação e informática, esta com 22 colaboradores.

Ao longo dos anos a DGO tem investido na informática para poder assegurar o seu funcionamento, melhorar a resposta aos organismos e poder criar aplicações à medida das novas necessidades.

A área de informática encontra-se separada em 4 grandes áreas:

- Desenvolvimento de aplicações orçamentais,
- Desenvolvimento de aplicações de suporte ao funcionamento,
- Business Intelligence do Orçamento
- Infraestruturas composta por Sistemas, Comunicações e Infocentro.

A área de infraestrutura tem que assegurar a base de crescimento informático, tendo como responsabilidades:

- Assegurar o bom funcionamento de toda a infraestrutura informática
- Criar soluções para os novos desafios tecnológicos.
- Aquisições de equipamentos/software informáticos,
- Gestão de contratos de equipamentos e licenciamento,
- Segurança Informática
- Apoio ao utilizador informaticamente
- Manutenção do pleno funcionamento de servidores e comunicações
- Monitorização do funcionamento dos sistemas informáticos e verificação de SLAs.

Atual infraestrutura da DGO a nível de equipamentos informáticos e software é constituída por:

- 55 servidores físicos e cerca de 150 servidores virtuais
- 50 equipamentos de comunicações e segurança (Firewalls, Proxys, Switchs e Routers)
- Bases de dados, email, proxy, sharepoint, web sites, aplicação de suporte ao utilizador, mecanismos de instalação de PCs automatizados, monitorização de servidores e comunicações, aplicação de serviço de impressão central, etc.

A nível aplicacional, a DGO tem ao longo dos anos aumentado o seu número de instalações aplicacionais ao dispor dos seus utilizadores internos e organismos externos, nomeadamente:

- 90 aplicações orçamentais e business intelligence
- 50 aplicações de apoio ao funcionamento (assiduidade, administrativas, etc.)

Até recentemente a infraestrutura da DGO assentava substancialmente em alojamento local (IT Tradicional) e ao longo dos anos, algumas aplicações foram desenvolvidas e alojadas em parceria com a ESPAP (Entidade de Serviços Partilhados da Administração Pública) em sistema de SaaS (fig. 17).

A razão de se equacionar a mudança de grande parte da infraestrutura para o novo sistema de CN, prende-se que centro de dados da DGO, construído há cerca de 25 anos vem a apresentar alguns problemas de adaptação às novas exigências de:

- **Dimensionamento:** com o elevado crescimento do número de servidores e equipamentos de comunicações, chegou ao seu limite de capacidade. Também o sistema de refrigeração dimensionado para um número bastante inferior de equipamentos atingiu o seu limite de funcionamento
- **Segurança:** o centro de dados encontra-se instalado na Praça do Comércio, zona considerada de risco para este tipo de instalação (tenhamos em conta o facto histórico do terramoto de 1755). Além disso, não tem condições de segurança contra intrusões, incêndios, inundações ou cataclismos de ordem diversa e exigidas atualmente.

A área de infraestruturas da DGO e, dado os problemas evidenciados, iniciou um conjunto de estudos para mudança da sua infraestrutura, onde pudesse manter o seu pleno funcionamento, liberdade de decisão, melhorar resiliência a falhas, aumentar a sua capacidade de processamento e, portanto, como objetivo final, melhorar o serviço interno e a todos os organismos da Administração Pública.

Com isso, iniciou alguns anos atrás um estudo entre vários fornecedores de Computação na Nuvem a operar em Portugal (mesmo de fornecedores estrangeiros) para instalação do seu centro de dados. No entanto, tendo sido emitido recentemente uma diretiva governamental para concentração dos centros de dados, foi decidido em parceria com a ESPAP, aproveitar a infraestrutura deste último para uma solução de Computação em Nuvem Governamental e pontualmente utilizar-se serviços de outros fornecedores de CN.

Estando ainda este processo a decorrer, no futuro próximo, a realidade da infraestrutura de sistemas da DGO será bastante diferente e mais complexa:

- 41 servidores em sistema Housing no centro de dados da ESPAP, que albergam diversas aplicações orçamentais e de suporte ao funcionamento da DGO.
- Diversas aplicações orçamentais num **modelo de serviço SaaS** alojadas na Infraestrutura da ESPAP.
- A infraestrutura de Business Intelligence em **modelo de serviço IaaS** com alojamento na Infraestrutura da ESPAP e gestão da DGO.
- Backups off-site num projeto piloto e em estudo de viabilidade em **modelo de serviço BaaS** com a empresa Microsoft.
- Aplicações de monitorização e de suporte ao funcionamento informático de base não críticos instalados no centro de dados da DGO (Sistema Antivírus, instalação automatizada de PCs, Sistemas de segurança e monitorização, etc.) (ver fig. 17).

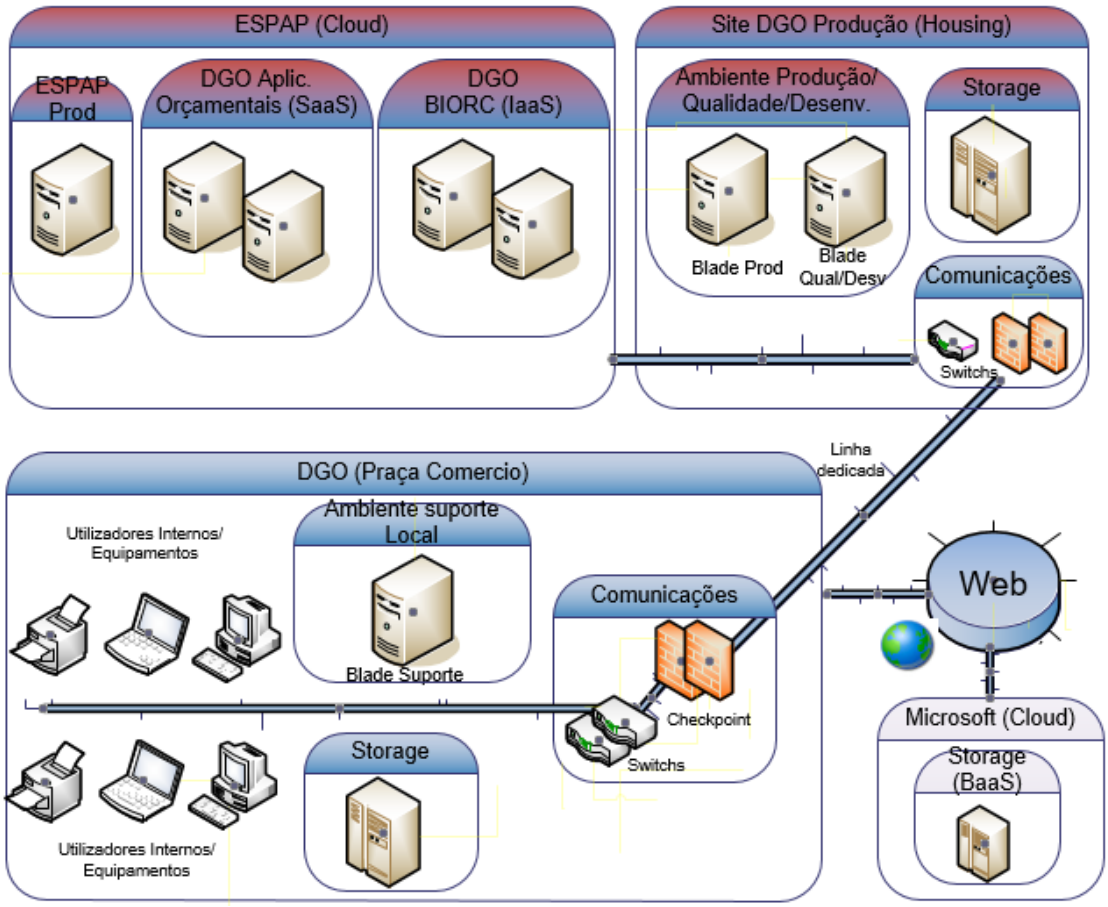


Figura 15 – Infraestrutura DGO

Nesta complexidade de infraestrutura de sistemas informáticos é fundamental existirem planos de continuidade de negócio e uma análise e gestão do risco que possa comunicar e tranquilizar todos os *stakeholders* internos e externos à organização.

5.2 – Aplicação prática

As alterações em que a infraestrutura informática da DGO está envolvida, com vários serviços de computação em nuvem e, obviamente todos os riscos envolvidos, propiciam a realização deste caso prático.

Para identificação dos eventos de risco e consequências, optámos por duas abordagens:

1. Troca de informações com os técnicos de sistemas de forma que nos identificassem possíveis eventos de riscos e consequências, no funcionamento do novo paradigma de computação em nuvem e, dando valores de verosimilhança e impacto (técnica qualitativa) e por outro lado,
2. Investigar o que organizações de referência na área de gestão do risco, já tinham identificado como risco. As organizações que tivemos em foco foram:
    - **ENISA**, organização que elaborou um estudo em riscos de computação em nuvem, realizado por um grupo de especialistas, composto por representantes das indústrias, universidades e organizações governamentais.
    - **Microsoft**, uma das empresas líderes em soluções de computação em nuvem. Ao longo destes anos tem criado estudos de riscos de adoção de Computação em Nuvem.
    - **CSA**, é a organização líder mundial dedicada a definir e dar a conhecer as melhores práticas para ajudar a garantir um ambiente de computação em nuvem segura.
    - **NSA**, Agência de Segurança Nacional dos Estados Unidos, tendo estudos em segurança e riscos de Computação em Nuvem.
    - **OWASP**, Organização sem fins lucrativos focada em melhorar a segurança em software.
    - **COSO**, Organização orientada para o desenvolvimento de frameworks para gestão do risco.

Utilizando estas duas abordagens (Anexo1 - tabela 27), permitiu-nos entender que possíveis riscos poderíamos ter como resultados dos nossos eventos e consequência encontrados.

Seguindo a base da Norma NP ISO 31000 (ISO.org, 2013) (e tal como referido no capitulo 4) iniciamos o processo de registo de risco que se encontram em detalhe nos anexos da tese e descritos abaixo:

1 - Definição do contexto (5.3):

- O ambiente externo e interno da organização (políticas, cultura, etc) está descrito no ponto 5.1 deste capítulo.
- Modelo de serviço de Computação em Nuvem: SaaS, IaaS, BaaS e mantendo ainda parte de infraestrutura de apoio em sistema IT tradicional.
- Modelo de implementação de Computação em Nuvem: Nuvem Híbrida.
- Capacidade necessária em comunicações: capacidade de comunicações 400Mbits, redundância de linhas de comunicações.
- Sistema de backups em off-site.

Realizou-se uma pesquisa dos ativos da DGO, e o seu valor para a organização. Este processo foi realizado, tendo em conta o conhecimento que detemos da organização e seu "negócio" e apoiado em estudos de outras organizações, como a ENISA (anexo 1 tabela 25).

Tabela 11 – Ativos DGO

ATIVOS		
ID	**NOME**	**DGO**
A1	Informação/Dados	Dados informáticos (Bases da Dados, *File Shares*)
A2	Recursos humanos	Pessoal contratado
A3	Capital Financeiro	Orçamento disponível para projetos e funcionamento
A4	Conhecimento (*know how*)	Conhecimento do negócio orçamental
A5	Tecnologia	Infraestrutura Informática da DGO
A6	Operação	Funcionamento da organização
A7	Reputação da organização	Confiabilidade da Instituição para parceiros

2 - Apreciação do Risco (5.4)

Este processo foi realizado tendo em conta o conhecimento que se detém da DGO e de estudos de outras organizações que têm trabalhos em gestão do risco ENISA, Microsoft, CSA, NSA, COSO, OWASP.

a) Identificação dos Riscos (5.4.2):

i) Identificação de Eventos de Risco: Partindo de um cenário de Computação na Nuvem e tendo em conta os ativos da DGO, foi realizado levantamento de quais os eventos suscetíveis de causar danos nos mesmos. Este levantamento foi principalmente elaborado a partir de troca de impressões com os técnicos da DGO e tendo em conta estudos de outras organizações como a ENISA (Anexo1 – Tabela 26) e Microsoft. A informação foi então vertida no Registo do Risco e exposto na tabela 12.

Tabela 12 – Registo de eventos

EVENTOS	
ID	**NOME**
ER1	Ataque informático
ER2	Escassez de recursos técnicos especializados
ER3	Ineficiente gestão financeira e de IT
ER4	Inexperiência e falta de conhecimento em gestão Computação em Nuvem
ER5	Ataques de engenharia social
ER6	Não aplicabilidade de normas de segurança.
ER7	Mudança de um paradigma de IT tradicional para Computação em Nuvem.
ER8	Falta de definição contratual de responsabilidades e sua operacionalização.
ER9	Emissão de novas legislações sobre segurança ou armazenamento de dados na Nuvem
ER10	Dificuldade de monitorização dos níveis de serviço do fornecedor Computação em Nuvem
ER11	Falhas de funcionamento de serviço.
ER12	Incapacidade do fornecedor CN alocar recursos IT face às necessidades
ER13	Fornecedor de serviço não adequado às necessidades da organização
ER14	Necessidade de rápida implementação de serviços e redução de custos
ER15	Desastre Natural

ii) Identificação e levantamento das possíveis consequências de cada risco: para esta etapa, tendo em conta os eventos de riscos, realizou-se um estudo de quais as possíveis consequências que cada evento pode provocar. Este levantamento foi principalmente elaborado a partir de troca de impressões com os técnicos da DGO e tendo também em conta o estudo da organização ENISA (Anexo1 – Tabela 27). O resultado, encontra-se resumido na tabela 13.

Tabela 13 – Registo de Consequências (DGO)

CONSEQUÊNCIAS	
ID	**NOME**
C1	Inatividade da organização.
C2	Deterioração da imagem e confiabilidade da DGO e fornecedor CN
C3	Dificuldade de operacionalidade ou cumprimentos de objetivos.
C4	Necessidade de mudança de serviço *Cloud* ou regresso a sistema IT tradicional.
C5	Danos em equipamentos.
C6	Implicações criminais
C7	Divulgação ou inconsistência de dados privados
C8	Dificuldade de colocar em funcionamento novos serviços
C9	Dificuldade de aplicação de coimas ou indeminizações
C10	Perda de informação
C11	Não concretização da mudança para a *Cloud* ou sua manutenção
C12	Quebra de serviço ou inatividade da organização
C13	Funcionamento deficiente por dificuldade de aplicar melhorias
C14	Segurança reduzida
C15	Falta de conetividade aos dados e inoperacionalidade da DGO

iii) Identificação de riscos: a partir evento – consequência, elaboramos a lista de riscos - a tabela 14. Para melhor entendimento tipificaram-se em 3 grupos: técnicos, legais e organizacionais. Verificou-se como os riscos encontrados estariam de acordo com outros estudos (ex: ENISA, Microsoft, etc.) estando tal trabalho vertido no anexo 1 nas tabelas 31 e 32, verificando-se que estão dentro dos padrões.

Tabela 14 - Registo do Risco (DGO)

RISCOS	
ID Risco	**NOME RISCO**
RISCOS ORGANIZACIONAIS	
RO1	Perda e não integridade de dados
RO2	Dificuldade de contratação de pessoal especializado
RO3	Custos Financeiros não contabilizados/suportados
RO4	Dificuldade de governação do sistema *Cloud*
RO5	Ataques de engenharia social
RO6	Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas)
RO7	Falta de uma efetiva responsabilidade sobre os dados
RO8	Desastres Naturais

RISCOS LEGAIS	
RL1	Mudanças legislativas de segurança ou armazenamento de dados na *Cloud* (apagar dados, segurança periférica, *backups* e políticas de testes, etc)
RISCOS TÉCNICOS	
RT1	Dificuldade de mudança para novo fornecedor de serviço de *Cloud - Lockin*
RT2	Maior dependência de terceiros
RT3	Incumprimento ou difícil análise de SLA's por parte dos fornecedores de serviço
RT4	Maior exposição a ataques informáticos.
RT5	Dificuldade de isolamento de aplicações e serviços
RT6	Incapacidade do fornecedor cloud alocar recursos IT às necessidades da organização.

b) Análise do Risco (5.4.3)

i) Cálculo do valor do ativo: após termo realizado o levantamento dos ativos/eventos/consequências e riscos, é necessário imputar valores a cada um dos atributos. O valor do Ativo foi, uma vez mais, calculado tendo em conta o conhecimento que detemos da organização e seu "negócio" (técnica qualitativa) e apoiado em estudos de outras organizações, como a ENISA (Anexo 1 tabela 27).

Tabela 15 - Cálculo valor Ativo (DGO)

ATIVOS			
ID	**NOME**	**DGO**	**Valor (ENISA)**
A1	Informação/Dados	Dados informáticos (Bases da Dados, File Shares)	Elevada
A2	Recursos humanos	Pessoal contratado	Alta
A3	Capital Financeiro	Orçamento disponível para projetos e funcionamento	Alta
A4	Conhecimento (*know how*)	Conhecimento do negócio orçamental	Alta
A5	Tecnologia	Infraestrutura Informática da DGO	Elevada
A6	Operação	Funcionamento da organização	Elevada
A7	Reputação da organização	Confiabilidade da Instituição para parceiros	Elevada

ii) Identificação da Verosimilhança de Evento: identificou-se os valores de probabilidade que determinado evento de risco aconteça e espelhados na tabela 16. Foram obtidos usando técnica qualitativa de questões a peritos na área sistemas e comunicações da DGO (inquérito anexo 1 tabela 32). O valor foi obtido pela forma de cálculo que se encontra descrita no anexo 1 tabela 23 e para verificação dos resultados (valores) tivemos em conta o estudo da ENISA (Anexo1 – Tabela 25).

Tabela 16 - Verosimilhança de Evento (DGO)

	EVENTOS		
ID	**NOME**	**Valor**	**Verosimilhança**
ER1	Ataque informático	0,96	Elevada
ER2	Escassez de recursos técnicos especializados	0,45	Média
ER3	Ineficiente gestão financeira e de IT	0,5	Média
ER4	Inexperiência e falta de conhecimento em gestão Computação em Nuvem	0,54	Média
ER5	Ataques de engenharia social	0,1	Muito baixa
ER6	Não aplicabilidade de normas de segurança.	0,92	Elevada
ER7	Mudança de um paradigma de IT tradicional para Computação em Nuvem.	0,71	Alta
ER8	Falta de definição contratual de responsabilidades e sua operacionalização.	0,79	Alta
ER9	Emissão de novas legislações sobre segurança ou armazenamento de dados na *Cloud*	0,26	Baixa
ER10	Dificuldade de monitorização dos níveis de serviço do fornecedor Computação em Nuvem	0,58	Média
ER11	Falhas de funcionamento de serviço.	0,5	Média
ER12	Incapacidade do fornecedor CN alocar recursos IT face às necessidades	0,1	Baixa
ER13	Fornecedor de serviço não adequado às necessidades da organização	0,58	Média
ER14	Necessidade de rápida implementação de serviços e redução de custos	0,46	Média
ER15	Desastre Natural	0,1	Muito baixa

Os intervalos dos valores de verosimilhança são:

M. Baixa: 0-0,19	Baixa: 0,20-0,44	Média: 0,45-0,69	Alta: 0,70-0,89	Elevada: 0,90-1

iii) Identificação do Impacto da consequência: nesta etapa identificou-se valores de impacto que os riscos podem ter nos Ativos e funcionamento da DGO. A técnica utilizada foi a mesma do ponto anterior (inquérito anexo 1 tabela 33). Os valores foram obtidos e espelhados na tabela 17. A forma de cálculo encontra-se espelhado no anexo 1 tabela 24. Para efeito de verificação dos resultados em organizações semelhantes, tivemos também em conta o estudo da organização ENISA (Anexo1 – Tabela 26).

Tabela 17 - Impacto de Consequências (DGO)

	CONSEQUÊNCIAS		
ID	**NOME**	**Valor**	**Impacto**
C1	Inatividade da organização.	36,7	Elevado
C2	Deterioração da imagem e confiabilidade da DGO e fornecedor CN	21,7	Alto
C3	Dificuldade de operacionalidade ou cumprimentos de objetivos.	36,7	Elevado
C4	Necessidade de mudança de serviço *Cloud* ou regresso a sistema IT tradicional.	11,7	Médio
C5	Danos em equipamentos e/ou Instalações	15,8	Alto
C6	Implicações criminais	21,7	Alto
C7	Divulgação ou inconsistência de dados privados	18,3	Elevado
C8	Dificuldade de colocar em funcionamento novos serviços	6,7	Baixo
C9	Dificuldade de aplicação de coimas ou indeminizações	12,5	Médio
C10	Perda e inconsistência de informação	40,0	Elevado
C11	Não concretização da mudança para a *Cloud* ou sua manutenção	21,7	Alto
C12	Quebra de serviço ou inatividade da organização	40,0	Elevado
C13	Funcionamento deficiente	1,6	Muito Baixo
C14	Segurança reduzida	36,7	Elevado
C15	Falta de conetividade aos dados e Inoperacionalidade da organização	36,7	Elevado

Os intervalos dos valores de impacto são:

M. Baixo: 1-3	Baixo: 4 a 8	Médio: 9 a 17	Alto: 18 a 34	Elevado: 35 a 40

iv) Cálculo da severidade do risco: estando já identificados os riscos, finalmente, nesta etapa faz-se o cálculo do nível/severidade que estes têm na organização. Para o caso

específico determinou-se como mais adequada a utilização da fórmula (ver Anexo 1 tabela 28):

Nível de risco = Verosimilhança * Impacto

Tabela 18 - Nível do Risco (DGO)

RISCOS			
ID Risco	**NOME RISCO**	**Valor**	**Nível Risco**
RISCOS ORGANIZACIONAIS			
RO1	Perda e não integridade de dados	38,40	Elevado
RO2	Dificuldade de contratação de pessoal especializado	16,52	Médio
RO3	Custos Financeiros não contabilizados/suportados	5,85	Baixo
RO4	Dificuldade de governação do sistema *cloud*	11,72	Médio
RO5	Ataques de engenharia social	1,58	M. Baixo
RO6	Não alinhamento de processos de segurança entre partes (organização, fornecedor *cloud*, outras empresas)	36,80	Elevado
RO7	Falta de uma efetiva responsabilidade sobre os dados	1,26	M. Baixo
RO8	Desastres Naturais	3,67	M. Baixo
RISCOS LEGAIS			
RL1	Mudanças legislativas de segurança ou armazenamento de dados na Cloud (apagar dados, segurança periférica, *backups* e políticas de testes, etc)	5,64	Baixo
RISCOS TÉCNICOS			
RT1	Dificuldade de mudança para novo fornecedor de serviço *cloud - lockin*	3,89	M. Baixo
RT2	Maior dependência de terceiros	18,35	Alto
RT3	Incumprimento ou difícil análise de SLA's por parte dos fornecedores de serviço	7,25	Baixo
RT4	Maior exposição a ataques informáticos.	12,99	Médio
RT5	Dificuldade de isolamento de aplicações e serviços	16,88	Médio
RT6	Incapacidade do fornecedor *cloud* alocar recursos IT às necessidades da organização.	2,17	M. Baixo

Onde para escala do nível de risco:

M. Baixo: 1-3	Baixo: 4 a 8	Médio: 9 a 17	Alto: 18 a 34	Elevado: 35 a 40

Os riscos que apresentam o maior nível de severidade para a organização são eles: R01 - Perda e não integridade de dados e R06 - Não alinhamento de processos de segurança entre partes (organização, fornecedor *cloud*, outras empresas).

Realizou-se também um trabalho de verificação de alinhamento dos resultados dos riscos com outros estudos de forma a verificarmos, se os riscos encontrados são de certa forma consonantes com o encontrado em cenários semelhantes (anexo1 – tabela 30). Verifica-se que de certa forma os riscos encontrados na DGO, têm uma correspondência com riscos identificados noutros estudos, no entanto, e obviamente onde o nível de risco é especifico ao caso da DGO.

i) é importante comunicar de uma forma simples a magnitude dos riscos e quais aqueles que a equipa de gestão do risco maior cuidado deve ter em conta. A matriz de risco, permite visualmente atingir o objetivo tendo em conta a verosimilhança dos eventos e impactos de consequência. Perante os dados obtidos, realizou-se a matriz do risco na tabela 19. Verificamos que tendo em conta a probabilidade de evento e o impacto das consequências **os riscos que apresentam um maior cuidado são RO1 – Perda e não integridade de dados e RO06 – Não alinhamento de processos de segurança entre partes**.

Tabela 19 – Matriz de risco

Verosimilhança-> Impacto	M. Baixa (0,1)	Baixa (0,25)	Média (0,5)	Alta (0,75)	Elevada (1)
Elevado (40)	RO8		RO2; RT2; RT5	RT4	RO1;RO6
Alto (20)	RO5	RL1; RT6	RO4		
Médio (10)			RO3; RT3		
Baixo (5)			RT1		
Muito Baixo (1)				RO7	

Onde RO: Riscos Organizacionais; RL: Riscos Legais; RT: Riscos Técnicos

3 - Tratamento do Risco (5.5)

a) Identificação dos controlos para minimizar a probabilidade da ocorrência desses eventos e impactos: nesta etapa, e através de estudos de artigos de especialidade e perante as equipas técnicas da DGO, foi levantado um conjunto de controlos que podem ser implementados para minorar os eventos de risco. Não sendo o foco desta tese, remetemos este processo para sugestão de trabalho futuro. Atendendo à Norma

NP ISO 31000 (ISO.org, 2013) “O plano de tratamento deverá claramente identificar a ordem de prioridade de implementação dos tratamentos individuais do risco”, no nosso entendimento, a organização DGO deverá concentrar os seus esforços e recursos prioritariamente no tratamento dos riscos RO1 e RO6.

4 - Comunicação e consulta (5.2):

a) Análise dos resultados e comunicação: nesta etapa, deve-se comunicar aos vários stakeholders os resultados obtidos usando a tabela de distribuição para evidenciar os focos de risco que mais atenção merecem e as tabelas de severidade de risco.
b) Devem-se gerar relatórios, que grande parte das ferramentas de software permitem (Microsoft Excel e outras de mercado)
c) Utilização de gráficos, tabelas de severidade de riscos e matriz de risco de forma a melhorar o entendimento dos riscos em causa.

5 - Monitorização e revisão (5.6): na última fase do processo de gestão do risco, simulou-se um registo de risco que permita ir monitorizando a aplicação dos controlos, responsáveis e metas a atingir. Não sendo o foco desta tese, remetemos este processo para sugestão de trabalho futuro.

Conclusão de capítulo: aplicámos o modelo proposto no capítulo 4, a uma situação real, mais concretamente na Infraestrutura de IT da Direção Geral do Orçamento. Esta organização devido às suas alterações na infraestrutura, com mudanças para serviços de computação em nuvem governamental e externa (SaaS, IaaS e BaaS) e ainda mantendo o seu sistema de IT tradicional, afigurou-se como ideal para o nosso estudo.

Para a realização do trabalho, recorremos ao conhecimento que se detém do funcionamento da DGO e dos seus serviços de IT. Além disso, de forma a alicerçar o estudo e a nossa análise, usamos técnicas qualitativas, fizemos um levantamento de estudos de outras organizações que têm trabalhos em gestão do risco como a ENISA, Microsoft, CSA, NSA, COSO, OWASP. No entanto, e primordialmente, dado a especificidade da organização, assentamos o nosso conhecimento no inquérito aos técnicos de forma para uma primeira abordagem dos eventos e consequências que esta pode estar exposta.

Seguindo a Norma NP ISO 31000 (ISO.org, 2013) e modelo proposto, realizamos as etapas:

- Definição de contexto (com identificação dos ativos)
- Apreciação do risco
- Comunicação e consulta
- Tratamento do risco
- Monitorização e revisão

Verificou-se que a proposta de modelo e registo de risco definidos, numa ótica de gestão do risco de computação em nuvem, foram perfeitamente aplicáveis à realidade da organização DGO.

Além disso, permitiu que através dos resultados obtidos, os vários *stakeholders* ficassem consciencializados de quais os eventos, consequências, riscos e ativos merecem uma maior atenção de tratamento e monitorização.

Verificamos que se deve ter um cuidado especial no tratamento (através de aplicação de controlos) e monitorização dos:

- Eventos por: Ataques informáticos e não implementação de normas de segurança.
- Consequências por possível: inatividade da organização; dificuldade de operacionalidade ou cumprimentos de objetivos; perda e inconsistência de informação; quebra de serviço ou inatividade da organização e falta de conetividade aos dados.
- Riscos: perda e não integridade de dados; Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas).

Esta página foi intencionalmente deixada em branco

6

CONCLUSÕES

e TRABALHO FUTURO

6.1 – Conclusões

Apresentam-se as conclusões sobre o trabalho realizado e também proposta de trabalho futuro.

As Infraestruturas de Computação em Nuvem são bastantes atrativas de implementação, por várias vantagens que oferecem às organizações e que são descritas ao longo da tese, no entanto, apresentam também um conjunto de desafios e riscos que devem ser meticulosamente ponderados e avaliados.

De forma a reduzir a incerteza de implementação ou manutenção, as organizações devem munir-se de métodos e modelos de forma a mitigarem os riscos a que ficam expostas.

A elaboração desta tese pretende dar uma resposta a este problema, desenvolvendo e focando-se numa análise genérica e uma proposta de repositório de risco, tendo como base a Norma NP ISO 31000 (ISO.org, 2013).

Para tal objetivo foi realizada uma pesquisa bibliográfica de várias fontes, recorreu-se a artigos de especialidade e, em paralelo, a estudos de outras organizações que se dedicam a esta matéria.

Foi ainda necessário alicerçar um conjunto de conhecimentos da temática de Computação em Nuvem, de modo a poder-se realizar uma análise de riscos de cada opção, suas caraterísticas (vantagens e desvantagens), e aplicabilidade real da gestão do risco.

Iniciou-se um trabalho de conhecimento do que existe a nível de gestão do risco, normas, estrutura, métodos e técnicas de cálculo do risco e tendo-nos, no final, focado na Norma NP ISO 31000 (ISO.org, 2013), que serviu de guia ao longo desta tese.

Tendo como base a norma indicada, iniciou-se a elaboração de um modelo que pudesse ser aplicado em casos reais de gestão do risco em computação em nuvem. O modelo apresentado tem como principal caraterística ser genérico e abrangente, de modo que se possa aplicar a todo o tipo de empresa ou setor que pretende iniciar uma gestão do risco na vertente computação em nuvem.

Era, no entanto, importante averiguar como o modelo proposto e o registo de risco se poderiam adequar a uma situação real. Nesse sentido, decidiu-se verificar a sua aplicabilidade no organismo Direcção-Geral do Orçamento (DGO), já que a sua infraestrutura de informática está numa fase de alterações para soluções de Computação em Nuvem.

Procurando o conhecimento técnico dentro da DGO e num levantamento de estudos de outras organizações, compilaram-se eventos, consequências e riscos. Realizou-se a análise de risco e um inicio de proposta de tratamento dos eventos e consequências de risco.

Usando os processos de cálculo de nível de risco e matriz de risco, verificamos que a DGO está exposta a um conjunto de eventos, consequências e riscos na sua implementação de computação em nuvem. Um dos maiores riscos que a DGO enfrenta é perda de dados por ataques informáticos, sendo também um risco que afeta, na generalidade, as restantes organizações. Um outro risco identificado com um elevado nível de severidade foi “a falta de alinhamento de processos de segurança entre fornecedor e a organização DGO”. No fundo, o que isto quer dizer é que, numa solução de computação em nuvem, todas as organizações que contratualizam serviços do fornecedor têm de ter preocupações de segurança alinhadas. Basta que uma das organizações ou fornecedor não tenham aplicado as melhores praticas, para que toda a infraestrutura *Cloud* fique exposta a uma vulnerabilidade. Isto pode representar um problema para algumas organizações por não terem os meios adequados, para implementar as melhores práticas.

Considera-se que foi alcançado o objetivo definido no inicio da presente tese, onde foi comprovada a aplicabilidade do modelo, método e registo de risco proposto numa organização de média dimensão (Direção Geral do Orçamento). Além disso, o trabalho realizado permitiu à organização melhorar o seu conhecimento dos riscos que enfrenta numa solução de computação em nuvem e de no futuro poder estar mais preparada para mitigar riscos da sua solução de computação em nuvem. Também vai permitir à organização poder utilizar um método de registo de risco consistente para a sua gestão de risco.

6.2 – Trabalho futuro

Nesta secção, apresentamos uma descrição do possível trabalho futuro a desenvolver de forma a complementar o modelo proposto, métodos e técnicas definidas nesta tese.

Esta tese centrou-se na criação de um modelo genérico de gestão do risco para Computação em Nuvem. Mas como é sabido, a realidade é feita de particularidades, onde os modelos generalistas terão de ser adaptados.

O caso prático realizado, teve em estudo uma organização da administração pública de média dimensão a nível organizacional e de TI. Seria importante ver como a nossa proposta se ajusta a outras organizações com níveis diferenciados de dimensão, setor, maturação tecnológica e de tecnologias de computação em nuvem.

Os dados que trabalhámos (verosimilhança de eventos e impactos de consequência), são obtidos maioritariamente através de técnicas qualitativas, nomeadamente através de inquérito aos técnicos e de pesquisa de estudos de outras organizações. A razão é que estamos numa primeira abordagem, onde a organização ainda não tem registos de acontecimentos (eventos e consequências). Sendo a gestão de risco um processo de melhoria continua (através de registo, tratamento e monitorização), no futuro os dados poderão ser tratados aplicando mais técnicas quantitativas, principalmente no cálculo de verosimilhança de evento e valor de impacto (ex: impacto financeiro). Esta nova realidade poderá ter de ser refletida na nossa proposta.

Ao mesmo tempo, seria interessante ver como as organizações poderão tirar partido do modelo proposto para ganhar vantagem competitiva relativamente às suas congéneres ou até usar a gestão do risco para negociar melhor contratos de Computação em Nuvem a nível financeiro ou de resiliência tecnológica/informação.

Tendo esta tese focado principalmente o processo de análise de risco, não nos foi possível ir ao detalhe no registo de risco para os processos de tratamento e monitorização do risco em computação em nuvem.

Iniciamos algum trabalho durante a tese que pode desde já servir de guia para futuro trabalho:

Tratamento do Risco (5.5):

a) Identificação dos controlos para minimizar a probabilidade da ocorrência de eventos e impactos: nesta etapa, através de estudos de artigos de especialidade e perante as equipas técnicas da DGO, foi levantado um conjunto de controlos que podem ser implementados para minorar os eventos de risco.

Tabela 20 - Controlos de redução de verosimilhança e impactos do risco

Evento	Redução de Verosimilhança de Evento de Risco
ER1 - Ataque informático. ……	**RVER1** - Manter sistemas atualizados. **RVER2** - Aplicar as melhores práticas de segurança (informática, acessibilidade). **RVER3** - Formação técnica em segurança ao pessoal da organização. **RVER5** - Contratação de serviços especializados em gestão *Cloud Computing*. **RVER4** - Auditorias periódicas em segurança. …….
Consequência	Redução de Impacto de Consequência
C1 - Inatividade da organização. …….	**RIC1** - Contratar sistemas redundantes de funcionamento (dados armazenados em dois fornecedores de serviço, comunicações ou internamente). **RIC2** - Sistema de *Backups* e *Disaster Recovery* operacional e documentado. …….

b) Identificação do responsável para tratamento para redução dos eventos e redução das consequências de risco

Tabela 21 - Responsável por tratamento da redução do eventos de risco

CONTROLO - REDUÇÃO de VEROSIMILHANÇA EVENTO / IMPACTO CONSEQUÊNCIA			
ID	**NOME**	**RESPONSÁVEL (ÁREA, TÉCN)**	**DATA TÉRMINO**
RVER1	Manter sistemas atualizados.	Sistemas; Comunicações	abr/16
RIC1	Contratação sistemas redundantes de funcionamento	Informática	jun/16
…..	…..	….	….

Monitorização e revisão (5.6): na última fase do processo de gestão do risco deve-se ir monitorizando o risco identificado e avaliando se o resultado das alterações necessárias estão a ser cumpridas. Onde se sugere, criar tabelas de responsabilização de monitorização de redução de eventos e consequências de risco, por questões de sigilo os nomes são fictícios.

Tabela 22 - Responsável e tarefas de monitorização de redução Eventos de Risco

MONITORIZAÇÃO REDUÇÂO EVENTOS/CONSEQUÊNCIAS				
ID	**Área**	**Técnico**	**Periodicidade**	**Meios a adquirir**
RVER1	Segurança	Jorge Silva	Todos os dias	Firewall
….	……	….	…..	……

Esta página foi intencionalmente deixada em branco

BIBLIOGRAFIA

Ackermann, T. (2012). *IT Security Risk.* Springer Gabler. Obtido de http://www.asecib.ase.ro/cc/carti/IT%20Security%20Risk%20Management%20in%20the%20Context%20of%20Cloud%20Computing%20[2013].pdf

Alliance, C. S. (2013). Cloud Computing Top Threats in 2013. 6. Obtido de https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Ashenden, A. J. (2005). The Changing Environment. Em A. J. Ashenden, *Risk Management for Computer Security Protecting Your Network and Information* (p. 22). Oxford: Elsevier Butterworth–Heinemann.

Australian/New Zealand Standard. (2004). *Risk Management (AS/NZS).* Australia and New Zealand: Standards Australia and Standards New Zealand.

Aven, e. a. (2008). *Risk Analysis - Assessing Uncertainties Beyond Expected Values and Probabilities.* John Wiley and Sons.

Barateiro, J. E. (2012). *Doctoral Dissertation - Risk Management Framework Applied to Digital Preservation.* Lisboa, Portugal: IST - Instituto Superior Técnico.

Bjelland , A. (2012). *Master Thesys - Project Risk Management.* University of Stavanger. Obtido de http://brage.bibsys.no/xmlui/bitstream/handle/11250/182141/Bjelland,%20Anders.pdf?sequence=1

Collier, P. M. (2007). *Risk and Management Accounting: Best Practice Guidelines for Enterprise-wide Internal Control Procedures.* CIMA Publishing.

COSO.ORG. (s.d.). *FAQs for COSO.* Obtido de http://www.coso.org/documents/ERM-FAQs.pdf

Dieder, M. (2011). Computação nas Nuvens, Virtualização e Software Livre - Como eles caminham juntos. *http://pt.slideshare.net/*, 7. Obtido de

http://pt.slideshare.net/mdieder/computao-nas-nuvens-virtualizao-e-software-livre-como-eles-caminham-juntos

Dorfman. (2007). *Introduction to Risk Management and Insurance.* Englewood Cliffs.

ENISA. (2009). *Cloud Computing Security Risk Assessment.* ENISA. Obtido de https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework

Forbes.com. (24 de 01 de 2015). *Roundup Of Cloud Computing Forecasts And Market Estimates, 2015*. Obtido de Forbes.com: http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/

Forrsights. (s.d.). *The true state of cloud adoption*. Obtido de Forrester.com: http://www.slideserve.com/gunnar/the-true-state-of-cloud-adoption

Forsberg, K. ,. (2005). *Visualizing Project Management Models and Frameworks for Mastering Complex Systems.* John Wiley & Sons Ltd.

Herrera, G. (19 de Setembro de 2014). *SaaS 101: IaaS, PaaS, SaaS and Cloud Computing*. Obtido de Starthq.com: https://starthq.com/blog/saas-101-iaas-paas-saas-and-cloud-computing

IDC Predictions 2015 - Portugal - Youtube.com. (s.d.). Obtido de https://www.youtube.com/watch?v=Za39DN5JFT0

ISO. (2009). *ISO 31010 - Risk management - Risk assessment techniques.* Genebra, Portugal: ISO.

ISO. (2009). *ISO Guide 73 - Risk management - Vocabulary.* Genebra, Portugal: ISO.

ISO. (2013). *ISO 27001 - Information security management.* Genebra, Portugal: ISO.

ISO. (2013). *ISO 31004 - Risk management - Guidance for the implementation of ISO 31000.* Genebra, Portugal: ISO.

ISO. (2014). *Information technology - Security techniques - Code of practice for protection of personally identifiable information in public clouds.* Genebra, Portugal: ISO.

ISO.org. (2013). *ISO 31000:2013 - Gestão do Risco - Linhas e Orientação.* Portugal: Instituto Português de Qualidade. Obtido de ISO.org: https://www.iso.org

Itchannel.com. (07 de 07 de 2015). *Investimentos em infraestrutura cloud deverão crescer 26% este ano*. Obtido em 08 de 2015, de http://www.itchannel.pt/article.php?a=14142

Jared Carstensen, J. M. (2012). *Cloud Computing - Assessing the risks.* IT Governance.

Kohout, K. (2013). IT Risk Register. p. 1. Obtido de http://www.diplomovaprace.cz/2013/42/kohout_karel_it_risk_register.pdf

KPMG-IPQ. (2013). Gestão do Risco em Portugal: Desafios para as empresas. 39. Obtido de https://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/surveyERM2013.pdf

Management Solutions. (2014). *Model Risk Management - Quantitative and Qualitative Aspects.* Management Solutions.

Meadows, R. (2009). *The Risk IT Practitioner Guide.* ISACA.

Mell, P. (2011). *The NIST Definition of Cloud.* Reports on Computer Systems Technology.

Napp, A.-K. (09 de 2011). Master Thesys - Financial Risk Management in SME. p. 10.

Napp, A.-K. (09 de 2011). Master Thesys - Financial Risk Management in SME. p. 8. Obtido de http://pure.au.dk/portal-asb-student/files/39817962/Thesis_A_Napp.pdf

PMBOK. (2004). *A Guide to the Project Management Body of Knowledge - pag 237.* Project Management Institute; Newton Square.

Stokes, D. (2013). *Compliant Cloud Computing - Managing the Risks.*

Wikipedia. (10 de 2015). *Computação em nuvem*. Obtido de Wikipedia.com: https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem

Wiley, Chapman C. and Ward S. (2003). *Project Risk Management.* John Wiley & Sons.

Young, E. a. (1 de Setembro de 2011). *The evolving IT risk landscape: The why and how of IT Risk Management.* Obtido de http://www.ey.com/Publication/vwLUAssets/La_evolucion_del_riesgo_en_TI/$FILE/EY_IT_Risk_Landscape.pdf

ANEXO 1

Tabela 23 – Resultado do inquérito de verosimilhança de eventos CN

INQ-RESP EVENTOS (Probabilidade)								
ER	**Inq-Resp 1**	**Inq-Resp 2**	**Inq-Resp 3**	**Inq-Resp 4**	**Inq-Resp 5**	**Inq-Resp 6**	**Cálculo Ver**	**Verosimilhança**
ER1	Elevada	Elevada	Elevada	Alta	Elevada	Elevada	0,96	Elevada
ER2	Média	Baixo	Média	Média	Média	Média	0,45	Média
ER3	Média	Média	Média	Média	Média	Média	0,5	Média
ER4	Baixa	Média	Média	Elevada	Média	Média	0,54	Média
ER5	M. Baixa	M. Baixa	M. Baixa	M. Baixa	M. Baixa	M. Baixa	0,1	Muito baixa
ER6	Alta	Elevada	Alta	Elevada	Elevada	Elevada	0,92	Elevada
ER7	Alta	Alta	Elevada	Alta	Média	Média	0,71	Alta
ER8	Alta	Alta	Elevada	Alta	Alta	Alta	0,79	Alta
ER9	Baixa	Média	Baixa	Baixa	M. Baixa	Baixa	0,26	Baixa
ER10	Alta	Média	Alta	Média	Média	Média	0,58	Média
ER11	Média	Média	Média	Média	Média	Média	0,5	Média
ER12	Baixa	Baixa	Baixa	Baixa	Média	Baixa	0,1	Baixa
ER13	Alta	Média	Média	Média	Média	Alta	0,58	Média
ER14	Média	Média	Baixa	Média	Alta	Baixa	0,46	Média
ER15	M. Baixa	M. Baixa	M. Baixa	M. Baixa	M. Baixa	M. Baixa	0,1	Muito baixa

Valor de conversão consoante resposta (Inq-resposta valor):

M. Baixa: 0,1	Baixa: 0,25	Média: 0,5	Alta: 0,75	Elevada: 1

Cálculo Ver = $\sum_{i=1}^{6} R_i/6$; em que R = Inq-Resposta valor

Intervalos para cálculo dos valores de verosimilhança:

M. Baixa: 0-0,19	Baixa: 0,20-0,44	Média: 0,45-0,69	Alta: 0,70-0,89	Elevada: 0,90-1

Tabela 24 - Resultado do inquérito de impacto de consequência CN

INQ-RESP CONSEQUÊNCIAS (Nível de Impacto)								
Cons.	**Inq-Resp 1**	**Inq-Resp 2**	**Inq-Resp 3**	**Inq-Resp 4**	**Inq-Resp 5**	**Inq-Resp 6**	**Cálculo**	**Impacto**
C1	Alto	Elevado	Elevado	Elevado	Elevado	Elevado	36,7	Elevado
C2	Médio	Alto	Elevado	Alto	Alto	Alto	21,7	Alto
C3	Elevado	Elevado	Elevado	Elevado	Elevado	Alto	36,7	Elevado
C4	Médio	Médio	Médio	Alto	Médio	Médio	11,7	Médio
C5	Baixo	Médio	Alto	Alto	Alto	Alto	15,8	Alto
C6	Médio	Alto	Elevado	Alto	Alto	Alto	21,7	Alto
C7	Alto	Alto	Alto	Alto	Alto	Médio	18,3	Alto
C8	Médio	Baixo	Baixo	Médio	Baixo	Baixo	6,7	Baixo
C9	Alto	Alto	Baixo	Médio	Médio	Médio	12,5	Médio
C10	Elevado	Elevado	Elevado	Elevado	Elevado	Elevado	40,0	Elevado
C11	Alta	Alta	Alta	Média	Elevada	Alta	21,7	Alto
C12	Elevado	Elevado	Elevado	Elevado	Elevado	Elevado	40,0	Elevado
C13	Baixa	M. Baixa	M. Baixa	M. Baixa	M. Baixa	Baixa	1,6	Muito Baixo
C14	Alto	Elevado	Elevado	Elevado	Elevado	Elevado	36,7	Elevado
C15	Elevado	Elevado	Alta	Elevado	Elevado	Elevado	36,7	Elevado

Valor de conversão consoante resposta (Inq-resposta valor):

M. Baixo: 1	Baixo: 5	Médio: 10	Alto: 20	Elevado: 40

Cálculo = $\sum_{i=1}^{6} R_i/6$; em que R = Inq Resposta valor

Intervalos para cálculo dos valores de impacto são:

M. Baixo: 1-3	Baixo: 4 a 8	Médio: 9 a 17	Alto: 18 a 34	Elevado: 35 a 40

Tabela 25 - ENISA levantamento e valores de verosimilhança de eventos

EVENTOS		
ID	**NOME**	**ENISA Valor**
ER1	Ataque informático	Média
ER2	Escassez de recursos técnicos especializados	
ER3	Ineficiente gestão financeira e de IT	Elevada
ER4	Inexperiência e falta de conhecimento em gestão de IT Cloud.	Elevada
ER5	Ataques de engenharia social	Média
ER6	Não conformidade de normas de segurança.	Elevada
ER7	Mudança de um paradigma de IT tradicional para Cloud Computing.	
ER8	Falta de definição contratual de responsabilidades e sua operacionalização.	Elevada
ER9	Emissão de novas legislações sobre segurança ou armazenamento de dados na Cloud.	Elevada
ER10	Dificuldade de monitorização dos níveis de serviço do fornecedor de serviço cloud.	
ER11	Falhas de funcionamento de serviço.	N/A
ER12	Incapacidade do prestador alocar recursos IT face às necessidades (pontuais ou não) da organização	Muito baixa
ER13	Prestador de serviço não adequado às necessidades da organização	
ER14	Necessidade de rápida implementação de serviços e redução de custos	
ER15	Maior exposição a ataques Informáticos	
ER16	Desastre Natural	

Tabela 26 - ENISA levantamento e valores de impacto de consequência

CONSEQUÊNCIAS		
ID	**NOME**	**ENISA RANK**
C1	Inatividade da organização.	Elevado
C2	Deterioração da imagem e confiabilidade da DGO e fornecedor CN	Alto
C3	Dificuldade de operacionalidade ou cumprimentos de objetivos.	Elevado
C4	Necessidade de mudança de serviço CN ou regresso a sistema IT tradicional.	Médio
C5	Danos em equipamentos e/ou Instalações	Alto
C6	Implicações criminais	Alto
C7	Divulgação ou inconsistência de dados privados	Alto
C8	Dificuldade de colocar em funcionamento novos serviços	
C9	Dificuldade de aplicação de coimas ou indeminizações	
C10	Perda e inconsistência de informação	
C11	Não concretização da mudança para a Cloud ou sua manutenção	
C12	Quebra de serviço ou inatividade da organização	
C13	Funcionamento deficiente	
C14	Segurança reduzida	
C15	Falta de conetividade aos dados e Inoperacionalidade da organização	

Tabela 27 - ENISA levantamento e valores dos Ativos de uma organização

ENISA List of ASSETS	VALOR
A1 Company reputation	Very High
A2 Customer trust	Very High
A3 Employee loyalty and experience	High
A4 Intellectual property	High
A5 Personal sensitive data	Very High
A6 Personal data	Medium
A7 Personal data - critical	High
A8 HR data	High
A9 Service delivery – real time services	Very High
A10 Service delivery	Medium
A11 Access control	High
A12 Credentials	Very High
A13 User directory	High
A14 Cloud service mng Interface	Very High
A15 Management interface APIs	Medium
A16 Network (connections, etc)	High
A17 Physical hardware	Low

Tabela 28 - Cálculo do nível de risco

ID Evento	NOME EVENTO	VEROSIM.	Valor	ID Risco	NOME RISCO
ER1	Ataque informático	Elevada	0,96	RO1	Perda e não integridade de dados
ER2	Escassez de recursos técnicos especializados	Média	0,45	RO2	Dificuldade de contratação de pessoal especializado
ER3	Ineficiente gestão financeira e de IT	Média	0,5	RO3	Custos Financeiros não contabilizados/suportados
ER4	Inexperiência e falta de conhecimento em gestão Computação em Nuvem	Média	0,54	RO4	Dificuldade de governação do sistema *Cloud*
ER5	Ataques de engenharia social	M.Baixa	0,1	RO5	Ataques de engenharia social
ER6	Não aplicabilidade de normas de segurança.	Elevada	0,92	RO6	Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas)
ER8	Falta de definição contratual de responsabilidades e sua operacionalização.	Alta	0,71	RO7	Falta de uma efetiva responsabilidade sobre os dados
ER15	Desastre Natural	M. Baixa	0,79	RO8	Desastres Naturais
ER9	Emissão de novas legislações sobre segurança ou armazenamento de dados na *Cloud*	Baixa	0,26	RL1	Mudanças legislativas de segurança ou armazenamento de dados na *Cloud* (apagar dados, segurança periférica, backups e políticas de testes, etc)
ER13	fornecedor de serviço não adequado às necessidades da organização	Média	0,58	RT1	Dificuldade de mudança para novo fornecedor de serviço *Cloud - Lockin*
ER11	Falhas de funcionamento de serviço.	Média	0,5	RT2	Maior dependência de terceiros
ER10	Dificuldade de monitorização dos níveis de serviço do fornecedor Computação em Nuvem	Média	0,1	RT3	Incumprimento ou difícil análise de SLA's por parte dos fornecedores de serviço
ER7	Mudança de um paradigma de IT tradicional para Computação em Nuvem.	Alta	0,58	RT4	Maior exposição a ataques informáticos.
ER14	Necessidade de rápida implementação de serviços e redução de custos	Média	0,46	RT5	Dificuldade de isolamento de aplicações e serviços
ER12	Incapacidade do fornecedor CN alocar recursos IT face às necessidades	Baixa	0,1	RT6	Incapacidade do fornecedor cloud alocar recursos IT às necessidades da organização.

Tabela 29 - Cálculo nível de risco (cont)

D Risco	NOME RISCO	ID Cq	NOME CONSEQUÊNCIA	IMP.	Valor #	Valor N. Ri	N.Risco
RO1	Perda e não integridade de dados	C10	Perda e inconsistência de informação	Elevado	40	38,40	Elevado
RO2	Dificuldade de contratação de pessoal especializado	C3	Dificuldade de operacionalidade ou cumprimentos de objetivos.	Elevado	36,7	16,52	Médio
RO3	Custos Financeiros não contabilizados/suportados	C4	Necessidade de mudança de serviço Cloud ou regresso a sistema IT tradicional.	Médio	11,7	5,85	Baixo
RO4	Dificuldade de governação do sistema Cloud	C11	Não concretização da mudança para a Cloud ou sua manutenção	Alto	21,7	11,72	Médio
RO5	Ataques de engenharia social	C5	Danos em equipamentos e/ou Instalações	Alto	15,8	1,58	M. Baixo
RO6	Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas)	C12	Quebra de serviço ou inatividade da organização	Elevado	40	36,80	Elevado
RO7	Falta de uma efetiva responsabilidade sobre os dados	C13	Funcionamento deficiente	Muito Baixo	1,6	1,26	M. Baixo
RO8	Desastres Naturais	C15	Falta de conetividade aos dados e Inoperacionalidade da organização	Elevado	36,7	3,67	M. Baixo
RL1	Mudanças legislativas de segurança ou armazenamento de dados na Cloud (apagar dados, segurança periférica, backups e políticas de testes, etc)	C6	Implicações criminais	Alto	21,7	5,64	Baixo
RT1	Dificuldade de mudança para novo fornecedor de serviço Cloud - *Lockin*	C8	Dificuldade de colocar em funcionamento novos serviços	Baixo	6,7	3,89	M. Baixo
RT2	Maior dependência de terceiros	C1	Inatividade da organização.	Elevado	36,7	18,35	Alto
RT3	Incumprimento ou difícil análise de SLA's por parte dos fornecedores de serviço	C9	Dificuldade de aplicação de coimas ou indeminizações	Médio	12,5	7,25	Baixo
RT4	Maior exposição a ataques informáticos.	C7	Divulgação ou inconsistência de dados privados	Elevado	18,3	12,99	Médio
RT5	Dificuldade de isolamento de aplicações e serviços	C14	Segurança reduzida	Elevado	36,7	16,88	Médio
RT6	Incapacidade do fornecedor cloud alocar recursos IT às necessidades da organização.	C2	Deterioração da imagem e confiabilidade da organização e fornecedor de serviço Cloud.	Alto	21,7	2,17	M. Baixo

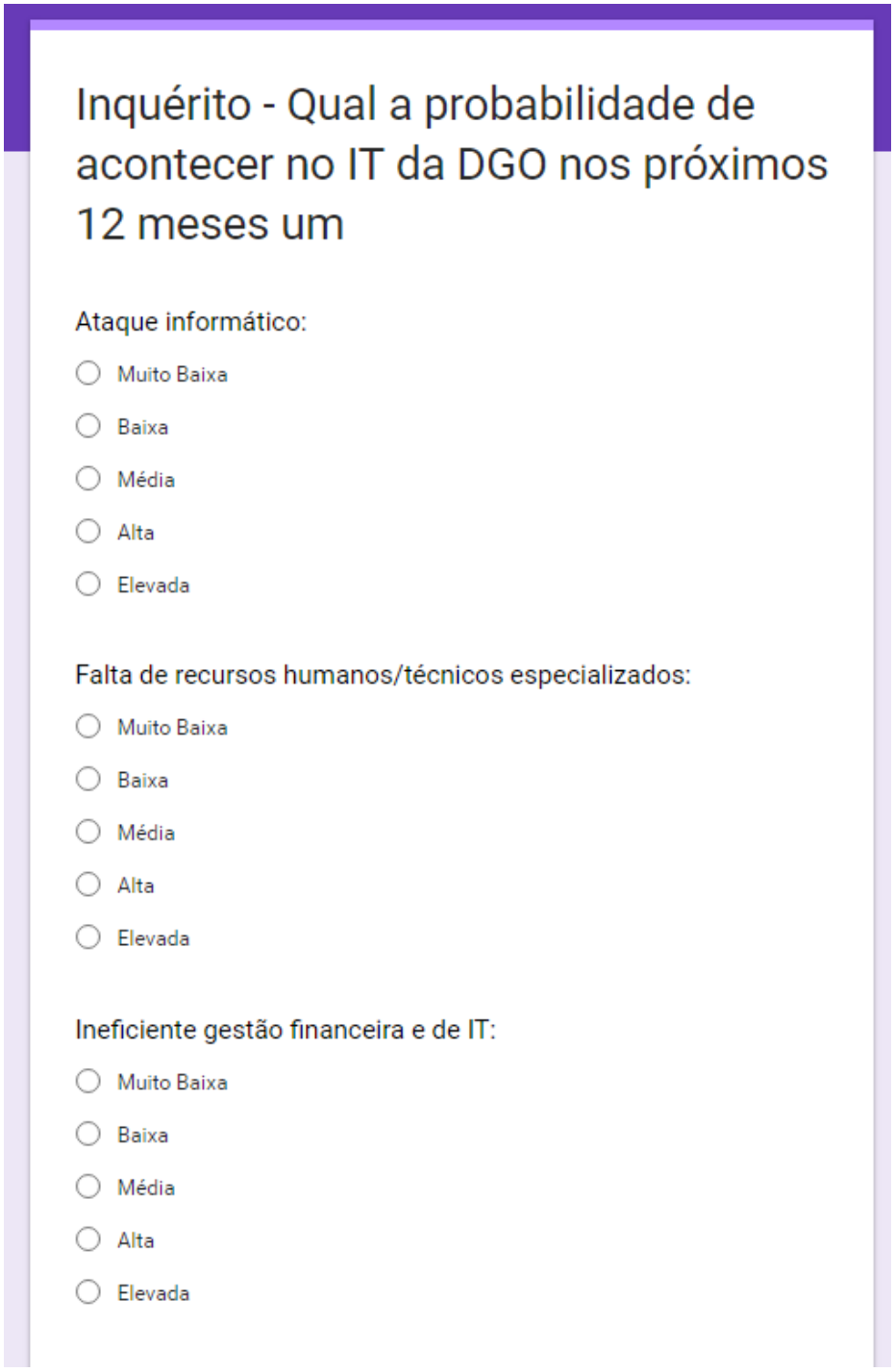
Tabela 30 - Estudo riscos de outras organizações comparando com os riscos definidos no caso prático

ID	NOME RISCO Tese	ENISA	COSO	Organização OWSAP
RISCOS ORGANIZACIONAIS				
R01	Perca de informação	R15 - Loss of Cryptographic Keys R17 - Loss of Backups	Risk of data leakage	
R02	Dificuldade de contratação de pessoal			
R03	Custos Financeiros não			Financial Risk
R04	Dificuldade de governação do sistema Computação em Nuvem	R2 - Loss of governance	IT organizational changes	R2 - User Identity Federation
R05	Ataques de engenharia social	R5 - Social engineering attacks		R10 - Non Production Environment
R06	Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas)	R4 - Conflicts between customer hardening procedures and cloud environment		R9 - Infrastructure Security
R07	Falta de uma efetiva responsabilidade			R1 - Accountability and Data Ownership
R08	Desastres Naturais	R18 - Natural disasters		
RISCOS LEGAIS				
RL1	Mudanças legislativas de segurança ou armazenamento de dados na Cloud (apagar dados, segurança periférica, backups e politicas de testes, etc)	R19 - Subpoena and e-discovery R20 - Risk from changes of jurisdiction R21 - Data protection risks Legislation	Security and compliance concerns	R3 - Regulatory Compliance R8 - Incidence Analysis and Forensic Support
RISCOS TÉCNICOS				
RT1	Dificuldade de mudança para novo fornecedor de serviço cloud - lockin	R1 - Lock-in R23 - Intellectual Property Issues - Locked services	Vendor lock-in and lack of application portability or interoperability Residing in the same risk ecosystem as the CSP and other tenants of the cloud	
RT2	Maior dependência de terceiros	R3 - Supply Chain Failure	Cloud service provider viability	
RT3	Incumprimento ou difícil análise de SLA's dos fornecedores de serviço	R22 - Licensing Issues	Lack of transparency	R4 - Business Continuity and Resiliency
RT4	Maior exposição a ataques informáticos.	R8 - Cloud provider malicious insider - abuse of high privilege roles R9 - Management interface compromise (manipulation, availability of infrastructure) R12 - Distributed denial of service (DDoS) R13 - Economic denial of service (EDoS)	High-value cyber-attack targets	R5 - User Privacy and Secondary Usage o
RT5	Dificuldade de isolamento de aplicações e serviços	R7 - Isolation failure		R7 - Multi Tenancy and Physical Security
RT6	Não Integridade de dados	R10 - Intercepting data in transit		R6 - Service and Data Integration
RT7	Incapacidade do fornecedor cloud alocar recursos TI às necessidades da	R6 - Resource Exhaustion	Reliability and performance issues	

Tabela 31 - Estudo riscos de outras organizações comparando com os riscos definidos no caso prático (cont)

ID	NOME RISCO Tese	Microsoft	Organização CSA	Organização NSA
RISCOS ORGANIZACIONAIS				
RO1	Perca de informação	Backup Failure Log & Tracing failure Theft of Computer Equipment	Data Loss	
RO2	Dificuldade de contratação de pessoal	Human Resource Constraints	Insufient Due Deligence	
RO3	Custos Financeiros não			
RO4	Dificuldade de governação do sistema Computação em Nuvem	Governance and Enterprise Risk Management Governance Degradation Poor Provider Selection	Misaligned or cloud strategy	
RO5	Ataques de engenharia social			
RO6	Não alinhamento de processos de segurança entre partes (organização, fornecedor cloud, outras empresas)	Compliance and Audit Management Audit or Certification unavailable Compliance Degradation Information Management and Data Security Sensitive Media Sanitization Sensitive Information Leakage	Misaligned or cloud strategy	Reliability and Denial of Servic
RO7	Falta de uma efetiva responsabilidade			
RO8	Desastres Naturais			
RISCOS LEGAIS				
RL1	Mudanças legislativas de segurança ou armazenamento de dados na Cloud (apagar dados, segurança periférica, backups e politicas de testes, etc)	Legal Issues : Contracts and Electronic Discovery Storage of data in multiple jurisdictions and lack of transparency		
RISCOS TÉCNICOS				
RT1	Dificuldade de mudança para novo fornecedor de serviço cloud - lockin	Lock-In Data migration from on-premise into the cloud (regardless whether public, private or hybrid)		Cloud Portability and continui
RT2	Maior dependência de terceiros			
RT3	Incumprimento ou difícil análise de SLA's dos fornecedores de serviço	Incident Response Lack of Supplier Redundancy Incident Response		
RT4	Maior exposição a ataques informáticos.	Malicious Activities from an Insider	Denial of Service Data Breaches Abuse and Nefarious Cloud Services Malicious Insiders Advanced Persisten Threads	
RT5	Dificuldade de isolamento de aplicações e serviços	Interoperability and Portability Isolation Failure	Insecure API Shared Tecnologies Issue System and Application Vulnerabilities	Insecure API Multi-Tenancy
RT6	Não Integridade de dados	Data Protection Risks Sensitive Information Leakage		
RT7	Incapacidade do fornecedor cloud alocar recursos TI às necessidades da	Capacity Management Environment Agility / Time to Market		

Tabela 32 - Inquérito realizado aos técnicos para cálculo de probabilidade de evento (extrato de inquérito)



Inquérito - Qual a probabilidade de acontecer no IT da DGO nos próximos 12 meses um

Ataque informático:

- Muito Baixa
- Baixa
- Média
- Alta
- Elevada

Falta de recursos humanos/técnicos especializados:

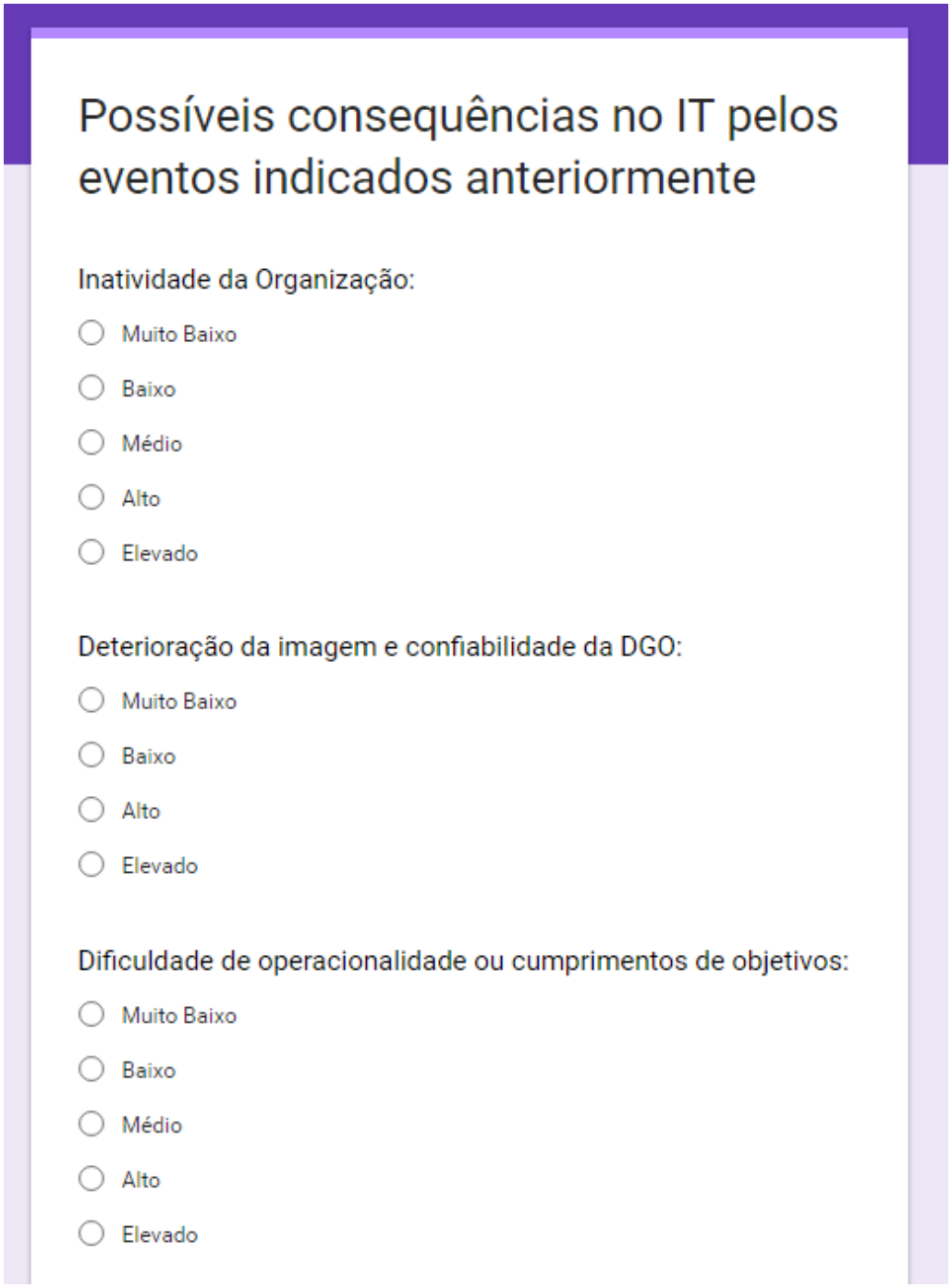
- Muito Baixa
- Baixa
- Média
- Alta
- Elevada

Ineficiente gestão financeira e de IT:

- Muito Baixa
- Baixa
- Média
- Alta
- Elevada

~

Tabela 33 - Inquérito realizado aos técnicos para cálculo do valor de impato de evento (extrato de inquérito)



Possíveis consequências no IT pelos eventos indicados anteriormente

Inatividade da Organização:

- ○ Muito Baixo
- ○ Baixo
- ○ Médio
- ○ Alto
- ○ Elevado

Deterioração da imagem e confiabilidade da DGO:

- ○ Muito Baixo
- ○ Baixo
- ○ Alto
- ○ Elevado

Dificuldade de operacionalidade ou cumprimentos de objetivos:

- ○ Muito Baixo
- ○ Baixo
- ○ Médio
- ○ Alto
- ○ Elevado