Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Proposta de um instrumento de análise de riscos para auxiliar na tomada de decisão de migração de ambiente tradicional para Nuvem privada: Um estudo de caso da Fundação Oswaldo Cruz

Tharcísio Marcos Ferreira de Queiroz Mendonça

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. Edgard Costa Oliveira

Brasília
2018

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Mp

Mendonça, Tharcísio Marcos Ferreira de Queiroz
Proposta de um instrumento de análise de riscos para auxiliar na tomada de decisão de migração de ambiente tradicional para Nuvem privada: Um estudo de caso da Fundação Oswaldo Cruz / Tharcísio Marcos Ferreira de Queiroz Mendonça; orientador Edgard Costa Oliveira. -- Brasília, 2018.
102 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2018.

1. Computação em nuvem. 2. Decisão de migração. 3. Gestão de riscos. I. Oliveira, Edgard Costa, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Proposta de um instrumento de análise de riscos para auxiliar na tomada de decisão de migração de ambiente tradicional para Nuvem privada: Um estudo de caso da Fundação Oswaldo Cruz

Tharcísio Marcos Ferreira de Queiroz Mendonça

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Edgard Costa Oliveira (Orientador)
CIC/UnB

Prof.ª Dr.ª Simone Borges Simão Monteiro
EPR/UnB

Prof. Dr. Ricardo Barros Sampaio
Fiocruz/UNB

Prof.ª Dr.ª Aletéia Patrícia Favacho de Araújo
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 09 de julho de 2018

Dedicatória

Primeiramente a Deus por todas as conquistas e pela fortaleza que tem sido na minha vida.

A minha mãe por todo amor, carinho e dedicação.

A minha querida esposa Emely Nogueira por todo amor, compreensão e apoio ao longo dessa trajetória.

Ao meu filho amado Arthur Queiroz que é a maior benção que Deus na vida da nossa família.

Agradecimentos

Agradeço principalmente ao orientador e amigo Prof.Dr. Edgard Costa pela confiança, paciência e serenidade.

Agradeço aos meus colegas de trabalho Misael Araújo e Fernando Provazzi por todo apoio prestado.

Agradeço especialmente ao PPCA (Programa de Pós-Graduação em Computação Aplicada) e a Universidade de Brasília-UNB por todo conhecimento e apoio ao longo de toda trajetória de acadêmica.

Resumo

A computação em nuvem propõe uma nova abordagem de tecnologia como serviço contrapondo os dispendiosos e caros centros de dados mantidos pelas organizações. Nessa perspectiva, a Fiocruz construiu um centro de dados em nuvem para oferecer infraestrutura como serviços (IaaS) para as suas unidades regionais, com a proposta de reduzir gastos com infraestrutura de TIC local. Porém, após todo investimento ainda assim poucas unidades migraram seus serviços para nuvem Fiocruz. Diante disso, este estudo propôs uma ferramenta alinhada ao processo de avaliação de riscos sob a ótica da norma NBR ISO 31000:2009 para auxiliar os tomadores de decisão das unidades regionais da Fiocruz a migrar suas soluções tecnológicas, que rodam em ambientes locais das próprias unidades, para a plataforma de computação em nuvem projetada pela Fiocruz. Para tanto, o desenho da ferramenta tomou como base os principais estudos, por meio de pesquisa bibliográfica e documental na literatura, sobre gestão de riscos alinhados ao processo de migração em nuvem. A partir desses estudos, foi possível definir os principais métodos e técnicas alinhados ao processo de gestão de riscos da norma NBR ISO 31000:2009 aplicadas na migração para nuvem. O fluxo da ferramenta passa inicialmente pela ponderação dos critérios de decisão e objetivos estratégicos, realizados a partir de análise multicritério. A próxima etapa cria os mapas de riscos para os ambientes local e em nuvem para que seja encontrado o Nível de Risco Residual (NRR) agrupados por critérios de riscos definidos. Essa etapa utiliza matriz de probabilidade e impacto para calcular o NRR. Por fim, a etapa final cria uma matriz de decisão que apresenta a melhor decisão a partir do cálculo do NRR com os critérios de decisão ponderados. A validação de aplicação da ferramenta foi realizada no contexto da Gerência Regional de Brasília-GEREB da Fiocruz, no qual demonstrou ser viável o uso da ferramenta para auxiliar no processo de tomada de decisão.

Palavras-chave: computação em nuvem, decisão de migração, gestão de riscos

Abstract

Cloud computing proposes a new technology-as-a-service approach by countering the costly and expensive data centers maintained by organizations. In this perspective, Fiocruz has built a cloud data center to provide infrastructure as a service (IaaS) for its regional units, with a proposal to reduce spending on local ICT infrastructure. However, after all the investment, however, few units migrated their services to Fiocruz cloud. In view of this, this study proposed a tool aligned to the process of risk assessment from the perspective of the ISO 31000: 2009 standard to help decision makers of the Fiocruz regional units to migrate their technological solutions, which run in local environments of the units themselves , for the cloud computing platform designed by Fiocruz. To do so, the tool design was based on the main studies through bibliographic and documentary research in the literature on risk management aligned in the process of migration in the cloud. From these studies it was possible to define the main methods and techniques in line with the risk management process of NBR ISO 31000: 2009 standard applied to the migration to the cloud. The flow of the tool initially passes through the weighting of the decision criteria and strategic objectives, based on multicriteria analysis. The next step creates risk maps for the local and cloud environments to find the Residual Risk Level (NRR) grouped by defined risk criteria. This step uses probability and impact matrix to calculate the NRR. Finally, the final step creates a decision matrix that presents the best decision from the calculation of the NRR with the weighted decision criteria. The validation of the application of the tool was carried out in the context of the Regional Management of Brasília-GEREB of Fiocruz, in which it proved feasible the use of the tool to assist in the decision-making process.

Keywords: cloud computing, decision migration, risk management

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

APF Administração Pública Federal.

Fiocruz Fundação Oswaldo Cruz.

IaaS Infraestrutura como Serviço.

MP Ministério do Planejamento.

MS Ministério da Saúde.

NIST National Institute of Standards and Technology.

PaaS Plataforma como Serviço.

PDTI Plano Diretor de Tecnologia da Informação.

PETI Planejamento Estratégico de Tecnologia da Informação.

SaaS Software como Serviço.

SISP Sistema de Administração dos Recursos de Tecnologia da Informação.

SUS Sistema Único de Saúde.

TCU Tribunal de Contas da União.

Capítulo 1

Introdução

1.1 Contextualização

Um dado é uma pequena parcela responsável por agregar valor a uma informação. Siqueira [18] define que "a informação pode ser definida como um dado acrescido de contexto, relevância e propósito". O que tem sido relevante é a mudança fundamental no significado que a informação assume na nova realidade mundial de uma sociedade globalizada: agora a informação não é apenas um recurso, mas o recurso [19].

No entanto, esse importante recurso vem exigindo cada vez mais aporte computacional, tecnológico e de recursos humanos para o seu tratamento. Seja na área da saúde, educação ou em qualquer área do conhecimento, sempre haverá a necessidade de uma plataforma tecnológica para processar e gerar o conhecimento esperado. Costa et al. [20] destacam que é reconhecido que muitos dos avanços recentes em pesquisas científicas somente foram possíveis devido à habilidade dos cientistas em usar eficientemente computadores para gerar e processar grandes quantidades de dados. Araújo [21] acrescenta que a dependência cada vez maior dos serviços de TI, cresce a expectativa das organizações sobre uma área de TI eficiente e capaz de suportar adequadamente seus objetivos.

Para Marston et al. [22], a computação, como sabemos hoje, reflete um paradoxo - por um lado, os computadores continuam a se tornar exponencialmente mais poderosos e o custo por unidade de computação continua a cair rapidamente, de tal forma que o poder de computação atualmente é considerado como uma commodity.

Nessa perspectiva, surgem modelos atraentes capazes de proporcionar uma infraestrutura super provisionada com escalabilidade, confiabilidade e interoperabilidade em nuvem [23]. As nuvens são um grande conjunto de recursos virtuais facilmente utilizáveis e acessíveis, como hardware, plataformas de desenvolvimento e serviços [24].

Segundo Gartner [25], em um estudo realizado em 2016, mais de US$ 1 trilhão em gastos com TI serão direta ou indiretamente afetados pela mudança para a nuvem durante

os próximos cinco anos. De acordo com a empresa, as despesas de TI estão mudando constantemente das ofertas tradicionais (*on-premise*) de TI para serviços em nuvem (mudança de nuvem). A quantidade agregada de mudança para nuvem em 2016 é estimada em US $ 111 bilhões, aumentando para US $ 216 bilhões em 2020. No Brasil, estimativas da Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação (Brasscom) indicam que o setor de TICs representa cerca de 8% do PIB brasileiro, com viés de crescimento [26]. Segundo dados do Tribunal de Contas da União (TCU) [26], para o exercício de 2014 o orçamento de TI de todo Governo Federal totalizou R$ 16,3 bilhões. O relatório do TCU aponta que as maiores despesas de TI são, por ordem: serviços técnicos profissionais de TI, equipamentos, suporte de infraestrutura, comunicação de dados, manutenção de software, aquisição de software, desenvolvimento de software e suporte a usuários.

Diante do cenário político e financeiro, diversas empresas, órgãos de governo, universidades e até mesmo fundações e institutos de pesquisa vem aderindo ao modelo de computação em nuvem. Em 2012, a USP iniciou um processo de construção de um ambiente de nuvem privada para ajudá-la a superar o desafio de ter 150 ambientes de TI diferentes e uma crescente demanda por recursos computacionais e de armazenamento em seu dinâmico ambiente de pesquisas. A proposta da solução é facilitar o monitoramento e o gerenciamento dos servidores, além do controle dos backups e dimensionamento da real necessidade de processamento e armazenamento de cada unidade da USP, eliminando gastos com equipamentos ociosos [27]. A primeira versão da InterNuvem USP reduziu os 150 datacenters da universidade para apenas 6 e consolidou os ambientes corporativo, educacional e de pesquisas em um único com recursos consolidados que podem ser requisitados diretamente pelos usuários. O projeto inicial foi um grande sucesso e permitiu que a universidade reduzisse seus recursos físicos de armazenamento em 90%, embora os dados em si tenham crescido mais de 300%, possibilitando aumentar enormemente a eficiência operacional de TI [28].

Esse novo conceito, cercado por várias tecnologias e procedimentos inovadores, apresenta também uma série de riscos que exigem dos tomadores de decisão um instrumento de gestão de riscos capaz de auxiliá-los nesse processo de mudança. Migrar todo um ambiente, ou mesmo parte dele, para uma plataforma de nuvem envolve uma série de fatores de riscos que poderão influenciar os objetivos da organização.

Nessa linha, uma pesquisa realizada pela Symantec em 2011 [29] verificou que as organizações que já implementaram tecnologias de nuvem não alcançaram os objetivos esperados. Os resultados apresentaram discrepâncias significativas entre o que as organizações estavam esperando alcançar e o que elas realmente obtiveram. Segundo a pesquisa, 89 por cento dos entrevistados esperavam que com Cloud, melhoraria a agilidade da TI.

Mas apenas 47 por cento constataram que isso realmente aconteceu. Mas grande parte desta discrepância está relacionada à equipe de TI das organizações. Três entre quatro organizações admitiram que "alterar a forma como a TI opera" foi um desafio "significativo" ou até "extremo" para alcançar o sucesso na nuvem.

A migração de infraestruturas de TI tradicionais ou *on-premise* para a nuvem levanta atualmente uma série de perguntas. Procedimentos comuns inexistentes e a falta de ferramentas para suporte estão entre as principais preocupações. Especialistas em migração contam com sua própria experiência e algumas ferramentas básicas para facilitar o processo [30]. Além disso, a heterogeneidade dos sistemas dentro das organizações e suas necessidades aumentaram a complexidade da tomada de decisões no que diz respeito à migração para soluções baseadas em nuvem. A decisão de migrar os sistemas existentes para as soluções de nuvem pode ser complicada, uma vez que requer a avaliação dos benefícios, riscos e custos que não são muito simples [31].

Estratégia de negócios e ambiente de nuvem constituem a fase de inteligência do processo de tomada de decisão que podem ser apoiados através do nível de inteligência da base de conhecimento institucional. O processo começa definindo a estratégia de negócios para a migração. As organizações buscam explorar a nuvem para alcançar três objetivos principais: redução de custos, inovação de negócios e backup. Eles precisam examinar ambientes internos e externos para adotar uma estratégia que atenda às suas necessidades e lhes permita ganhar uma vantagem competitiva [31].

No entanto, para que a computação em nuvem atinja seu potencial, é necessário que haja uma compreensão clara dos vários problemas envolvidos, tanto das perspectivas dos provedores quanto dos consumidores da tecnologia [22]. Como pode ser observado, esse processo de migração para uma plataforma em nuvem envolve incertezas que precisam ser gerenciadas. Para tanto, a gestão de riscos sob a ótica da norma NBR ISO 31000:2009 é um instrumento capaz de auxiliar os tomadores de decisão a partir de um modelo que possibilita a organização [3], por exemplo:

- Aumentar a probabilidade de atingir os objetivos;
- Melhorar a identificação de oportunidades e ameaças;
- Melhorar a confiança das partes interessadas;
- estabelecer uma base confiável para a tomada de decisão e o planejamento;
- Melhorar a eficácia e a eficiência operacional;
- Minimizar perdas;

1.2 Descrição do problema

O advento da computação em nuvem (*cloud computing*) proporcionou uma nova forma de prover soluções de Tecnologia da Informação em formato de serviços. Contrapondo os dispendiosos e caros centros de dados (*datacenters*), a computação em nuvem apresenta nesse formato diversos benefícios que vão desde a rapidez em prover uma ou mais soluções sob demanda, em poucos minutos, até o acesso a uma variedade de recursos em que toda complexidade tecnológica é abstraída para o cliente. Porém, a proposta de migrar as soluções de seus ambientes locais para uma plataforma em nuvem gera um certo receio por parte dos gestores de TI que necessitam de meios para gerenciar os riscos envolvidos nesse processo de tomada de decisão.

Nessa perspectiva, a Fundação Oswaldo Cruz investiu alto para desenvolver o projeto de Nuvem Fiocruz com o objetivo de prover as unidades regionais uma plataforma de infraestrutura (IaaS) em formato de serviços. Foram pouco mais de R$ 53.254.082,00 investidos para construção do projeto Nuvem Fiocruz. Porém, desde a sua inauguração, no segundo semestre de 2016, ainda é tímida a migração da unidades para a nova plataforma tecnológica.

Entretanto, após uma análise nos dados de uso da plataforma de nuvem Fiocruz, foi possível analisarmos que somente 6 unidades fazem algum tipo de uso da solução, conforme apresentado na tabela 1.1. Segundo relatório apresentado na tabela 1.1, todos os serviços em uso na plataforma estão custando por volta de R$ 111.001,79 por ano desde a sua inauguração em novembro de 2016.

Tabela 1.1: Relação de unidades que fazem uso da Nuvem Fiocruz .

Unidade	**Gasto anual**	**vCPU (Qtd)**	**RAM (MB)**	**Disco (GB)**	**Instancias**
A	R$ 37.810,70	44	90.112	12000	13
B	R$ 27.908,18	46	69.632	2000	17
C	R$ 27.468,75	48	98304	3000	6
D	R$ 10.727,02	10	10240	3000	1
E	R$ 6.134,03	12	1228	180	3
F	R$ 953,11	9	18432	360	5
Total	**R$ 111.001,79**	**169**	**287.948**	**20.540**	**45**

Após realizar um balanço orçamentário do período de 2014 a 2017, com base nos PDTIs de 2015-2016 e 2016-2017, contatou-se que a quantidade de investimentos orçados em datacenter para as unidades regionais saltou de R$ 13.656.863,96, no PDTI de 2015-2016, para R$ 30.637.305,42, PDTI 2016-2017, conforme demostrado na Figura 1.2. Em relação a tabela 1.1 e a figura 1.2, percebemos que as unidades reginais tem preterido investimentos nos datacenters locais ou tradicionais (*on-premise*) ao invés de migrarem suas soluções para nuvem Fiocruz. Esse visão é importante porque demonstra certo

receio pelas unidades regionais em fazer uso da nova plataforma de serviços em nuvem da Fiocruz.

Tabela 1.2: Balanço orçamentário de TI Fiocruz 2015 a 2017 (Elaboração própria)

Unidade	Orçamento PDTI 2015-2016	Orçamento datacenter 2015-2016	Orçamento PDTI 2016-2017	Orçamento datacenter 2016-2017
IOC	R$ 5.790.679,00	R$ 350.000,00	R$ 9.946.883,28	R$ 617.971,28
IFF	R$ 8.294.942,52	R$ 225.000,00	R$ 8.245.460,00	R$ 550.000,00
ENSP	R$ 9.575.276,51	R$ -	R$ 14.892.198,98	R$ 4.655.680,00
ICICT	R$ 1.899.200,00	R$ 705.650,00	R$ 1.857.500,00	R$ 707.650,00
Biomanguinhos	R$ 19.406.581,08	R$ 960.000,00	R$ 70.805.004,59	R$ 3.830.421,99
Farmanguinhos	R$ 13.908.450,00	R$ 2.379.615,00	R$ 29.732.680,00	R$ 11.446.000,00
EPSJV	R$ 913.155,12	R$ -	R$ 2.154.409,97	R$ -
COC	R$ 942.040,00	R$ 516.620,00	R$ 716.800,00	R$ 386.200,00
INI	R$ 2.528.138,00	R$ -	R$ 503.640,00	R$ -
ICTB	R$ 753.138,92	R$ 12.000,00	R$ 772.739,02	R$ 8.000,00
CPqRR	R$ 1.207.548,70	R$ -	R$ 2.066.967,60	R$ 870.510,00
CPqAM	R$ 1.060.500,00	R$ 85.000,00	R$ 575.100,00	R$ 15.000,00
CPqGM	R$ 3.977.915,29	R$ 1.381.620,50	R$ 6.093.589,77	R$ 1.504.314,70
ILMD	R$ 619.000,00	R$ -	R$ 496.256,60	R$ -
ICC	R$ 772.208,46	R$ 166.358,46	R$ 2.349.867,90	R$ 915.167,90
INCQS	R$ 5.119.832,09	R$ -	R$ 11.685.810,05	R$ 3.077.888,55
Fiocruz Rondônia	R$ 87.387,00	R$ -	R$ 66.000,00	R$ 36.000,00
Fiocruz MS	R$ 50.400,00	R$ -	R$ 119.000,00	R$ 16.500,00
GEREB	R$ 14.123.484,18	R$ 6.875.000,00	R$ 8.251.240,34	R$ 2.000.000,00
Presidência	R$ 81.426.730,94	R$ -	R$ 64.483.409,71	R$ -
Total Geral	**R$ 172.456.607,81**	**R$ 13.656.863,96**	**R$ 235.814.557,81**	**R$ 30.637.304,42**

Além do mais, como as diversas unidades da Fiocruz possuem fontes diversas de recursos que não dependem da União, os gastos infraestrutura de TIC tendem a ser maiores que os apresentados na tabela 1.2.

Diante do cenário apresentado, as unidades da Fiocruz tem a disposição uma importante plataforma para migração dos ambientes tradicionais para Nuvem Privada da própria instituição. Apesar das facilidades e propostas que essa plataforma oferece, vários vetores de riscos influenciam ou não esse processo de decisão. Dessa forma, é possível destacar alguns fatores para o problema:

- Como auxiliar as unidades da Fiocruz no processo de decisão de migração do ambiente tradicional para Nuvem Privada?
- Quais riscos envolvidos?
- Quais critérios considerar nesse processo de migração?
- Como a gestão de riscos pode auxiliar no processo de tomada de decisão?

1.3 Justificativa

A diversidade das unidades regionais da Fiocruz, bem como as suas particularidades, exigem um grau de cuidado maior para se definir um processo de migração de um ambiente tradicional para a nuvem privada Fiocruz. Há unidades que trabalham em ambientes críticos com plataforma de EAD (Educação a Distância), por exemplo, que exigem recursos contínuos e boa infraestrutura para atender aos alunos em qualquer período de tempo. Outras que desenvolvem projetos científicos interdisciplinares nas áreas de epidemiologia, estatística, bioinformática, computação entre outras, para estudos em grandes bases de dados ("big data") e que exigem recursos computacionais de alto desempenho e seguro.

Além do mais, há unidades da Fiocruz que possuem fontes de recursos diversas como projetos e financiamentos por instituições de fomento a ensino e pesquisa como CNPq[1], OPAS[2] e FAPDF[3], por exemplo. Essas unidades acabam por financiar os próprios projetos de TIC sem necessariamente precisar de recursos da União e, consequentemente, diretamente da própria Fiocruz. Diante disso, a Fiocruz possui um grande desafio de auxiliar os tomadores de decisão dessas unidades a migrar seus ambientes de TIC para Nuvem Fiocruz.

A norma NBR ISO/IEC 3104:2015 apresenta que uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e resultados consistentes, confiáveis e comparáveis [32]. Segundo a norma, uma abordagem consistente para gerir riscos no momento da tomada de decisões tornará a organização mais eficiente, e pode fornecer resultados que criam confiança e sucesso. Isto requer práticas organizacionais que considerem os riscos associados a todas as decisões, bem como a utilização de critérios de riscos consistentes que se relacionam com os objetivos das organizações e o escopo de suas atividades [32].

Uma abordagem oportuna significa que o processo de gestão de riscos é aplicado no ponto ideal do processo e tomada de decisões. Diante disso, a contribuição esperada nesse estudo é que a ferramenta alinhada ao processo de avaliação de riscos, sob a ótica da norma NBR ISO/IEC 31000:2009, sirva como instrumento capaz de fornecer às partes responsáveis das unidades regionais da Fiocruz um entendimento aprimorado dos riscos de modo a auxiliá-los no processo de tomada de decisão para migração de seus ambientes tradicionais para Nuvem Fiocruz.

[1]Conselho Nacional de Desenvolvimento Científico e Tecnológico
[2]Organização Pan-Americana da Saúde
[3]Fundação de Apoio a Pesquisa do Distrito Federal

1.4 Objetivos

1.4.1 Objetivo Geral

Proposta de um instrumento de análise de riscos para auxiliar na tomada de decisão estratégica de migração de um ambiente tradicional para nuvem

1.4.2 Objetivos Específicos

- Definir critérios para tomada de decisão de migração para ambiente de nuvem
- Desenhar o fluxograma de atividades da ferramenta com base em critérios definidos
- Validar a aplicação da ferramenta no contexto de uma unidade regional da Fiocruz

1.5 Estrutura do trabalho

Este trabalho está estruturado em sete capítulos.

- **Capítulo 1** - Desenvolve a introdução a partir da contextualização do assunto, além de apresentar a problemática, justificativa e objetivos geral e específicos da pesquisa.
- **Capítulo 2** - Apresenta a revisão de literatura que trata dos aspectos inerentes relacionados a computação em nuvem e gestão de riscos bem como o estado da arte.
- **Capítulo 3** -Desenvolve a metodologia de pesquisa.
- **Capítulo 4** - Apresenta a proposta da ferramenta e o desenho do fluxograma de atividades.
- **Capítulo 5** - Estabelece o contexto da unidade no qual será aplicada a ferramenta.
- **Capítulo 6** - Valida a aplicação da ferramenta em uma unidade regional da Fiocruz a partir do contexto estabelecido no capítulo 5.
- **Capítulo 7** - Apresenta a conclusão do pesquisa.

Capítulo 2

Revisão de literatura

2.1 Computação em nuvem

A proposta da computação em nuvem veio com o objetivo de abstrair toda complexidade tecnológica envolvida para prover ao usuário um modelo simplificado em formato serviço. De acordo com Sultan [33], termo "nuvem"provavelmente foi inspirado por ilustrações de livros de texto de TI que descrevem ambientes remotos (por exemplo, a Internet) como imagens de nuvem, a fim de ocultar a complexidade que está por trás delas.

De modo geral, a computação em nuvem (*cloud computing*) remete-se a um modelo computacional que deve prover,a partir de uma rede de dados, uma estrutura tecnológica por meio de serviços. Serviços que são caracterizados por uma necessidade de maior flexibilidade, escalabilidade e benefícios de custo [34].

Segundo o NIST [2], a computação em nuvem refere-se a um modelo prático para permitir o acesso via rede a um conjunto compartilhado de recursos computacionais configuráveis sob demanda (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços.

A computação em nuvem representa uma convergência de duas grandes tendências em tecnologia da informação: (a) eficiência de TI, por meio da qual o poder dos computadores modernos é utilizado de forma mais eficiente através de recursos altamente escaláveis de hardware e software e (b) agilidade de negócios, competitiva através da rápida implantação, processamento em lote paralelo, uso de computação intensiva analítica de negócios e aplicações móveis interativas que respondem em tempo real aos requisitos do usuário [22].

2.1.1 Comparativo entre ambiente tradicional e ambiente em nuvem

Porém, para entender um ambiente em nuvem é fundamental diferenciar de um ambiente tradicional. O ambiente tradicional ou local (*on-premise*) remete-se ao modelo de infraestrutura de TI no qual os sistemas corporativos são configurados e gerenciados em centros de dados (*datacenters*) da própria empresa. Esses ambientes são mantidos por profissionais qualificados, terceirizados ou do próprio quadro de empregados da empresa. que gerenciam todas as soluções de armazenamento (storage), servidores de dados, redes de telecomunicações entre outros serviços. Já o ambiente de nuvem abstrai essa complexidade e apresenta ao cliente em formato de um serviço. Esse formato pode ser estruturado em modelos de serviço (IaaS, PaaS e SaaS) e modelos de implantação (Nuvem privada, Nuvem comunitária, Nuvem pública e Nuvem híbrida). Essa estrutura pode ser analisada de a acordo com a Figura 2.1.

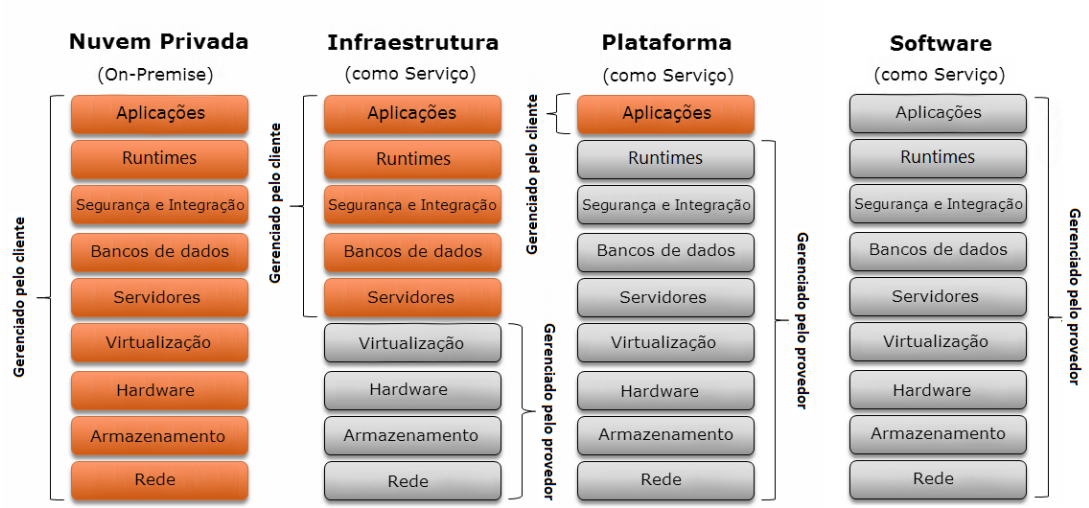

Figura 2.1: Divisão de responsabilidades entre cliente e fornecedor de nuvem [1].

A hospedagem com base em nuvem possui muitas vantagens em relação ao hospedagem tradicional (*on-premise*), como melhor escalabilidade, facilidade de gerenciamento e economia de custos [35]. Os dados sensíveis de cada empresa, que está em um modelo tradicional de implantação de aplicativos *on-premise*, continuam a residir dentro do limite da empresa e estão sujeitos às suas políticas físicas logísticas e de segurança de pessoal e controle de acesso [7]. O que deve ficar claro é que o ambiente de computação em nuvem é essencialmente diferente do ambiente tradicional de computação. Muda-se de um modelo amparado em equipamentos para um modelo orientado a serviços [27].

2.1.2 Características essenciais

Para tanto, as principais qualidades apresentadas na computação em nuvem referem-se:

- Auto-atendimento sob demanda - Um consumidor pode unilateralmente fornecer capacidades de computação, como tempo do servidor e armazenamento em rede, conforme necessário automaticamente [1, 2].
- Amplo acesso à rede - As capacidades estão disponíveis na rede e são acessadas por meio de mecanismos padrão que promovem o uso por plataformas diversas (celular, web, etc) [1, 2].
- Agrupamento de recursos - Os recursos de computação do provedor são agrupados para atender múltiplos consumidores usando um modelo de multitenant, com diferentes recursos físicos e virtuais dinamicamente atribuídos e reatribuídos de acordo com a demanda do consumidor. Exemplos de recursos incluem armazenamento, processamento, memória e largura de banda da rede [2].
- Elasticidade - Todo o processo de provisionamento de infraestrutura e execução de aplicativos é simples na nuvem. As capacidades podem ser elasticamente provisionadas e liberadas, em alguns casos automaticamente, para escalar rapidamente de acordo com demanda. Para o consumidor, as capacidades disponíveis para fornecimento muitas vezes parecem ser ilimitadas e podem ser apropriadas em qualquer quantidade a qualquer momento [2, 5, 36, 37].
- Serviço medido por utilização - Os sistemas em nuvem controlam e otimizam automaticamente o uso de recursos, alavancando um recurso de medição em algum nível de abstração apropriado ao tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de usuário ativas). O uso de recursos pode ser monitorado, controlado e relatado, proporcionando transparência tanto para o provedor como para o consumidor do serviço utilizado [1, 2].

2.1.3 Modelos de serviços

O modelo de serviço refere-se aos formatos para fornecer os serviços. Nos últimos anos, as iniciativas de computação em nuvem receberam uma atenção significativa no sentido de atender a esses requisitos, oferecendo serviços em várias formas, como SaaS (software como serviço), PaaS (plataforma como serviço) e IaaS (infraestrutura como serviço) universalmente acessível sobre a nuvem, e pagável com base na demanda de uso do serviço [38]. A figura 2.2 apresenta a estrutura do modelo de serviços.

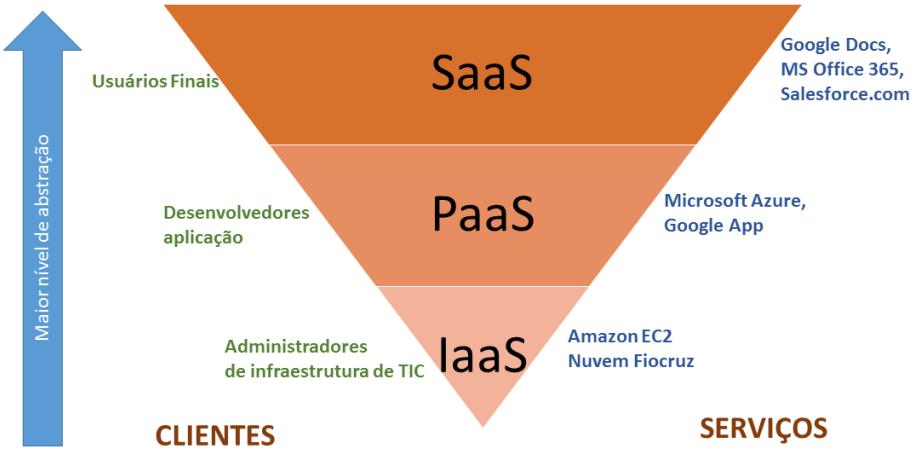

Figura 2.2: Modelos de serviços de nuvem.

No Software como Serviço (SaaS) a capacidade fornecida ao consumidor é usar os aplicativos do provedor em execução em uma infraestrutura em nuvem. As aplicações são acessíveis a partir de vários dispositivos cliente, como um navegador da web ou uma interface de programa. O consumidor não gerencia nem controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento ou até mesmo recursos de aplicativos individuais, com a possível exceção de configurações de configuração específicas de usuários específicas[2]. Dessa forma, conforme destacado na figura 2.2, o modelo SaaS apresenta maior nível de abstração da complexidade tecnológica para cliente. Serviços como Google Docs, Salesforce.com e Microsoft Office 365, são alguns exemplos de SaaS [39, 40, 41].

Na Plataforma como Serviço (PaaS) a capacidade é oferecida como plataforma para aplicativos criados ou adquiridos pelo consumidor para linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. O consumidor não gerencia ou controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre os aplicativos implantados e, possivelmente, configurações para o ambiente de hospedagem de aplicativos [2]. Serviços como Microsoft Azure e Google Apps são exemplos de PaaS [7, 39, 40, 41].

Na Infraestrutura como Serviço (IaaS) a capacidade oferecida ao consumidor é fornecer processamento, armazenamento, redes e outros recursos de computação fundamentais, onde o consumidor é capaz de implantar e executar software arbitrário, que pode incluir sistemas operacionais e aplicativos. O consumidor não gerencia ou controla a infraestru-

tura de nuvem subjacente, mas tem controle sobre sistemas operacionais, armazenamento e aplicativos implantados; E possivelmente controle limitado de componentes de rede selecionados (por exemplo, firewalls de host) [2].A plataforma Amazon Elastic Compute Cloud (EC2) é um exemplo de IaaS [7, 40, 41].

2.1.4 Modelos de implantação

Os modelos de implantação referem-se as formas como a nuvem pode ser provisionada para o consumidor.

Nuvem privada - A infraestrutura da nuvem é provisionada para uso exclusivo por uma única organização, figura 2.3 que compreende vários consumidores (por exemplo, unidades de negócios). Pode ser de propriedade, gerenciado e operado pela organização, um terceiro, ou alguma combinação deles, e pode existir dentro ou fora das instalações [2].

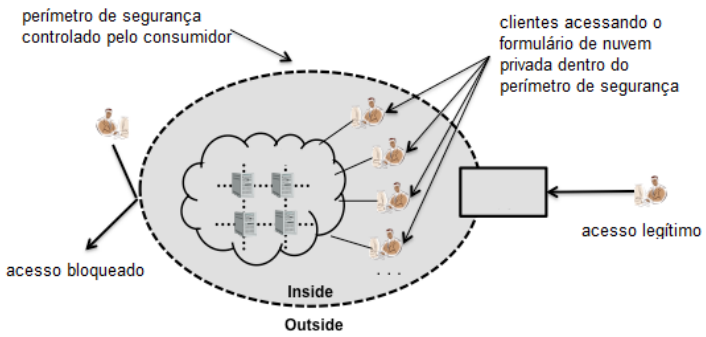

Figura 2.3: Nuvem Privada [2].

Cabe destacar que a nuvem privada não necessariamente será instalada localmente. Enquanto a maioria das nuvens privadas é instalada localmente (baseadas na evolução dos investimentos existentes em virtualização, uma porcentagem crescente será terceirizada e/ou não instalada localmente [27], conforme podemos observar na figura 2.4. Na imagem é apresenta uma abordagem no qual a nuvem privada é provisionada em um ambiente externo da organização. Nessa situação, a nuvem privada é definida para garantir a privacidade.

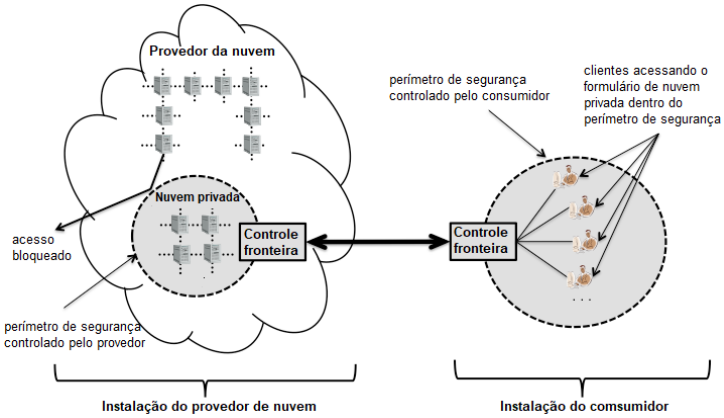

Figura 2.4: Nuvem Privada terceirizada [2].

Este tipo de nuvem pode realocar recursos de maneira mais eficiente para atender aos requisitos organizacionais, reduzindo custos de capital para hardware [27].

Nuvem comunitária - A infraestrutura da nuvem é provisionada para uso exclusivo por uma comunidade específica de consumidores de organizações que têm preocupações compartilhadas (por exemplo, missão, requisitos de segurança, política e considerações de conformidade). Ela pode ser de propriedade, gerenciada e operada por uma ou mais organizações da comunidade, por um terceiro, ou por alguma combinação deles, e pode existir dentro ou fora das instalações [2].

Nuvem pública A infraestrutura da nuvem é provisionada para uso aberto pelo público em geral. Pode ser de propriedade, gerenciado e operado por uma empresa, acadêmica ou organização governamental, ou alguma combinação deles. Ele existe nas instalações do provedor de nuvem [2].

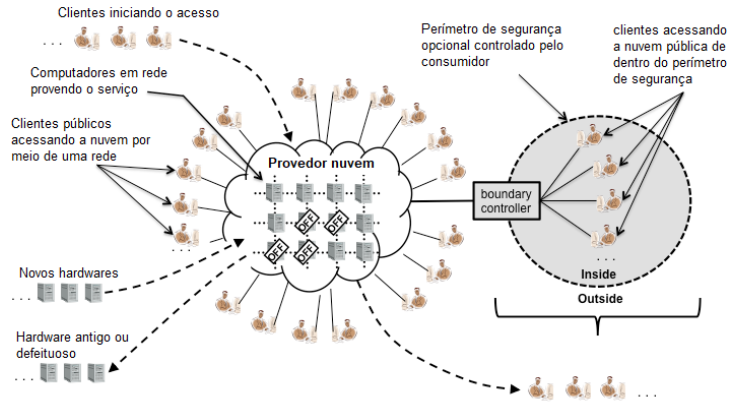

Figura 2.5: Nuvem pública [2].

Nuvem híbrida - A infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem distintas (privadas, comunitárias ou públicas) que permanecem como entidades exclusivas, mas que são unidas pela tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos (por exemplo, nuvens) [2].

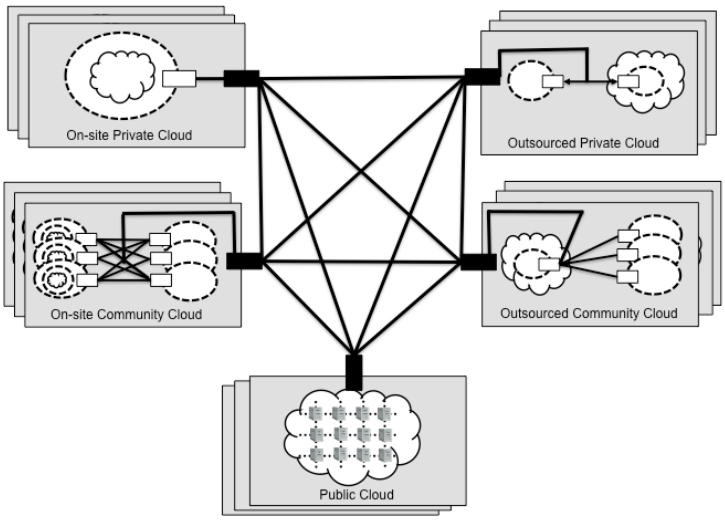

Figura 2.6: Nuvem híbrida [2].

Paiva [37] destaca que 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.

2.1.5 Principais vantagens proposta pela computação em nuvem

De modo geral, a proposta da computação em nuvem é apresentar um novo modelo de tecnologia da informação com base em serviços. Com isso, busca-se reduzir investimentos em tecnologia da informação para que as instituições foquem mais nos objetivos do negócio. O fato é que a computação em nuvem faz uso da economia em escala e isso proporciona que recursos compartilhados possam ser provisionados para vários clientes [27]. Para o TCU [1], as principais vantagens são:

- **Redução de custos de infraestrutura e serviços de TI** - O benefício mais significativo vem de hospedar aplicações em infraestrutura em nuvem devido à redução de custos de capital (capital expenditure - Capex) e custos operacionais (operacional expenditure - Opex).

- **Otimização da produtividade da equipe de TI** - A mudança para o uso de IaaS, ao acelerar o desenvolvimento e a implantação de aplicações, bem como automatizar o seu gerenciamento, torna a equipe de TI mais produtiva e capaz de melhorar o suporte de operações de missão crítica.
- **Melhoria da produtividade do usuário final** - Os usuários finais beneficiaram-se de menor indisponibilidade do serviço e recuperação mais rápida, reduzindo o tempo de inatividade em 72% e economizando expressivos recursos de cada aplicativo por ano.
- **Aumento de benefícios do negócio** - Muitas das empresas estão empregando soluções em nuvem para possibilitar novos modelos de negócios e suportar aplicações de geração de receita, atingindo um maior número de usuários/clientes.
- **Melhorar capacidade de resposta** - Computação em nuvem fornece serviços flexíveis e escaláveis que podem ser implementados rapidamente para fornecer às organizações a capacidade de responder a mudanças de requisitos e a períodos de picos.
- **Ciclo mais rápido de inovação** - No ambiente de nuvem, a inovação é tratada muito mais rápido do que dentro da empresa. O gerenciamento de *patches* e atualizações para novas versões tornam-se mais flexíveis.
- **Redução do tempo para implementação** - Computação em nuvem oferece poder de processamento e capacidade de armazenamento de dados conforme a necessidade, quase em tempo real.
- **Resiliência** - Computação em nuvem pode fornecer um ambiente altamente resiliente e reduzir o potencial de falha e o risco de *downtime*.
- ***Multi-tenancy* ou multi-inquilino** - Permite que múltiplos inquilinos compartilhem dos mesmos recursos físicos [27].

2.1.6 Orientações e estratégias para serviços em nuvem na APF

A proposta na redução de custos e a facilidade no gerenciamento sob demanda são alguns dos fatores que contribuem para que diversos órgãos da APF avaliem a proposta de migração de seus ambientes tradicionais de TIC para plataformas de serviços em nuvem. Para o Ministério do Planejamento (MP), órgão da Administração Federal responsável pela formulação do planejamento estratégico nacional, destaca que o modelo tradicional de provimento de recursos de TI, adotado pelos órgãos do SISP, com o uso de salas-

cofre e *datacenters* seguros torna-se dispendioso, com perda de escala e eficiência, além de apresentar maior complexidade de operação e manutenção de equipamentos.

Além do mais, a burocracia no processo de contratação de recursos e serviços de TIC, que passa por uma série de exigências legais, processos e procedimentos, exige cautela dos gestores de TI. Essa preocupação se justifica diante de toda logística necessária para implantação desses serviços como: capacitações, renovações de licenças de software, instalações, infraestrutura adequada, pessoal especializado e etc. Toda esse processo, moroso diante da complexidade para contratação e manutenção, contribui para que os órgãos integrantes do SISP reflitam cada vez mais em contratar serviços em nuvem.

DECRETO 8.135/2013

O armazenamento compartilhado de recursos e a segurança da informação são alguns fatores inerentes na contratação de serviços de nuvem que preocupam gestores de TI da APF, em especial por conta do Decreto 8.135/2013 que dispõe sobre a comunicação de dados na APF e destaca a dispensa na contratação de serviços de TIC que possam impactar a segurança nacional [42]. Esse decreto foi criado em resposta aos casos de espionagem norte americana para tornar mais restritivo o acesso a dados dos órgãos da APF. O decreto dispõe que "as comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de TI fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias"[42].

Porém, há de se ponderar também que as defesas baseadas em nuvem muitas vezes são mais robustas, escaláveis, eficientes e baratas se comparadas às soluções internas, em razão da especialização dos provedores e do ganho de escala [1].

ACÓRDÃO 1.739/2015 - TCU

Diante desse cenário e levando-se em consideração que os órgãos do SISP possuem baixa maturidade na contratação e uso de serviços de computação em nuvem [1], o TCU, a partir do Acórdão 1.739/2015, realizou um levantamento com objetivo principal de identificar riscos em contratações na APF sob o modelo de computação em nuvem. Como resultado desse trabalho, foi elaborada uma tabela de riscos e possíveis controles associados à contratação desses serviços e uma matriz de referência contendo questões, procedimentos e possíveis achados de auditoria, de modo a auxiliar os auditores do TCU em futuras fiscalizações [1]. O acórdão destaca ainda algumas vantagens específicas da computação em nuvem para o governo, tais como:

1. Maior agilidade da administração pública na entrega de serviços e em sua atualização tecnológica, pois os processos formais de contratação pública podem dificultar a manutenção de uma infraestrutura de TI própria atualizada e que responda rapidamente às demandas de seus usuários.

2. Suporte a iniciativas de Big Data e Dados Abertos, facilitando a abertura de informações governamentais que hoje encontram-se em sistemas que controlam as operações cotidianas do Estado e portanto são fechados com acesso limitado aos seus operadores. O uso de nuvem pública permitiria ampliar o acesso a esses dados a um custo menor, sem comprometer a segurança, a disponibilidade e o desempenho operacional dos sistemas originais. Uma vez os dados governamentais estando facilmente acessíveis, torna-se possível maior participação da sociedade na criação de novos serviços com base nesses dados.

3. Atendimento a picos de demanda sazonal de serviços públicos pela Internet sem necessidade de alocar grande quantidade de recursos fixos. Várias atividades estatais acarretam picos sazonais de demanda de serviços próximos a datas limite como: entregas de declarações de imposto de renda, inscrições e resultados do Enem, resultados eleitorais e listagem de gestores públicos inelegíveis, períodos de recadastramento do INSS, listagem dos percentuais do fundo de participação dos municípios, etc.

4. **A contratação de serviços em nuvem de IaaS ou PaaS pode levar a uma redução de oportunidades de desvios e irregularidades, quando comparada às múltiplas contratações de máquinas, licenças de software, manutenção e suporte necessárias para a operação de CPD próprio. As ofertas de IaaS e PaaS identificadas neste levantamento são todas por contrato de adesão, utilizando métricas de precificação com custos unitários divulgados publicamente e iguais para todos os clientes, o que facilita a pesquisa de preços** (grifo nosso).

5. Agilidade e economia na entrega de serviços para instituições públicas com unidades descentralizadas, que podem ter serviços disponibilizados por meio de acesso à internet, mais barato que as interconexões via redes privadas atualmente utilizadas.

PORTARIA MP/STI nº 20/2016

Nessa linha, o MP editou um documento de boas práticas e orientações para contratação de serviços em nuvem vinculada a Portaria MP/STI nº 20, de 14 de junho de 2016, que orienta as contratações de TI na APF. Dentre as orientações é possível destacar, por

exemplo, que os órgãos que não possuem infraestrutura de TI própria ou que necessitem renová-la ou ampliá-la devem contratar Infraestrutura como Serviço (IaaS). Nesse ponto, o dispositivo veda a contratação de salas-cofre e salas seguras por órgãos integrantes do SISP [43]. O documento também flexibiliza a possibilidade de contratação de serviços de nuvem híbrida para os casos de serviços de TIC que não comprometam a segurança nacional[43]. Destaca também que os órgãos deverão exigir, no momento da contratação de serviços em nuvem de fornecedores privados, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013 [43].

Na contratação de serviços em nuvem com empresas privadas os órgãos deverão exigir, por meio de cláusulas contratuais, em conformidade com o disposto na NC 14/IN01 /DSIC /GSIPR, que os dados e informações do contratante residam exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem. Além do mais, disponibilidade dos serviços de no mínimo, 99,741%.

NORMA COMPLEMENTAR nº 14/IN01/DSIC/GSIPR 2018

Porém, os benefícios oferecidos pela computação em nuvem, como economicidade e eficiência, podem também ocasionar o surgimento de riscos. Nessa sentido, a Norma complementar nº 14/IN01/DSIC/GSIPR de 19 de março de 2018, estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. A norma destaca, por exemplo, que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, devem residir em território brasileiro. Além do mais, aborda que na adoção de serviços de computação em nuvem, o órgão ou entidade da APF deve assegurar em instrumento contratual ou similar:

1. Requisitos que garantam a DICA das informações tratadas em ambiente de computação em nuvem;
2. Processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente;
3. Requisitos necessários para a realização de auditorias;
4. Que os dados, metadados, informações e conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos

do previsto no referido instrumento contratual ou similar, sob nenhuma hipótese, sem autorização formal do órgão ou entidade da APF;

5. Requisitos necessários para a continuidade de negócio;

6. Requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva dos dados, metadados, informações e conhecimento;

2.2 Conceitos de riscos

A todo instante nos deparamos com diversas incertezas que podem influenciar de forma positiva ou negativa. Empresas, organizações, pessoas etc, passam diariamente por todo tipo de incerteza que, de algum modo, pode contribuir para um sucesso na vida profissional, ou mesmo para o fracasso de uma organização. Essas incertezas não devem ser entendidas necessariamente como algo negativo, ao contrário, podem ser positivas e devem ser vistas como uma oportunidade a ser trabalhada em favor da organização para alcance de seus objetivos [21].

2.2.1 Riscos

A norma NBR ISO 31000:2009 [3] trata que o efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco". Ainda, segundo a norma, a incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

Já a NBR ISO GUIA 73:2015 [32] define **risco como a combinação da probabilidade de um evento e de suas consequências** (grifo nosso). Sendo que a consequência é resultado de um evento e a probabilidade o grau de possibilidade de que um evento ocorra. A norma destaca que em alguns casos, o risco decorre da possibilidade de desvio em relação ao evento ou resultado esperado.

Em geral, eles podem representar oportunidades de benefícios ou ameaças ao sucesso, ou seja, impactos positivos e negativos dos riscos nos objetivos de uma organização. A incerteza vem de eventos internos e externos que podem ou não acontecer [44]. Assim, e ao contrário das estratégias tradicionais de prevenção de riscos (mitigação), a adoção de riscos positivos pode levar à obtenção de benefícios significativos do ponto de vista comercial.

Nessa linha, Marshall [45] recomenda distinguir o termo risco de incerteza. De acordo com o autor, risco é algo já experimentado, apresentando base histórica de informações

e aceito por antecipação ao processo de investimento, constituindo-se assim numa ação consciente. A incerteza, porém, refere-se à imprevisibilidade de um fenômeno por total desconhecimento.

2.2.2 Gestão de riscos

De modo geral, a gestão é riscos apresenta uma série de procedimentos capazes de auxiliar os tomadores de decisão no controle de riscos. Apesar da diversidade de termos referentes a gestão de riscos, porém, todas traduzem de forma similar o seu significado [46]. Para tanto, a norma ABNT ISO GUIA 73:2009[47] define gestão de riscos como as atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. O gerenciamento de riscos pode ser visto como um processo de otimização que faz com que as organizações minimizem as incertezas na consecução de seus objetivos [44].

A gestão de riscos é um componente integral da gestão, uma vez que envolve atividades coordenadas relacionadas com o efeito da incerteza nesses objetivos. É por isso que, para ser eficaz, é importante que a gestão de riscos seja completamente integrada aos processos e sistema de gestão da organização [32].

A TI tornou-se onipresente e essencial para qualquer negócio. Devido à sua natureza indispensável, a gestão de riscos também se tornou vital. Em todos os domínios, as atividades de gestão de risco devem estar sob controle. Esta situação é cada vez mais frequente e requer atenção para redução de custos, redução da complexidade, eficiência e eficácia [48]. Isto é particularmente verdadeiro para a gestão de risco, que é central em organizações de TI com sistemas de gestão integrada e pensamento com base em risco.

2.3 NBR ISO 31000:2009 - Processo de gestão de riscos

A norma NBR ISO/IEC 31000:2009 define o processo de gestão de riscos como uma "aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos" [3]. O principal objetivo é obter benefícios e valores sustentáveis para o negócio em cada uma de suas atividades [44]. Uma estrutura de gerenciamento de risco deve fornecer uma diretriz abrangente para avaliar e gerenciar os riscos identificados [4].

Segundo a norma NBR ISO/IEC 3104:2015, o processo de gestão de riscos identifica vários elementos de uma estrutura para gerenciar riscos. A norma destaca que há diversas vantagens que podem surgir quando os elementos desta estrutura são integrados

na governança, funções e processos de uma organização. Estas relacionam-se a eficácia organizacional, sólida tomada de decisões e eficiência [32].

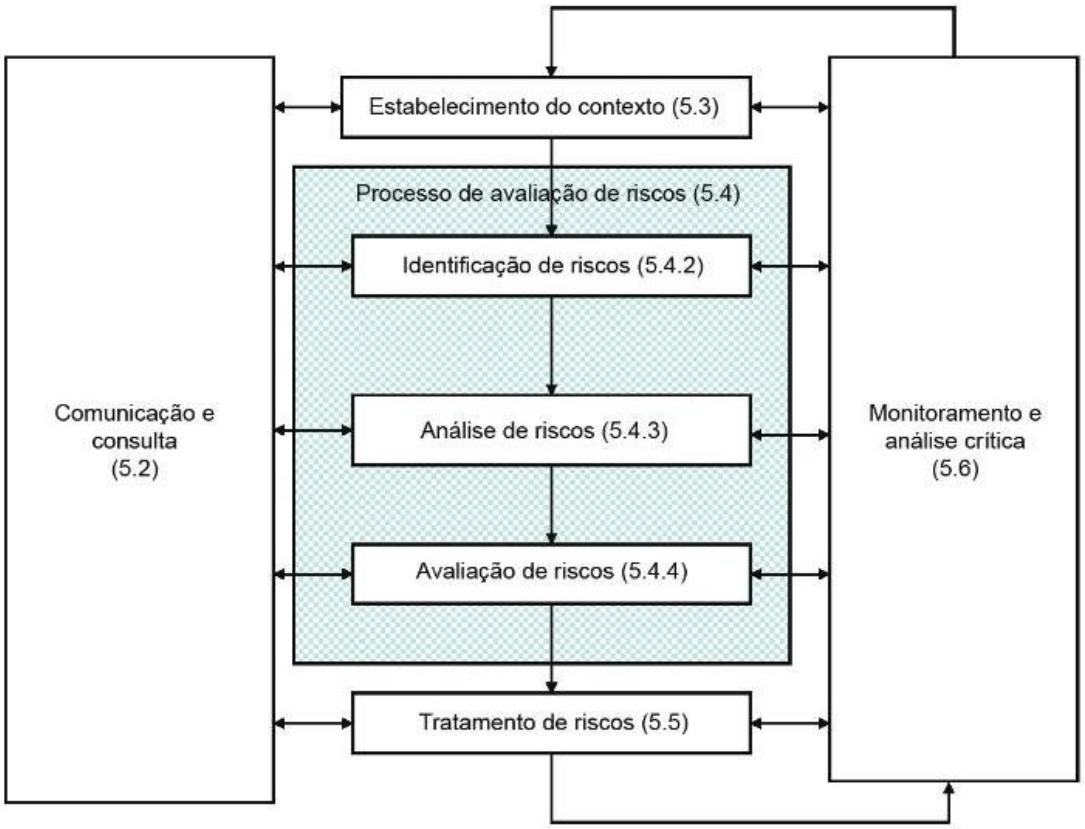

Figura 2.7: Processo de Gestao de Riscos [3].

Segundo a norma, as organizações gerenciam o risco, identificando-o, analisando-o e, em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco. O processo de gestão riscos, de acordo com a norma NBR ISO/IEC 31000:2009, conforme apresentado na figura 2.7, compreende [3]:

- **Comunicação e consulta** - Processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos.
- **Estabelecimento do contexto (interno e externo)** - Processo que define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos;

- **Processo de avaliação de riscos** - Processo global de identificação de riscos, análise de riscos e avaliação de riscos. Além do mais, não se trata de uma atividade autônoma, mas totalmente integrada ao processo de gestão de riscos [14].
  - **Identificação de riscos** - Processo de busca, reconhecimento e descrição de riscos. Essa busca envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.
  - **Análise de riscos** - Processo de compreender a natureza do risco e determinar o nível de risco. Além do mais, fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.
  - **Avaliação de riscos** - Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável. A avaliação de riscos auxilia na decisão sobre o tratamento de riscos.
- Tratamento de riscos - Envolve selecionar e acordar uma ou mais opções pertinentes para alterar a probabilidade de ocorrência, o efeito dos riscos, ou ambos, e a implementação destas opções.
- Monitoramento e análise crítica - O monitoramento e análise crítica são duas atividades distintas destinadas a determinar se suposições e decisões continuam válidas. Tem por objetivo assegurar razoavelmente que os riscos estão adequadamente gerenciados [32].

2.4 NBR ISO 31010:2012 - Técnicas para o processo de avaliação de riscos

Esta norma tem como objetivo apoiar a norma NBR ISO/IEC 31000:2009 com orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos. Ela destina-se a refletir as boas práticas atuais na seleção e utilização das técnicas para o processo de avaliação de riscos e não se refere a conceitos novos ou em evolução que não tenham atingido um nível satisfatório de consenso profissional [32]. O processo de avaliação de riscos é a parte da gestão de riscos que fornece um processo estruturado para identificar como os objetivos podem ser afetados. e analisa o risco antes de decidir se um tratamento adicional é requerido. Diante disso, a norma destaca alguns dos principais benefícios da realização do processo de avaliação de riscos, que incluem, entre outros:

- entender o risco e seu potencial impacto sobre os objetivos;

- **fornecer informações aos tomadores de decisão**(grifo nosso);
- contribuir para o entendimento dos riscos a fim de auxiliar na seleção das opções de tratamento;
- comparar riscos em sistemas, tecnologias ou abordagens alternativos;
- fornecer informações que ajudarão a avaliar a conveniência da aceitação de riscos quando comparados com critérios predefinidos;

Ainda de acordo com a norma, o processo de avaliação de riscos fornece aos tomadores de decisão e às partes responsáveis um entendimento aprimorado dos riscos que poderiam afetar o alcance dos objetivos, bem como a adequação e eficácia dos controles em uso. Isto fornece uma base para decisões sobre a abordagem mais apropriada a ser utilizada para tratar os riscos. A saída do processo de avaliação de riscos é uma entrada para os processos de tomada de decisão da organização [32].

O processo de avaliação de riscos pode ser conduzido em vários graus de profundidade e detalhe e utilizando um ou muitos métodos que vão do simples ao complexo. Convém que a forma de avaliação e sua saída sejam compatíveis com os critérios de risco, desenvolvidos como parte do estabelecimento do contexto [32]. Na tabela 2.1 apresenta uma relação conceituai entre as amplas categorias das técnicas para o processo de avaliação de riscos e os fatores presentes numa determinada situação de risco.

Tabela 2.1: Ferramentas utilizadas para o processo de avaliação de riscos [14]

Ferramentas e técnicas	**Processo de avaliação de riscos**				
	Identificação de riscos	**Análise de riscos**			**Avaliação de riscos**
		Consequência	**Probabilidade**	**Nível de risco**	
Brainstorming	FA	NA	NA	NA	NA
Entrevistas estruturadas ou semi-estruturadas	FA	NA	NA	NA	NA
Delphi	FA	NA	NA	NA	NA
Listas de verificação	FA	NA	NA	NA	NA
Análise preliminar de perigos (APP)	FA	NA	NA	NA	NA
Estudo de perigos e operabilidade (HAZOP)	FA	FA	A	A	A
Análise de perigos e pontos críticos de controle (APPCC)	FA	FA	NA	NA	FA

Tabela 2.1 (cont.)Ferramentas utilizadas para o processo de avaliação de riscos [14]

Ferramentas e técnicas	**Processo de avaliação de riscos**				
	Identificação de riscos	**Análise de riscos**			**Avaliação de riscos**
		Consequência	**Probabilidade**	**Nível de risco**	
Avaliação de risco ambiental	FA	FA	FA	FA	FA
Técnica estruturada "E se" (SWIFT)	FA	FA	FA	FA	FA
Análise de cenários	FA	FA	A	A	A
Análise de impactos de negócio	A	FA	A	A	A
Análise de causa-raiz	NA	FA	FA	FA	FA
Análise de modos de falha e efeito	FA	FA	FA	FA	FA
Análise de árvore de falhas	A	NA	FA	A	A
Análise de árvore de eventos	A	FA	A	A	NA
Análise de causa e consequência	A	FA	FA	A	A
Análise de causa e efeito	FA	FA	NA	NA	NA
Análise de camada de proteção (LOPA)	A	FA	A	A	NA
Árvore de decisões	NA	FA	FA	A	A
Análise de confiabilidade humana	FA	FA	FA	FA	A
Análise Bow tie	NA	A	FA	FA	A
Manutenção centrada em confiabilidade	FA	FA	FA	FA	FA
Sneak analysis (SA) e sneak circuit analysis (SCA)	A	NA	NA	NA	NA
Análise de Markov	A	FA	NA	NA	NA
Simulação de Monte Carlo	NA	NA	NA	NA	FA
Estatística Bayesiana e Rede de Bayes	NA	FA	NA	NA	FA
Curvas FN	A	FA	FA	A	FA

Tabela 2.1 (cont.)Ferramentas utilizadas para o processo de avaliação de riscos [14]

Ferramentas e técnicas	**Processo de avaliação de riscos**				
	Identificação de riscos	**Análise de riscos**			**Avaliação de riscos**
		Consequência	**Probabilidade**	**Nível de risco**	
Índice de risco	A	FA	FA	A	FA
Matriz de probabilidade / consequência	FA	FA	FA	FA	A
Análise de custo / benefício	A	FA	A	A	A
Análise de decisão por multicritérios (MCDA)	A	FA	A	FA	A
FA - Fortemente aplicável NA - Não aplicável A - Aplicável					

A norma NBR ISO/IEC 31010:2015 destaca que as razões para a escolha das técnicas sejam dadas com relação a pertinência e adequação . Além disso, a norma enfatiza que as técnicas sejam selecionadas com base em fatores aplicáveis, tais como [32]:

- Os objetivos de estudo - Os objetivos do processo de avaliação de riscos terão uma influência direta sobre as técnicas utilizadas.
- As necessidades dos tomadores de decisão - Em alguns caso o alto nível de detalhe é necessário para tomar uma boa decisão, em outros um entendimento mais geral é suficiente;
- o tipo e a gama de riscos que estão sendo analisados;
- a disponibilidade de informações e dados. Algumas técnicas requerem mais informações e dados do que outras;

Diante disso, serão apresentadas as principais técnicas a serem utilizadas no estudo a partir de informações a serem levantadas no contexto do estudo de caso para auxiliar nas etapas do processo de avaliação de riscos.

2.4.1 Análise de decisão por multicritérios (MCDA)

Os processos com múltiplos critérios de tomada de decisão surgiram a partir do reconhecimento de necessidades geradas por problemas complexos, onde é preciso analisar vários critérios [49]. A principal característica é utilizar uma faixa de critérios para avaliar de forma objetiva e transparente o valor global de um conjunto de opções [14].

Existem diferentes métodos pelos quais a ponderação para cada critério pode ser deduzida e diferentes formas de agregar as pontuações dos critérios para cada opção em uma pontuação única de multi atributos [14]. Dentre eles, destaca-se o Método de Análise Hierárquica, ou Analytic Hierarchy Process -AHP, desenvolvido por Thomas L. Saaty em 1977. Segundo Saaty [16], um dos usos de uma hierarquia é que nos permite enfocar o julgamento separadamente em cada uma das várias propriedades essenciais para tomar uma decisão acertada. A maneira mais eficaz de concentrar o julgamento é pegar um par de elementos e compará-los em uma única propriedade sem se preocupar com outras propriedades ou outros elementos.

Organizar as metas, atributos, problemas e partes interessadas em uma hierarquia serve a dois propósitos. Ele fornece uma visão geral das relações complexas inerentes à situação; e ajuda o decisor a avaliar se as questões em cada nível são da mesma ordem de grandeza, para que ele possa comparar esses elementos homogêneos com precisão [16].

2.4.2 Brainstorming

Trata-se de uma técnica que consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas, em qualquer estágio do processo de gestão de riscos, com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado [14, 15].

Esta técnica é particularmente útil para identificar riscos de novas atividades, novas tecnologias ou em situações em que não há dados disponíveis. O produto a ser gerado depende do contexto, podendo ser, por exemplo, uma lista de riscos e de controles [15].

2.5 Gestão de riscos aplicada ao processo de migração para nuvem

Embora vários benefícios da computação em nuvem sejam bem conhecidos e documentados, as empresas ainda estão preocupadas com os riscos e as consequências de mover aplicações críticas para a nuvem [39]. O gerenciamento de riscos para a nuvem envolve o suporte a decisões complexas de migração; portanto, o plano deve considerar uma abordagem proativa para o controle de risco. O plano também determina a risco do potencial projeto migrado, em particular, quão arriscada a migração da nuvem termos de custo, cronograma, controle de risco e continuidade de negócios [4].

As atividades de uma organização, incluindo as tomadas de decisão, dão origem a riscos. Além do mais, a gestão de riscos ajuda os tomadores de decisão a fazerem escolhas informadas, priorizarem ações e distinguirem entre cursos alternativos de ação [32]. Diante

disso, a norma NBR ISO/IEC 31004:2015 destaca que convém que a gestão de riscos seja aplicada como parte de uma decisão, no momento em que é tomada a decisão (ou seja, de forma proativa), e não após a decisão ser tomada (ou seja, de forma reativa).

2.5.1 Uma estrutura de gerenciamento de riscos para suporte à decisão de migração para nuvem

A norma NBR ISO/IEC 31000[3] apresenta que a análise de riscos também pode fornecer uma entrada para a tomada de decisões em que escolhas precisam ser feitas e as opções envolvem diferentes tipos e níveis de risco. Nesse sentido, Islam et al [4] propõem uma estrutura de gerenciamento de riscos para suportar usuários com decisões de migração em nuvem. Segundo os autores, a estrutura proposta fornece uma visão abrangente dos riscos para apoiar uma organização na tomada da decisão de migração na nuvem e equilibra os benefícios com os riscos potenciais. O escopo da estrutura de gerenciamento de riscos é apoiar a decisão de migração na nuvem e monitorar os riscos durante a operação. A estrutura inclui áreas de gerenciamento de riscos, visão conceitual e um processo para essa finalidade.

Para tanto, a proposta dos autores para o processo de gerenciamento de riscos compreende quatro coletas sistemáticas sequenciais de atividades com entradas e resultados específicos, seguindo as diretrizes dos padrões de gestão de riscos existentes na ISO 31000 e ISO 27001:2013. Conforme abaixo:

1. **Atividade - Inicializar o gerenciamento de riscos:** estabelece o contexto de gerenciamento de riscos seguindo o perfil de migração na nuvem e aprova formalmente as atividades de gerenciamento de riscos dentro da organização. Essa atividade inclui duas tarefas: definir o perfil de migração e planejar o gerenciamento de riscos.

   (a) Definir perfil de migração: Analisa o perfil de migração no contexto organizacional existente e racionaliza as necessidades de migração. Essa fase identifica as metas de migração (valor para o negócio, função organizacional, confidencialidade, integridade, disponibilidade e transparência), os pontos fortes e fracos da organização, o tipo de migração e o possível perfil de ativos migrados.

   (b) Planejar o gerenciamento de riscos: Essa tarefa inicia a implementação do gerenciamento de riscos determinando o escopo, o cronograma e os recursos de gerenciamento de riscos, o tratamento de riscos e a estratégia de monitoramento (se aplicável) com base no perfil de migração.

2. **Atividade - Identificar e Categorizar Riscos:** Identifica todos os possíveis riscos que podem ter impacto na migração da nuvem. Os resultados da atividade anterior são entradas para essa atividade. Essa atividade consiste em duas tarefas:

   (a) identificar riscos: identifica todos os possíveis riscos e fatores associados que podem ter impacto no projeto de migração da nuvem

   (b) categorizar os riscos: Após os riscos serem identificados, são categorizados com base em seu impacto na continuidade do negócio da organização. Os riscos foram categorizados em três grupos: empresarial, organizacional e técnico.

3. **Atividade - Analisar e Controlar Riscos:** avalia os riscos para determinar o valor do risco líquido e identifica a ação de controle necessária para mitigar os riscos. As metas priorizadas são usadas para avaliar os riscos usando uma abordagem semiquantitativa para determinar o nível de risco. Essa atividade consiste em duas tarefas:

   (a) avaliar os riscos: Essa tarefa calcula o valor de risco líquido com base na importância relativa da meta de migração afetada. Para tanto, essa tarefa foi dividida em duas etapas. A primeira etapa utiliza do processo de análise hierárquica (AHP) para calcular a importância relativa das metas de migração. A segunda etapa elabora o cálculo de risco líquido a partir dos valores associados ao fator de risco, onde Cada valor do fator de risco é estimado pelo produto de sua probabilidade e impacto do risco global.

   (b) Identificar possíveis medidas de controle de risco: As ações de controle de risco são identificadas com base nos níveis de risco. Essa tarefa identifica as possíveis medidas de controle que podem reduzir e eliminar os riscos identificados no ambiente de nuvem.

4. **Atividade - Decisão de Migração e Monitoramento de Risco:** Finalmente, a decisão de migração é tomada com base na garantia de que os potenciais provedores de nuvem oferecem as medidas de controle necessárias para os riscos que estão fora do controle dos usuários. A saída da atividade suporta principalmente a decisão de migração, examinando as ofertas existentes de provedores de serviços de nuvem escolhidos e monitorando o risco em determinado intervalo. Esta atividade consiste em três tarefas.

   (a) Garantia de Medidas de Controle: Verifica as capacidades do CSP para cumprir as medidas de controle identificadas para os riscos que são responsabilidades do provedor de serviços. A garantia verifica a conclusão das medidas de controle e atribui um dos três níveis:

- Nível 1 Sem conclusão: Não há evidências mínimas ou mínimas para a garantia de atributos de medidas de controle para gerenciar os riscos.
- Nível 2 Conclusão parcial: Há alguma evidência para a garantia dos atributos de medida de controle para gerenciar os riscos.
- Nível 3 Conclusão completa: Há evidências adequadas para a garantia de atributos de medidas de controle para gerenciar os riscos.

(b) Decisão de migração: Essa tarefa considera como a nuvem poderia suportar uma organização em termos de controle de risco se a decisão de migração for tomada. A estratégia de migração na nuvem inclui vários parâmetros, como tamanho da migração, tipo de hospedagem, número de servidores e licença e largura de banda, candidato a CSP, monitor de riscos e funções e responsabilidades.

(c) Monitorar os riscos em operação: Esta tarefa monitora os riscos existentes para garantir que os riscos estejam sob controle e identifica novos riscos após a conclusão da implementação na nuvem

Após a definição da estrutura, os autores empregaram a proposta no mundo real na empresa Secure Business Austria (SBA). Para tanto, eles integraram o método de estudo de caso com pesquisa-ação para demonstrar a aplicabilidade da abordagem. A Figura 2.8 mostra o estudo de caso combinado com os componentes do projeto de pesquisa-ação. O desenho da pesquisa considera os componentes típicos do design, como construção do estudo, técnicas e análise de coleta de dados, observação, ação e conclusão.

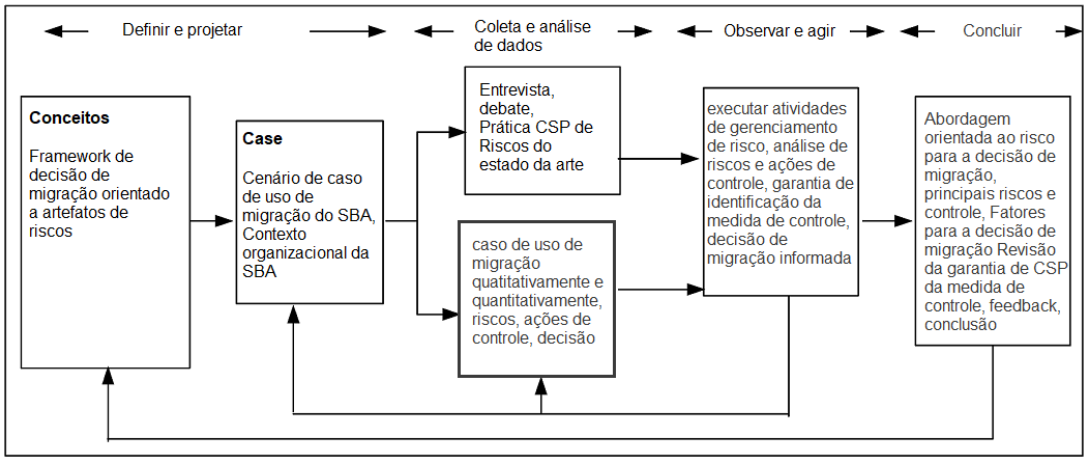

Figura 2.8: Detalhes de aplicação do estudo [4].

Por fim, após aplicar a estrutura no estudo de caso, os autores chegaram a conclusão que o modelo apresentado foi útil para a SBA na avaliação dos riscos e na tomada de uma

decisão de migração da nuvem. Os resultados mostraram que a abordagem orientada ao risco fornece um alerta antecipado sobre os problemas que precisam de atenção adequada antes de tomar a decisão de migração. Para os autores, a estrutura fornece uma análise abrangente dos riscos de várias dimensões relevantes para o contexto estudado.

2.5.2 Proposta de uma metodologia de riscos para migração em nuvem

Yuusuf e Tubb [5] analisam os benefícios e riscos da nuvem e apresentam uma metodologia que propõe medidas específicas que as empresas podem adotar para garantir que a migração e a integração entre o ambiente local e a nuvem ocorram com o mínimo de interrupção do negócio e resulte em benefício máximo de custo sustentável. A metodologia proposta é denominada Metodologia Homeostática de Risco para a migração na nuvem. Para tanto, os autores fazem uma análise dos principais benefícios e riscos a partir de uma abordagem que considera: os processos de negócios, a arquitetura dos sistemas existentes, a arquitetura dos serviços disponíveis, a interoperabilidade entre o ambiente local e virtual, a maturidade da tecnologia e os padrões de virtualização, economias de custos a longo prazo, sustentabilidade, dados / segurança / regulamentação, adoção pelos usuários, acordos de nível de serviço (SLAs) disponíveis e importância para os negócios.

A metodologia proposta pelos autores tem como objetivo auxiliar as empresas no processo transição ao se adotar a migração para o ambiente de nuvem. Segundo os autores, essa metodologia é denominada Metodologia Homeostática de Risco para a Migração para a Nuvem, conforme ilustrada na figura 2.9.

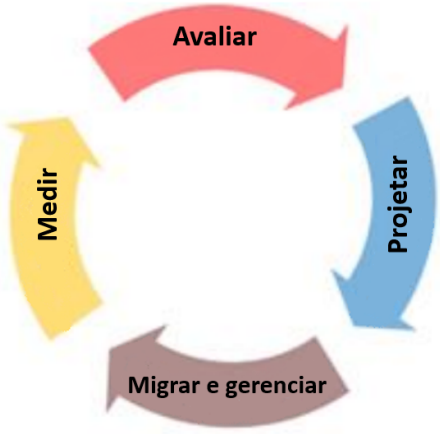

Figura 2.9: Metodologia de homeostase de risco para migrar para a nuvem [5].

Na visão do autores, a metodologia é genérica e pode ser adotada e customizada pelas empresas para defender ou não a migração para a nuvem. Segundo eles, os resultados da

metodologia auxilia a responder as seguintes questões: devemos migrar para a nuvem ou não, o que devemos mudar, quando devemos nos mover. Dado que a empresa tomou a decisão de migrar para o ambiente virtual, esta metodologia orienta sobre como migrar para o ambiente de nuvem - quais são as oportunidades atuais no ambiente de nuvem, quais arquiteturas estão disponíveis, quais aplicativos são bons candidatos para qual arquitetura de nuvem? Cada fase da metodologia contém vários processos. A maioria dos processos pode acontecer simultaneamente (dependendo dos recursos de avaliação) e a saída de um pode ser a entrada de outro, ou a saída de um pode alterar a entrada de outro e vice-versa. O objetivo final dessa metodologia é ajudar as empresas a decidirem se migram para a nuvem ou não e o que devem migrar para a nuvem. As quatro fases da metodologia contêm os seguintes processos e atividades:

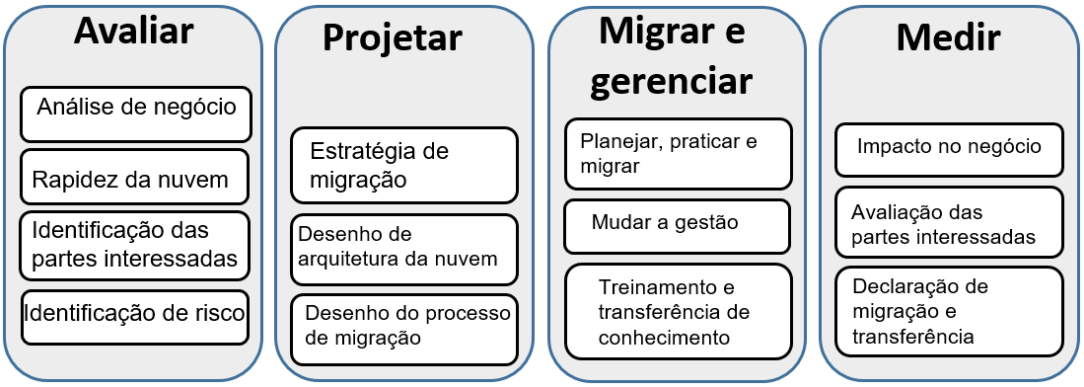

Figura 2.10: Detalhes de aplicação do estudo [5].

1. **Avaliação** (*Assessment*): A avaliação incluirá as métricas que indicam a análise de negócios, a prontidão da nuvem, a identificação de riscos e as principais partes interessadas, que fornecerão motivos claros para se mudar (ou não) para a nuvem;

2. **Projeto** (*Design*):Uma vez que a avaliação da empresa esteja em vigor, as próximas etapas seriam projetar a estratégia de migração da computação em nuvem, alinhando a investigação à estratégia de negócios e mostrando como ela pode agregar valor aos negócios. Mostre como a investigação pode levar a alterações que afetarão os negócios e o ambiente de arquitetura de TI. Uma parte importante da Estratégia será trabalhar com as principais partes interessadas para identificar as necessidades de negócios. Nesta fase, avaliamos quais modelos, arquiteturas, tecnologias e práticas recomendadas de computação em nuvem farão sentido implementar (por exemplo, Private, Public ou Hybrid Cloud) em sua configuração corporativa. Avalie também os requisitos orçamentários, de recursos e técnicos necessários para

preparar o negócio para a fase piloto / de teste da investigação. Do ponto de vista financeiro, desenvolva uma análise do custo total de propriedade e analise as políticas estabelecidas para avaliar o gerenciamento de mudanças de área de risco.

3. **Migrar e Gerenciar** (*Migrate and Manage*): O objetivo desta fase é aprender sobre os recursos de tecnologia e garantir que nossas suposições sobre a adequação para migração para a nuvem sejam precisas. Nessa fase, o avaliador pode implantar um grupo de sistemas e, no processo, começar testar o provedor de nuvem. O novo ambiente dará ao avaliador uma visão mais clara sobre os obstáculos que precisam ser superados para seguir em frente.

4. **Medição** (*Evaluation*): Nesta fase, medimos o resultado de cada fase e tomamos decisões a favor ou contra a migração. Isso permitirá que a organização entenda as tendências da nuvem e avalie quais são seus possíveis impactos no objetivo, nas estratégias e nos processos de negócios. A avaliação indicará o que deve mudar - e quais necessidades não mudam e um cronograma experimental para essas mudanças. Essa etapa permite que o gerenciamento tenha um trabalho mais fácil para decidir como investir, percebendo o custo de cada ameaça. As partes interessadas estarão ativamente envolvidas na avaliação.

2.5.3 Um modelo de análise de risco para ambientes PACS na nuvem

Os autores Cordeiro e Azevedo-Marques[6] apresentam no estudo alguns dos pontos de verificação mais importantes encontrados nos projetos de implantação ou migração para ambientes PACS (Picture Archiving and Communication System) para a nuvem. Os *checkpoints* foram mapeados na tabela de avaliação de risco, proposta pela ENISA (Agência da União Europeia para Segurança de Redes e Informações), para aplicativos executados a partir de serviços de computação em nuvem. Os pesquisadores da ENISA apontaram para cada risco uma probabilidade e um nível de impacto comercial, ambos aceitando os rótulos "muito baixo"(VL), "baixo"(L), "médio"(M), "alto"(H) e "muito alto "(VH). Os riscos identificados e sua classificação para, respectivamente, probabilidade e impacto são:

Tabela 2.2: Riscos identificados e classificados segundo ENISA [6] (Adaptado)

Código	**Risco**
R.2	perda de governança (VH / VH)
R.3	desafios de conformidade (VH / H)

Table 2.2 (continuação)

Código	Risco
R.4	perda de reputação comercial devido a atividades de outros inquilino (L / H)
R.5	paralisação ou falha do serviço em nuvem (NA / VH)
R.8A	incapacidade de fornecer capacidade adicional a um cliente (M / M)
R.8B	incapacidade de fornecer o nível de capacidade atual acordado (L / H)
R.10	provedor de nuvem malicioso - abuso de funções de alto privilégio (M / VH)
R.11	comprometimento da interface de gerenciamento (M / VH)
R.12	interceptar dados em trânsito (M / H)
R.13	vazamento de dados em up / download, intra-cloud (M / H)
R.14	inseguro de eliminação ineficaz de dados (M / VH)
R.15	negação de serviço distribuída (M / H)
R.16	negação de serviço econômica (L / H)
R.17	perdade chaves de criptografia (L / H)
R.19	comprometer o mecanismo de serviço (L / VH)
R.20	conflitos entre procedimentos de proteção do cliente e ambiente de nuvem (L / M)
R.22	risco de mudanças de jurisdição (VH / H)
R.23	riscos de proteção de dados (H / H)
R.24	riscos de licenciamento (M / M)
R.25	quebras de rede (L / VH)
R.26	gerenciamento de rede (M / VH)
R.27	modificando o tráfego de rede (L / H)
R.29	ataques de engenharia social (M / H)
R.30	perda ou comprometimento de logs operacionais (L / M)
R.31	perda ou comprometimento de logs de segurança (L / M)
R.32	backups perdidos, roubados (L / H)
R.33	acesso não autorizado a instalações (LV / H)
R.34	roubo de equipamento de informática (VL/ H)
R.35	desastres naturais (VL / H)

Os pontos de verificação são questões colocadas para identificar recursos relevantes do PACS e seus riscos relacionados. O trabalho apresentado pelos autores considerou 18 pontos de verificação:

- O provedor de nuvem tem planos de continuidade de negócios e recuperação de desastres? Essa documentação está disponível para os clientes?
- O provedor garante aos clientes a manutenção de seus direitos sobre os dados armazenados na nuvem?
- O provedor de nuvem oferece exclusão segura de dados?

- Qual esquema de licenciamento de software a organização adotará na nuvem?
- O serviço oferecido pelo provedor de nuvem é construído a partir da infraestrutura compartilhada com outras organizações?
- Quais mecanismos de segurança serão adotados para proteger os dados armazenados no PACS com base em nuvem?
- A transferência de dados é feita através de um canal de comunicação seguro?
- As taxas de transferência de dados para o provedor de nuvem são suficientes para as comunicações esperadas em uma rede PACS?
- A conexão com os serviços de nuvem pode ser feita através de vários provedores de serviços de Internet (ISPs)?
- O provedor de nuvem explica nos termos do contrato os procedimentos a serem adotados em caso de suspensão dos serviços?
- O provedor de nuvem permite que os clientes executem ou tenham acesso a documentos de auditoria de TI?
- O provedor de nuvem oferece capacidades de armazenamento compatíveis com o PACS?
- Na eventual migração para outro serviço de nuvem, o provedor suporta a exportação de dados e aplicativos?
- Os recursos de software que são executados no PACS com base em nuvem podem ser registrados com as agências reguladoras governamentais apropriadas?
- A legislação obedecida pelo provedor de serviços em nuvem garante a confidencialidade das informações armazenadas no PACS?
- O provedor de serviços oferece algum tipo de proteção contra ataques de negação de serviço?
- Como os visualizadores DICOM serão integrados ao ambiente de nuvem e disponibilizados aos usuários?
- Que tipo de suporte será oferecido pelo provedor para o PACS crescer?

Em seguida, um modelo de análise de risco para ambientes PACS na nuvem foi proposto e avaliado. O modelo de análise de risco foi aplicado ao PACS do Centro de Ciências da Imagem e Física Médica (Centro Médico Universitário da Faculdade de Medicina de Ribeirão Preto da Universidade de São Paulo, Brasil), atualmente sendo testado para

migração para a nuvem. Baseando-se nos recursos do PACS, no provedor de nuvem e nas políticas de gerenciamento adotadas, todas as perguntas nos pontos de verificação foram respondidas. Os riscos associados a cada *checkpoint* foram avaliados e, quando justificáveis, eliminados. A figura 2.11 resume a análise de risco, que indica, por exemplo, que o gerenciamento de rede (R.26) e o abuso de direitos administrativos (R.10) são questões que merecem atenção no ambiente analisado. Os valores em ambos os eixos, probabilidade e impacto, variam de 0 para 4, representando os 5 possíveis rótulos de classificação VL, L, M, H, VH. A combinação dessas duas variáveis permite a identificação da severidade do risco, representada pelas cores amarelo (menos grave), laranja e vermelho (mais grave).

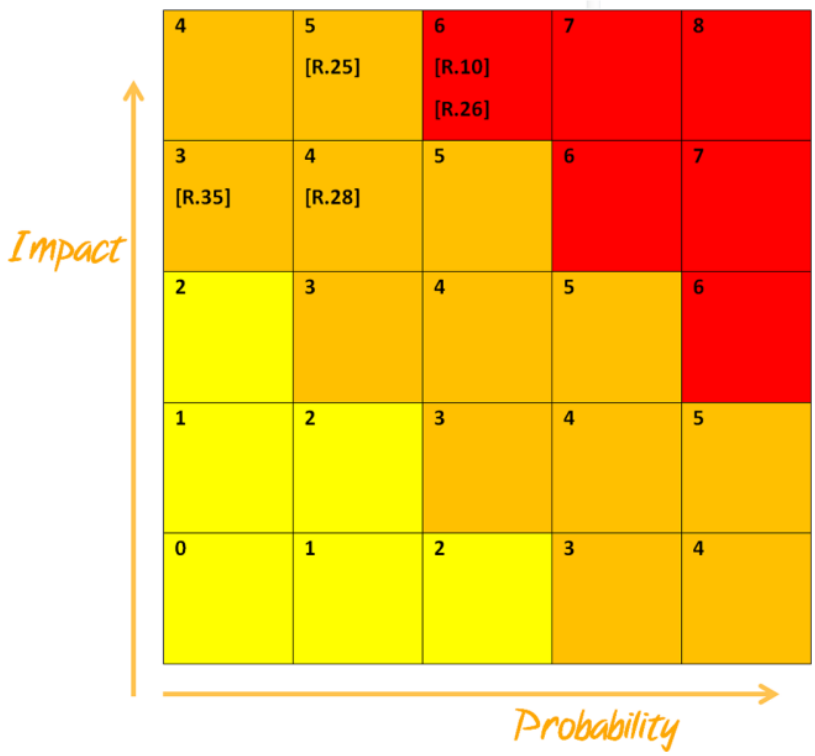

Figura 2.11: Os riscos mais relevantes identificados após os pontos de avaliação [6].

Os autores concluem que o modelo de análise de risco apresentado no estudo foi capaz de conduzir uma avaliação estruturada e bem organizada das vulnerabilidades de um ambiente PACS na nuvem. Para eles, a abordagem de vincular riscos a atividades em pontos de verificação também pode ser usada para definir quais tarefas devem ser executadas para mitigar os riscos.

2.5.4 Um estudo de caso da migração de um sistema corporativos para a IaaS

Khajeh-Hosseini et al [50], elaboraram um estudo que ilustra os benefícios e riscos potenciais associados à migração de um sistema de TI na indústria de petróleo e gás de um centro de dados interno para a Amazon EC2 a partir de uma ampla variedade de perspectivas das partes interessadas em toda a empresa. O caso de uso de migração compreende a viabilidade da migração de uma das principais ofertas de serviços da organização (um sistema de monitoramento de qualidade e aquisição de dados) para o Amazon EC2. A empresa C é uma pequena empresa de petróleo e gás que possui alguns ativos *offshore* nos campos petrolíferos do Mar do Norte. A empresa C precisava de um sistema de aquisição de dados que lhes permitisse gerenciar suas operações offshore, monitorando os dados de seus ativos minuto a minuto. Os ativos da empresa C contam com as instalações de produção da Empresa A (uma grande empresa de petróleo), portanto, os dados chegam ao país por meio dos links de comunicação da Empresa A. A empresa C não possui a capacidade de desenvolver seus próprios sistemas de TI, portanto terceirizou o desenvolvimento e o gerenciamento do sistema para a empresa B, que é uma empresa de soluções de TI com um pequeno data center.

A partir de então, os autores realizaram um trabalho de campo nos escritórios da Empresa B, no qual todos os documentos relacionados ao sistema sob investigação foram coletados e estudados. O trabalho de campo teve três etapas:

Fase 1: Os custos de infraestrutura do sistema foram calculados a partir dos relatórios e faturas do projeto. Esses custos foram comparados com os custos de uma configuração de infraestrutura semelhante no Amazon EC2.

Fase 2: A empresa B possui um banco de dados de todos os problemas de suporte e manutenção relacionados aos sistemas que eles suportam. Esse banco de dados foi pesquisado manualmente e todas as chamadas de suporte potencialmente afetadas pela migração foram identificadas e analisadas.

Fase 3: Consistem em uma análise do impacto das partes interessadas para identificar as fontes potenciais de benefícios e riscos a partir das perspectivas de várias partes interessadas e é realizada analisando as transcrições das entrevistas. É composto por:

1. Identificar os principais interessados;
2. Identificar as mudanças nas tarefas que seriam necessárias para executar e como deveriam realizá-las;
3. Identificar quais são as prováveis consequências das mudanças em relação ao tempo, recursos, capacidades, valores, status e satisfação das partes interessadas;

4. Analisar essas mudanças dentro do contexto mais amplo de fatores relacionais, como o tempo

Os resultados do estudo mostraram que a infraestrutura do sistema no estudo de caso teria custado 37% menos ao longo de 5 anos na EC2, e usando a computação em nuvem poderia ter potencialmente eliminado 21% das chamadas de suporte para este sistema. Essas descobertas parecem suficientemente significativas para exigir uma migração do sistema para a nuvem, mas a análise de impacto das partes interessadas revelou que há riscos significativos associados a isso. Porém, os autores destacaram as limitações para quantificar os custos. Segundo os autores, os custos de pessoal de suporte são difíceis de quantificar, pois primeiro exigiriam que o sistema fosse migrado para a nuvem e fossem executados por um período de tempo para estudar quaisquer problemas que surgissem. Há também custos de longo prazo associados à migração de sistemas, como o custo de migrar para outro provedor de nuvem se o provedor atual for inadequado ou aumentar seus planos de custo ou até mesmo os custos associados à perda de experiência / conhecimento se uma empresa precisar para reimplementar o sistema internamente. Além do mais, as desvantagens incluem riscos para a satisfação do cliente e qualidade geral do serviço devido à difusão do controle para terceiros; diminuição da satisfação no trabalho devido a mudanças na natureza do trabalho; e abrir a organização para a volatilidade de custos de longo prazo em termos de custos de uso de nuvem e transferência de dados.

2.5.5 A estratégia de gerenciamento de riscos na computação em nuvem

Fan e Chen [7] desenvolveram um estudo para identificar e analisar riscos relacionados a computação em nuvem por meio de métodos científicos e objetivos que fornecem as informações necessárias de apoio a decisão aos administradores em de gestão de risco. O estudo se desenvolveu em três fases:

Na primeira fase, os fatores-chave de sucesso para computação em nuvem e estrutura hierárquica de avaliação são identificados usando o método Delphi. O objetivo dessa fase foi desenvolver uma estrutura hierárquica de avaliação para riscos de Cloud Computing.

Na segunda fase, a estrutura de critérios é elaborada, como resultado da primeira fase, conforme apresentado na figura 2.12. Nessa fase, os pesos dos riscos de frequência e gravidade em nuvem também são usados como critérios de avaliação e são calculados efetivamente empregando o Analytic Network Process (ANP).

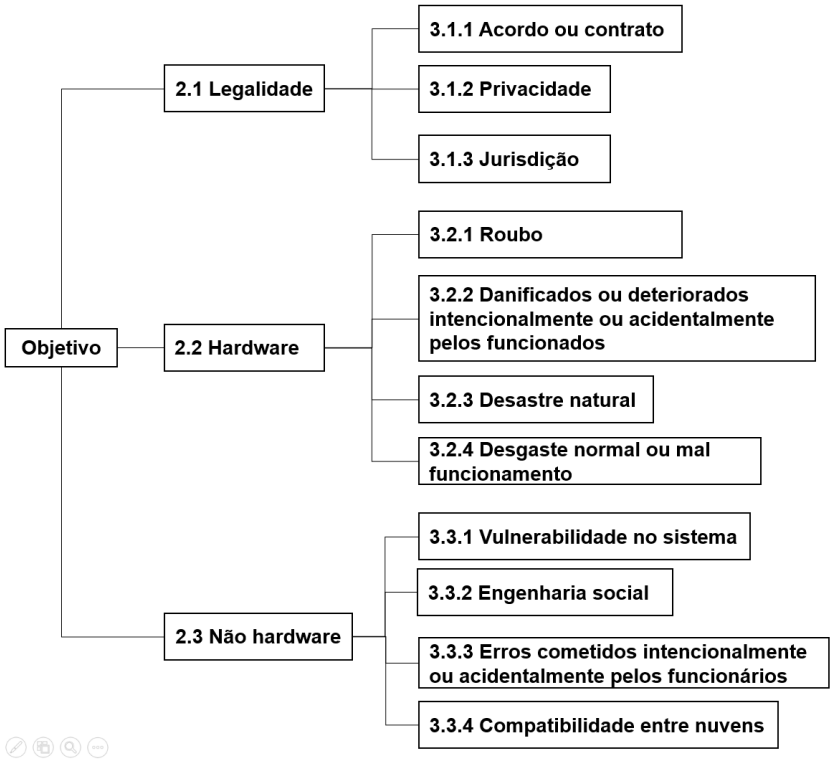

Figura 2.12: Estrutura de critérios e subcritérios [7].

Na terceira fase, as diferenças entre os pesos dos riscos da computação em nuvem e as prioridades de tratamento são reconhecidas usando a "Matriz de Gerenciamento de Riscos". A figura 2.13 representa uma matriz de gerenciamento de risco que ilustra uma prioridade clara do gerenciamento de risco. Na figura, a maior frequência de risco entre todos os onze riscos é a “Compatibilidade Cross-Cloud” (3.3.4), a segunda maior frequência é “Engenharia Social” (3.3.2), enquanto a terceira é “Erros cometidos pelos funcionários intencionalmente ou acidentalmente”(3.3.3).

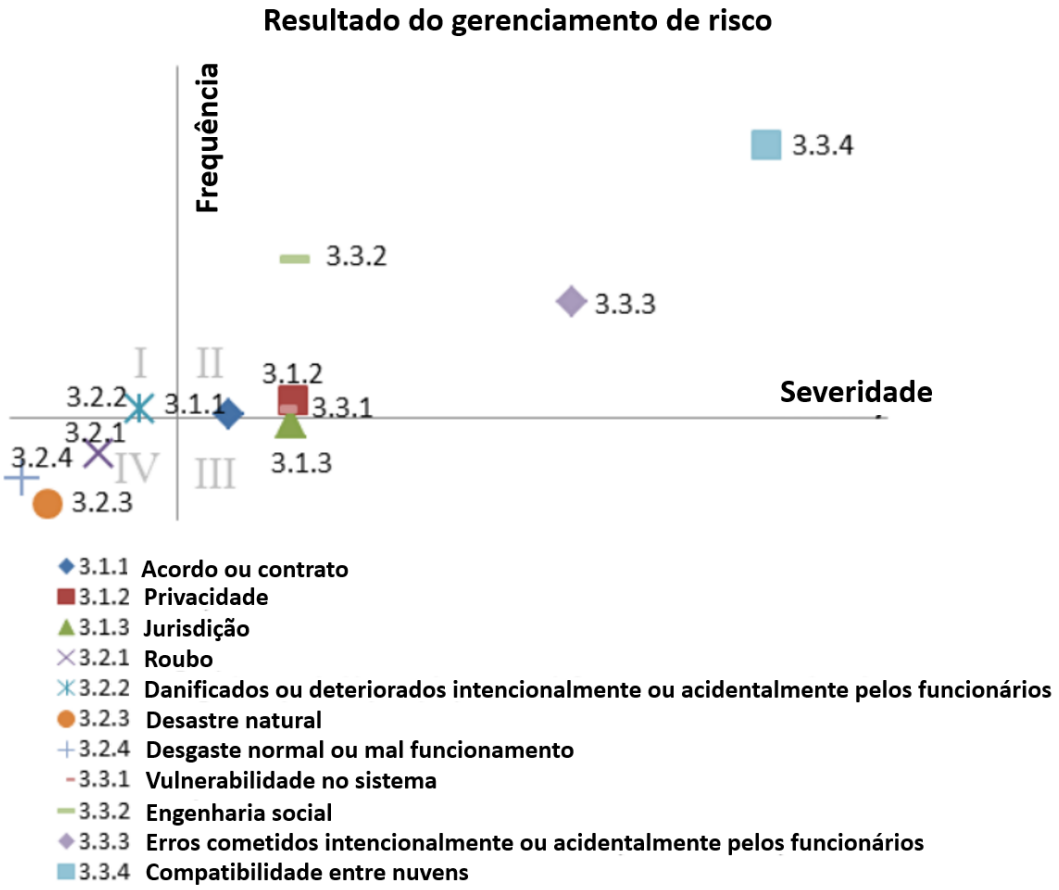

Figura 2.13: Resultado do gerenciamento de risco [7].

Os autores concluíra que a implementação do método ANP permite que os tomadores de decisão visualizem o impacto de vários critérios no resultado final, além de medir a gravidade e a frequência do risco dos serviços de computação em nuvem. Aplique o método ANP para avaliar o peso relativo separadamente. Em seguida, coloque o peso na matriz de gerenciamento de riscos, uma técnica geral para medir riscos, e avance para priorizar os riscos. O estudo identificou "Engenharia Social", "Compatibilidade entre Nuvens"e "Erros cometidos por funcionários intencionalmente ou acidentalmente"são riscos de alta prioridade a serem tratados. Segundo os autores, recomenda-se evitar o risco localizado no quadrante II.

2.5.6 Estrutura de gerenciamento de riscos com COBIT 5 para integração de computação em nuvem

Khrisna e Harlili [8] desenvolveram um estudo que foi capaz de integrar o Framework COBIT 5 com o Gerenciamento de Risco para Computação em Nuvem, figura 2.14, de modo a produzir uma estrutura de gerenciamento de risco mais completa em que aspectos de governança de risco e computação em nuvem são levados em consideração .

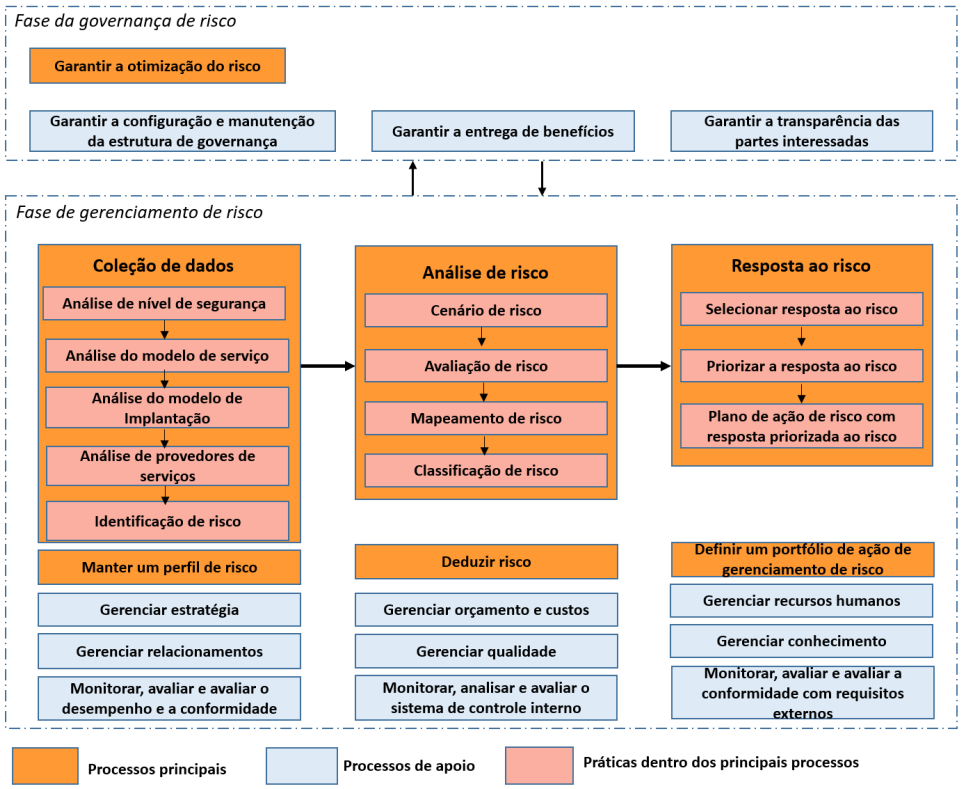

Figura 2.14: Resultado da integração [8].

O COBIT 5 é usado como a integração de base e para determinar a estratégia de governança de risco pelo qual o Risk Management Framework para Cloud Computing é usado para adicionar elementos de uso de computação em nuvem no processo de coleta de dados ao lado de técnicas de análise de risco. O resultado da integração é composto por duas fases: governança de risco e gestão de risco. Cada fase consiste em processos principais e processos de apoio. Os principais processos descrevem como conduzir a otimização de risco, identificação de risco, análise de risco e resposta de risco, enquanto os processos de apoio descrevem o que é necessário para construir e manter uma gestão eficaz e eficiente de riscos e fases de gerenciamento de riscos.

2.6 Tomada de decisão de migração para nuvem

Convém que o processo de tomada de decisões avalie consistentemente e, se necessário, trate o risco. Tomar ou não decisões envolve riscos, e é importante ter uma compreensão dos riscos associados em ambas as situações [32].

Zhao e Zhou [24] destacam que a migração do sistema legado para a nuvem traz grandes desafios e benefícios, de modo que existem várias pesquisas acadêmicas e aplicações industriais na migração do sistema legado para a nuvem.

Khajeh-Hosseini et al. [51] propõem duas ferramentas que visam apoiar a tomada de decisão durante a migração de sistemas de TI para a nuvem. A primeira é uma ferramenta de modelagem que produz estimativas de custo de uso de nuvens públicas IaaS. A ferramenta permite aos arquitetos de TI modelar suas aplicações, dados e requisitos de infraestrutura, além de seus padrões computacionais de uso de recursos. A ferramenta pode ser usada para comparar o custo de diferentes provedores de nuvem, opções de implantação e cenários de uso. A segunda ferramenta é uma planilha que descreve os benefícios e riscos de usar nuvens IaaS de uma perspectiva empresarial; Esta ferramenta fornece um ponto de partida para a avaliação de risco. Dois estudos de caso foram utilizados para avaliar as ferramentas. As ferramentas foram úteis, pois informaram os tomadores de decisão sobre os custos, benefícios e riscos do uso da nuvem.

Ribas et al.[52] apresentaram uma metodologia para tomada de decisão multi critério, visando a escolha sobre a adoção da utilização de serviços na nuvem, considerando os custos e fatores qualitativos importantes, como segurança, desempenho e qualidade. A proposta combina os fatores mais relevantes a serem analisados, usando o processo de decisão multi critério AHP (Analytic Hierarchy Process) visando a geração de um fator moderador para comparar a diferença de custos entre as duas soluções (SaaS e hospedagem interna). A pesquisa apresentada mostrou útil no cálculo da viabilidade da adoção ou não de uma plataforma SaaS quando se tem definidas todas as variáveis em um determinado cenário e tempo.

Pahl e Xiong [30] analisaram as preocupações de arquitetura e programação de software no contexto da migração para soluções PaaS, ou seja, a transição de sistemas de plataforma de soluções on-premise para nuvem. Foram investigadas as melhores práticas na codificação cloud-aware na forma de padrões e formulamos estes como um processo de migração. Objetivou-se as semelhanças no processo de migração PaaS, utilizando as camadas IaaS / PaaS / SaaS como o principal fator de diferenciação para extrair as preocupações específicas da PaaS e representá-las como um processo genérico de migração. Estabeleceram um quadro de processos de migração que delineia grandes etapas e suas preocupações. Isso serviu de base para extrair problemas críticos em termos comerciais e técnicos. A discussão de estudos de caso, apresentados nas entrevistas com profissionais

especializados, evidenciou a imaturidade em termos de procedimentos estabelecidos e a disponibilidade de ferramentas para apoiar o processo de migração de arquitetura.

Alkhalil et al. [31] propõe um modelo que fornece uma estrutura para auxiliar o processo de tomada de decisão para a migração de recursos de TI das organizações para serviços com bases em nuvem. Essa estrutura orienta sistematicamente os decisores por meio de um processo de migração da nuvem. O modelo inclui três fases: inteligência (identificar problemas, requisitos e oportunidades dentro do ambiente em nuvem), design (adequação do serviço e avaliação de risco) e escolhas. Estas fases são expandidas em seis etapas principais que cada uma tem um número de tarefas a ser executadas. As etapas e tarefas são discutidas neste artigo, com referência à interação que cada tarefa tem com a base de conhecimento. Este modelo oferece uma estrutura preliminar encorajadora para o desenvolvimento de um Knowledge-Based Decision Support System (KBDSS) em nuvem.

2.7 Consolidação das pesquisas aplicadas na migração para nuvem

Com base na pesquisa bibliográfica, a partir da relação dos principais estudos levantados no enfoque meta analítico, chegou-se a uma consolidação das principais técnicas e métodos utilizadas no processo de migração para nuvem, conforme apresentado na figura 2.3.

Tabela 2.3: Relação dos principais estudos e técnicas aplicadas no processo de migração

Estudo/Autor	**Técnicas de riscos utilizadas**	**Ano**
Uma estrutura de gerenciamento de riscos para suporte à decisão de migração para nuvem segundo Islam et al	Entrevistas Listas de verificação AHP	2017
Proposta de uma metodologia de riscos para migração em nuvem segundo Yuusuf e Tubb	Proposta de metodologia de riscos	2013
Um modelo de análise de risco para ambientes PACS na nuvem segundo Cordeiro e Azevedo-Marques	Listas de verificação Matriz de probabilidade / impacto	2015
Um estudo de caso da migração de um sistema de TI corporativo para a IaaS segundo Khajeh-Hosseini et al	Entrevistas Listas de verificação Análise de relatórios Análise de custo/benefício	2010

A estratégia de gerenciamento de riscos da aplicação da computação em nuvem segundo Fan e Chen	Delphi ANP Matriz de frequência / severidade	2012
Estrutura de gerenciamento de riscos com COBIT 5 para integração de computação em nuvem segundo Khrisna e Harlili	Proposta de modelo de riscos com COBIT 5	2014
Ferramenta para apoio as decisões de adoção da nuvem segundo Khajeh-Hosseini et al	Análise de custo	2010
Tomada de decisão multicritério na migração de aplicativos para ambientes de nuvem segundo Ribas et al	Análise de custo AHP	2014
Processo de Migração e Preocupações Arquiteturais segundo Pahl e Xiong	Entrevistas no-SQL	2013
Aplicação do método de análise hierárquica na tomada de decisão para adoção de computação em nuvem: um estudo de caso segundo Oliveira	Entrevistas AHP	2011
Uma aplicação do método Fuzzy-electre-topsis para seleção de serviços de computação em nuvem segundo Luz	AHP Fuzzy-electre-topsis	2014
Análise de risco para Computação em Nuvem segundo Paiva	Listas de verificação Matriz de probabilidade / impacto	2016

A partir desse estudo, conforme destacado na tabela 2.3, foi possível constatar que as ferramentas propostas para o processo de tomada de decisão de migração para nuvem focam, na maioria das vezes, nas plataformas e tipos de serviços da tecnologia em nuvem. A maioria dos estudos apresentados não levam em consideração os aspectos de riscos do ambiente local no processo de decisão. Diante disso, a presente pesquisa irá alinhar os principais métodos aplicados nas pesquisas apresentadas na tabela 2.3 levando-se em consideração os aspectos de riscos tanto de ambiente em nuvem quanto em ambiente local.

Capítulo 3

Metodologia de pesquisa

3.1 Método da pesquisa

O conceito de ciência está ligado ao conceito de método científico [53]. A ciência tem como objetivo fundamental chegar a veracidade dos fatos [54]. O conhecimento caracteriza-se pela procura do porquê de um fenômeno, pela necessidade de explicar a ocorrência do fenômeno [53]. O método é o conjunto das atividades, sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo [55], ou seja, se os passos definidos no método forem executados, os resultados obtidos deverão ser convincentes [56]. Já método científico como o conjunto de procedimentos intelectuais e técnicos adaptados para se atingir o conhecimento. A metodologia são as regras estabelecidas para o método científico, por exemplo: a necessidade de observar, a necessidade de formular hipoteses, a elaboração de instrumentos etc [53]. Para tanto, a pesquisa caracteriza-se como o processo formal e sistemático de desenvolvimento do método científico, cujo o objetivo fundamental é descobrir respostas para problemas mediante o emprego de procedimentos científicos [53]. Ela requer um tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais [55].

No contexto científico, a pesquisa pode ser classificada de acordo com diferentes critérios. Entre eles, é possível diferenciar tipos de pesquisa de acordo com sua natureza, objetivos ou procedimentos técnicos [56]. Para o presente estudo, a natureza da pesquisa é aplicada pois caracteriza-se para que os resultados sejam aplicados na solução de problemas que ocorrem na realidade [55]. Trata-se de uma motivação pela necessidade de resolver problemas concretos [57]. Dessa forma, a natureza aplicada se justifica pela aplicação da gestão de riscos, a partir de instrumentos de governança, como auxilio no processo de tomada de decisão para migração do ambiente local na nuvem privada da instituição.

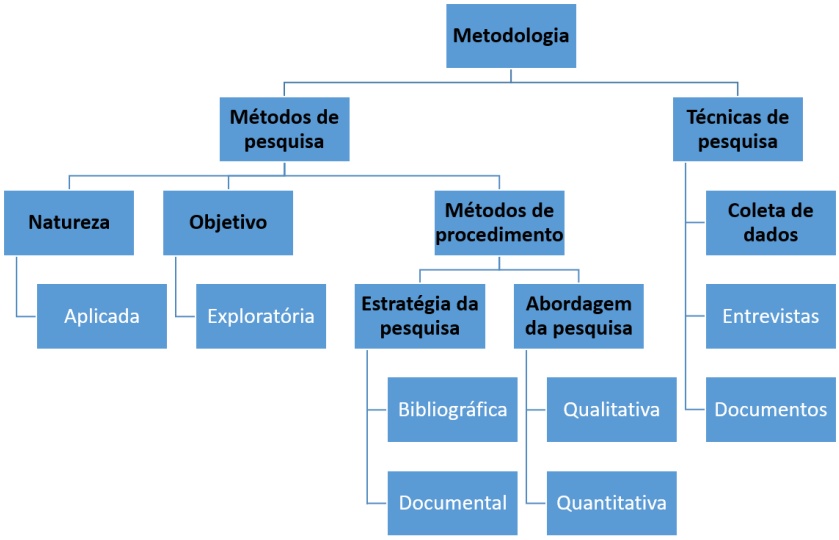

Figura 3.1: Método de pesquisa.

Em relação aos objetivos, a pesquisa é classificada como exploratória. Exploratória devido a necessidade de estudo para definição dos principais eventos de riscos e as principais abordagens de gestão de riscos no processo de migração para nuvem. Na pesquisa exploratória irá examinar um conjunto de fenômenos, buscando anomalias desconhecidas que possam ser a base para uma pesquisa mais elaborada [56]. São desenvolvidas com o objetivo de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato [54].

Quanto a estratégia da pesquisa, a pesquisa é classificada como bibliográfica, documental e estudo de caso. A pesquisa bibliográfica implica o estudo de artigos, teses, livros e outras publicações usualmente disponibilizadas por editoras indexadas[56]. Para tanto, com o objetivo de identificar as melhores contribuições para o estado da arte, bem como os principais eventos de riscos na migração para computação em nuvem, será utilizado o enfoque meta-analítico. Já a pesquisa documental será realizada por meio de materiais que ainda não receberam tratamento analítico, ou seja, as fontes primárias como relatórios, arquivos obtidos em órgãos públicos etc. Por fim, estudo de caso pois o trabalho será desenvolvido em uma instituição pública Federal. O estudo de caso busca, dentre outros, explorar situações da vida real cujos limites não estão claramente definidos e descrever situação do contexto em que está sendo feita determinada investigação [54]. Com isso, será realizado um estudo de caso minucioso e exaustivo para propor a gestão de riscos como instrumento que irá auxiliar os tomadores de decisão das unidades da Fiocruz em migrar ou não seus serviços de dados para o ambiente de nuvem.

Em relação a abordagem da pesquisa, foram utilizadas as abordagens qualitativa e quantitativa. Métodos semiquantitativos usam escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco. A utilização de um método qualitativo ou semiquantitativo, com base na opinião de especialistas, pode ser suficiente e eficaz [3, 15].

3.2 Estrutura da pesquisa

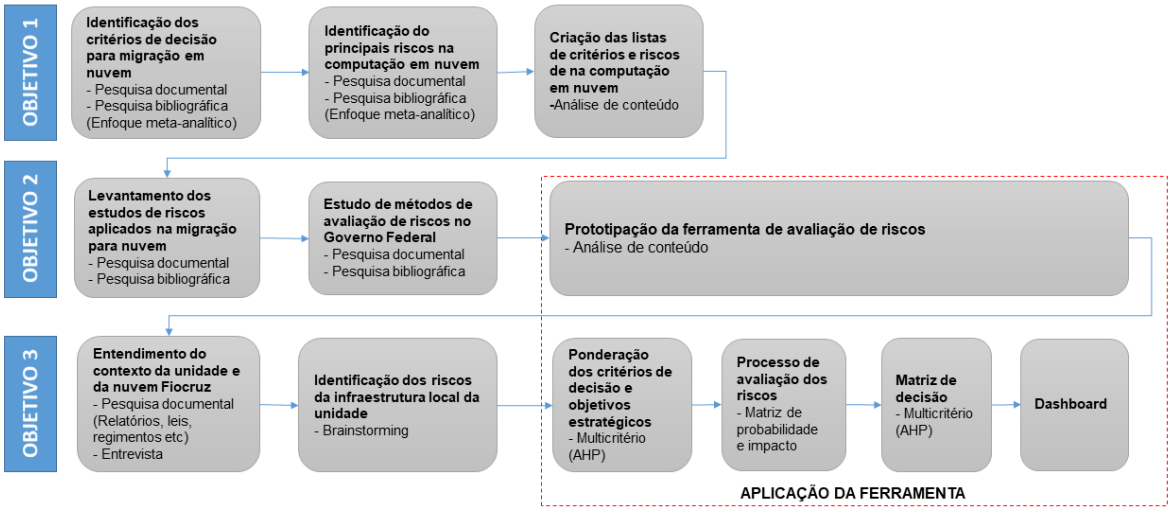

Figura 3.2: Estrutura da pesquisa .

De acordo com Wazlawick [56], o método consiste na sequência de passos necessários para demonstrar que o objetivo proposto foi atingido. Trata-se de um passo fundamental a ser executado logo após a definição do objetivo.

Dessa forma, o primeiro objetivo será fundamentado por meio de pesquisa documental e bibliográfica. Para a pesquisa documental, serão realizadas buscas em sites de governo e empresas especializadas a fim encontrar informações que possam contribuir com a pesquisa. Para a pesquisa bibliográfica será utilizada a metodologia baseada no enfoque meta-analítico. A partir do resultado dessa pesquisa, identifica-se os principais critérios a serem utilizados no processo de decisão para migração para nuvem bem como os eventos de riscos a serem utilizados no processo de avaliação de riscos.

O segundo objetivo será realizado por meio de uma pesquisa bibliográfica e documental. A partir do resultado do enfoque meta-analítico, serão destacados os principais estudos e aplicações de riscos no processo de migração para ambiente em nuvem. Ainda nessa etapa, serão identificados os principais documentos e normativos que orientem os

órgãos da APF em relação a gestão de riscos e governança. O resultado das duas pesquisas será a base para construção de um instrumento de apoio a decisão de migração para ambiente em nuvem com base em um processo de avaliação de riscos.

O terceiro objetivo será a aplicação do instrumento criado no objetivo anterior a partir do processo de gestão de riscos segundo a norma NBR ISO 31000:2009. Para tanto, será realizado o levantamento de contexto da unidade no qual será realizada a análise. Nesse processo será recorrido a documentos, regimentos, normas etc para levantar todas as informações que possam auxiliar no processo de avaliação dos riscos. Após a contextualização, será realizado o processo de avaliação de riscos a partir do instrumento criado.

3.3 Enfoque Meta-analítico

Segundo Mariano et al [58] O enfoque meta-analítico possibilita obter os melhores autores, artigos e revistas, e também realizar uma análise das técnicas estatísticas, das técnicas amostrais, das linhas mais pesquisadas e das abordagens utilizadas. Os autores destacam que o enfoque meta-analítco pode ser realizado em 4(quatro) ou 7(sete) etapas. Para este estudo foi realizada a abordagem com 4(quatro) etapas.

3.3.1 Análise e apresentação das revistas da disciplina

Para Calazans [59], essa análise engloba identificar as revistas mais utilizadas no contexto estudado. Nessa fase são pesquisadas as revistas relacionadas aos principais congressos, encontros da área de conhecimento de usabilidade móvel.

Para essa análise foi realizada uma busca na base de dados multidisciplinar de resumos e citações de artigos de periódicos acadêmicos Scopus. Os termos utilizados foram destacados em duas buscas destintas. A primeira busca foi realizada para identificar os principais trabalhos referentes a Decisão de migração em nuvem. Para tanto, foram utilizados os termos ***cloud AND migration AND decison***. A segunda busca foi para encontrar os principais trabalhos referentes a Riscos na migração em nuvem. Para tanto, foram utilizados os termos ***cloud AND migration AND risk***. Foram considerados artigos publicados durante o período 2010 a 2017.

Tabela 3.1: Quantidade de artigos publicados por termo período 2010 a 2017 .

Termo	**Quantidade de artigos**
cloud AND migration AND decison	299
cloud AND migration AND risk	154

3.3.2 Seleção de revistas relevantes da disciplina

Segundo Calazans et al [59], nessa etapa são selecionadas revistas relevantes da disciplina, ou seja, periódicos de maior destaque.

Na figura 3.3 foram destacados os periódicos com maior impacto com base no Citstore para o termo textbf*cloud AND migration AND decison*. CiteScore[1] é o número de citações recebidas por um jornal em um ano para documentos publicados nos três anos anteriores, divididos pela quantidade de documentos indexados na Scopus publicados nesses mesmos três anos.

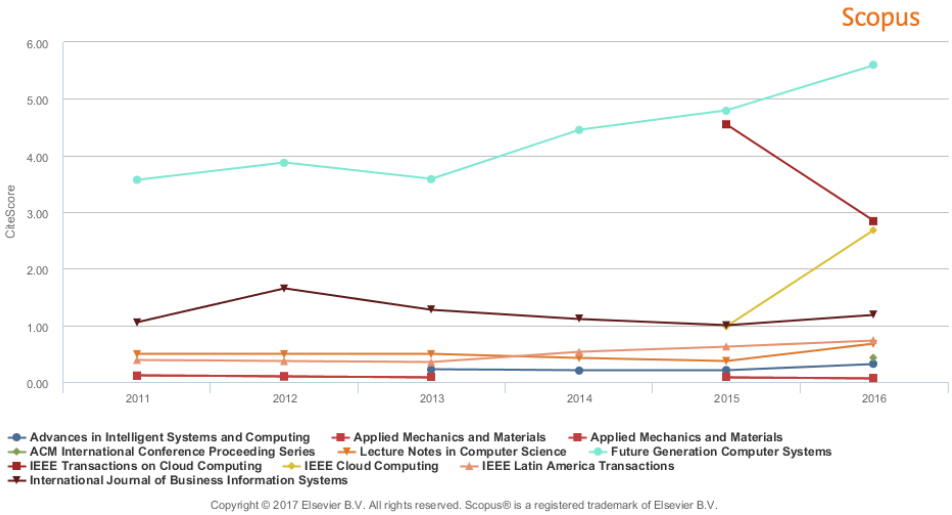

Figura 3.3: Principais periódicos selecionados para as termos cloud AND migration AND Decision.

Para o termo ***cloud AND migration AND risk*** foram destacados os seguintes periódicos com maior impacto com base no Citstore.

[1] `https://service.elsevier.com/app/answers/detail/a_id/14880/supporthub/scopus/`

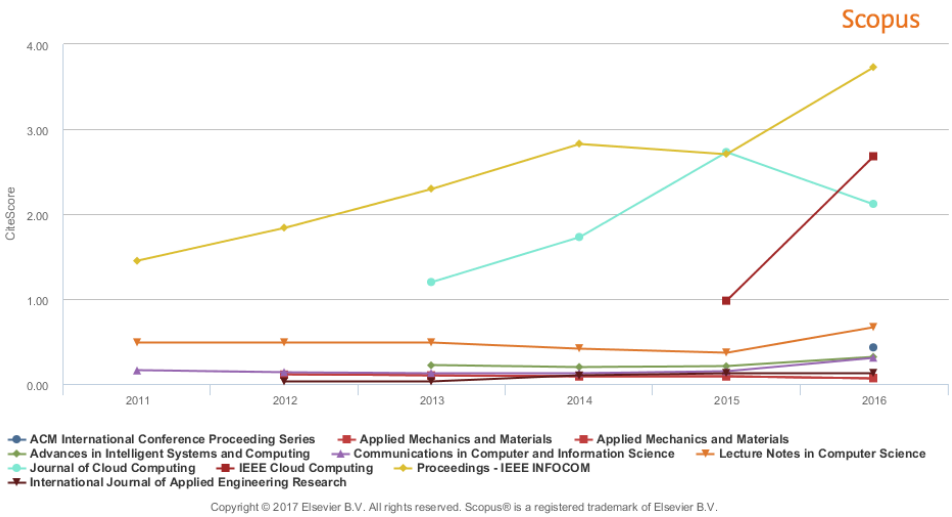

Figura 3.4: Principais periódicos selecionados para as termos cloud AND migration AND Risk.

3.3.3 Coleta de dados para alimentação da base de dados

A coleta engloba a realização da pesquisa sobre o tema usando como filtro as palavras chaves do estudo e as publicações selecionadas anteriormente [59].

Nessa etapa, foram selecionados os artigos com maior relação sobre a proposta da pesquisa. Dos 299 artigos destacados na Tabela 3.1 para o termo ***cloud AND migration AND decison***, foram selecionados 18 que tinham relação com a pesquisa. Dos 154 artigos destacados na Tabela 3.1 para o termo ***cloud AND migration AND risk***, forma selecionados 18 artigos relevantes para o estudo.

3.3.4 Análise dos artigos e autores

Segundo Calazans [59] o objetivo dessa análise consiste em avaliar a importância do tema ao longo dos anos. Essa análise permite visualizar a relação das revistas selecionadas em relação à pesquisa no período estudado.

Após uma análise dos artigos em relação a proposta do estudo, foram selecionados os trabalho dos autores abaixo, ordenados pelo maior impacto levando-se em consideração a citação.

Authors	Title	Cited by	Year	Qualis	Source title
Khajeh-Hosseini A., Greenwood D., Sommerville I.	Cloud migration: A case study of migrating an enterprise IT system to IaaS	128	2010	B2	IEEE 3rd CLOUD 2010
Khajeh-Hosseini A., Sommerville I., Bogaerts J., Teregowda P.	Decision support tools for cloud migration in the enterprise	81	2011	B2	IEEE 4th CLOUD 2011
Gkatzikis L., Koutsopoulos I.	Migrate or not? Exploiting dynamic task migration in mobile cloud computing systems	34	2013	A1	IEEE Wireless Communications
Babar M.A., Chauhan M.A.	A tale of migration to cloud computing for sharing experiences and observations	32	2011	A1	International Conference on Software Engineering
Tran V., Keung J., Liu A., Fekete A.	Application migration to cloud: A taxonomy of critical factors	26	2011	A1	International Conference on Software Engineering
Andrikopoulos V., Strauch S., Leymann F.	Decision support for application migration to the cloud challenges and vision	14	2013	B4	CLOSER 2013
Juan-Verdejo A., Baars H.	Decision support for partially moving applications to the cloud - The example of business intelligence	14	2013	B4	HotTopiCS 2013
Fehling C., Leymann F., Ruehl S.T., Rudek M., Verclas S.	Service migration patterns: Decision support and best practices for the migration of existing service-based applications to cloud environments	7	2013	A2	IEEE 6th SOCA 2013
Islam S., Weippl E.R., Krombholz K.	A decision framework model for migration into cloud: Business, application, security and privacy perspectives	3	2014		ACM Conference Proceeding Series
Andrikopoulos V., Darsow A., Karastoyanova D., Leymann F.	CloudDSF - The cloud decision support framework for application migration	3	2014		Lecture Notes in Computer Science
Razumnikov S.V., Zakharova A.A., Kremneva M.S.	A model of decision support on migration of enterprise itapplications in the cloud environment	3	2014	B2	Applied Mechanics and Materials
Deng L., Jin H., Chen H., Wu S.	Migration cost aware mitigating hot nodes in the cloud	1	2013	A1	CLOUDCOM-ASIA 2013
Alkhalil A., Sahandi R., John D.	An exploration of the determinants for decision to migrate existing resources to cloud computing using an integrated TOE-DOI model		2017	B2	Journal of Cloud Computing
Chen J., Li X.-Y.	Research on SLA-based business automatic deployment of private cloud platform		2017		ISAI 2016
Alkhalil A., Sahandi R., John D.	A decision process model to support migration to cloud computing		2017	A2	Inter. Journal of Business Information Systems
Melo M.M., Fagotto E.A.M.	A decision-making tool for datacenter migration		2015	B4	IEEE Latin America Transactions
Gómez R., Rosado D.G., Mellado D., Fernández-Medina E.	Security criteria in deciding on migration of systems to the cloud		2012	B1	WOSIS 2012, in ICEIS 2012
Yam C.-Y., Baldwin A., Ioannidis C., Shiu S.	Migration to cloud as real option: Investment decision under uncertainty		2011		HP Laboratories Technical Report

Figura 3.5: Relação de artigos e autores selecionados referentes ao termo cloud AND migration AND decison .

Durante o estudo foi possível encontrar dois artigos em comum aos termos pesquisados, conforme demonstrado nas figuras 3.5 e 3.6. Após uma análise, constatou-se que ambos as contribuições possuem grande impacto e relação com a proposta da pesquisa.

Authors	Title	Cited by	Year	Qualis	Source title
Khajeh-Hosseini A., Greenwood D., Som	Cloud migration: A case study of migrating an enterprise IT system to IaaS	128	2010	A1	IEEE 3rd CLOUD 2010
Khajeh-Hosseini A., Sommerville I., Boga	Decision support tools for cloud migration in the enterprise	81	2011	A1	IEEE 4th CLOUD 2011
Beserra P.V., Camara A., Ximenes R., Al	Cloudstep: A step-by-step decision process to support legacy application migration to the cloud	28	2012		IEEE 6th MESOCA 2012
Bermudez I., Traverso S., Mellia M., Muna	Exploring the cloud from passive measurements: The Amazon AWS case	15	2013	A1	IEEE INFOCOM
Alonso J., Orue-Echevarria L., Escalante	Cloud modernization assessment framework: Analyzing the impact of a potential migration to Cloud	6	2013		IEEE 7th MESOCA 2013
Bijon K., Krishnan R., Sandhu R.	Mitigating multi-tenancy risks in IaaS cloud through constraints-driven virtual resource scheduling	5	2015	A1	ACM SACMAT
Opara-Martins J., Sahandi R., Tian F.	Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective	3	2016	B2	Journal of Cloud Computing
Razumnikov S.V., Zakharova A.A., Kremn	itapplications in the cloud environment	3	2014	B2	Applied Mechanics and Materials
Lonea A.M., Popescu D.E., Prostean O.	The overall process taken by enterprises to manage the IaaS cloud services	2	2012		6th ECIME 2012
Razumnikov S.V., Kremneva M.S.	Decision support system of transition IT-applications in the cloud enviroment	1	2015		SIBCON 2015
Wang H., Zhao G., Chen Q., Tang Y.	Trust management for IaaS with group signature	1	2013		4th EIDWT 2013
Bazi H.R., Hassanzadeh A., Moeini A.	A comprehensive framework for cloud computing migration using Meta-synthesis approach		2017	A2	Journal of Systems and Software
Chihi H., Chainbi W., Ghdira K.	Cloud computing architecture and migration strategy for universities and higher education		2016	B1	IEEE/ACS AICCSA
Chopra A., Prasad P.W.C., Alsadoon A., A	Cloud computing potability with risk assessment		2016		4th IEEE MobileCloud 2016
Vijayakumar K., Arun C.	A survey on risk assessment in cloud migration		2015	B3	Journal of Applied Engineering Researc
Cordeiro S.D.S., Santana F.S., Suzuki K.	A risk analysis model for PACS environments in the cloud		2015	B1	IEEE Symposium on Computer-Based
Maher N., Kavanagh P., Glowatz M.	A vendor perspective on issues with security, governance and risk for Cloud Computing		2013		26th Bled eConference
Gómez R., Rosado D.G., Mellado D., Fe	Security criteria in deciding on migration of systems to the cloud		2012	B1	9th WOSIS 2012, in ICEIS 2012

Figura 3.6: Relação de artigos e autores selecionados referentes ao termo cloud AND migration AND risk .

De acordo com as figuras 3.5 e 3.6, podemos observar que os principais trabalhos selecionados são de periódicos com conceitos QUALIS variando entre B2 a A1, em sua grande maioria. Diante disso, a partir do estudo foi possível identificarmos as contribuições científicas mais relevantes para o estudo em questão.

Capítulo 4

Proposta de ferramenta para avaliação de riscos

4.1 Contextualização

Toda e qualquer mudança em uma organização exige dos tomadores de decisão avaliar os impactos que podem ocorrer durante esse processo. Além da desconfiança, há riscos que precisam ser identificados e avaliados para que seja decidido qual melhor caminho seguir. Apesar de existir diversas técnicas e métodos para o processo de avaliação de riscos, a escolha para cada caso específico ainda exige dos avaliadores uma capacidade além do seu conhecimento.

Conforme já destacado, migrar serviços e tecnologias corporativas para plataforma em nuvem não é uma tarefa trivial, pois exige que diversos fatores e riscos sejam mapeados e avaliados. Além do mais, não basta avaliar somente a questão tecnológica, é preciso entender todo o contexto institucional para se identificar todos os riscos para cada caso. A norma NBR ISO 31000:2009 apresenta um processo sistemático capaz de guiar a organização no processo de avaliação de riscos. Diante disso, o apoio de uma ferramenta nesse processo contribuirá para melhoria do nível de confiança dos resultados da avaliação dos riscos.

Dessa forma, a proposta de ferramenta de avaliação de riscos para auxiliar no processo de tomada de decisão para migração de um ambiente tradicional para nuvem foi desenvolvida a partir do resultado da consolidação do estudo apresentado na tabela 2.3.

Para tanto, a ferramenta foi elaborada utilizando o software Microsoft Excel pela facilidade no registro de informações em planilhas e para os cálculos necessários durante o processo.

4.2 Objetivo

O objetivo da ferramenta é servir como instrumento de apoio as unidades regionais da Fiocruz na tomada de decisão para migração em nuvem a partir de um processo sistemático de gestão de riscos, segundo a norma NBR ISO 31000:2009.

4.3 Definição dos critérios de decisão para migração em nuvem

Avaliar a mudança de um ambiente tradicional para computação em nuvem envolvem critérios que precisam ser identificados e analisados com a finalidade de preparar a organização de forma adequada para a transição [60]. Dessa forma, os critérios de decisão para migração em nuvem foram identificados com o objetivo de auxiliar os gestores a hierarquizar os critérios de maior importância no contexto institucional. Diante disso, foi realizado um estudo para mapear os principais critérios a serem considerados no processo de tomada de decisão para migração em nuvem. Esses critérios estão listados na tabela 4.1.

Tabela 4.1: Relação de critérios (Elaboração própria)

Critério	Subcritério	Referências
Ambiente organizacional	Alinhamento às normas de SIC	[1, 4, 31]
	Alinhamento estratégico com TIC	[1, 4, 31]
	Envolvimento da alta direção	[1, 4, 27, 31]
Gestão de serviços	Acordos de Níveis de Serviços (SLA)	[1, 27, 31]
	Gestão contratual	[1, 27, 31, 51]
	Gestão de capacidade	[1, 31, 37, 52]
Infraestrutura TIC	Soluções de conectividade	[1, 31, 61, 62]
	Soluções de armazenamento	[1, 31, 49, 61, 62]
	Soluções de processamento	[1, 31, 49, 61, 62]
	Soluções de memória volátil	[1, 61, 62]
	Elasticidade e escalabilidade	[1, 37, 52]
Segurança da Informação	Disponibilidade	[1, 4, 27, 31, 37, 51, 52]
	Integridade	[1, 4, 27, 31, 37, 51, 52]
	Confidencialidade	[1, 4, 27, 31, 37, 51, 52]
	Autenticidade	[1, 4, 27, 31, 37, 51, 52]
Financeiro/orçamentário	Operacionalização	[1, 27, 37, 51, 52]
	Manutenção	[1, 27, 37, 51, 52]
	Orçamento	[1, 31, 51]

Governança	Planejamento	[1, 4, 31]
	Política de recursos humanos	[1, 27, 31]
	Gestão de mudanças	[1, 4, 31, 51, 52]
	Gestão de maturidade	[1, 4, 31]

Os critérios apresentados na tabela 4.1 foram agrupados a partir das referências identificadas do enfoque meta-analítico, além de pesquisa documental e pesquisa bibliográfica em trabalhos acadêmicos relacionados ao tema. O resultado dessa pesquisa chegou aos seguintes critérios de decisão de migração para nuvem:

- **Ambiente organizacional:** Refere-se ao conjunto de elementos que integram o contexto da organização, tais como: os costumes, os colaboradores, conhecimento, envolvimento da alta direção com a gestão de TI, alinhamento as normas e estratégias internas com a TI etc.
- **Gestão de serviços:** Refere-se ao conjunto de capacidades organizacionais para prover um valor para o cliente na forma de serviços, tais como: Acordo de Nível de Serviço (SLA), gestão contratual, gestão de capacidades, adesão do prestador com normativos legais etc.
- **Infraestrutura de TIC:** Refere-se aos componentes e serviços que fornecem a base para sustentar todos os sistemas de informação de uma organização, tais como: soluções de conectividade, armazenamento de dados, processamento, memória volátil, escalabilidade, desempenho etc.
- **Segurança da Informação:** Refere-se ao conjunto de ações capazes de garantir as propriedades básicas da segurança da informação da organização, são elas: disponibilidade, integridade, confidencialidade e autenticidade.
- **Financeiro / Orçamentário:** Refere-se ao conjunto de ações que impactem nos planejamentos orçamentário e financeiro da organização, tais como: custos de manutenção, compra de ativos físicos e lógicos de TI, custos de operação etc.
- **Governança:** Refere-se a um conjunto de práticas, padrões assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com o objetivo de garantir controles efetivos com vistas à condução de políticas pública e à prestação de serviços de interesse da sociedade.

4.4 Matriz de probabilidade X Impacto

A matriz de probabilidade e Impacto combina abordagens qualitativas ou semiquantitativas de consequências (impactos) e probabilidades, a fim de produzir um nível de risco ou classificação de risco [14, 15].

Conforme é demonstrado na tabela 2.1, a matriz de probabilidade e impacto é fortemente aplicada na identificação e análise de riscos, ao passo que na avaliação de riscos ela é considerada aplicável. Também pode ser utilizada para auxiliar a comunicação de uma compreensão comum dos níveis qualitativos dos riscos em toda a organização.

Além de ser instrumento para várias pesquisas aplicadas no processo de riscos para migração em nuvem, conforme apresentado na tabela 2.3, essa técnica é proposta como guia de gestão de riscos para o MP [10], TCU [15] e também como ferramenta para avaliação de riscos no Modelo de Gestão de Riscos em Segurança da Informação e Comunicações - GRSIC da Fiocruz, conforme definido pela Portaria 001/2016/VPGDI [9].

4.4.1 Definição da escala de Impacto

O impacto deve considerar os potenciais prejuízos causados, caso o incidente se concretize. Quanto maior a relevância do ativo, maior será a severidade de um incidente [9]. A definição da escala de impacto da ferramenta foi elaborada a partir dos objetivos estratégicos da Fiocruz alinhada a escala de impacto do Modelo de GRSIC da Fiocruz. O resultado é demonstrado na figura 4.1. Conforme é apresentado na figura, a medida que cresce a escala, maior o impacto para nos objetivos estratégicos da instituição. Os objetivos estratégicos, ou processos estratégicos, da Fiocruz são apresentados na seção 5.1.1.

		IMPACTO				
PROCESSOS ESTRATÉGICOS	**Desafios SUS**	Os danos são insignificantes para promoção, vigilância e informação em saúde, além da formação de quadros profissionais para o SUS.	A organização consegue reparar os danos a promoção, vigilância e informação em saúde, além da formação de quadros profissionais para o SUS, com seus próprios recursos.	A recuperação dos danos a promoção, vigilância e informação em saúde, além da formação de quadros profissionais para o SUS extrapola os recursos da organização	Danos a promoção, vigilância e informação em saúde, além da formação de quadros profissionais para o SUS que venham a manchar a imagem do órgão ou gerar algum incidente grave.	Os danos que venham a causar destruição irreparável a imagem do órgão, além da sociedade afetada pela impossibilidade de formação dos profissionais do SUS.
	C&T, Saúde e Sociedade	Os danos são insignificantes para difusão e compartilhamento do conhecimento em CT&I e saúde	Com recursos próprios, a organização consegue reparar danos a difusão e compartilhamento do conhecimento em CT&I e saúde	A recuperação dos danos a difusão e compartilhamento do conhecimento em CT&I e saúde extrapola os recursos da organização	Danos a a difusão e compartilhamento do conhecimento em CT&I e saúde que venham a manchar a imagem do órgão ou gerar algum incidente grave.	Comprometimento a difusão e compartilhamento do conhecimento em CT&I e saúde capaz de causar destruição irreparável a imagem do órgão, além de impactar diretamente na sociedade.
	Complexo Produtivo e Inovação em saúde	Os danos são insignificantes para produção de insumos para a saúde	A organização consegue reparar os danos a produção de insumos para a saúde com recursos próprios	A recuperação dos danos a produção de insumos para a saúde extrapola os recurso da organização.	Danos a produção de insumos para a saúde que vem a manchar a imagem do órgão e que gere algum desabastecimento temporário a população	Comprometimento total a produção de insumos para a saúde capaz de causar destruição irreparável a imagem do órgão e o desabastecimento a população.
	Saúde ambiental e promoção da saúde pública	Os danos são insignificantes para o desenvolvimento científico-tecnológico e nos processos formativos	A organização consegue reparar os danos ao para o desenvolvimento científico-tecnológico e nos processos formativos com seus próprios recursos	A recuperação dos danos para o desenvolvimento científico-tecnológico e nos processos formativos extrapola os recursos da organização	Danos ao desenvolvimento científico-tecnológico e nos processos formativos que venham a manchar a imagem do órgão	Os danos que venham a causar a destruição irreparável a imagem do órgão.
	Saúde, Estado e cooperação Internacional	O danos são insignificantes para as articulações de cooperação estratégica e internacional	A organização consegue reparar os danos para as articulações de cooperação estratégica e internacional com seus próprios recursos	A recuperação dos danos para as articulações de cooperação estratégica e internacional extrapola os recursos da organização	Danos que venham a dificultar articulações de cooperação estratégica e internacional	Danos que venham a impossibilitar completamente articulações de cooperação estratégica e internacional
	Inovação na gestão	Evento cujo impacto pode ser absorvido por meio de atividades normais	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Evento significativo que pode ser gerenciado em circunstâncias normais	Evento crítico, mas que com a devida gestão pode ser suportado	Evento com potencial levar o serviço ao colapso
		Muito baixo	**Baixo**	**Médio**	**Alto**	**Muito alto**
		1	**2**	**3**	**4**	**5**

Figura 4.1: Escala de impacto.

4.4.2 Definição da escala de Probabilidade

A probabilidade representa a possibilidade de que um determinado evento ocorrerá [10], ou a como a chance de uma ameaça se concretizar [9]. A tabela 4.2 apresenta a escala de probabilidade do Modelo de GRSIC da Fiocruz.

Tabela 4.2: Escala de probabilidade [9]

Valor	Probabilidade	Descrição
1	Muito baixa	Muito improvável de acontecer (1a 10%)
2	Baixa	Improvável de ocorrer (11 a 30%)
3	Média	Ocorre ocasionalmente (31 a 70%)
4	Alta	Provável de ocorrer (71 a 90%)
5	Muito alta	Ocorre frequentemente (91 a 100%)

4.4.3 Cálculo da matriz

Os quadrantes da matriz de riscos são resultantes do cálculo impacto x probabilidade, conforme apresentado na figura 4.2.

			IMPACTO				
			Muito baixo	Baixo	Médio	Alto	Muito alto
			1	2	3	4	5
PROBABILIDADE	Muito baixa	1	1	2	3	4	5
	Baixa	2	2	4	6	8	10
	Média	3	3	6	9	12	15
	Alta	4	4	8	12	16	20
	Muito alta	5	5	10	15	20	25

Figura 4.2: Matriz de risco [9, 10] (adaptado).

Os eventos de riscos situados nos quadrantes definidos como risco alto e risco muito alto são indicativos de necessidade de controles mais rígidos, enquanto os riscos situados nos quadrantes de risco pequeno e moderado seriam um indicativo de controles mais moderados. Em alguns casos não haveria necessidade de implementar controles e/ou até retirar controles [10].

4.4.4 Nível de risco

O nível de risco expressa a magnitude de um determinado evento de risco, em termos da combinação de seu impacto e probabilidade de ocorrência [10, 14, 15], figura 4.3.

ESCALA DE NÍVEL DE RISCOS						Critérios
Níveis		Pontuação				
RMA	Risco Muito Alto	>=	16	<=	25	Os riscos são inaceitáveis e os responsáveis devem ser orientados para minimizar imediatamente.
RA	Risco alto	>=	10	<=	15,99	Os riscos são inaceitáveis e os responsáveis devem minimamente controlá-los.
RM	Risco moderado	>=	6	<=	9,99	Os riscos podem ser aceitos após a revisão e confirmação dos responsáveis. Entretanto, a aceitação dos riscos deve ser feita por meios formais.
RB	Risco pequeno	>=	4	<=	5,99	Os riscos podem ser aceitáveis, entretanto deve ser feita a revisão e confirmação dos responsáveis.
RMB	Risco Muito baixo	>=	1	<=	3,99	Os riscos são aceitáveis e devem ser informados aos responsáveis.

Figura 4.3: Escala de riscos..

- **Nível de Risco Inerente (NRI)** é o nível de risco antes da consideração das respostas para reduzir a probabilidade do evento ou os seus impactos nos objetivos, incluindo controles internos [15].
- **Nível de Risco Residual (NRR)** é o risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações [15].

Os níveis de riscos obtidos com aplicação desta matriz orientarão os gestores na adoção de ações para responder os eventos de riscos identificados.

4.5 Resposta ao risco

Após a etapa de avaliação de riscos, em que o risco é mensurado, o gestor deverá responder aos riscos. Esta fase é responsável por implementar ações orientadas pelo resultado da avaliação dos riscos. Para esta ferramenta, são utilizadas as quatro formas definidas no modelo de GRSIC da Fiocruz alinhadas aos parâmetros de análise de resposta a riscos proposta pelo MP, conforme apresentado na tabela 4.3.

Tabela 4.3: Tipos de respostas a riscos

Nível de Risco	**Parâmetro de análise para adoção da resposta**	**Tipo de resposta**
RMA	A alta administração decide não realizar a atividade, a fim de não envolver ou agir de forma a se retirar de uma situação de risco	**Evitar**
RA	Implementa ações para reduzir a probabilidade, as consequências negativas, ou ambas.	**Reduzir**
RM	Compartilhar com outra entidade o ônus associado a um risco	**Transferir**
RB	Assume as responsabilidade caso ocorra o risco identificado.	**Aceitar**
RMB		

Formas de resposta a riscos podem variar entre aceitar, reduzir, evitar ou compartilhar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas sejam efetivamente aplicadas [15]. É fundamental que o gestor considere o apetite ao risco quando propor as ações de controle em resposta aos riscos [10].

4.6 Atividades de controle

São medidas implementadas pelas organizações para modificar o risco. Essas medidas incluem qualquer processo, política, dispositivo, prática ou outras ações, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela administração possibilitando o alcance dos objetivos [3, 15, 32].

4.6.1 Riscos de controle

O TCU destaca que uma forma de avaliar o efeito dos controles internos na mitigação de riscos consiste em estimar a eficácia de cada controle e determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação do controle, conforme listado na tabela 4.4.

Tabela 4.4: Escala para avaliação de controles [15] (Adaptado)

Nível de Confiança		**Avaliação do desenho e implmentação dos controles (Atributos do controle)**	**Risco de Controle (RC)**	
Inexistente	NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mau implementados, isto é, não funcionais.	1,0	**Muito Alto**
Fraco	NC = 20% (0,2)	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8	**Alto**
Mediado	NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiência no desenho ou nas ferramentas utilizadas.	0,6	**Médio**
Satisfatório	NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4	**Baixo**
Forte	NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos do risco.	0,2	**Muito Baixo**

Após definido o NC, pode-se determinar o Risco de Controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC [15]. O Cálculo do RC é apresentado na equação Equação 4.1.

$$RC = 1 - NC \tag{4.1}$$

Conforme apresentado, o RC é inversamente proporcional ao NC, ou seja, quanto mais eficaz for o projeto e a implementação dos controles, ou seja, quanto maior for o NC, menor será o RC e vice-versa [15].

4.7 Fluxograma de atividades da ferramenta

A ferramenta segue basicamente o processo de avaliação de riscos da norma NBR ISO 31000:2009, conforme já apresentado na figura 2.7. Antes, porém, é fundamental que seja realizada uma análise de contexto, conforme preconiza a norma, para que o processo aplicado na ferramenta seja o mais próximo da realidade organizacional. A figura 4.4 apresenta o passo a passo do fluxo de atividades de cada etapa a ser executado na ferramenta.

1. **Definição dos pesos:** Nessa etapa é utilizada a análise multicritério para definição dos pesos relativos aos critérios de decisão para migração em nuvem e dos objetivos estratégicos. A primeira análise tem como objetivo ponderar os critérios do processo de migração para nuvem em um contexto organizacional. Os critérios foram definidos a partir do estudo elaborado na seção 4.3. O resultado dessa análise será utilizado na matriz de decisão após os cálculos de riscos do ambiente local e do ambiente em nuvem. A segunda análise irá ponderar os objetivos estratégicos identificados no estabelecimento do contexto. Os objetivos são a essência da definição do contexto, pois a gestão de riscos ocorre no contexto dos objetivos da organização [15]. O resultado dessa análise será utilizado para ponderar o cálculo de impacto do risco no objetivo institucional.

2. **Mapa de riscos ambiente local:** Nessa etapa é criado o mapa de riscos do ambiente local a partir das informações levantadas utilizando a técnica de brainstorning com a equipe técnica da unidade. As atividades de análise e avaliação são realizadas por meio da técnica de matriz de probabilidade e impacto, onde os julgamentos são realizados a partir do contexto da infraestrutura de TI local da unidade da Fiocruz.

3. **Mapa de riscos ambiente em nuvem:** Nessa etapa é criado o mapa de riscos do ambiente em nuvem a partir das informações levantadas nos resultados da pesquisa para identificação de riscos em ambientes em nuvem. As atividades de análise e avaliação são realizadas por meio da técnica de matriz de probabilidade e impacto, onde os julgamentos são realizados a partir do contexto da unidade da Fiocruz.

4. **Matriz de decisão:** Após todos os riscos serem identificados, analisados e avaliados nos mapas dos ambientes Local e em Nuvem, os resultados das duas etapas serão harmonizados e normalizados para serem ponderados na matriz de decisão com os resultados dos critérios de decisão em nuvem. Ao final será calculada uma decisão para qual ambiente a unidade deverá seguir.

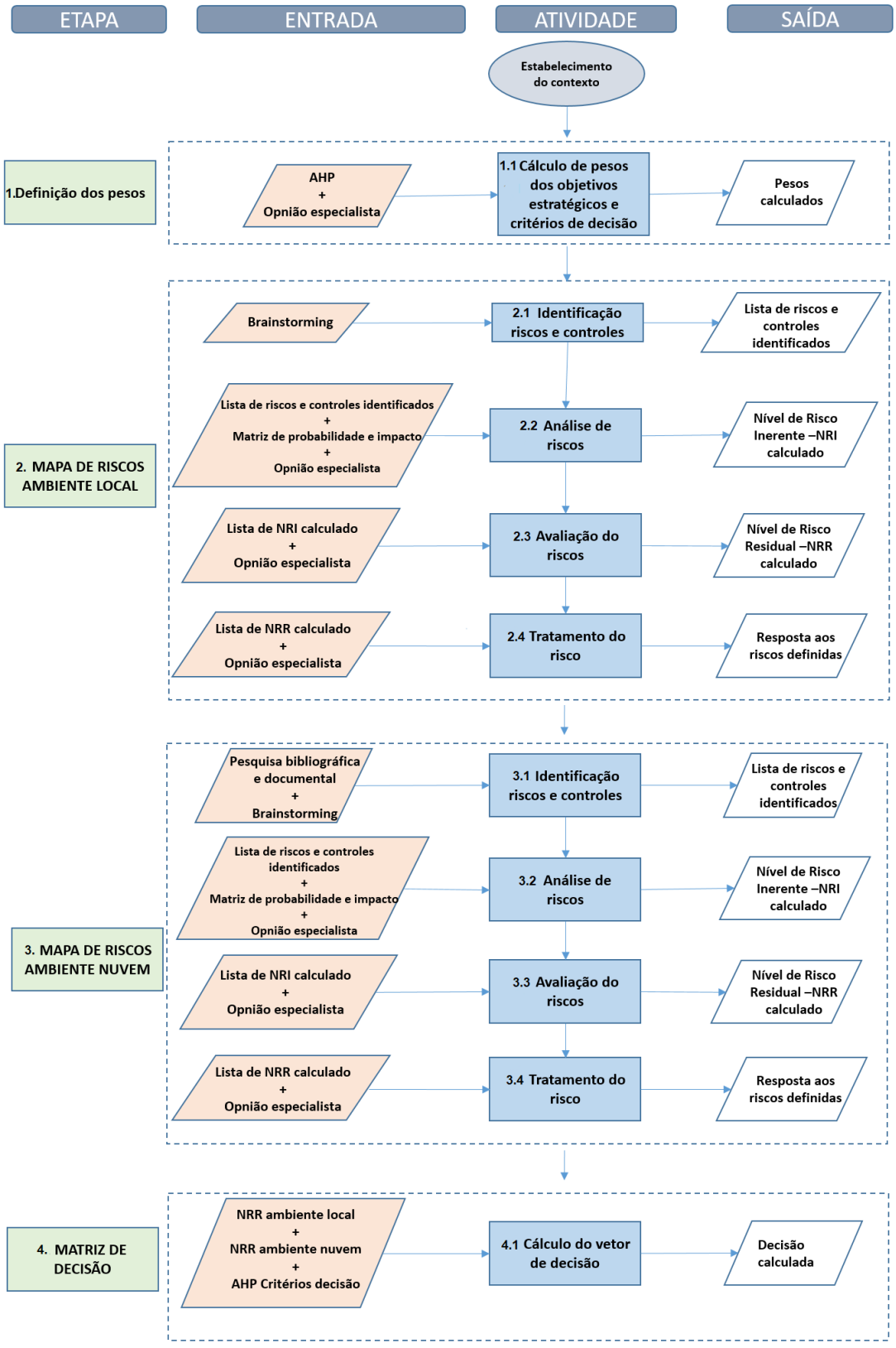

Figura 4.4: Fluxograma de atividades da ferramenta.

4.7.1 Definição de pesos para Critérios de Decisão e Objetivos Estratégicos

Como forma para reduzir a subjetividade no processo, o método AHP é utilizado para definição de pesos dos critérios de decisão e dos objetivos estratégicos. O objetivo global é produzir uma ordem de preferência entre as opções disponíveis [14]. Segundo Saaty [16], um dos usos de uma hierarquia é que nos permite enfocar o julgamento separadamente em cada uma das várias propriedades essenciais para tomar uma decisão acertada. Para tanto, a definição dos valores dos elementos relacionados aos critérios de decisão e aos objetivos estratégicos deverão seguir a escala fundamental definida por Saaty, conforme apresentado na tabela 4.5.

Tabela 4.5: Escala fundamental de Saaty [16]

Escala numérica	**Escala conceitual**	**Descrição**
1	**Igual**	Os dois elementos comparados contribuem igualmente para o objetivo.
3	**Moderada**	O elemento comparado é ligeiramente importante ao outro.
5	**Forte**	A experiência e o julgamento favorecem fortemente o elemento em relação ao outro.
7	**Muito fote**	O elemento comparado é muito mais forte em relação ao outro, e tal importância pode ser observada na prática.
9	**Absoluta**	O elemento comparado apresenta o mais alto nível de evidência possível a seu favor.
2,4,6,8	Valores intermediários entre dois julgamentos, utilizados quando o decisor sentir dificuldade ao escolher entre dois graus de importância adjacentes.	

Nas figuras 4.5 e 4.6 são apresentados as AHPs para os critérios de decisão e para os objetivos estratégicos, respectivamente, no qual serão calculados os pesos, seguindo os valores definidos na tabela 4.5 .

CRITÉRIOS DE DECISÃO								
	Ambiente organizacional	Gestão de serviços	Infraestrutura de TIC	Segurança da Informação	Custos	Governança	Auto Vetor	A.V.N
Ambiente organizacional	1	3	1/3	3	5	3	1,89	23%
Gestão de serviços	1/3	1	1/5	1	1	1	0,64	8%
Infraestrutura de TIC	3	5	1	5	7	5	3,71	45%
Segurança da Informação	1/3	1	1/5	1	1/3	1/5	0,42	5%
Custos	1/5	1	1/7	3	1	1/5	0,51	6%
Governança	1/3	1	1/5	5	5	1	1,09	13%
Σ	5,20	12,00	2,08	18,00	19,33	10,40	8,26	100%
λ-max	6,528164847							
IC	0,105632969							
RC	9%							

Figura 4.5: Critérios de decisão - Exemplo.

A partir do exemplo apresentado na figura 4.5, podemos observar que o critério de decisão com maior importância para o gestor, a partir da análise multicritério, é Infraestrutura de TIC com 45%.

OBJETIVOS ESTRATÉGICOS								
	Desafios SUS	C&T, Saúde e Sociedade	Complexo Produtivo de inovação em saúde	Saúde ambiental e promoção da saúde pública	Saúde, Estado e cooperação internacional	Inovação gestão	Auto Vetor	A.V.N
Desafio SUS	1	1	5	7	3	3	2,61	29%
C&T, Saúde e Sociedade	1	1	7	7	5	1	2,50	28%
Complexo produtivo de inovação em saúde	1/5	1/7	1	3	5	1/9	0,60	7%
Saúde ambiental e promoção da saúde pública	1/7	1/7	1/3	1	1	1/9	0,30	3%
Saúde, Estado e cooperação internacional	1/3	1/5	1/5	1	1	1/9	0,34	4%
Inovação gestão	1/3	1	9	9	9	1	2,50	28%
Σ	3,01	3,49	22,53	28,00	24,00	5,33	8,85	100%
λ-max	5,275998389							
IC	0,055199678							
RC	4%							

Figura 4.6: Objetivos estratégicos - Exemplo.

No exemplo apresentado na figura 4.6, o Desafio do SUS foi definido como o objetivo estratégico de maior importância, a partir da análise multicritério realizado pelo gestor.

No espaço em branco apresentado nas figuras, o gestor deverá realizar a comparação entre os pares obedecendo a escala de Saaty, tabela 4.5. De acordo com Saaty [16], o grau de consistência é satisfatório quando os valores da Razão de Consistência (RC) forem inferiores a 10%. Quando encontrados valores de RC superiores a 10% , o autor recomenda reavaliar os dados levantados, verificando se eles não se equivocaram durante o processo de levantamento.

4.7.2 Mapa de riscos: Identificação dos riscos

Essa área da ferramenta é destinada para listagem dos riscos identificados. O objetivo é produzir uma lista abrangente de riscos, incluindo causas, consequências e eventos de risco que possam ter algum impacto na consecução dos objetivos estratégicos identificados na etapa de estabelecimento do contexto [15].

Critério de decisão	Código	Eventos de risco	Causas	Efeitos / Consequências
Infraestrutura de TIC	RLIT02	Falha no fornecimento de energia elétrica na unidade	2. Falta de manutenção na rede elétrica da organização;	1. Queima de ativos de TIC (Servidores, swtiches, etc); 2. Indisponibilidade de serviços e sistemas estratégicos;
	RLIT03	Falha no fornecimento de energia elétrica pela distruidora	1. Problemas de fornecimento na região;	1. Queima de ativos de TIC (Servidores, swtiches, etc); 2. Indisponibilidade de serviços e sistemas estratégicos;
	RLIT04	Falha no fornecimento de ar refrigerado no ambiente de datacenter	1. Falha no equipamento; 2. Falta de manutenção;	1. Superaquecimento de ativos no datacenter (Servidores, swtches etc) ocasionando queimas desses equipamentos;
	RLIT05	Instalação física de datacenter em ambiente inadequado (próximo a lugares que deixem vulneráveis a eventos da natureza, por exemplo)	1. Falta de planejamento; 2. Falta de espaço físico;	1. O ambiente ser exposto a eventos da natureza (Alagamentos, incêndios etc)
	RLIT06	Falha nos ativos de TIC por sucateamento	1. Falta de orçamento e recursos para STI; 2. Fora da garantia;	1. Falhas nos equipamentos e indisponibilidade de sistemas e informações
	RLIT07	Problemas no armazenamento centralizado de dados (Storage)	1. Falta de orçamento e recursos para STI para suporte; 2. Não possuir uma solução de armazenamento centralizado de dados;	1. Armazenamento de dados relaizado de forma descentralizadas nos servidores; 2. Dados vulneráveis a falhas nos servidores;
	RLIT08	Problemas na solução de backup	1. Falta de orçamento e recursos para STI para suporte; 2. Não possuir uma solução de backup; 3. Não possuir poliicas de backup; 4. A solução não ser adequada;	1. Backups de dados não realizados ocasionando perdas de informações estratégicas

Figura 4.7: Identificação de riscos - Exemplo.

De acordo com a figura 4.7, é possível perceber que a ferramenta permite a inclusão das seguintes informações:

1. Código: Trata-se de um identificador para o risco;
2. Eventos de risco: Refere-se a ocorrência do incidente;
3. Causas: São listadas todas as causas dão origem ao risco;
4. Consequências: São listadas todas as consequências caso o evento ocorra;

4.7.3 Mapa de riscos: Análise dos riscos

Após os riscos serem identificados na seção 4.7.2, a fase seguinte é de análise dos riscos. Essa fase corresponde a definição do impacto do risco em cada objetivo estratégico e da probabilidade do risco ocorrer. O valor do impacto é calculado pela média ponderada dos pesos de cada objetivo estratégico, apresentados na seção 4.7.1 com o valor definido pelo gestor responsável pela análise. Dessa forma, o impacto é calculado de acordo com a

Equação 4.2, onde x é o valor a ser inserido pelo gestor e p o valor ponderado do objetivo estratégico.

$$Impacto = \frac{\sum_{i=1}^{n} x_i p_i}{\sum_{i=1}^{n} p_i} \tag{4.2}$$

Conforme demonstra na figura 4.8, após definido os impactos nos objetivos estratégicos e a probabilidade pelo gestor para cada risco, é calculado o Nível de Risco Inerente (NRI).

;COS										
		Risco inerente								
Critério de decisão	Código	Impacto						Probabilidade	NRI	Resposta ao risco
		Desafios SUS	C&T, Saúde e Sociedade	Complexo Produtivo de inovação em saúde	Saúde ambiental e promoção da saúde pública	Saúde, Estado e cooperação internacional	Inovação gestão			
		29%	28%	7%	3%	4%	28%			
Infraestrutura de TIC	RLIT01	3	2	2	2	2	2	5	11,47	Reduzir
	RLIT02	5	5	3	4	2	3	3	12,45	Reduzir
	RLIT03	5	3	5	4	4	4	4	16,32	Evitar
	RLIT04	4	5	3	3	3	3	5	19,30	Evitar
	RLIT05	3	4	4	3	3	4	3	10,90	Reduzir
	RLIT06	3	3	3	3	3	3	4	12,00	Reduzir
	RLIT07	4	5	5	5	5	5	3	14,12	Reduzir
	RLIT08	3	3	3	3	3	3	3	9,00	Transferir

Figura 4.8: Análise de riscos - Exemplo.

O NRI é calculado pelo produto do Impacto com a Probabilidade, conforme Equação Equação 4.3.

$$NRI = ImpactoxProbabilidade \tag{4.3}$$

O cálculo do NRI apresentado na figura 4.8 corresponde aos riscos identificados na figura 4.7.

4.7.4 Mapa de riscos: Avaliação dos riscos

Nessa fase avalia a efetividade das atividades de controles, definidas na fase de identificação de riscos e controle, no NRI, como apresentado na figura 4.9. Essa etapa corresponde ao cálculo do Nível de Risco Residual (NRR) com o RC, de acordo com a escala definida na tabela 4.4.

		AVALIAÇÃO DOS RISCOS					
		Atividades de controle					
Critério de decisão	Código	Descrição	Responsabilidade	Nível de Confiança (NC)	Risco de controle	NRR	NRC
Infraestrutura de TIC	RLIT01	1. Apoio da alta administração; 2. Orientação das áreas para evitarem a compra sem aval do setor de TI;	Direção STI Áreas da Fiocruz Brasília	Fraco	80%	9,18	7,49
	RLIT02	1. Redundância no quadro de energia	SINFRA	Satisfatório	40%	4,98	
	RLIT03	1. Nobreaks 2. Gerador de energia	SINFRA	Satisfatório	40%	6,53	
	RLIT04	1. Equipe especializada no suporte de equipamentos de refrigeração de ar	SINFRA	Mediano	60%	11,58	
	RLIT05	1. Extintor de incêndio; 2. Bombas centrifuga (água)	SINFRA	Fraco	80%	8,72	
	RLIT06	1. Redundância lógica em outros locais (nuvem Fiocruz ou outros servidores)	STI	Mediano	60%	7,20	
	RLIT07	1. Redundância lógica em outros locais (nuvem Fiocruz ou outros servidores)	STI	Mediano	60%	8,47	
	RLIT08	1. Redundância lógica em outros locais (nuvem Fiocruz ou outros servidores)	STI	Mediano	60%	5,40	

Figura 4.9: Atividades de controle - Exemplo.

Para isso, deduz-se do NRI o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC [15], utilizando a seguinte Equação 4.4.

$$NRR = NRIxRC \tag{4.4}$$

O NRC refere-se ao Nível de Risco do Critério, que é calculado a partir da média geométrica do NRR de todos os riscos de cada critério de decisão. O NRC é o resultado que será utilizado na matriz de decisão para cada critério avaliado nos mapas de riscos (ambiente local e em nuvem).

4.7.5 Matriz de decisão

Nessa fase é calculado o vetor de decisão após o cálculo dos NRRs de cada critério de decisão para os ambiente local e em nuvem. Para tanto, a primeira parte nesse processo é calcular a média geométrica para cada critério de decisão de ambos os ambientes. A fase seguinte realiza a harmonização e a normalização dos NRRs calculados, conforme figura 4.10.

CRITÉRIOS		AMBIENTE LOCAL	NUVEM FIOCRUZ	Total
Ambiente organizacional	NRR	7,80	5,70	13,50
	Harmonizar	1,73	2,37	4,10
	Normalizar	42%	58%	100%
Gestão de serviços	NRR	4,70	3,70	8,40
	Harmonizar	1,79	2,27	4,06
	Normalizar	44%	56%	100%
Infraestrutura de TIC	NRR	7,49	6,69	14,18
	Harmonizar	1,89	2,12	4,01
	Normalizar	47%	53%	100%
Segurança da Informação	NRR	8,32	7,45	15,77
	Harmonizar	1,90	2,12	4,01
	Normalizar	47%	53%	100%
Financeiro / orçamentário	NRR	11,80	10,70	22,50
	Harmonizar	1,91	2,10	4,01
	Normalizar	48%	52%	100%
Governança	NRR	7,12	7,50	14,62
	Harmonizar	2,05	1,95	4,00
	Normalizar	51%	49%	100%

Figura 4.10: NRC Normalizados - Exemplo.

Após normalização dos NRRs, o próximo passo é calcular a decisão a partir dos pesos dos critérios de decisão para migração em nuvem, definidos na etapa inicial da ferramenta por meio da técnica AHP. Ao final, a ferramenta apresenta a melhor decisão com base nos riscos definidos para o ambiente local e em nuvem, conforme figura 4.11.

	Ambiente organizacional	Gestão de serviços	Infraestrutura de TIC	Segurança da Informação	Financeiro / Orçamentário	Governança	
Vetor dos critérios	23%	8%	45%	5%	6%	13%	
ALTERNATIVAS							Vetor de decisão
Ambiente local	42%	44%	47%	47%	48%	51%	46%
Nuvem Fiocruz	58%	56%	53%	53%	52%	49%	54%

Figura 4.11: Resultado matriz de decisão - Exemplo.

Capítulo 5

Estabelecimento do contexto

5.1 Contexto externo

O estabelecimento do contexto envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos [15]

5.1.1 Fundação Oswaldo Cruz-Fiocruz

Promover a saúde e o desenvolvimento social, gerar e difundir conhecimento científico e tecnológico, ser um agente da cidadania [63]. Estes são os conceitos que pautam a atuação da Fundação Oswaldo Cruz (Fiocruz), vinculada ao Ministério da Saúde (MS). A Fiocruz é a principal instituição não-universitária de formação e qualificação de recursos humanos para o SUS e para a área de ciência e tecnologia no Brasil.

Na fundação são executados mais de mil projetos de pesquisa e desenvolvimento tecnológico, que produzem conhecimentos para controle de doenças como Aids, malária, chagas etc. Além do mais, trabalha na geração do conhecimento atuando no desenvolvimento de produtos e processos com aplicação potencial como: novas vacinas, medicamentos à base de plantas etc [63]. Presente em dez estados brasileiros, e contando com cerca de 12.800 colaboradores, a Fiocruz tem colocado seu conhecimento a serviço da população brasileira, buscando, através da inovação tecnológica e social, melhorar as condições de vida e saúde de todos [21].

No planejamento estratégico da Fiocruz para 2022, os objetivos estratégicos são apresentados por meio de cinco eixos finalísticos da instituição, além dos objetivos corporativos para a gestão (Inovação da Gestão) que dá suporte aos demais eixos. Para cada eixo foi

desenhado um mapa, que sintetiza a visão, bem como os resultados para a sociedade e os processos internos que o compõem o respectivo eixo[64], conforme Figura 5.1:

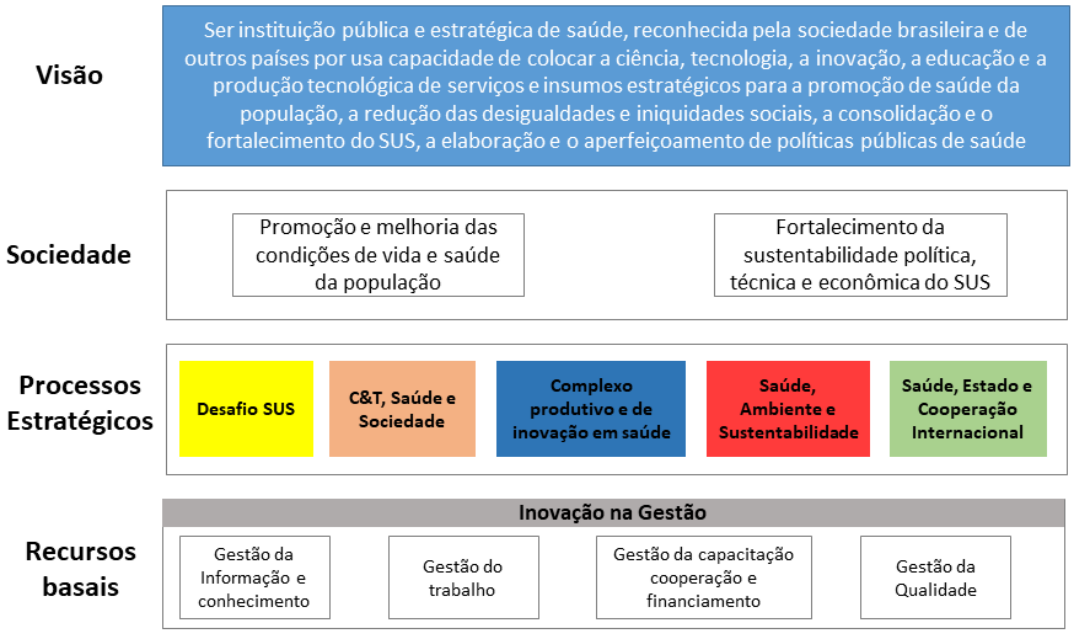

Figura 5.1: Mapa estratégico Fiocruz 2022 [11].

A vinculação entre o Plano Estratégico da Instituição e seus planos anuais se dá através da articulação entre as ações a serem desenvolvidas em cada um dos macroprocessos finalísticos da Fiocruz e os respectivos eixos que compõem o seu Plano Estratégico, como apresentado a seguir [11]:

- **Eixo Atenção, Promoção, Vigilâncias, Geração de Conhecimentos e Formação para o SUS**: Ser instituição de referência na promoção, vigilâncias, informação e comunicação em saúde, formação de quadros profissionais para o SUS, geração de conhecimentos que contribuam para a formulação de políticas públicas de saúde e modelos de atenção integral, em especial nos campos da saúde da mulher, da criança e do adolescente, da infectologia e da atenção primária em saúde.
- **Eixo Ciência, Tecnologia, Saúde e Sociedade**: Ser instituição de referência na geração, difusão e compartilhamento do conhecimento em CT&I e saúde, na pesquisa, no desenvolvimento, na inovação, na educação, na formação de profissionais, na informação e comunicação, orientada à cidadania, às necessidades sanitárias e ao perfil epidemiológico da população brasileira e ao fortalecimento do SUS.
- **Eixo Inovação e Complexo Produtivo em Saúde**: Ser instituição pública de referência em inovação, desenvolvimento e produção de insumos para a saúde

orientada às necessidades sanitárias e perfil epidemiológico da população brasileira, prioritariamente, e ao fortalecimento do SUS.

- **Eixo Saúde e Sustentabilidade Socioambiental**:Ser instituição de referência no desenvolvimento científico-tecnológico e nos processos formativos, inovando na compreensão da saúde e de seus determinantes e contribuindo para políticas públicas intersetoriais, na perspectiva da sustentabilidade socioambiental.
- **Eixo Saúde, Estado e Cooperação Internacional**:Ser instituição de excelência em diplomacia da saúde, articulando os demais eixos temáticos na captação e oferta de cooperação estratégica e estruturante para o fortalecimento de Sistemas de Saúde e de CT&I em Saúde.

A importância da TI se destaca em todos os eixos estratégicos da instituição. O eixo **Ciência, Tecnologia, Saúde e Sociedade**, por exemplo, aborda a consolidação das redes de pesquisa e plataformas tecnológicas em áreas estratégicas para o SUS e para C&T, em alinhamento com os programas de inovação. O eixo **Complexo Produtivo e de Inovação em Saúde** busca, entre outros, contribuir para o desenvolvimento de uma base produtiva nacional na área de TIC (Tecnologias da Informação e Comunicação) aplicadas às necessidades do SUS. Já o eixo **Inovação na Gestão** apresenta como objetivos as melhorias em infraestrutura e logística em TI, informação e comunicação e também a implantação de um sistema integrado de gestão na Fiocruz, a fim de gerar melhoria na qualidade (tempo, flexibilidade, velocidade, integração e transparência) da tomada de decisão [65].

O eixo **Inovação na Gestão** aborda a computação em nuvem como área portadora de futuro na administração publica [64] e abarcou a Nuvem Fiocruz como um projeto estratégico de inovação para instituição. Conforme destacado, o eixo **Inovação na Gestão** dá suporte aos processos críticos dos demais eixos finalísticos adotados pela Fiocruz. Dessa forma, podemos observar que a nuvem Fiocruz tem impacto direto nos objetivos estratégicos que envolvam processamento de dados e TIC.

Porém, a complexidade da Fiocruz se expressa no desenvolvimento de atividades de diferentes naturezas, na existência de diversas unidades, na dispersão geográfica e no número expressivo da força de trabalho, o que torna essencial um planejamento integrado e a coordenação das ações de TI [66].

5.1.2 Ambiente social

Os serviços e produtos da Fiocruz atingem potencialmente a sociedade em geral, representada principalmente por meio dos gestores e profissionais do SUS e de países com os quais

formaliza acordos de cooperação técnica, assim como pela comunidade científica nacional e internacional no campo da C&T em Saúde e dos usuários diretos dos serviços de ensino e de atenção à saúde.

As iniciativas desenvolvidas pela Fiocruz se articulam, especialmente, com organizações de base sociocomunitárias, grupos e movimentos sociais em territórios em situação de vulnerabilidade civil, social e ambiental, visando a proposição, a participação e o controle de políticas públicas promotoras de saúde [67].

Além do mais, os valores da Fiocruz, pautados pela relevância da atuação da organização para a sociedade, são os alicerces de atitudes, comportamentos e características que configuram a doutrina essencial da organização. São valores da Fundação [63]:

1. Compromisso institucional com o caráter público e estatal.
2. Ciência e inovação como base do desenvolvimento socioeconômico e da promoção da saúde.
3. Ética e transparência.
4. Cooperação e integração.
5. Diversidade étnica, de gênero e sociocultural.
6. Valorização dos trabalhadores, alunos e colaboradores.
7. Qualidade e excelência.
8. Redução das iniquidades.
9. Compromisso com as principais metas de transformação social do Estado brasileiro.
10. Compromisso socioambiental.
11. Democracia participativa.
12. Democratização do conhecimento.
13. Educação como processo emancipatório.

5.1.3 Ambiente legal

De acordo com o Decreto 8932/2016, a Fundação Oswaldo Cruz - FIOCRUZ, criada pelo Decreto no 66.624, de 22 de maio de 1970, dotada de personalidade jurídica de direito público, vinculada ao Ministério da Saúde, com sede na cidade do Rio de Janeiro, tem por finalidade desenvolver atividades nos campos da saúde, da educação e do desenvolvimento científico e tecnológico, devendo, dentre outros:

- participar da formulação e da execução da Política Nacional de Saúde, e na área relacionada à saúde, da Política Nacional de Ciência e Tecnologia e da Política Nacional de Educação;
- promover e realizar pesquisas básicas e aplicadas para a consecução das finalidades a que se refere o caput e propor critérios e mecanismos para o desenvolvimento das atividades de pesquisa e tecnologia para a saúde;
- formar e capacitar recursos humanos para as áreas de saúde, ciência e tecnologia;
- desenvolver tecnologias de produção, produtos e processos e outras tecnologias de interesse para a saúde;
- fabricar produtos biológicos, diagnósticos, profiláticos, prognósticos, medicamentos, fármacos e outros produtos de interesse para a saúde;
- desenvolver atividades assistenciais de referência, em apoio ao Sistema Único de Saúde - SUS, ao desenvolvimento científico e tecnológico, e aos projetos de pesquisa;
- desenvolver atividades de produção, captação e armazenamento, análise e difusão da informação para as áreas de saúde, ciência e tecnologia;
- desenvolver atividades de prestação de serviços e de cooperação técnica nos campos da saúde, da ciência e da tecnologia;
- promover atividades de pesquisa, ensino, desenvolvimento tecnológico e cooperação técnica voltadas para a conservação do meio ambiente e da biodiversidade.

No que se refere a contratação de serviços de tecnologia da informação, há uma relação de normativos que orientam órgãos e entidades da APF, como a Fiocruz. Diante disso, a tabela 5.1 apresenta uma relação desses normativos.

Tabela 5.1: Relação de normativos

Normativo	Descrição
LEI Nº 8.666/1993	Institui normas para licitações e contratos da Administração Pública
INº 04/2014	Dispõe sobre o processo de contratação de TI pelos órgãos do SISP
LEI Nº 12.527/2011	Lei de acesso a informação
DECRETO 8.135/2013 e Portaria Interministerial 141/2014	Dispõe sobre a comunicação de dados na APF
ACÓRDÃO 1.739/2015	Orienta os órgãos da APF sobre riscos na contratação de serviços em nuvem
PORTARIA MP/STI nº 20/2016	Dispõe sobre orientações para contratação de soluções de TI no âmbito da APF
NORMA COMPLEMENTAR nº 14/IN01/DSIC/GSIPR 2018	Estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da APF

5.1.4 Ambiente político

Atualmente a Fiocruz é composta por diversas unidades internas, com papéis específicos e experiências consolidadas em seus campos. Ao todo, são 16 unidades técnico-científicas, voltadas para ensino, pesquisa, inovação, assistência, desenvolvimento tecnológico e extensão no âmbito da saúde. Deste conjunto, 11 estão situadas no Rio de Janeiro e cinco em outras unidades da federação (Amazonas, Bahia, Minas Gerais, Paraná e Pernambuco). Também há quatro escritórios em outros estados (Ceará, Mato Grosso do Sul, Piauí e Rondônia). Ademais, a Fiocruz possui sua representação em Brasília (GEREB), como órgão vinculado à Presidência. Todas essas unidades ou órgãos já atuam no ensino e pesquisa [67].

Por ser uma instituição federal com atuação em todo o país e com profundas ligações com a saúde pública em qualquer território, a Fiocruz desenvolve diversas parcerias e cooperações com órgãos Federais, instituições não governamentais e organismos internacionais, tais como: Ministério da Educação (MEC), Ministério da Cultura (MinC) e Ministério do Desenvolvimento Social (MDS), Organização Mundial da Saúde (OMS), Conselho Nacional de Secretários de Saúde(CONASS) etc.

Dessa forma, qualquer mudança de governo, ministros, secretários executivos etc possui grande impacto em projetos, parcerias e cooperações com outros órgãos e entidades.

5.1.5 Ambiente Financeiro / Orçamentário

As necessidades identificadas, apoiadas não apenas nas discussões internas, mas também em estudos orçamentários que avaliam a evolução de gastos, são consolidadas pela COGEPLAN e submetidas ao Ministério da Saúde. Para inclusão na Lei Orçamentária Anual, principal fonte de financiamento da Fiocruz [11].

Após aprovação da LOA, outras rodadas de negociações internas são realizadas, de forma a garantir os recursos necessários, após possíveis cortes ou contingenciamentos, para os projetos estratégicos e para as metas operacionais das diversas Unidades, O resultado destas negociações, conduzidas pela VPGDI e pela Diplan, são apresentados e aprovados pelo CD da Fiocruz [11].

As principais fontes de recursos financeiros para a composição orçamentária são os recursos do Tesouro (LOA) e recursos financeiros de origem nacional e internacional, provenientes de acordos de cooperação em seus variados instrumentos. A composição do orçamento de cada unidade da Fiocruz, que deve assegurar as metas pactuadas anualmente, faz-se pela dotação orçamentária com base tanto na LOA quanto nos projetos e operações propostos e desenvolvidos. Agregam-se a estes valores, os recursos externos, captados e desenvolvidos por cada unidade [11].

5.1.6 Coordenação Geral de Tecnologia da Informação - COGETIC

Coordenação Geral de Tecnologia da Informação - COGETIC é responsável por toda a gestão e operacionalização das tecnologias da informação no âmbito da Presidência da Fiocruz e de suas Unidades de apoio (Audin, Dirac, Dirad, Direb, Direh, Diplan, Ouvidoria). Ainda, coordena as atividades inerentes à governança e gestão da tecnologia de informação, construindo arcabouço de conhecimentos, técnicas e padrões que propiciem a segurança das informações e comunicações na Fiocruz, promovendo a construção de políticas institucionais de maneira inclusiva e participativa[67].

5.1.7 Comitê Gestor de Segurança da Informação e Comunicações – CSIC

Instituído pela Portaria nº 143/2011-PR de 28 de abril de 2011, é um órgão de assessoramento ao Serviço de Segurança da Informação e Comunicações da Coordenação de Gestão de Tecnologia da Informação da Fiocruzs. Dessa forma, faz-se necessário observar as políticas e normas estabelecidas pelo CSIC.

5.1.8 PETI e PDTI

Com objetivo de aprimorar a governança de Tecnologia da Informação, a Fiocruz desenvolve anualmente o Planejamento Estratégico de Tecnologia da Informação (PETI) onde são estabelecidas as diretrizes e as metas que orientam a construção do Plano Diretor de Tecnologia da Informação (PDTI) [66]. O PDTI tem como objetivo apresentar os projetos e atividades de TI necessários para atingir as metas definidas no PETI e como consequência auxiliar a Fiocruz no alcance de seus objetivos institucionais [68].

O investimento total do período de 2014 a 2017 foi R$ 189,37 milhões em aquisições, serviços e infraestrutura de TI, considerando o empenho realizado nas naturezas de despesas específicas de tecnologia da informação, conforme o Sistema Integrado de Administração Financeira – SIAFI[69] Tabela 5.2.

Tabela 5.2: Valor executado em TI no período de 2014 a 2017 .

Período	**Investimento em TI**
2014	R$ 41.821.576
2015	R$ 51.786.478
2016	R$ 43.587.202
2017	R$ 52.176.383
Total	**R$ 189.371.638**

De acordo com o PDTI 2015-2016 da Fiocruz [68], dos 172,4 milhões programados em TI, as despesas de capital da ordem de 97,7 milhões representam 57% do orçamento total do PDTI 2015-2016, enquanto que o investimento representa 43%.Um dos principais investimentos da Fiocruz para 2015, e o principal que impacta neste PDTI, é o projeto coordenado pela CGTI/Presidência, que é Implantação do Data Center, no Campus Manguinhos/RJ. Este projeto abrange todas as unidades da Fiocruz do campus,que, ao longo do tempo, migrarão seus serviços para o Data Center, trazendo, principalmente, impacto no custeio da Fiocruz e eficiência e qualidade dos serviços em TI.

Segundo o PDTI 2016-2017 da Fiocruz [70], dos 235 milhões programados em TI, as despesas de custeio representam 54% da programação, diferente do PDTI 2015-2016, onde o capital representava a maior parte dos gastos. Este fato ocorreu pois a Fiocruz investiu em um dos principais projetos da área de TI em 2015, o projeto coordenado pela CGTI/Presidência, que foi Implantação da Nuvem Fiocruz.

Diante disso, o relatório de Gestão de 2015 enfatizou que "o portfólio de projeto de maior destaque na área de TI foi o Nuvem Fiocruz, composto de dois projetos Sala Cofre e Datacenter. O objetivo do projeto Sala Cofre é construir um ambiente físico certificado, com proteção contra diversos riscos físicos, como fogo, água, gases corrosivos e explosões e etc, com infraestrutura redundante e com controle de acesso biométrico [65].

5.1.9 Centro de Dados para Computação em Nuvem - Nuvem Fiocruz

Estabelecido sobre a plataforma RedHat OpenStack, o Centro de Dados para Computação em Nuvem tem como finalidade oferecer inicialmente Infraestrutura como Serviço (IaaS)– às Unidades Correlatas da Fiocruz, podendo evoluir para Plataforma como Serviço (PaaS) ou até Software como Serviço (SaaS), se houver necessidade, e backup. A COGETIC é responsável em prover e manter o ambiente computacional, e os beneficiados ficarão responsáveis pelo controle e administração dos recursos que lhes serão disponibilizados. Cada unidade da instituição possui um projeto com recursos e administração totalmente independentes. Entretanto, o provisionamento de mais recursos está condicionado a justificativa junto a COGETIC.

A Nuvem Fiocruz é composta de uma sala cofre e um Data Center, localizados no Campus Manguinhos/RJ. Enquanto a sala cofre fornece um ambiente seguro para a infraestrutura de TI, conforme apresentado na figura 5.2, o Data Center fornece um ambiente computacional adequado para fornecer recursos, como, processamento e armazenamento que possibilite maior confiabilidade e disponibilidade aos serviços alocados neste ambiente. Já em funcionamento, o Data Center abrange todas as unidades da Fiocruz do campus, que, ao longo do tempo, migrarão seus serviços para o Data Center, trazendo, principalmente, impacto no custeio da Fiocruz e eficiência e qualidade dos serviços em TI [70].

Figura 5.2: Sala cofre certificada NBR 15247 [12].

Nota-se, portanto, que a Fiocruz vem apostando alto em um ambiente tecnológico centralizado de Nuvem Privada para contingenciar recursos de infraestrutura, processamento de dados, soluções de software e entre outros, com o propósito de implementar um serviço

do tipo IaaS (infraestrutura) para as unidades da insituição. Na figura 5.3 é possível ver os cenários de crescimento do datacenter da Fiocruz entre 2014 a 2017.

	Atual	Primeira Fase – Julho 2015	Segunda Fase - 2016	Terceira Fase - 2017
Servidores Blade	9	12	29	34
Processamento	1 ?	9,6 Teraflop/s	14,4 Teraflop/s	19,2 Teraflop/s
Memória	256 GB	3 TB	8 TB	10 TB
Storage	35 TB	310 TB	780 TB	1.3 PB
Velocidade de conexão interna	1 Gbps	10 Gbps	40 Gbps	40 Gbps

Figura 5.3: Cenários de crescimento do datacenter Fiocruz [12].

Entretanto, devido a forte crise econômica e política entre o período de 2016 a 2017, somente metade desse cenário previsto foi cumprido.

Política de uso

A Política de Uso do Centro de Dados para Computação em Nuvem tem por objetivo estabelecer parâmetros de gestão dos serviços da infraestrutura tecnológica Fiocruz, de modo a promover a qualidade e estabilidade [71]. Esse documento destaca, entre outras coisas, padrões de gestão de serviços como: armazenamento, backup, responsabilidades e penalidades.

Plataforma para gerenciamentos dos serviços

Todo gerenciamento é realizado por meio de uma plataforma online no qual cada unidade regional dispõe de um ambiente para gerenciar seus serviços. Conforme é apresentado na figura 5.4, a plataforma permite gerenciar as instâncias (servidores como serviços), volumes de dados, regras de acesso e segurança, além de configurações básicas de rede.

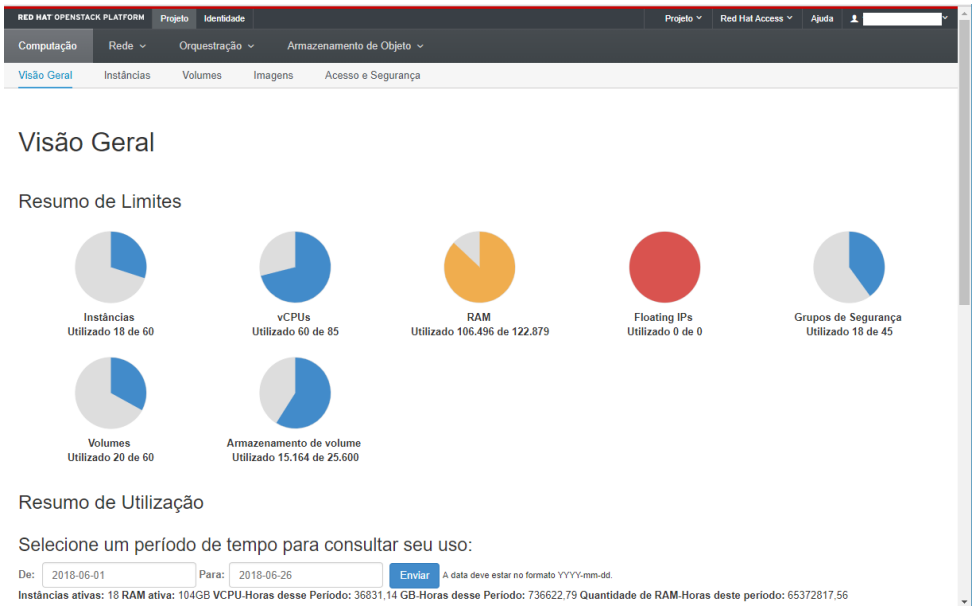

Figura 5.4: Plataforma de gerenciamento de serviços da Nuvem Fiocruz..

Atualmente a plataforma possui modelos de instâncias pré-configuradas nos sistemas operacionais Linux Debian, Ubuntu, Fedora, Red Hat Enterprise e Windows Server. Entretanto, é possível realizar a criação de ambientes pré-configurados e utilizá-los como modelos para outras instâncias de forma rápida e elástica. Além do mais, a plataforma permite que sejam criadas regras de acesso a instâncias, somente em ambientes linux, a partir de chaves públicas configuradas, garantindo mais segurança no processo de autenticação com as instâncias.

Catálogo de Serviços de TI

O apoio técnico prestado pela COGETIC às unidades regionais é realizado por meio do sistema de Requisições e Serviços Institucionais (RSI). Atualmente a COGETIC possui um catálogo de serviços de TI agrupados em 5 grandes categorias: Sistemas, Segurança da Informação, Inovação em TI, Suporte ao usuário e infraestrutura em TI [17]. Não há uma categoria específica para computação em nuvem. Na tabela 5.3 é listado alguns serviços do catálogo que possuem relação direta com a plataforma de nuvem.

Tabela 5.3: Catálogo de serviços de TI Fiocruz [17]

Categoria	Serviço	Pacote	Complexidade
Segurança da informação	Acompanhamento da execução de serviços	Sala Cofre	Médio
Segurança da informação	Agendamento devisita	Sala cofre	Médio
Segurança da informação	Comunicação de acesso emergencial	Sala cofre	Médio
Segurança da informação	Comunicação de acesso programado	Sala cofre	Médio
Segurança da informação	Emissão de credencial de acesso	Sala cofre	Médio
Infraestrutura	Troubleshooting	Openstack -Nuvem Fiocruz	Alto
Infraestrutura	Ajuda técnica	Openstack -Nuvem Fiocruz	Alto
Infraestrutura	Adicionar um host	Suporte à Openstack	Alto
Infraestrutura	Remover um host	Suporte à Openstack	Alto
Infraestrutura	Configurar rede	Suporte à Openstack	Médio
Infraesturuta	Criar instância	Suporte à Openstack	Médio

Apesar do catálogo apresentar poucos serviços específicos para plataforma em nuvem, ainda assim o catálogo relaciona centenas de outros que possuem relação indireta, tais como: serviços de virtualização, regras de Firewall, monitoramento e análise de logs, configuração de volumes de dados etc.

5.2 Contexto interno

5.2.1 Gerência Regional de Brasília - GEREB

No âmbito regional, as ações e projetos realizados pela Gerência Regional de Brasília - GEREB, antiga Diretoria Regional de Brasília-DIREB, vêm sendo orientados, cada vez mais, para assumir um caráter estratégico para as políticas públicas. Com base nisso, a unidade regional de Brasília definiu os três eixos internos de desenvolvimento institucional, conforme apresentado na figura 5.5.

Figura 5.5: Eixos estratégicos Fiocruz Brasília [13].

- O **eixo Integração** corresponde ao apoio e fortalecimento das ações cooperativas que são realizadas entre áreas e unidades da Fiocruz, bem como outras instituições que potencializem a continuidade dessas ações, além da ativação de redes de políticas públicas e saúde.
- O **eixo Inteligência** corresponde a um processo de produção de conhecimento científico de recomendações, análises e avaliações. Um processo de pesquisa destinado a orientar a tomada de decisão sobre temas relacionados às ações políticas públicas de saúde.
- O **eixo Formação** é conduzido pela Escola Fiocruz de Governo (EGS) juntamente com a Universidade Aberta do SUS (UNA-SUS), e busca atender a demanda por capacitação e aperfeiçoamento dos trabalhadores ligados à saúde, majoritariamente no âmbito federal.

5.2.2 Alinhamento estratégico

Conforme já apresentado, os processos estratégicos destacados no mapa estratégico Fiocruz 2022, figura 5.1, são a base para o plano estratégico global da Fiocruz. Diante disso, os três eixos estratégicos da unidade regional de Brasília, definidos na Oficina de Planejamento 2016, estão diretamente alinhados aos processos estratégicos Desafio do SUS; Ciência e Tecnologia, Saúde e Sociedade e inovação na gestão. No processo estratégico Desafio do SUS com projetos de apoio à formação de recursos humanos para

o SUS. No processo Ciência e tecnologia, Saúde e Sociedade por meio da presença da Fiocruz no território nacional, do fortalecimento da Escola Fiocruz de Governo (EFG) e do fortalecimento de pesquisas estratégicas do SUS. Já na estratégia Inovação em Gestão, com projetos de apoio à gestão do conhecimento e do apoio à integração estratégica, destacando-se o trabalho com redes de cooperação [13]. Essa relação está demonstrada na tabela 5.4.

Tabela 5.4: Alinhamento estratégico GEREB com objetivos estratégicos da Fiocruz

Objetivos estratégicos Fiocruz	**Eixos estratégicos GEREB**	**Objetivos estratégicos**	**Objetivos do STI**
Desafio SUS **C&T, Saúde e Sociedade** **Inovação na Gestão**	**Integração**	Integração entre Ensino, Pesquisa e Aplicação	Auxiliar fornecimento de infraestrutura de TIC para dar suporte aos projetos
		Papel da Fiocruz Brasília no FUR	Desenvolver plataforma de gestão corporativa de projetos de cooperação técnica para dar apoio a integração do FUR
	Formação	EFG e UNA-SUS alinhadas	Auxiliar fornecimento de infraestrutura de TIC para dar suporte aos projetos
		EFG introduzida na rede UNA-SUS	Auxiliar fornecimento de infraestrutura de TIC para dar suporte aos projetos
	Inteligência	Processos de gestão melhorados	Desenvolver plataforma de gestão corporativa de projetos de cooperação técnica
		Estratégias para otimização dos processos para aumentar a eficiência/efetividade institucional implantadas	Implementar a governança de TI alinhada aos processos institucionais
		STI legitimado como centro estratégico da Fiocruz Brasília	Apoiar a instituição no processo de adequação do STI como área estratégica

Na tabela 5.4 apresenta os objetivos estratégicos de cada eixo, discutidos na Oficina de Planejamento 2016, que possuem alinhamento com as atividade de TI do Serviço de Tecnologia da Informação-STI [13].

5.2.3 Serviço de Tecnologia da Informação - STI

O Serviço de Tecnologia da Informação - STI é o setor responsável em prover soluções tecnologia da informação, infraestrutura de redes, segurança da informação e suporte técnico da GEREB.

5.2.4 Orçamento em TI

A programação orçamentária prevista para o período de 2016 a 2017 da GEREB foi de R$ 8.251.240,34 [69]. Desse orçamento, mais de 90% envolve direta ou indiretamente infraestrutura de TI. Esse orçamento engloba, entre outras coisas, a reestruturação do datacenter da unidade, licenças de software, contratação de mão de obra especializada e reestruturação de todos os ativos de rede de dados.

Entretanto, os serviços oferecidos pelo STI são duramente comprometidos por falta da liberação do orçamento. Esse tem sido um dos principais pontos que influenciam na qualidade dos serviços de infraestrutura de TI na unidade.

5.2.5 Visão estratégica do STI

Enquanto diversos órgãos e unidades públicas destacam a área de Tecnologia da Informação como estratégica, a exemplo da Coordenação-Geral de Tecnologia da Informação (COGETIC) que se equiparou a outras diretorias, na GEREB a área ainda é vista como suporte técnico básico. Porém, em grande parte trata-se de um problema pela baixa capacidade do STI em atender as demandas e aos projetos com qualidade. Isso desencadeia um processo de descentralização da TI, pois os projetos, por possuírem recursos próprios, contratam profissionais para atender as suas demandas que envolvam TI.

5.2.6 Infraestrutura tecnológica

Toda infraestrutura de redes de dados e telecomunicações é precária. Além do mais, o datacenter da GEREB é incompatível para servir com essa finalidade. Todos os servidores estão fora de garantia e não possuem suporte especializado para dar apoio necessário. Além do mais, a diversidade de projetos em que o STI não faz parte contribui para um ambiente heterogêneo e de difícil manutenção.

Rede Nacional de Ensino e Pesquisa – RNP

A Rede Nacional de Ensino e Pesquisa (RNP) provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa. Está presente em todas as unidades da federação por meio de 27 Pontos de Presença, que formam a espinha dorsal da rede acadêmica nacional, a rede Ipê. A RNP é a responsável por prover, entre outros:

- O link de internet de 1Gbps com suporte técnico;
- Comunidade Acadêmica Federada – Cafe - um serviço de gestão de identidade que reúne instituições de ensino e pesquisa brasileiras através da integração de suas bases de dados. Isso significa que, por meio de uma conta única (modelo single sign-on), o usuário pode acessar, de onde estiver, os serviços de sua própria instituição e os oferecidos pelas outras organizações que participam da federação;
- Monitoramento a incidentes de segurança a rede e aos serviços da GEREB;
- Emissão de certificados digitais para servidor por meio da ICPEdu;
- Serviço para conferência web;

5.2.7 Capacidades técnicas

O STI se destaca pela capacidade técnica na prestação de serviço e apoio tecnológico a toda GEREB.

- Composta de três servidores concursados especialistas em TI, dois colaboradores de suporte técnico e dois colaboradores de infraestrutura de redes e serviços de TI;
- Equipe técnica qualificada;
- Boa relação com as demais áreas da Fiocruz em geral;

5.3 Matriz SWOT

A análise de SWOT tem a finalidade de avaliar os ambientes internos e externos, para identificar os pontos fortes e fracos de uma organização, formulando estratégias de negócio para a empresa com a finalidade de otimizar seu desempenho. Dessa forma, com base na contextualização foi possível estabelecer quais as Fraquezas, Oportunidades, Forças e Ameaças no processo, conforme apresentado na figura 5.5.

Tabela 5.5: Matriz SWOT

	Oportunidades	**Ameaças**
Ambiente Externo	Ambientes social e legal Normas (Decretos, Leis, ISOs etc) COGETIC CSIC Nuvem Fiocruz	Ambiente político Ambiente Financeiro/orçamentário PETI/PDTI Governança Governança
	Forças	**Fraquezas**
Ambiente Interno	Relação com COGETIC Serviço Nuvem Fiocruz Capacidades técnicas Normas (portarias, alertas, PDTI) RNP STI	Infraestrutura de TIC da Unidade Operacionalização das normas Alinhamento estratégico Visão estratégica STI Processos de negócio e SLAs Orçamento de TI

Com base no que foi destacado, para o ambiente externo as oportunidades identificadas foram o ambiente social e legal, pelo impacto institucional que a Fiocruz possui diante da sociedade; os diversos normativos que orientam sobre a contratação de serviços em nuvem na APF; a COGETIC, que possui apoio institucional para implantação do projeto da Nuvem Fiocruz; a CSIC, que presta toda orientação no que se refere a segurança da informação na Fiocruz de modo geral e, por fim, o projeto de Nuvem Fiocruz, que apresenta uma nova abordagem para prestação de serviços em nuvem para as demais unidades da instituição. Porém, as ameaças identificadas são: ambientes político e financeiro/orçamentário, pelos impactos que podem comprometer o projeto da nuvem Fiocruz, além da maturidade na governança institucional.

Para o ambiente interno as forças destacadas que influenciam positivamente no processo de migração para nuvem Fiocruz são: relação com a COGETIC, o próprio serviço Nuvem Fiocruz disponível para GEREB, capacidades técnicas, normativos, a RNP e o próprio STI. Porém, as principais fraquezas identificadas foram: A infraestrutura de TIC da GEREB; a operacionalização e apoio para adequação aos normativos (POSIC, por exemplo); alinhamento e visão estratégica da TIC; processos de negócios; e orçamento de TIC, que tem grande influência para prover serviços com qualidade para GEREB.

Capítulo 6

Validação da ferramenta de risco na Fiocruz

6.1 Contexto do processo de gestão de riscos

6.1.1 Responsabilidades

Diante da ausência de uma unidade setorial de gerenciamento de riscos, o processo ficará sob responsabilidade do Gestor de Tecnologia da Informação do STI.

6.1.2 Escopo

O escopo desse processo será limitado no contexto da infraestrutura de TIC da Gerência Regional de Brasília - GEREB no qual está sendo avaliado a migração para o ambiente de privada Nuvem da Fiocruz como IaaS. Para tanto, todas as etapas do processo levaram em consideração as informações apresentadas no estabelecimento de contexto, na seção 5.1.

6.1.3 Metodologias de processo de avaliação de riscos

Todo processo será conduzido seguindo o fluxo da ferramenta proposta na seção 4. Para tanto, as técnicas para coleta de dados foram realizadas conforme abaixo:

- **Definição dos pesos para os critérios de decisão e objetivos estratégicos:** Opnião de especialista
- **Identificação dos riscos:** Pesquisa documental (leis, decretos, guias, normas, relatórios etc) e Brainstorning com a equipe de TIC da unidade;
- **Análise de riscos:** Opinião de especialista;
- **Avaliação de riscos**: Opinião de especialista;

6.2 Etapa 1: Definição dos pesos para os critérios de decisão e objetivos estratégicos

As análises multicritério para definição dos critérios de decisão e dos objetivos estratégicos foram realizadas pelo gestor de TIC da GEREB. Para definir qual critério tinha relevância sobre o outro, o gestor fez referência as informações definidas no estabelecimento de contexto, da seção 5.1. Após esse processo, foram definidas os pesos para cada um dos objetos, conforme apresentado nas tabelas 6.1 e 6.2.

6.2.1 Cálculo dos critérios de decisão

A análise multicritério realizada nessa fase pelo gestor levou em consideração, a partir das informações apresentadas no estabelecimento de contexto. De modo geral, a unidade de Brasília dispõe de portais e plataformas de Ensino a Distância (EAD) que necessitam de boa infraestrutura, alta disponibilidade e segurança da informação. A tabela 6.1 destaca os resultados da análise realizada pelo gestor.

Tabela 6.1: Definição dos pesos para o critério de decisão

CRITÉRIOS DECISÃO	A.V.N
Ambiente organizacional	15%
Gestão de serviços	5%
Infraestrutura de TIC	22%
Segurança da Informação	47%
Custos	8%
Governança	3%
Total	100%
RC	3%

De acordo com a tabela 6.1 o maior peso definido pela análise multicritério foi segurança da informação seguida de infraestrutura de TIC, ambiente organizacional, Financeiro, gestão de serviços e governança, nessa ordem.

6.2.2 Cálculo dos Objetivos estratégicos

Para calcular os pesos dos objetivos estratégicos, em que os pesos serão utilizados para calcular o impacto dos riscos nos objetivos estratégicos institucionais na GEREB, foram realizadas com base nas informações apresentadas no contexto interno , na seção 5.2. A partir da análise realizada pelo gestor, constatou-se que os três eixos estratégicos da unidade possuem relação direta com os seguintes objetivos estratégicos da Fiocruz: Desafio SUS, C&T, Saúde e Sociedade e Inovação em gestão. A tabela 6.2 apresenta os resultados da análise multicritério realizada para os objetivos estratégicos.

Tabela 6.2: Definição dos pesos para os objetivos estratégicos

OBJETIVOS ESTRATÉGICOS	A.V.N
Desafio SUS	31%
C&T, Saúde e Sociedade	31%
Complexo produtivo de inovação em saúde	3%
Saúde ambiental e promoção da saúde pública	3%
Saúde, Estado e cooperação internacional	4%
Inovação gestão	26%
Total	100%
RC	1%

De acordo com a tabela 6.2, Desafio do SUS e C&T e inovação gestão foram os objetivos estratégicos com maior peso, seguido de Inovação a gestão. Essa análise é coerente com as informações apresentadas no contexto interno, na seção 5.2. Dessa forma, esses objetivos terão maior peso nos impactos dos riscos identificados para os ambientes em nuvem e local.

6.3 Etapas 2 e 3: Mapa de riscos - Ambiente Local e em Nuvem

Conforme já apresentado na seção 4, o mapa de risco compreende basicamente o processo de avaliação de riscos (identificação, análise e avaliação dos riscos). Para tanto, cada ambiente (local e em nuvem) possui um mapa (representado por uma planilha em excel cada um) no qual foram identificados, analisados e avaliados os respectivos riscos.

6.3.1 Identificação dos riscos

As coletas para identificação dos riscos e controles foram realizadas de forma distinta para cada ambiente. Para identificação de riscos e controles do ambiente local, foi utilizada a técnica de brainstorming com equipe de 7 colaboradores de TIC da unidade, sendo: três gestores, dois profissionais de infraestrutura de TIC e dois profissionais de suporte técnico. A equipe foi reunida para identificar, a partir de cada critério de decisão, definido na seção 4.3, os riscos e controles da infraestrutura de TIC local da GEREB. Como resultado, foram identificados 39 riscos agrupados conforme apresentado na figura 6.1.

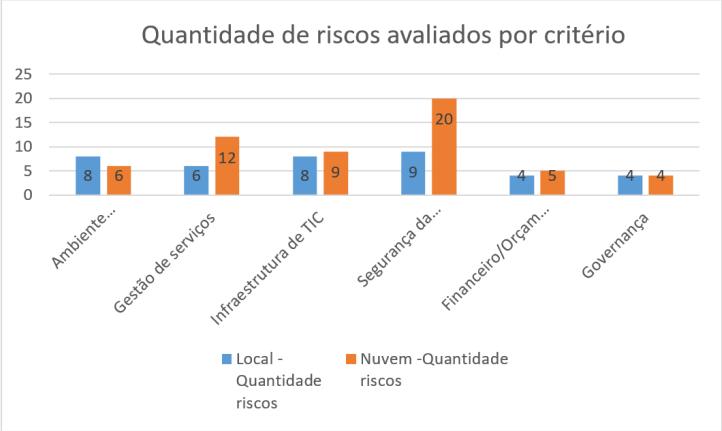

Figura 6.1: Quantidade de riscos por critério.

Como a migração em nuvem ainda é um procedimento relativamente novo para algumas instituições, identificar riscos e controles não seria uma tarefa trivial para a maioria das equipes de TIC. Para tanto, a identificação de riscos foi realizado por meio de pesquisa documental no qual foi possível identificar 56 riscos agrupados conforme apresentado na figura 6.1. Os riscos e controles identificados para o ambiente em nuvem foram retirados do acórdão 1.739/2015 [1], visto que o acórdão tem como objetivo principal orientar os órgãos e entidades da APF a aplicar a gestão de riscos no processo de contratação de serviços em nuvem.

Nessa etapa também foram discutidas as causas e consequências para cada riscos de ambos os ambientes. Nessa etapa também foi utilizada a técnica de brainstorming com equipe de 7 colaboradores de TIC da unidade.

A partir dos riscos identificados para cada ambiente, todas as informações foram incluídas na ferramenta para que os riscos fossem analisados e avaliados pelo gestor. Os riscos identificados para o ambiente local foram incluídos na planilha Mapa de Riscos Ambiente local e os riscos identificados na nuvem na planilha Mapa de Riscos Ambiente Nuvem.

6.3.2 Análise dos riscos

Os riscos foram analisados em cada mapa de riscos (Local e Nuvem Fiocruz) pela gestão de TIC da unidade a partir das informações definidas nos contextos, apresentadas na seção 5.1. Nessa etapa o gestor analisou o impacto dos riscos em cada objetivo estratégico, bem como a probabilidade do risco ocorrer. Ao final desse processo cada risco tinha calculado seu NRI. A figura 6.2 apresenta o gráfico com a média para cada ambiente, agrupados pelos critérios de decisão.

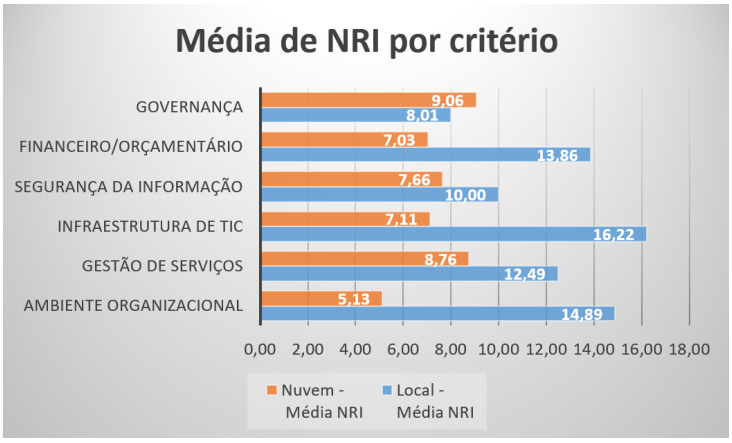

Figura 6.2: Média de NRI por critério.

No gráfico é possível observarmos que a média de riscos no ambiente local é maior em quase todos os critérios, com exceção da Governança. A partir dessas informações, podemos perceber que os riscos inerentes (sem o tratamento pelos controles) do ambiente local são mais críticos em relação ao ambiente em nuvem. Esses resultados corroboram com as informações apresentadas no estabelecimento de contexto, em que destaca que a infraestrutura de TIC depreciada da unidade tem contribuído para maior exposição aos riscos. Além do mais, quatro critérios analisados (Financeiro/orçamentário, infraestrutura

de TIC, gestão de serviços e ambiente organizacional) do ambiente local estão na escala de riscos como Risco Alto, segundo escala definida na seção 4.4.4.

6.3.3 Avaliação dos riscos

Após mensurar o valor dos risco, o gestor avaliou para cada risco o nível de confiança dos controles definidos. O procedimento foi realizado em ambos os mapas de riscos (Local e Nuvem). Ao final desse procedimento, cada risco tinha calculado o NRR. A figura 6.3 apresenta o gráfico com a média de NRR para cada critério de decisão.

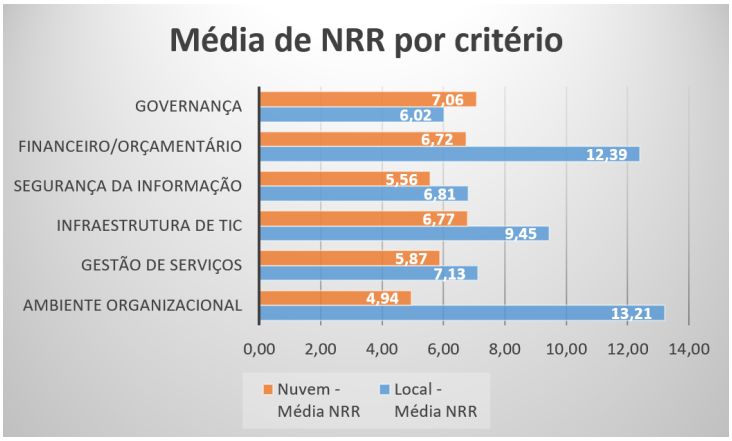

Figura 6.3: Média de NRR por critério.

No gráfico é possível observarmos que os controles existentes foram capazes de reduzir a média do risco em todos os critérios avaliados. Entretanto, os controles não foram capazes de modificar a ordem apresentada na figura 6.2, no qual a média de NRI era maior para ambiente local. Na tabela apresenta um resumo dos resultados desse processo 6.3.

Tabela 6.3: Resumo do processo de avaliação de risco realizado apoiado pela ferramenta

	AMBIENTE LOCAL			AMBIENTE NUVEM		
Critérios de decisão	**Local - Quantidade riscos**	**Local - Média NRI**	**Local - Média NRR**	**Nuvem - Quantidade riscos**	**Nuvem - Média NRI**	**Nuvem - Média NRR**
Ambiente organizacional	8	14,89	13,21	6	5,13	4,94
Gestão de serviços	6	12,49	7,13	12	8,76	5,87
Infraestrutura de TIC	8	16,22	9,45	9	7,11	6,77
Segurança da informação	9	10,00	6,81	20	7,66	5,56
Financeiro/Orçamentário	4	13,86	12,39	5	7,03	6,72
Governança	4	8,01	6,02	4	9,06	7,06
Total	**39**	**12,58**	**9,17**	**56**	**7,46**	**6,16**

Podemos observar na tabela que o ambiente local ainda apresenta maior risco para a maioria dos critérios avaliados. Isso é um importante indicativo para que a unidade possa entender que a melhor estratégia seja migrar para o ambiente em nuvem.

6.4 Etapa 4: Matriz de decisão

Para auxiliar na tomada de decisão, os resultados dos NRR de cada critério foram harmonizados e normalizados para serem analisados a partir dos pesos definidos como resultado apresentado na tabela 6.1. A tabela 6.4 apresenta essas informações.

Tabela 6.4: Dados de NRR harmonizados e normalizados

CRITÉRIOS		AMBIENTE LOCAL	NUVEM FIOCRUZ	Total
Ambiente organizacional	NRR	13,21	4,94	18,15
	Harmonizar	1,37	3,67	5,05
	Normalizar	**27%**	**73%**	100%
Gestão de serviços	NRR	7,13	5,87	13,00
	Harmonizar	1,82	2,21	4,04
	Normalizar	**45%**	**55%**	100%
Infraestrutura de TIC	NRR	9,45	6,77	16,22
	Harmonizar	1,72	2,40	4,11
	Normalizar	**42%**	**58%**	100%
Segurança da Informação	NRR	6,81	5,54	12,35
	Harmonizar	1,81	2,23	4,04
	Normalizar	**45%**	**55%**	**100%**
Financeiro / orçamentário	NRR	12,39	6,72	19,12
	Harmonizar	1,54	2,84	4,39
	Normalizar	**35%**	**65%**	100%
Governança	NRR	6,02	7,06	13,09
	Harmonizar	2,17	1,85	4,03
	Normalizar	**54%**	**46%**	100%

Podemos observar na tabela 6.4 que o ambiente em nuvem se destaca em quase todos os critérios, com exceção no critério Governança. Após as informações serem normalizadas, os dados são calculados na matriz de decisão a partir da média ponderada dos pesos definidos nos critérios de decisão, na tabela 6.1 da etapa 1, com as dados de NRR normalizados da tabela 6.4. A tabela 6.5 apresenta o resultado final dessa análise.

Tabela 6.5: Resultado da matriz de decisão

	Ambiente organizacional	Gestão de serviços	Infraestrutura de TIC	Segurança da Informação	Financeiro / Orçamentário	Governança	
Vetor dos critérios	15%	5%	22%	47%	8%	3%	
ALTERNATIVAS							**Vetor de decisão**
Ambiente local	27%	45%	42%	45%	35%	54%	41%
Nuvem Fiocruz	73%	55%	58%	55%	65%	46%	59%

Conforme demonstrado na tabela 6.5, após o processo de avaliação de riscos, no qual foram calculados os riscos dos ambientes local e nuvem Fiocruz, a matriz de decisão calculou que a melhor decisão para a GEREB é a nuvem Fiocruz. Além do mais, com

base na escala de riscos definida na seção 4.4.4, podemos perceber na tabela 6.4 que no Ambiente local os critérios de decisão Ambiente organizacional, infraestrutura de TIC e Financeiro/Orçamentário estão com NRR de Risco Alto (valores entre 10 e 15,99). Os demais critérios do ambiente local apresentam o NRR com Risco Moderado (valores entre 6 e 9,99), assim como os critérios de decisão Infraestrutura de TIC, Financeiro/Orçamentário e Governança para o Ambiente em Nuvem. Os demais critérios para o Ambiente em Nuvem apresentam NRR com Risco Pequeno (valores entre 4 a 5,99).

Dessa forma, as informações demonstram que os riscos para o Ambiente Local são maiores em relação aos riscos para o Ambiente em Nuvem. Diante da situação analisada no contexto da GEREB, a exposição maior aos riscos no ambiente local foi fundamental para que a unidade desenvolvesse um esforço em colaboração com a COGETIC para migração dos principais serviços da unidade na Nuvem Fiocruz. Esse processo contribuiu para que a Fiocruz reduzisse no orçamento de R$ 14.123.484,18, no PDTI 2015/2016, para R$ 8.251.240,34, no PDTI 2016/2018, devido ao corte de recursos como soluções de armazenamento, servidores, backup e outras soluções de datacenter. Entretanto, é importante destacar que toda decisão será realizada pela alta direção alinhada com a gestão de TIC da unidade.

Capítulo 7

Conclusão

Apesar dos diversos benefícios que a computação em nuvem propõe, ainda assim a sua adesão é um paradigma a ser quebrado pois envolve vários riscos que precisam ser avaliados em um contexto da infraestrutura de TIC local da organização. Uma decisão equivocada pode comprometer seriamente os objetivos estratégicos da instituição. Diante disso, este trabalho de pesquisa apresentou uma ferramenta para apoio a tomada de decisão de migração em um ambiente local para nuvem privada institucional a partir de um processo de avaliação de riscos sob a ótica da norma NBR ISO 31000:2009.

O estudo bibliográfico demonstrou que existem poucas pesquisas que alinham técnicas e métodos com a gestão de riscos no processo de migração para nuvem. Na maioria são utilizadas técnicas e métodos isolados, como análise multicritério em conjunto com DELPHI, por exemplo, para auxiliar nesse processo de tomada de decisão.

Para tanto, o processo de decisão necessitava de critérios para serem avaliados no contexto da migração em nuvem. Dessa forma, a partir do estudo bibliográfico e documental foi possível definir os critérios de decisão para migração em nuvem. Esses critérios foram utilizados pela ferramenta para ponderar o cálculo de decisão a partir dos riscos avaliados tanto no ambiente local como em nuvem.

O desenho da ferramenta alinhou as principais técnicas e métodos de riscos identificados no estudo bibliográfico e documental ao processo de avaliação de riscos da norma NBR ISO 31000:2009. O fluxo da ferramenta passa inicialmente pela ponderação dos critérios de decisão e objetivos estratégicos. Para tanto, é utilizada a técnica AHP para diminuir a subjetividade nesse procedimento. A próxima etapa cria os mapas de riscos para os ambientes local e em nuvem. Os mapas de riscos utilizaram matriz de probabilidade e impacto para calcular o Nível de Risco Inerente (NRI) e, após cálculo dos riscos de controle, o Nível de Risco Residual (NRR). A matriz de decisão é a etapa final do processo. Nessa etapa é harmonizado e normalizado os NRRs dos mapas de riscos dos ambientes local e em nuvem. O cálculo de decisão é realizado a partir da ponderação dos

critérios de decisão, definidos na etapa inicial, com os resultados normalizados dos NRRs, agrupados pelos critérios apresentados no parágrafo anterior, de ambos os ambientes.

A validação de aplicação da ferramenta foi realizada no contexto da Gerência Regional de Brasília-GEREB da Fiocruz, no qual demonstrou ser viável o uso da ferramenta para auxiliar no processo de tomada de decisão. Para tanto, todo o contexto foi estabelecido por meio de pesquisa documental e análise de documentos para auxiliar na análise e avaliação dos riscos. Os riscos para o ambiente local foram identificados a partir da técnica de brainstorming com a equipe de TIC da unidade. Como a computação em nuvem ainda é um processo incipiente na grande maioria das organizações, identificar riscos por métodos convencionais seria complexo. Dessa forma, o estudo bibliográfico e documental listou os principais riscos em nuvem para que pudesse ser avaliado no mapa de riscos do ambiente em nuvem. Após todo os riscos serem avaliados pelos gestores, ao final a ferramenta calculou e definiu com 59% que a melhor decisão seria a unidade migrar para nuvem Fiocruz. Entretanto, é importante ressaltar que a ferramenta auxilia no processo de tomada de decisão a partir do processo de avaliação de riscos em ambos ambientes. A decisão final cabe a alta direção da unidade alinhada com a gestão de TIC da unidade.

A computação em nuvem é uma realidade no qual as instituição deverão de adaptar cada vez mais. Com isso, espera-se que esse estudo influencie novas abordagens para gestão de riscos aplicados no contexto de migração em nuvem para trabalhos futuros.

Diante disso, podemos concluir que a ferramenta apresenta uma grande contribuição para apoio ao processo de decisão de migração para o ambiente em nuvem. Alinhada a um processo de avaliação de riscos, esse importante instrumento, além de contribuir para melhoria da governança em risco, auxilia a organização a decidir sobre a migração para computação em nuvem. Além do mais, atende a uma exigência dos principais normativos do Tribunal de Contas da União-TCU, Ministério do Planejamento-MP e do Departamento de Segurança da Informação e Comunicação-DSIC que estabelecem que toda contratação de serviços em nuvem deverá ser precedida de um processo de gestão de riscos. Dessa forma, essa ferramenta também poderá ser uma importante contribuição aos demais órgãos de governo.

Referências

[1] TCU: *Acórdão 1.739/2015-TCU-Plenário*, 2015. http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc, acesso em 2017-07-13TZ. xi, 9, 10, 14, 16, 53, 54, 89

[2] Badger, Lee, Tim Grance, Robert Patt-Corner e Jeff Voas: *Cloud computing synopsis and recommendations*. NIST special publication, 800:146, 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf, acesso em 2017-03-22TZ. xi, 8, 10, 11, 12, 13, 14

[3] ISO, ABNT ABNT NBR: *IEC 31000-2009: Gestão de riscos-princípios e diretrizes*. norma técnica. Technical report, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Rio de Janeiro, Brasil, 39(4):2, 2009. xi, 3, 19, 20, 21, 27, 46, 59

[4] Islam, Shareeful, Stefan Fenz, Edgar Weippl e Haralambos Mouratidis: *A Risk Management Framework for Cloud Migration Decision Support*. Journal of Risk and Financial Management, 10(2):10, abril 2017, ISSN 1911-8074. http://www.mdpi.com/1911-8074/10/2/10, acesso em 2018-04-03TZ. xi, 20, 26, 27, 29, 53, 54

[5] Yuusuf, Hamse e Christopher Tubb: *Migration to cloud computing: a risk homeostasis methodology*. International Journal of Computer Applications, 77(7), 2013. http://search.proquest.com/openview/d87f078e7530975e7eea261214333b64/1?pq-origsite=gscholar&cbl=136216, acesso em 2017-04-13TZ. xi, 10, 30, 31

[6] Cordeiro, S. d S., F. S. SantAna, K. M. F. Suzuki e P. M. Azevedo-Marques: *A Risk Analysis Model for PACS Environments in the Cloud*. Em *2015 IEEE 28th International Symposium on Computer-Based Medical Systems*, páginas 356–357, junho 2015. xi, xiii, 32, 35

[7] Fan, Chiang Ku e Tien Chun Chen: *The risk management strategy of applying cloud computing*. Risk Management, 3(9), 2012. http://www.chinacloud.cn/upload/2012-10/12100614526693.pdf, acesso em 2017-04-04TZ. xi, 9, 11, 12, 37, 38, 39

[8] Khrisna, A. e Harlili: *Risk management framework with COBIT 5 and risk management framework for cloud computing integration*. Em *2014 International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA)*, páginas 103–108, 2014. xi, 40

[9] VPGDI, Vice Presidencia de Gestão e Desenvolvimento Institucional: *PORTARIA 001/2016-VPGDI*, 2016. https://cogetic.fiocruz.br/admin/docs/p0012016-modelogrsic.pdf, acesso em 2017-07-18. xi, xiii, 55, 57

[10] BRASIL, MINISTÉRIO PLANEJAMENTO, BRASIL: *Matriz de Riscos*. http://www.planejamento.gov.br/assuntos/gestao/controle-interno/matriz-de-riscos, acesso em 2018-06-29TZ. xi, 55, 57, 58, 59

[11] DIPLAN, Diretoria de Planejamento Estratégico: *RELATÓRIO DE GESTÃO DO EXERCÍCIO DE 2016*. Relatório Técnico, 2017. https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/relatorio_de_gestao_2016_fiocruz.pdf. xii, 70, 75

[12] Lemme, Alvaro Funcia: *Nuvem Fiocruz - Centro de Dados para Computação em Nuvem (CDCN)*, maio 2015. https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/alvaro_funcia_lemme.pdf. xii, 77, 78

[13] DIREB, Diretoria Regional de Brasília: *Fiocruz Brasília: Uma nova institucionalidade*. dezembro 2016. xii, 81, 82, 83

[14] ISO, ABNT ABNT NBR: *IEC 31010-2012: Gestão de riscos-técnicas para o processo de avaliação de riscos*. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2012. xiii, 22, 23, 24, 25, 26, 55, 58, 63

[15] União, Tribunal de Contas da: *Referencial Básico de Gestão de Riscos | Portal TCU*. https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm, acesso em 2018-06-05TZ. xiii, 26, 46, 55, 58, 59, 60, 61, 65, 67, 69

[16] Saaty, Thomas L.: *How to make a decision: The analytic hierarchy process*. European Journal of Operational Research, 48(1):9–26, setembro 1990, ISSN 03772217. http://linkinghub.elsevier.com/retrieve/pii/037722179090057I, acesso em 2018-07-01TZ. xiii, 26, 63, 64

[17] COGETIC, Coordenação Geral de Tecnologia da Informação e Comunicação: *Catálogo de serviços de TI Fiocruz*. https://cogetic.fiocruz.br/admin/docs/catalogodeservicos-julho-17-publicacaov2.pdf. xiii, 79, 80

[18] Siqueira, Marcelo Costa: *Gestão estratégica da informação*. Brasport, 2005. 1

[19] Moresi, Eduardo Amadeu Dutra: *Delineando o valor do sistema de informação de uma organização*. Ciência da Informação, Brasília, 29(1):14–24, 2000. http://www.scielo.br/pdf/ci/v29n1/v29n1a2, acesso em 2017-03-15TZ. 1

[20] Costa, Rostand, F. Brasileiro, G. Lemos Filho e Dênio Mariz Sousa: *eScience-as-a-Service: Desafios e Oportunidades para a Criação de Nuvens Científicas*. Em *Proceedings of the 5th Brazilian e-Science Workshop*, páginas 1–8, 2011. https://www.researchgate.net/profile/Francisco_Brasileiro/publication/264886053_eScience-as-a-Service_Desafios_e_Oportunidades_para_a_Criao_de_Nuvens_Cientficas/links/5407101a0cf2bba34c1e8851.pdf, acesso em 2017-03-15TZ. 1

[21] Araújo, Misael Sousa de: *Análise de maturidade da gestão de riscos de TI na Fiocruz : definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional*, dezembro 2014. http://repositorio.unb.br/handle/10482/17275, acesso em 2017-03-15TZ. 1, 19, 69

[22] Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang e Anand Ghalsasi: *Cloud computing — The business perspective*. Decision Support Systems, 51(1):176–189, abril 2011, ISSN 01679236. http://linkinghub.elsevier.com/retrieve/pii/S0167923610002393, acesso em 2017-03-15TZ. 1, 3, 8

[23] Jamshidi, Pooyan, Aakash Ahmad e Claus Pahl: *Cloud Migration Research: A Systematic Review*. IEEE Transactions on Cloud Computing, 1(2):142–157, 2013, ISSN 2168-7161. http://ieeexplore.ieee.org/document/6624108/, acesso em 2017-03-15TZ. 1

[24] Zhao, Jun Feng e Jian Tao Zhou: *Strategies and Methods for Cloud Migration*. International Journal of Automation and Computing, 11(2):143–152, abril 2014, ISSN 1476-8186, 1751-8520. http://link.springer.com/10.1007/s11633-014-0776-7, acesso em 2017-03-15TZ. 1, 41

[25] *Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending*. http://www.gartner.com/newsroom/id/3384720, acesso em 2017-07-21TZ. 1

[26] Rodrigues, Walton Alencar: *Relatório Sistêmico de Fiscalização de Tecnologia da Informação*. Relatório Técnico, TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015. http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A250058951015005FADCE57B51&inline=1, acesso em 2017-12-03. 2

[27] DIOGENES, Y. e M.V. DE SOUSA NETO: *CERTIFICAÇAO CLOUD ESSENTIALS: GUIA PREPARATORIO PARA O EXAME CLO-001*. NOVATERRA, ISBN 978-85-61893-26-2. https://books.google.com.br/books?id=w6wWvgAACAAJ. 2, 9, 12, 13, 14, 15, 53, 54

[28] USP: *USP executa maior nuvem educacional da América Latina em #SoftwareLivre - Página Principal do Stoa*. https://social.stoa.usp.br/stoa/rea/usp-executa-maior-nuvem-educacional-da-america-latina-em-softwarelivre, acesso em 2017-03-15TZ. 2

[29] Symantec: *Pesquisa sobre Situação de Cloud Computing - Resultados América Latina*. Relatório Técnico, 2011. https://www.symantec.com/content/pt/br/enterprise/images/theme/state-of-cloud/State-of-Cloud-Report-LAM-PORT-FN.pdf. 2

[30] Pahl, Claus e Huanhuan Xiong: *Migration to PaaS clouds - Migration process and architectural concerns*. páginas 86–91. IEEE, setembro 2013, ISBN 978-1-4673-4889-8. http://ieeexplore.ieee.org/document/6632740/, acesso em 2017-03-15TZ. 3, 41

[31] Alkhalil, Adel, Reza Sahandi e David John: *Migration to Cloud Computing: A Decision Process Model*. Em *Central European Conference on Information and Intelligent Systems*, página 154. Faculty of Organization and Informatics Varazdin, 2014. 3, 42, 53, 54

[32] ISO, ABNT ABNT NBR: *IEC 31004-2015: Gestão de riscos - Guia para implementação*. norma técnica. Technical report, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Rio de Janeiro, Brasil, página 44, 2015. 6, 19, 20, 21, 22, 23, 25, 26, 41, 59

[33] Sultan, Nabil: *Cloud computing for education: A new dawn?* International Journal of Information Management, 30(2):109–116, abril 2010, ISSN 02684012. `http://linkinghub.elsevier.com/retrieve/pii/S0268401209001170`, acesso em 2017-03-22TZ. 8

[34] Wang, Heyong, Wu He e Feng Kwei Wang: *Enterprise cloud service architectures*. Information Technology and Management, 13(4):445–454, dezembro 2012, ISSN 1385-951X, 1573-7667. `http://link.springer.com/10.1007/s10799-012-0139-4`, acesso em 2017-03-20TZ. 8

[35] Tak, B. C., B. Urgaonkar e A. Sivasubramaniam: *Cloudy with a Chance of Cost Savings*. IEEE Transactions on Parallel and Distributed Systems, 24(6):1223–1233, junho 2013, ISSN 1045-9219. 9

[36] Silva, Hilson Barbosa da: *Uma investigação sobre o procesoo migrátorio para a plataforma de computação em nuvem no Brasil*. janeiro 2016. `https://repositorio.ufpe.br/handle/123456789/18034`, acesso em 2018-04-02TZ. 10

[37] Paiva, Luís Manuel Marques: *Análise de risco para computação em nuvem*. agosto 2016. `https://repositorioaberto.uab.pt/handle/10400.2/5635`, acesso em 2018-04-02TZ. 10, 14, 53

[38] Gholami, Mahdi Fahmideh, Farhad Daneshgar, Graham Low e Ghassan Beydoun: *Cloud migration process—A survey, evaluation framework, and open challenges*. Journal of Systems and Software, 120:31–69, outubro 2016, ISSN 01641212. `http://linkinghub.elsevier.com/retrieve/pii/S0164121216300966`, acesso em 2017-03-22TZ. 10

[39] El-Gazzar, Rania, Eli Hustad e Dag H. Olsen: *Understanding cloud computing adoption issues: A Delphi study approach*. Journal of Systems and Software, 118:64–84, agosto 2016, ISSN 01641212. `http://linkinghub.elsevier.com/retrieve/pii/S016412121630036X`, acesso em 2017-05-04TZ. 11, 26

[40] Bayramusta, Merve e V. Aslihan Nasir: *A Fad or Future of IT?* Int. J. Inf. Manag., 36(4):635–644, agosto 2016, ISSN 0268-4012. `http://dx.doi.org/10.1016/j.ijinfomgt.2016.04.006`, acesso em 2017-07-20TZ. 11, 12

[41] Kalloniatis, Christos, Haralambos Mouratidis e Shareeful Islam: *Evaluating cloud deployment scenarios based on security and privacy requirements*. Requirements Engineering, 18(4):299–319, novembro 2013, ISSN 0947-3602, 1432-010X. `http:`

//link.springer.com/10.1007/s00766-013-0166-7, acesso em 2017-03-20TZ. 11, 12

[42] BRASIL: *Decreto nº 8135/2013 - Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.*, abril 2013. http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm, acesso em 2017-07-16TZ. 16

[43] MP: *Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem*, 2016. https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf, acesso em 2017-07-19TZ. 18

[44] Fitó, J. Oriol e Jordi Guitart: *Business-driven management of infrastructure-level risks in Cloud providers.* Future Generation Computer Systems, 32:41–53, março 2014, ISSN 0167739X. http://linkinghub.elsevier.com/retrieve/pii/S0167739X12001045, acesso em 2017-05-04TZ. 19, 20

[45] Marshall, Christopher: *Medindo e gerenciando riscos operacionais em instituições financeiras.* Qualitymark Editora Ltda, 2002. 19

[46] Araujo, Misael Sousa de, Edgard Costa Oliveira, Simone Borges Simão Monteiro e Tharcísio Marcos Ferreira de Queiroz Mendonça: *Risk Management Maturity Evaluation Artifact to Enhance Enterprise IT Quality.* Em *Proceedings of the 19th International Conference on Enterprise Information Systems - Volume 3: ICEIS,*, páginas 425–432. ScitePress, 2017, ISBN 978-989-758-249-3. 20

[47] ABNT, AB de NT: *NBR ISO/IEC Guia 73–Gestão de riscos–Vocabulário–Recomendações para uso em normas.* Rio de Janeiro: ABNT, 2005. 20

[48] Barafort, Béatrix, Antoni Lluís Mesquida e Antonia Mas: *Integrating risk management in IT settings from ISO standards and management systems perspectives.* Computer Standards & Interfaces, novembro 2016, ISSN 09205489. http://linkinghub.elsevier.com/retrieve/pii/S0920548916301866, acesso em 2017-05-04TZ. 20

[49] OLIVEIRA, ADRIANE ARAÚJO DE: *APLICAÇÃO DO MÉTODO DE ANÁLISE HIERÁRQUICA NA TOMADA DE DECISÃO PARA ADOÇÃO DE COMPUTAÇÃO EM NUVEM. UM ESTUDO DE CASO NA FEDERAÇÃO DAS INDÚSTRIAS DO RN.* página 128. http://repositorio.ufrn.br:8080/jspui/handle/123456789/15011. 25, 53

[50] Khajeh-Hosseini, A., D. Greenwood e I. Sommerville: *Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS.* Em *2010 IEEE 3rd International Conference on Cloud Computing*, páginas 450–457, julho 2010. 36

[51] Khajeh-Hosseini, Ali, David Greenwood, James W. Smith e Ian Sommerville: *The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise.*

agosto 2010. https://arxiv.org/abs/1008.1900, acesso em 2017-03-19TZ. 41, 53, 54

[52] Ribas, Maristella, Alberto Sampaio Lima, José Neuman de Souza, Flávio Rubens de Carvalho Sousa e Germano Fenner: *Tomada de decisão multicritério na migração de aplicativos para ambientes de nuvem do tipo software as a service*. Revista Brasileira de Administração Científica, 5(2):83, novembro 2014, ISSN 2179-684X. http://sustenere.co/journals/index.php/rbadm/article/view/SPC2179-684X.2014.002.0007, acesso em 2017-03-22TZ. 41, 53, 54

[53] Richardson, Roberto Jarry e José Augusto de Souza Peres: *Pesquisa social: métodos e técnicas*. Atlas, São Paulo, 3. ed. rev e ampl edição, 1999, ISBN 978-85-224-2111-4. OCLC: 46755954. 44

[54] Gil, Antônio Carlos: *Métodos e técnicas de pesquisa social*. Atlas, São Paulo, 2008, ISBN 978-85-224-5142-5. OCLC: 298931695. 44, 45

[55] Marconi, Marina de Andrade e Eva Maria Lakatos: *Metodologia científica*. Atlas, São Paulo, 2009, ISBN 978-85-224-4762-6. OCLC: 422876997. 44

[56] Wazlawick, Raul Sidnei: *Metodologia de pesquisa para ciência da computação*. 2014, ISBN 978-85-352-7783-8. http://www.sciencedirect.com/science/book/9788535277821, acesso em 2017-05-03TZ, OCLC: 902734376. 44, 45, 46

[57] VERGARA, Sylvia Constant: *Projetos e relatórios de pesquisa em administração. São Paulo: Atlas, 2000*. Métodos de pesquisa em administração, 3, 2009. 44

[58] Mariano, Ari Melo, Rosario García Cruz e Jorge Arenas Gaitán: *Meta análises como instrumento de pesquisa: Uma revisão sistemática da bibliografia aplicada ao estudo das alianças estratégicas internacionais*. Em *Congresso Internacional de Administração-Inovação Colaborativa e Competitividade*, 2011. 47

[59] Calazans, Angélica Toffano Seidel, Ari Melo Mariano e Roberto Avila Paldes: *Uma revisão sistemática da bibliografia sobre m?tricas funcionais de tamanho de software utilizando o enfoque meta-analítico*. Universitas: Gestão e TI, 5(2), dezembro 2015, ISSN 2179-832X, 2179-8311. http://www.publicacoes.uniceub.br/index.php/gti/article/view/3532, acesso em 2017-06-20TZ. 47, 48, 49

[60] Evangelista, Wellington Galdino: *Critérios para avaliação de viabilidade da adoção de computação em nuvem por parte de organizações da Administração Pública Federal*. fevereiro 2014. https://bdtd.ucb.br:8443/jspui/handle/123456789/1424, acesso em 2018-04-02TZ. 53

[61] Luz, Lucas Martorelli Gondim: *Uma aplicação do método fuzzy-electre-topsis para seleção de serviços de computação em nuvem*. setembro 2014. https://repositorio.ufrn.br/handle/123456789/20292, acesso em 2018-04-04TZ. 53

[62] Melo, Marcelo Morais de: *Auxílio à tomada de decisão no processo de migração para computação em nuvem*. março 2014. http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui//handle/tede/546, acesso em 2018-04-04TZ. 53

[63] *Fundação Oswaldo Cruz*. http://portal.fiocruz.br/pt-br, acesso em 2016-09-04TZ. 69, 72

[64] FIOCRUZ: *A Fiocruz como instituição estratégica de Estado para a saúde - PLANO QUADRIENAL (2011-2014)*. Relatório Técnico, Fundação Oswaldo Cruz. http://www.fiocruz.br/media/planoquadrienal20112014.pdf, acesso em 2017-12-06. 70, 71

[65] FIOCRUZ: *RELATÓRIO DE GESTÃO DO EXERCÍCIO DE 2015*. Relatório Técnico, Fundação Oswaldo Cruz. https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/relatorio_de_gestao_fiocruz_2015_0.pdf, acesso em 2017-12-06. 71, 76

[66] Campos, Andre, Anderson Ferreira, Kizzy Benjamin e Tazio Fernandes: *Plano Estratégico de Tecnologia da Informação - PETI 2016/2017 da FIOCRUZ*. Relatório Técnico, FIOCRUZ - CGTI, setembro 2016. https://cgti.fiocruz.br/admin/docs/petifiocruz2016-2017.pdf. 71, 76

[67] VPEIC, Informação e Comunicação, Vice Presidência de Ensino: *Plano de Desenvolvimento Institucional da Fiocruz 2016 - 2020*. Relatório Técnico, fevereiro 2016. 72, 74, 75

[68] FIOCRUZ: *Plano Diretor de Tecnologia da Informação - PDTI 2015/2016 da FIOCRUZ*. Relatório Técnico, FIOCRUZ - CGTI, 2014. https://cgti.fiocruz.br/admin/docs/pdtifiocruz20152016assinado.pdf. 76

[69] FIOCRUZ: *PDTI 2016-2017 - BALANÇO*. Relatório Técnico, Fiocruz. https://cogetic.fiocruz.br/admin/docs/balancopdti2016-2017.pdf, acesso em 2018-03-28. 76, 83

[70] FIOCRUZ: *Plano Diretor de Tecnologia da Informação - PDTI 2016/2017 da FIOCRUZ*. Relatório Técnico, FIOCRUZ - CGTI, novembro 2016. https://cgti.fiocruz.br/admin/docs/pdtifiocruz20152016assinado.pdf. 76, 77

[71] COGETIC, Coordenação Geral de Tecnologia da Informação e Comunicação: *Centro de dados para computação em nuvem - Política de uso*. Relatório Técnico, Fiocruz, abril 2016. https://cogetic.fiocruz.br/admin/docs/centrodedadosparacomputacaoemnuvem-politicadeusov0. 78