TRABALHO FINAL DE GRADUAÇÃO

# O PAPEL DAS TAGS EM CLOUD COMPUTING NA GESTÃO DE RISCO DE PROJETOS E COMPLIANCE

**Beatriz Hanae Fujimoto**

**Orientador Prof. Dr. Georges Daniel Amvame Nze**

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO FINAL DE GRADUAÇÃO

# O PAPEL DAS TAGS EM CLOUD COMPUTING NA GESTÃO DE RISCO DE PROJETOS E COMPLIANCE

**Beatriz Hanae Fujimoto**

**Orientador Prof. Dr. Georges Daniel Amvame Nze**

*Trabalho Final de Graduação submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação*

Banca Examinadora

Prof. Dr. Georges Daniel Amvame Nzee, ENE/UnB _____
*Orientador*

Prof. Valério Aymoré Martins, ENE/UnB _____
*Examinador Interno*

Felipe Barreto _____
*Examinador externo*

## AGRADECIMENTOS

Por todas as significativas contribuições que recebi ao longo desta jornada acadêmica, expresso minha profunda gratidão.

Acima de tudo, agradeço a Deus, cuja fé sustentou-me ao longo dos anos, guiou-me pelo caminho e proporcionou bênçãos mesmo nas adversidades mais desafiadoras desta etapa. Em segundo lugar, à minha avó, Eiko Fujimoto, a pessoa mais importante da minha existência, e que sempre depositou plena confiança em cada um dos meus passos, sendo minha principal fonte de inspiração e incentivo para concluir este curso na UnB. Em terceiro lugar, a minha irmã Michelle Kiemy Fujimoto, que sempre esteve ao meu lado, me apoiou e me ajudou a levantar quando mais precisei, tanto antes quanto durante esse processo de vivência na universidade.

Expresso minha gratidão à minha família como um todo, em especial ao meu pai, Hisao, e minha madrasta, Ana Paula, que suportaram minhas diárias queixas de cansaço e exaustão mental, sempre encorajando-me a persistir, pois sabiam que valeria a pena no final. Além deles, meu cunhado Irivan Ferreira e aos meus tios por suas tentativas de amenizar as adversidades ao longo desse caminho.

Ao meu namorado e melhor amigo, Thomás Costa Rodrigues, dedico meu apreço especial por suas palavras de incentivo e carinho, sendo meu companheiro e compartilhando momentos de estudo na Biblioteca Central da Universidade de Brasília durante esta fase final.

Agradeço de coração a todos os meus amigos, em particular à minha melhor amiga Rayssa Souza Feitosa, e aos amigos Thaís Cristina Freitas, Maisa Felipe Veloso, Alicia Fuentes, Antonio Carlos Ribeiro e Matheus Souza Feitosa. Cada um contribuiu e me acompanhou singularmente, e sou grata por diversas vezes suavizarem as pressões da vida universitária.

Aos meus colegas de universidade, em especial Adrielle da Silva Custódio e Letícia Fernandes Rios, que compartilharam experiências e conhecimentos além das aulas, expresso minha sincera gratidão. Não posso deixar de mencionar Anne Caroline Ramos, Aline Teles de Franca e Gabriel Lima Sertão, que não apenas foram parceiros em trabalhos acadêmicos, mas também se tornaram grandes amigos ao longo da graduação.

Por fim, agradeço ao professor Georges Daniel, cuja ajuda, ensinamentos e paciência foram elementos fundamentais para o sucesso deste trabalho e para minha jornada acadêmica como um todo.

Beatriz Hanae Fujimoto

## RESUMO

A transformação significativa promovida pela computação em nuvem na Tecnologia da Informação, vem oferecendo flexibilidade e eficiência às organizações. Líderes do setor, como Microsoft, Amazon e Google, impulsionaram esse modelo de fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, através da Internet para oferecer inovações mais rápidas, recursos flexíveis e economias de escala. No entanto, a implementação requer uma abordagem cuidadosa, enfatizando a importância da Governança, Gerenciamento de Riscos e Conformidade (GRC). Pois, a falta de governança pode levar a gastos excessivos, evidenciando a necessidade de estratégias organizadas, além de exposição à ataques cibernéticos, que colocam em riscos toda a infraestrutura de uma empresa e por fim sem a garantia de conformidade com as leis. Com a conclusão deste trabalho, espera-se que o framework proposto para a marcação de recursos na nuvem, focado em GRC, visando otimizar o uso eficiente e evitar custos adicionais, colabore para a eficiência operacional, contabilidade de custos e análise de riscos na nuvem, sendo crucial para a Governança, Risco e Conformidade em projetos de Cloud Computing.



**Palavras-chave: Computação em Nuvem, Tags, Governança, Risco, Conformidade**

## ABSTRACT

The significant transformation driven by cloud computing in Information Technology has been providing flexibility and efficiency to organizations. Industry leaders such as Microsoft, Amazon, and Google have propelled this service delivery model, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to offer faster innovations, flexible resources, and economies of scale. However, implementation requires a careful approach, emphasizing the importance of Governance, Risk Management, and Compliance (GRC). The lack of governance can lead to overspending, highlighting the need for organized strategies, along with exposure to cyber attacks that pose risks to an entire company's infrastructure, ultimately without guaranteeing compliance with laws. With the completion of this work, it is expected that the proposed framework for cloud resource tagging, focused on GRC, aiming to optimize efficient use and avoid additional costs, will contribute to operational efficiency, cost accounting, and risk analysis in the cloud. This is crucial for Governance, Risk, and Compliance in Cloud Computing projects.



**Keywords: Cloud Computing, Tags, Governance, Risk, Compliance**

# SUMÁRIO


**1 INTRODUÇÃO ..... 1**
1.1 OBJETIVOS ..... 2
1.1.1 OBJETIVO GERAL ..... 2
1.1.2 OBJETIVOS ESPECÍFICOS ..... 2
1.2 JUSTIFICATIVA ..... 2

**2 TRABALHOS RELACIONADOS ..... 4**
2.1 GESTÃO DE RISCOS E CONFORMIDADE PARA SERVIÇOS DE COMPUTAÇÃO EM NUVEM: PROJETANDO UM MODELO DE REFERÊNCIA ..... 4
2.2 IMPLEMENTANDO UMA ESTRATÉGIA DE MARCAÇÃO PARA *cloud* IAAS E PAAS ..... 6
2.3 A AGREGAÇÃO DE *tags* EM NUVENS PÚBLICAS/PRIVADAS ..... 9
2.4 UMA SOLUÇÃO DE RASTREAMENTO PARA GERENCIAMENTO DE ATIVOS E RECURSOS DE TI ..... 11

**3 FUNDAMENTAÇÃO TEÓRICA ..... 15**
3.1 COMPUTAÇÃO EM NUVEM ..... 15
3.1.1 DEFINIÇÕES E CONCEITOS ..... 15
3.1.2 MODELOS DE SERVIÇO EM NUVEM ..... 16
3.1.3 MODELOS DE IMPLEMENTAÇÃO EM NUVEM ..... 18
3.1.4 PRINCIPAIS PROVEDORES ..... 20
3.2 GRC - GOVERNANÇA, RISCO E CONFORMIDADE ..... 26
3.2.1 GOVERNANÇA ..... 28
3.2.2 GESTÃO DE RISCO ..... 31
3.2.3 *compliance* ..... 36
3.3 TAGS ..... 40
3.3.1 DEFINIÇÃO DE TAGS ..... 40
3.3.2 DEFINIÇÃO DE *tags* EM COMPUTAÇÃO EM NUVEMM ..... 42

**4 PROPOSTA DE FRAMEWORK ..... 46**
4.1 CENÁRIO SEM UTILIZAÇÃO DE *tags* ..... 46
4.2 *Tags* PARA FINS DE GRC ..... 48
4.3 PROPOSTA DE FRAMEWORK ..... 50
4.3.1 IMPLEMENTAÇÃO DE *tags* EM PROVEDORES DE NUVEM ..... 55
4.4 MELHORES PRÁTICAS NO USO DE *tags* ..... 73
4.5 DESAFIOS ..... 75

**5 CONCLUSÃO ..... 76**
5.1 TRABALHOS FUTUROS ..... 77

**REFERÊNCIAS BIBLIOGRÁFICAS ..... 78**

# LISTA DE FIGURAS


2.1 Abordagem de pesquisa subjacente para a construção do modelo de referência ..... 4
2.2 Modelo de Meta-referência para o gerenciamente de risco e conformidade na nuvem. ..... 5
2.3 Serviço de Computação em Nuvem e Perspectiva de KPI. ..... 5
2.4 Perspectiva de risco e conformidade ..... 6
2.5 Proposta de guia estruturado ..... 7
2.6 Exemplo de Sistema de Tecido em Nuvem Unificado e Seguro ..... 9
2.7 Exemplo de Método de Importação de Etiquetas de Diferentes Provedores ..... 10
2.8 Exemplo de Método de Atribuição de Espaços de Nomes ..... 10
2.9 Exemplo de Método de Propagação de uma Política para Pontos de Execução ..... 10
2.10 Exemplo de Etiqueta Normalizada ..... 11
2.11 Diagrama de Fluxo do Sistema ..... 12

3.1 Ilustração da Divisão de Responsabilidade da nuvem, Fonte: ArtBackup ..... 17
3.2 Quadrante Mágico, Fonte: Gartner (MEINARDI, 2019). ..... 20
3.3 Quadrante Mágico do Gartner para Serviços de Infraestrutura e Plataforma em Nuvem, Fonte: Gartner (CLOUD, 2023) ..... 21
3.4 Infraestrutura Global do AWS, Fonte: AWS (AWS Partner Network (APN) Blog, 2022) ..... 22
3.5 Infraestrutura Global do Microsoft Azure, Fonte: Microsoft (MARTINEKUAN, 2023) ..... 24
3.6 Infraestrutura Global do GCP, Fonte: GCP (CLOUD, 2023) ..... 26
3.7 Infraestrutura Global do GRC, Fonte: Al-Anzi (AL-ANZI; YADAV; SONI, 2014) ..... 27
3.8 Diversos modelos e padrões de governança para metas exclusivas de uma organização, Fonte: Isaca (5, 2012) ..... 29
3.9 Exemplo de *tags*, Fonte: AWS (AWS Partner Network (APN) Blog, 2022). ..... 43
3.10 *tags* criadas pelo provedor e pelo usuário, Fonte: AWS (AWS Partner Network (APN) Blog, 2022) ..... 43

4.1 Categoria Governança, Gestão de Riscos e Conformidade, Fonte: AWS (AWS, 2020) ..... 49
4.2 Implantação na Nuvem e Funções de Suporte, Fonte: AWS (AWS Partner Network (APN) Blog, 2022) ..... 50
4.3 Diagrama de processos proposto. ..... 51
4.4 Duas categorias de *tags*, Fonte: Documentação da AWS (AWS, 2022) ..... 56
4.5 Página de Resultados da pesquisa de recursos, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) ..... 57
4.6 Página de gerenciamento de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) ..... 58
4.7 Página de edição de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) ..... 58
4.8 Página de edição de *tags* de recursos selecionados, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) ..... 59

4.9 Alteração de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) 60
4.10 Valores de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022) 60
4.11 Aplicar alterações a todos os selecionados, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)..... 61
4.12 Lista de *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)..... 62
4.13 Página de edição de *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023) ..... 62
4.14 Lista com as *tags* criadas, Fonte: Learn Microsoft (MARTINEKUAN, 2023)..... 63
4.15 Editar as *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)..... 63
4.16 Lista de recursos, Fonte: Learn Microsoft (MARTINEKUAN, 2023) ..... 63
4.17 Atribuir etiquetas, Fonte: Learn Microsoft (MARTINEKUAN, 2023)..... 64
4.18 *Tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023) ..... 64
4.19 Recursos com a etiqueta ambiente: Produção, Fonte: Learn Microsoft (MARTINEKUAN, 2023) ..... 65
4.20 Aplicando políticas para *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023) ..... 65
4.21 Atribuição de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023) ..... 65
4.22 Grupo de recursos, Fonte: The Cloud Boot Camp (PEREIRA, 2023)..... 66
4.23 *Tag Name* e *Tag Value*, Fonte: The Cloud Boot Camp (PEREIRA, 2023) ..... 66
4.24 Criando a Política de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)..... 67
4.25 Erro de criação da política de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)..... 67
4.26 Estrutura de herança no Google Cloud Plataform, Fonte: GCP (CLOUD, 2023) ..... 70

# LISTA DE TABELAS

3.1 Descrição das *tags* para gerenciamento de recursos ..... 41

4.1 Descrição das *tags* para recursos na nuvem ..... 53
4.2 Comparação de *tags* entre Google, AWS e Azure ..... 56
4.3 Políticas para a marcação de recursos na nuvem ..... 68
4.4 *Tags* com foco econômico ..... 74

# LISTA DE ABREVIATURAS

Acrônimos

| | |
|---|---|
| ABNT | Associação Brasileira de Normas Técnicas |
| TI | Tecnologia da Informação |
| NIST | *National Institute of Standards and Technology* |
| AWS | *Amazon Web Service* |
| IaaS | *Infrastructure as a Service* |
| PaaS | *Plataform as a Service* |
| SaaS | *Software as a Service* |
| GCP | *Google Cloud Platform* |
| GRC | Governança, Gerenciamento de Risco e Conformidade |
| IBM | *International Business Machines Corporation* |
| DF | Distrito Federal |
| URL | *Uniform Resource Locator* |
| HTML | *HyperText Markup Language* |
| WAF | *Web Application Firewall* |
| HTTP | *Hypertext Transfer Protocol* |
| API | *Application Programming Interface* |
| TCU | Tribunal de Contas da União |
| AGU | Advocacia-Geral da União |
| KPI | Indicadores Chave de Desempenho |
| UML | Linguagem de Modelagem Unificada |
| SLA | Acordo de Nível de Serviço |
| ISE | Mecanismo de Serviços de Identidade |
| SMTP | Protocolo Simples de Transferência de Correio |
| WAN | Rede de Área Ampla |
| LDAP | Protocolo de Acesso a Diretórios Leves |
| POP3 | Protocolo dos Correios - Versão 3 |
| LGPD | Protocolo de Acesso a Diretórios Leves |
| LGPD | Lei Geral de Proteção de Dados |
| TCO | Custo Total de Propriedade |

# 1 INTRODUÇÃO

Nos últimos anos, a computação em nuvem tem sido amplamente adotada por empresas e organizações em todo o mundo, proporcionando maior flexibilidade, escalabilidade e eficiência nos serviços de TI. O surgimento deste novo modelo computacional teve um impacto significativo na indústria de Tecnologia da Informação (TI), pois as grandes organizações têm buscado estruturar seus modelos de negócios para aproveitar os benefícios dessa inovação. Além disso, empresas como Google, Amazon e Microsoft têm se empenhado em oferecer plataformas de computação em nuvem com maior poder de processamento, maior confiabilidade e melhores custos. (BARROS MAISA CRUZ BRAGA, 2012)

No entanto, com essa crescente dependência de *cloud*, desafios relacionados à gestão de risco de projetos e compliance aparecem. A gestão eficaz é fundamental para garantir que as vulnerabilidades do sistema, por exemplo, falhas de segurança, interrupções de serviços e perda de dados, sejam devidamente identificadas, avaliadas e prevenidas. Os riscos envolvem tanto aspectos técnicos, como falhas de segurança, interrupções de serviços e perda de dados, quanto considerações regulatórias e de conformidade, como a seleção do provedor, a responsabilidade pela informação e a conformidade com normas e leis aplicáveis. (JHONNYE, 2010)

Para lidar com esses riscos, é necessário implementar estratégias e metodologias adequadas. Entre elas estão a realização de avaliações completas de ameaças, a implementação de medidas de segurança e criptografia, o estabelecimento de acordos de nível de serviço (SLAs) claros com provedores de nuvem e a adoção de melhores práticas de governança de TI.

Uma outra estratégia para a gestão de risco de projetos e compliance, é a de aplicar *tags* em recursos da nuvem, pois elas funcionam como rótulos ou etiquetas que podem ser associadas a diversos elementos da infraestrutura em nuvem, como máquinas virtuais, bancos de dados e serviços. Ao atribuir etiquetas a esses recursos, as equipes de gerenciamento podem categorizá-los de acordo com projetos, departamentos ou outros critérios relevantes, facilitando a organização e o rastreamento dos ativos. (ADTSYS, 2022)

A utilização de *tags* traz benefícios significativos, destacam-se a maior visibilidade, pois é possível identificar facilmente quais recursos estão associados a um projeto específico, permitindo uma melhor análise e tomada de decisões. Além disso, os rótulos possibilitam a agilidade na alocação e realocação de recursos, otimizando o uso da nuvem e reduzindo custos operacionais. A capacidade de filtragem com base em etiquetas também agiliza o monitoramento de conformidade, permitindo que as equipes identifiquem rapidamente quais recursos estão em conformidade com as políticas estabelecidas.(CLOUD, 2017)

Nesse contexto, investir na aplicação de etiquetas em recursos da nuvem pode ser um processo que demanda um planejamento de implementação meticuloso. Diante desse cenário, a adoção de um framework especializado para auxiliar nesse processo emerge como uma escolha ideal para empresas que fazem amplo uso de recursos em nuvem em diversos contextos e projetos internos. Ao investir em um framework dedicado, as empresas podem otimizar a gestão e rastreamento de ativos, simplificando a categorização de recursos de acordo com critérios relevantes, como projetos e departamentos. Essa abordagem não apenas facilita a organização interna, mas também contribui para uma alocação mais ágil e eficiente de recursos,

resultando em benefícios operacionais tangíveis para as empresas envolvidas.

## 1.1 OBJETIVOS

Os objetivos gerais e específicos deste trabalho estão detalhados a seguir.

### 1.1.1 Objetivo Geral

Investigar, examinar e compreender a relevância das *tags* em *Cloud Computing* no contexto da gestão de riscos em projetos, bem como a avaliação do papel desempenhado por esses rótulos na garantia de conformidade com regulamentos e normas pertinentes. Identificar possíveis desafios e estratégias de controle para garantir o sucesso da implementação das tags em cloud computing. Buscando assegurar a adoção de tecnologias atualizadas e seguras, permitindo uma atualização ágil e confiável dessas etiquetas.

### 1.1.2 Objetivos Específicos

- Analisar a funcionalidade das *tags* em *Cloud Computing* e como elas podem ser aplicadas na categorização de recursos na nuvem.
- Avaliar os benefícios e desafios associados à implementação eficaz de estratégias de *tags* em ambientes de nuvem.
- Identificar os principais regulamentos e normas que afetam a gestão de dados na nuvem e como as *tags* podem ajudar na conformidade.
- Desenvolver uma proposta de framework para servir como guia estratégico e referência para as empresas.

## 1.2 JUSTIFICATIVA

A computação em nuvem é uma tecnologia em constante crescimento e evolução, desempenhando um papel fundamental na infraestrutura de TI de empresas de todos os portes. Contudo, essa adoção deve ser acompanhada de uma governança eficaz, a fim de atenuar riscos associados a projetos e garantir a conformidade das regulamentações vigentes. Assim, as inseguranças, demandas, e incertezas em relação à aplicação e gerenciamento de recursos em ambientes de nuvem, surgem como desafios a serem enfrentados pelos gestores de TI e responsáveis pela tomada de decisões nas organizações.

Logo, compreender como essas etiquetas podem ser aplicadas em ambientes de *cloud computing* é, uma vez que as organizações podem aprimorar suas práticas de gestão de riscos e conformidade, reduzindo potenciais ameaças e garantindo a integridade de seus dados. Além disso, é evidente que a utilização de *tags* em ambientes de computação em nuvem, pode oferecer uma abordagem mais eficiente e precisa na

rastreabilidade e controle dos recursos associados aos projetos, resultando em uma gestão financeira mais eficiente.

# 2 TRABALHOS RELACIONADOS

## 2.1 GESTÃO DE RISCOS E CONFORMIDADE PARA SERVIÇOS DE COMPUTAÇÃO EM NUVEM: PROJETANDO UM MODELO DE REFERÊNCIA

No artigo, Gestão de Riscos e Conformidade para Serviços de Computação em Nuvem: Projetando um Modelo de Referência, os autores exploram o potencial de transformação do setor de tecnologia pela Computação em Nuvem, destacando três principais categorias de serviços: SaaS, PaaS e IaaS. O foco está nos obstáculos e riscos associados à crescimento dos ambientes de Computação em Nuvem, especialmente nas áreas de Governança, Gerenciamento de Risco e Conformidade (GRC). Além disso, o destaca-se também os desafios relacionados aos riscos de conformidade regulatória, localização de dados e mecanismos de segurança no contexto da *Cloud*.

Portanto, os autores apresentam um modelo de referência de aplicação elaborado para auxiliar os desenvolvedores durante a fase conceitual de projetos de desenvolvimento de software. Esse modelo aborda questões essenciais concernentes ao design e desenvolvimento de referências GRC em *Cloud*, integrando perspectivas da teoria de governança de TI, incluindo Conformidade, Risco, Indicadores Chave de Desempenho (KPI) e Serviços de Computação em Nuvem. O principal objetivo do modelo é fornecer uma ferramenta eficaz para monitorar ativos de informação, identificar fatores de risco e garantir a conformidade, visando a redução de riscos por meio da detecção precoce de potenciais problemas. (MARTENS; TEUTEBERG, 2011)

Além disso, uma revisão sistemática da literatura foi realizada, e mais de 200 Serviços de Computação em Nuvem foram analisados a partir do banco de dados *CloudServiceMarket* dos autores. O banco de dados desempenhou um papel crucial na identificação e classificação de regulamentações de conformidade relevantes para a Computação em Nuvem. A análise detalhada desses serviços permitiu extrair elementos comuns, os quais foram incorporados ao modelo de referência em desenvolvimento. O processo de construção do modelo seguiu princípios, convenções e padrões bem estabelecidos na modelagem de referência, garantindo assim a qualidade do modelo resultante (MARTENS; TEUTEBERG, 2011).

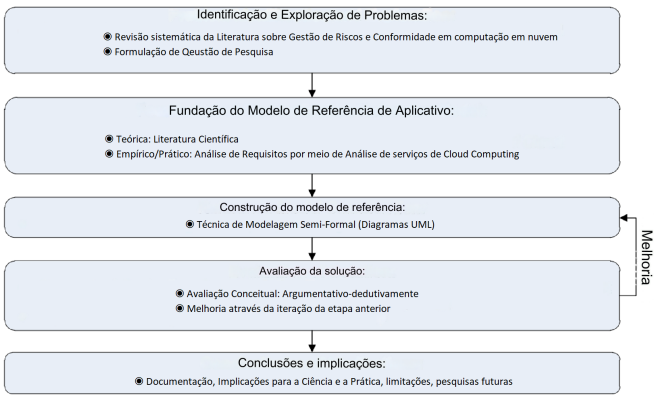


Figura 2.1: Abordagem de pesquisa subjacente para a construção do modelo de referência

Conforme mencionado anteriormente, o modelo apresentado no texto é um meta-modelo de referência projetado para estruturar o problema de aplicação e seus diversos aspectos, concentrando-se nas perspectivas de Indicadores Chave de Desempenho (KPI), Risco, Conformidade e Serviços de Computação em Nuvem. A Linguagem de Modelagem Unificada (UML) é escolhida como linguagem de modelagem, e diagramas de classes são usados para representar visualmente a estrutura estudada.

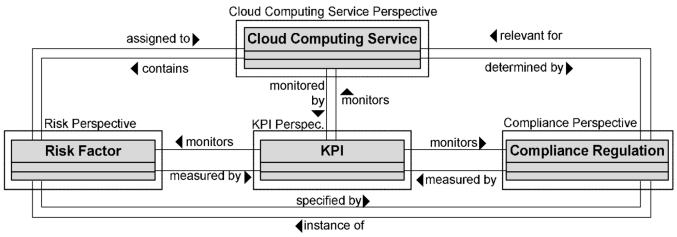


Figura 2.2: Modelo de Meta-referência para o gerenciamente de risco e conformidade na nuvem.

O meta-modelo de referência consiste em perspectivas interconectadas e, para uma melhor visualização, a estrutura foi dividida em duas figuras. A perspectiva de governança está integrada em vários componentes, incluindo processos apresentados na perspectiva de Serviços de Computação em Nuvem. O componente KPI desempenha um papel crucial ao oferecer mecanismos de monitoramento e controle para os tomadores de decisão. As perspectivas de risco e conformidade fornecem descrições detalhadas sobre os fatores de vulnerabilidade e à *compliance*, bem como esforços e resultados de auditoria.

A perspectiva de Serviços de Computação em Nuvem, situada no centro do meta-modelo de referência, abrange aspectos como SLA, processos de negócios e caracterização de serviços da Nuvem. Esta perspectiva está conectada a outras por meio de conectores, ilustrando a importância de fatores como a localização da entrega de serviço e medidas de segurança. A perspectiva de KPI desempenha um papel crucial no monitoramento do desempenho, fatores de risco e questões de conformidade, apoiando a operacionalização de medidas e objetivos estratégicos.

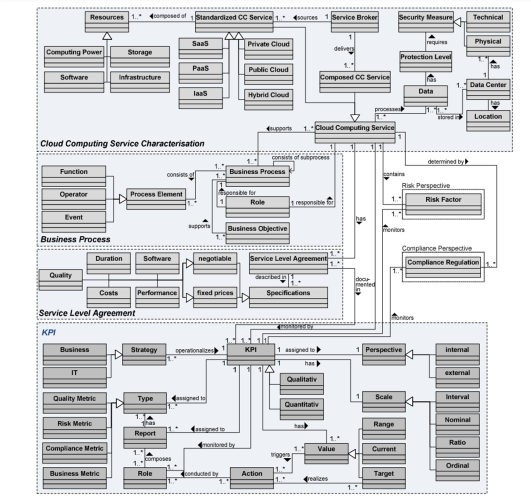


Figura 2.3: Serviço de Computação em Nuvem e Perspectiva de KPI.

Conforme ilustrado na Figura 2.4, é possível verificar vários elementos relacionados ao risco, como ati-

tude de risco, efeitos sobre ativos, documentação de risco e controles. No que diz respeito à conformidade, são considerados o nível de conformidade, auditoria e a descrição da regulamentação de conformidade. A monitorização dos fatores de risco é realizada por meio de Indicadores Chave de Desempenho (KPIs), que são especificados de acordo com as regulamentações de conformidade relevantes, onde são atribuídos aos serviços de *Cloud Computing*.

Em resumo, o texto destaca como as perspectivas de risco e conformidade são abordadas no contexto de *Cloud*, utilizando elementos como posicionamento de risco, efeitos sobre ativos, documentação de risco, controles, nível de conformidade, auditoria e regulamentação de conformidade, monitorados por meio de KPIs específicos. O texto conclui destacando a importância do processamento externo de dados, distinguindo entre a transferência de operações e o processamento de dados encomendado no contexto das leis de proteção de dados. A proposta apresentada no artigo constitui uma fundamentação sólida para a implementação de um sistema de rastreamento de recursos em ambientes de nuvem, servindo como um modelo referencial. No entanto, carece de orientações específicas sobre a metodologia de implementação e os elementos concretos a serem incorporados para viabilizar a análise efetiva dos recursos.

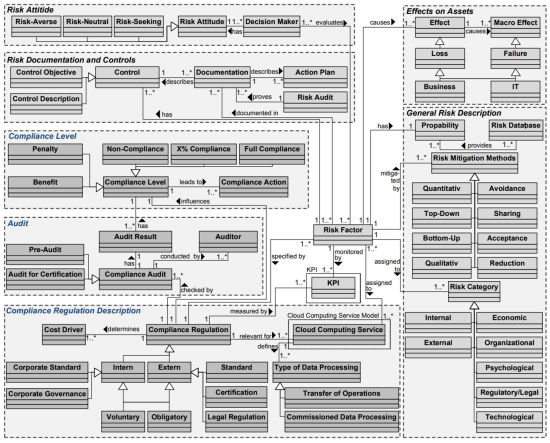


Figura 2.4: Perspectiva de risco e conformidade

## 2.2 IMPLEMENTANDO UMA ESTRATÉGIA DE MARCAÇÃO PARA *CLOUD* IAAS E PAAS

No artigo "*Implementing a Tagging Strategy for cloud IaaS and PaaS*", a gestão de metadados de recursos desempenha um papel fundamental na viabilização da governança de custos, controle de acesso e automação de serviços em ambientes de nuvem e operações de carga de trabalho. O framework de orientação do artigo, ajuda os profissionais técnicos de TI a definir e implementar com sucesso uma estratégia de marcação (tagging) para infraestrutura e plataformas como serviço (IaaS e PaaS) em nuvem. As principais conclusões abrangem a relevância das *tags* como um elemento essencial na estrutura de governança, os desafios comuns enfrentados em iniciativas de marcação e a evolução do suporte para *tags* nos principais provedores de nuvem como AWS, Azure e GCP.

É considerado que, empresas que alcançam êxito desenvolvem uma atmosfera de colaboração entre os

utilizadores de serviços em nuvem, atribuindo aos próprios usuários a responsabilidade pela marcação, ao passo que a equipe de governança desempenha predominantemente um papel de apoio. O artigo oferece recomendações para equipes de governança em nuvem, destacando a necessidade de desenvolver uma estratégia de marcação, estabelecer metas e utilizar a automação para facilitar a implementação consistente das etiquetas. O problema destacado é a complexidade no gerenciamento de *tags*, a baixa percepção de valor e a imaturidade das capacidades nativas dos provedores de nuvem. A pesquisa visa ajudar as organizações a superar esses desafios e ter sucesso em suas iniciativas de marcação. (MEINARDI, 2019)

Assim, a abordagem da Gartner para a implementação de estratégias de marcação difere das orientações comuns ao defender um framework estruturado que vai além de fornecer apenas uma lista de *tags* sugeridas. A Gartner recomenda um método que se concentra em maximizar o valor da marcação por meio de uma implementação consistente, garantindo conformidade e minimizando interrupções e resistências internas.(MEINARDI, 2019)

Um guia estruturado composto por quatro passos principais: definição, auditoria, automação e implementação é ilustrado na Figura 2.5.

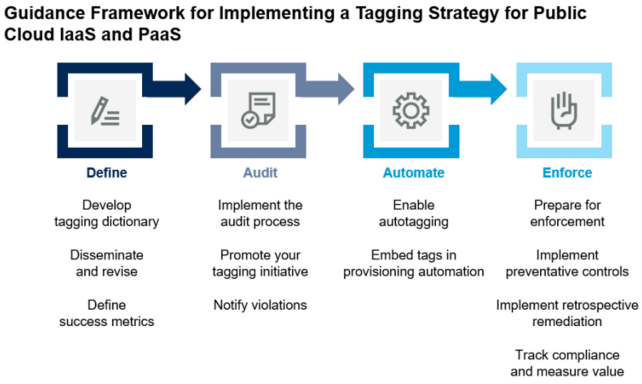


Figura 2.5: Proposta de guia estruturado

Como é mostrado, o framework sugere ações específicas, que vão desde a definição inicial das *tags* até a etapa final de aplicação, com o objetivo de incentivar a marcação e minimizar as cargas administrativas.

No artigo é destacado a importância de as organizações realizarem um trabalho preliminar em quatro áreas principais para garantir uma aplicação eficaz de metadados. Primeiramente, destaca a necessidade de definir metas e casos de uso para marcação, abrangendo áreas como alocação de custos, controle de acesso e automação. Em seguida, sugere a atribuição de responsabilidades e identificação de partes interessadas, recomendando a criação de um "Centro de Excelência em Nuvem"para colaboração entre equipes. Além disso, enfatiza a avaliação das capacidades de marcação oferecidas pelos provedores de nuvem, incentivando o uso independente de *tags* para flexibilidade. Por fim, ressalta a importância de considerar as diferenças entre provedores de nuvem ao desenvolver uma estratégia de marcação, incentivando uma abordagem multicloud desde o início e identificando desafios potenciais, como erros de entrada e gerenciamento de permissões. Esses desafios são destacados como considerações cruciais para organizações antes de iniciar a implementação da estratégia de marcação proposta.

Na Etapa 1 - Definir, é crucial criar um dicionário de marcação, identificando *tags* para atingir os obje-

tivos da iniciativa. Isso gera uma lista de chaves e valores acordados, disseminada pela organização para os usuários responsáveis pelo provisionamento de serviços em nuvem. O compartilhamento ocorre por meio de ferramentas de colaboração, com feedback coletado para melhorar as definições. Na mesma etapa, são estabelecidas métricas de sucesso, incluindo indicadores de conformidade e um "índice de conformidade de marcação", garantindo progresso consistente e mitigando riscos na implementação da estratégia.

Na Etapa 2 - Auditoria, a equipe encarregada da estratégia de marcação, possivelmente o CCOE, realiza uma auditoria na configuração dos recursos em nuvem, garantindo conformidade com as *tags* acordadas. Colaborando com a equipe de operações de TI ou segurança, essa etapa estabelece um processo contínuo de auditoria, utilizando ferramentas existentes. A auditoria verifica a conformidade das *tags* em relação ao dicionário de marcação, com notificações configuradas para violações. Por fim, a etapa é concluída com notificações de violações, seguindo uma abordagem de "remediação suave"para conscientizar e orientar os usuários. O objetivo é estabelecer visibilidade para monitorar a aderência às diretrizes de marcação, preparando o terreno para controles programáticos na próxima etapa, com o progresso e a conscientização dos usuários sendo cruciais para o sucesso da iniciativa.

Na Etapa 3 - Automatização, o foco é simplificar a implementação de *tags* por meio da automação, reduzindo a percepção de carga administrativa. A automação visa implementar *tags* automaticamente sempre que possível, abordando essa preocupação. A "Habilitação da Marcação Automática"busca implementar *tags* automaticamente, como identificar o usuário criador de um recurso através da API de auditoria em nuvem. Os principais provedores de nuvem oferecem capacidades de autotagging. A "Incorporação de *tags* na Automação do Provisionamento"destaca a integração de *tags* em ferramentas de provisionamento, sendo crucial para melhorar a conformidade de recursos existentes. O trabalho evidencia a importância da automação para o sucesso da iniciativa de marcação, alertando contra a exclusão completa desta etapa, mesmo que a conclusão total da estratégia de automação possa ser gradual.

Na Etapa 4 - Aplicar, a implementação programática das diretrizes de marcação é essencial, envolvendo políticas preventivas e retrospectivas. Antes de começar, é crucial garantir autoridade para medidas corretivas e formar uma equipe de suporte. A comunicação interna é vital para destacar a natureza disruptiva da abordagem. As medidas preventivas configuram ferramentas de provisionamento para verificar solicitações e negar as não conformes. A conformidade retrospectiva é implementada para garantir o uso de todas as *tags* em todos os recursos. Alternativas de correção "dura"são discutidas, incluindo a exclusão rápida de recursos não conformes. O rastreamento contínuo da conformidade e a medição do valor real das *tags* são enfatizados, com ênfase nas métricas de sucesso. O texto alerta contra implementação prematura, destacando a importância de suavizar o impacto antes de aplicar medidas programáticas. O sucesso envolve obter autoridade, preparar a organização e atingir metas para a conformidade de marcação.

Após a implementação do framework proposto, que estabelece uma estratégia de marcação, é necessário realizar um acompanhamento para melhorar a eficácia da estratégia. Algumas áreas de melhoria incluem monitorar falhas em solicitações de provisionamento e correções difíceis devido a violações de políticas de marcação, padronizar o processo de lidar com exceções, consolidar a estratégia de automação, evoluir a estratégia para garantir valores corretos de *tags* e destacar o valor da marcação. Adverte contra pular partes ou não completar cada etapa do framework, enfatizando a necessidade de aplicar medidas programáticas, automação e soft enforcement para garantir o sucesso da estratégia de marcação.

## 2.3 A AGREGAÇÃO DE *TAGS* EM NUVENS PÚBLICAS/PRIVADAS

Empresas que utilizam diversas nuvens públicas ou privadas enfrentam o desafio de organizar máquinas em grupos através de etiquetas. Assim, segundo Louis, é importante padronizar identificações em um espaço compartilhado, permitindo a transferência eficiente de etiquetas e regras entre nuvens e sistemas. As técnicas propostas resolvem o desafio ao permitir o uso de etiquetas nativas em diversas nuvens, padronizando grupos e regras para garantir uma aplicação eficiente e compatível, independentemente da nuvem, região ou endereço IP. (LOUIS, 2023)

Entende-se que, é uma prática comum as empresas que utilizam várias nuvens públicas ou privadas costumam organizar suas máquinas físicas ou virtuais em grupos identificados por meio de *tags*. Essas etiquetas são essenciais para usuários e serviços, pois ajudam a controlar o tráfego entre diferentes grupos, estabelecendo contratos específicos. No entanto, surge um desafio quando cada contrato é exclusivo para uma nuvem específica.

Para manter uma política consistente em diferentes nuvens, é crucial contar com um método que padronize essas identificações em um espaço de endereços compartilhado e permita a transferência eficaz de *tags* e regras entre nuvens e sistemas. Sem esse método, cada conjunto de marcadores e regras permanece válido apenas dentro da nuvem para a qual foi criado. Isso complica e prolonga a transferência de cargas de trabalho entre provedores de nuvem, pois é necessário recriar equivalentes na nuvem de destino.

As técnicas apresentadas oferecem uma solução ao permitir o uso de construções integradas de etiquetagem em diferentes ambientes de nuvem. Ao mesmo tempo, possibilitam a normalização de grupos e regras, garantindo uma aplicação eficaz que seja independente de nuvem, região ou endereço IP. O objetivo dessas técnicas é estabelecer um padrão para as *tags*, uniformizar o espaço de endereços e facilitar a propagação de *tags* e regras entre diferentes nuvens e sistemas, promovendo assim uma aplicação eficiente e compatíveis entre diferentes nuvens e sistemas.

A Figura 2.6, que foi apresentada em (LOUIS, 2023), é um diagrama que mostra um sistema seguro de nuvem. Esse sistema organiza etiquetas de diferentes empresas de nuvem de uma maneira especial, usando números de até 64 bits. Esses números podem ser usados como etiquetas em diferentes empresas de nuvem.

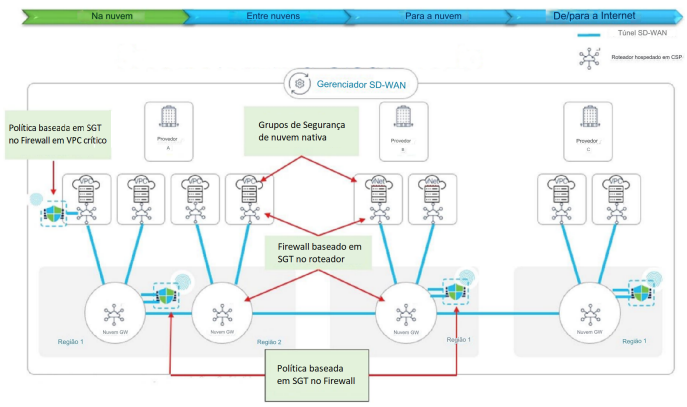


Figura 2.6: Exemplo de Sistema de Tecido em Nuvem Unificado e Seguro

No contexto apresentado, as metodologias visam facilitar a integração de identificações provenientes de várias empresas. Isso é alcançado ao designar nomes especiais para os fornecedores, regiões e/ou serviços, e incorporar esses nomes a um sistema de regras unificado. O Identity Service Engine (ISE) é utilizado para distribuir esses nomes especiais de volta para uma solução de Rede de Área Ampla Definida por Software (SD-WAN) e para os locais onde as atividades ocorrem (pontos de aplicação).

A Figura 2.7, abaixo, é um diagrama de fluxo ilustrando um método de importação de *tags* de diferentes provedores.

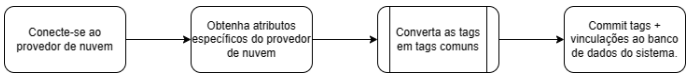


Figura 2.7: Exemplo de Método de Importação de Etiquetas de Diferentes Provedores

Figura 2.8, abaixo, é um diagrama de fluxo de um método de atribuição de espaços de nomes para provedores, regiões e/ou serviços.

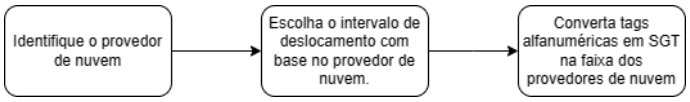


Figura 2.8: Exemplo de Método de Atribuição de Espaços de Nomes

A Figura 2.9, abaixo, é um diagrama de fluxo que ilustra um método de propagar uma política para os pontos de execução.

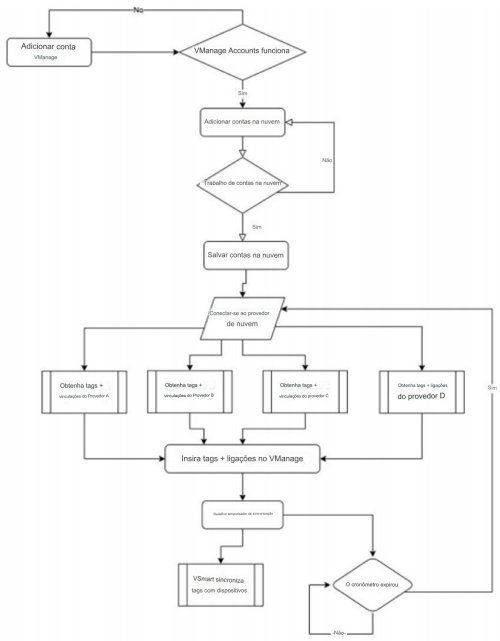


Figura 2.9: Exemplo de Método de Propagação de uma Política para Pontos de Execução

Conforme ilustrado na Figura 2.9, os *namespaces* dos provedores, regiões e/ou serviços são fornecidos a um mecanismo de política comum, sendo encaminhados para um conjunto de regras compreendido por

todos, como um "ISE". Esse conjunto de regras (ISE) então faz com que esses nomes especiais voltem para um sistema que gerencia como as redes funcionam (SD-WAN). Um gerenciador de SD-WAN é utilizado para propagar a política para pontos de execução (por exemplo, roteadores, switches, firewalls e/ou gateways), ou seja, para garantir que tudo funcione bem, utiliza-se um gerenciador especial para disseminar essas regras para esses locais importantes.

A figura 2.10 é um exemplo de etiqueta normalizada, conforme descrito nas técnicas apresentadas pelo artigo (LOUIS, 2023).

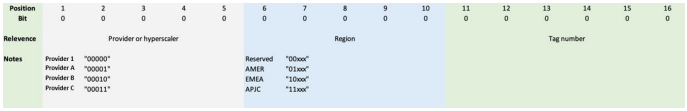


Figura 2.10: Exemplo de Etiqueta Normalizada

Em resumo, as abordagens delineadas neste contexto capacitam as organizações a progredirem em sua trajetória de digitalização, possibilitando a utilização de diversas nuvens e a transferência mais ágil de cargas de trabalho entre esses ambientes. As técnicas descritas promovem a interoperabilidade, viabilizando que um serviço transite entre nuvens com maior flexibilidade, agilidade na introdução no mercado e reforço na segurança mediante a implementação de políticas mais simplificadas em ambientes multicloud e com diferentes provedores.

## 2.4 UMA SOLUÇÃO DE RASTREAMENTO PARA GERENCIAMENTO DE ATIVOS E RECURSOS DE TI

Gerenciar os ativos de tecnologia da informação (TI) é como fazer uma lista de tudo que uma empresa possui em termos de tecnologia, proporcionando um quadro estruturado para o planejamento de investimentos. Como a tecnologia é cada vez mais importante para o funcionamento das empresas, o modo como é realizado a gestão de ativos, abrangendo diversas áreas, é muitas vezes manual e suscetível a erros. Portanto, zelar adequadamente por esses ativos de TI é fundamental para o sucesso de uma empresa na era digital, tornando-os a espinha dorsal do negócio. (DUTTA; SARKER, 2022)

A gestão eficiente de ativos de TI ajuda a reduzir custos e tempo, evitando compras desnecessárias e garantindo a segurança das informações, o que configura um desafio complexo. Sistemas de rastreamento de ativos de TI facilitam a supervisão construtiva, enquanto políticas claras devem ser estabelecidas para lidar com informações essenciais e sensíveis. O gerenciamento de hardware é uma parte integrante do gerenciamento de ativos, abrangendo desde a aquisição até a manutenção e descarte.

Além disso, ativos com informações e licenças digitais podem ser gerenciados de acordo com normas como a ISO 27001, que define requisitos para um Sistema de Gerenciamento de Segurança da Informação (ISMS). A ISO 27001 abrange ativos físicos e lógicos, fornecendo orientações abrangentes sobre a gestão de ativos para as organizações. Portanto, o modelo do sistema proposto no artigo, (DUTTA, 2022), em duas máquinas virtuais: uma para o Gerenciamento de Ativos e outra para o Controlador de Domínio.

A primeira utiliza o sistema operacional Linux CentOS 7 e dependências como o LAMP stack (Linux,

Apache, MariaDB e PHP) para criar um aplicativo de gerenciamento de ativos baseado na web. A instalação envolve a configuração do ambiente, download do aplicativo Snipe-IT, criação de um Virtual Host e configuração do banco de dados.

A segunda máquina virtual utiliza o Windows Server 2008 R2 para criar um Controlador de Domínio do Active Directory. Isso é necessário para rastrear os ativos atribuídos a usuários em uma organização, facilitando o monitoramento de check-ins e check-outs. O processo inclui a instalação do Windows Server, ativação dos recursos do Active Directory e criação de usuários por departamento.

O diagrama de fluxo do sistema, apresentado na Figura 2.11, ilustra o processo de trabalho do Sistema de Gerenciamento de Inventário de Ativos (DUTTA; SARKER, 2022). O fluxo inicia com a abertura do site, exibindo a página de login. Os usuários registrados inserem seu nome de usuário e senha; se as credenciais não corresponderem aos registros do banco de dados, o acesso é negado, solicitando que o usuário faça login novamente ou entre em contato com o administrador do sistema. Com credenciais válidas, o usuário é concedido acesso ao sistema, avançando para o Menu Principal. A partir deste menu, os usuários podem realizar diversas atividades, como registrar ativos, rastrear ativos e gerar relatórios, de acordo com suas permissões. Após a conclusão bem-sucedida das operações, os usuários podem fazer logout do sistema.

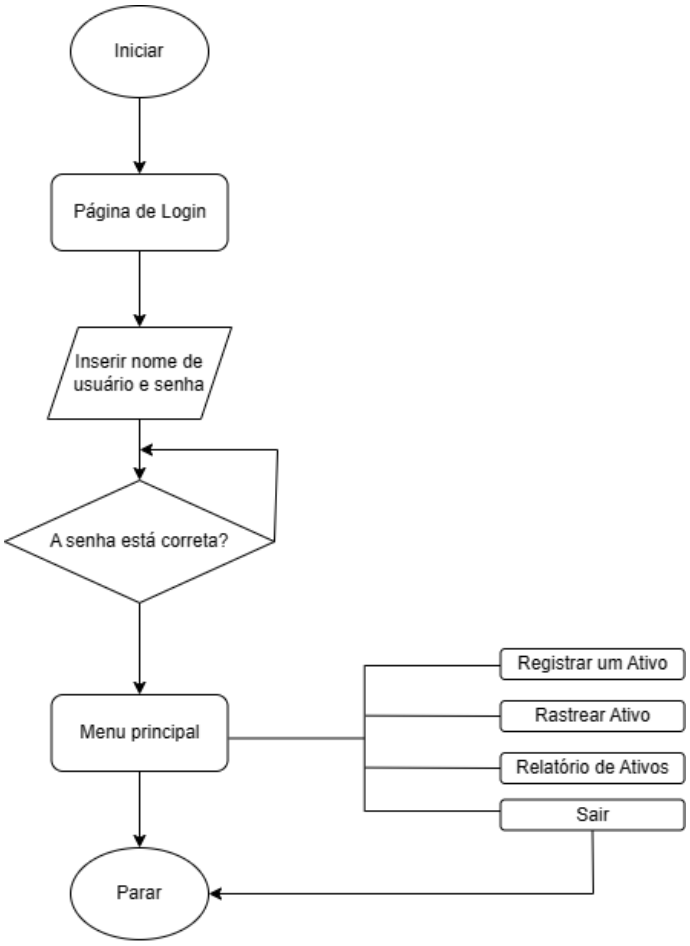


Figura 2.11: Diagrama de Fluxo do Sistema

Na implementação do sistema, destaca-se a integração LDAP (Protocolo de Acesso Leve a Diretórios) para sincronizar usuários do servidor Microsoft Windows para o sistema Linux. O servidor LDAP é configurado como um servidor Active Directory, garantindo a autenticação e autorização adequadas. O processo é detalhado, envolvendo a verificação da configuração do servidor LDAP, a sincronização com o servidor AD e a codificação bem-sucedida das credenciais.

Além disso, a integração de e-mail é realizada usando o servidor SMTP Postfix, que é rápido e amplamente utilizado. O Postfix é instalado e configurado para encaminhar e-mails localmente ou para destinos externos. O Dovecot, servidor IMAP e POP3, é instalado para lidar com e-mails de saída e entrada. A configuração detalhada inclui a edição de arquivos de configuração, desativação da autenticação em texto simples e garantia de autenticação criptografada.

Para enviar e-mails a partir de uma plataforma web (webmail), é instalado o Squirrelmail, um cliente web PHP. A configuração do Squirrelmail envolve ajustes no arquivo de configuração do Apache e a garantia de acesso ao webmail. O processo de instalação do Squirrelmail é simplificado, proporcionando uma solução completa para integração de e-mail no sistema.

Na seção de operação funcional do sistema, diversas etapas essenciais são destacadas, incluindo a criação de modelos de ativos, conjuntos de campos, fornecedores e ativos, além do gerenciamento de licenças. Na criação de modelos de ativos, são configurados modelos com campos personalizados, visando detalhes como nome, fabricante, categoria, número do modelo e depreciação. Campos específicos são definidos para facilitar a identificação e organização dos ativos. A criação de conjuntos de campos abrange especificações para diferentes tipos de ativos, associando detalhes como memória, disco rígido e sistema operacional. A seção de fornecedores registra informações cruciais, gerando relatórios de confirmação de preço unitário para uma visualização clara dos custos. A criação de ativos específicos considera informações de faturamento, memória, sistema operacional, entre outros, com sincronização facilitada com o Active Directory. Recursos como busca e clonagem agilizam a criação de novos ativos. No gerenciamento de licenças, são registradas informações detalhadas, categorizadas em períodos anuais, periódicos ou perpétuos para facilitar o acompanhamento. A associação de responsáveis otimiza a comunicação e organização nessas área, tornando uma solução abrangente para o gerenciamento eficiente de ativos, desde a criação de modelos até o monitoramento de licenças e fornecedores. (DUTTA; SARKER, 2022)

Na análise de desempenho, destaca-se a eficácia do sistema em gerenciar ativos, abrangendo a verificação de e-mail e a conformidade com o padrão ISO 27001. No processo de verificação de e-mail, a alocação de ativos gera notificações no sistema de webmail do Linux, facilitando o *check-out* e a associação de ativos a usuários por meio de integração com o Active Directory. A notificação é enviada ao usuário via e-mail, permitindo a aceitação do ativo por meio de um link fornecido na mensagem. Quanto à conformidade com o ISO 27001, a implementação do IT Asset Management System (ITAMS) visa atender aos requisitos, abrangendo ativos que vão além de hardware e software. O sistema facilita a criação de um inventário, priorizando e filtrando ativos de acordo com as necessidades organizacionais. A conformidade é alcançada por meio de uma gestão adequada do inventário, assegurando estabilidade, segurança da informação, categorização apropriada e gestão eficaz de licenças e certificados. Essas análises destacam a eficácia do sistema em todo o processo, desde a alocação de ativos até a conformidade com padrões de segurança internacionais.

Portanto, o Gerenciamento de Inventário de TI é uma plataforma crucial que permite a uma organização monitorar seus aplicativos, software, hardware e outros recursos, proporcionando respostas detalhadas sobre data de aquisição, custo, uso por usuários, responsáveis e outras informações precisas. Essa abordagem é essencial para uma instituição, e a solução proposta no trabalho de (Dutta,2022) oferece uma gestão eficiente e abrangente desses ativos, alinhando os requisitos tecnológicos com as metas organizacionais. O objetivo principal dessa proposta é economizar recursos, proporcionar controle sobre o ambiente de TI da organização, garantir organização no ciclo de vida de TI e reduzir o desperdício por meio do gerenciamento adequado da disposição de ativos de TI. (DUTTA; SARKER, 2022)

# 3 FUNDAMENTAÇÃO TEÓRICA

## 3.1 COMPUTAÇÃO EM NUVEM

A computação em nuvem é como uma revolução no mundo da tecnologia da informação, mas a ideia por trás dela já tinha sido pensada há muito tempo. Em 1961, John McCarthy teve uma visão de que a computação poderia se tornar algo tão comum quanto usar eletricidade ou água. (DOUGLAS, 1966)

### 3.1.1 Definições e Conceitos

A computação em nuvem, também conhecida como *cloud computing*, é um termo que tem ganhado destaque nas últimas décadas devido aos avanços na tecnologia da informação e comunicação. O seu conceito básico envolve o fornecimento de serviços e recursos de TI por meio da internet, permitindo o acesso sob demanda a uma ampla gama de recursos configuráveis, como servidores, armazenamento, aplicativos e serviços (SURBIRYALA; RONG, 2019).

Quando se aborda a definição de *cloud computing*, a descrição mais amplamente reconhecida, é aquela estabelecida pelo National Institute of Standards and Technology (NIST), a qual afirma:

> "A computação em nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda a uma pool compartilhada de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser provisionados e liberados rapidamente com esforço mínimo de gerenciamento ou interação com o provedor de serviços."(MELL; GRANCE, 2011)

Já a Associação Brasileira de Normas e Técnicas (ABNT) traduziu o conceito de Computação em Nuvem criado pela International Organization for Standardization (ISO) como:

> "Um paradigma para habilitar o acesso, via rede, a um grupo escalável e elástico de recursos, físicos ou virtuais, com autoprovisionamento e administração sob demanda".(ABNT, 2016)

Hoje em dia, organizações como Oracle, Microsoft, Amazon e Google são alguns dos principais provedores de serviços em nuvem, oferecendo uma ampla gama de soluções para atender às variadas necessidades das empresas. A escalabilidade e a capacidade de se adaptar rapidamente às mudanças nas necessidades das empresas são características que tornam a computação em nuvem uma escolha estratégica (WERFF et al., 2019).

A computação em nuvem é um paradigma tecnológico que oferece diversas características essenciais que, conforme o Instituto Nacional de Padrões e Tecnologia (NIST) (MELL; GRANCE, 2011), temos:

- Autoatendimento sob Demanda: A capacidade de provisionar recursos computacionais de forma unilateral, sem a necessidade de interação humana com o provedor de serviços. Os usuários podem adquirir recursos, como tempo de processamento e armazenamento em rede, de maneira automática e conveniente, de acordo com suas necessidades .
- Amplo Acesso à Rede: Os recursos e serviços da computação em nuvem estão disponíveis na rede e podem ser acessados por uma variedade de dispositivos, sejam telefones celulares ou laptops, desde

que tenham acesso à Internet. Isso proporciona flexibilidade e mobilidade aos usuários .

- Agrupamento de Recursos: Os provedores de serviços em nuvem organizam seus recursos em um pool para atender a múltiplos usuários, utilizando um modelo multi-inquilino. Isso permite que os recursos físicos e virtuais sejam atribuídos dinamicamente de acordo com a demanda dos consumidores, oferecendo independência de localização .
- Elasticidade Rápida: Os recursos podem ser escalados para cima ou para baixo de forma rápida e automática, de acordo com as necessidades dos usuários. Isso proporciona a sensação de que os recursos disponíveis são praticamente ilimitados e podem ser ajustados a qualquer momento.
- Serviços Mensuráveis: Os sistemas em nuvem monitoram e otimizam automaticamente o uso de recursos, utilizando mecanismos de medição adequados ao tipo de serviço. Isso permite a transparência tanto para o provedor quanto para o usuário em relação ao uso de recursos e facilita a cobrança com base no uso efetivo.

Essas características tornam a computação em nuvem uma solução flexível, escalável e eficiente para atender às necessidades de empresas e usuários finais em todo o mundo.

### 3.1.2 Modelos de Serviço em Nuvem

Os modelos de serviços em nuvem, como definidos por Mell e Grance (VERAS, 2012; MELL, GRACE, 2011), representam uma evolução fundamental na forma como as organizações consomem recursos de tecnologia da informação (TI). Esses modelos descrevem como os serviços são disponibilizados aos consumidores, abordando diferentes níveis de abstração computacional e responsabilidades compartilhadas entre os provedores de serviços em nuvem e os usuários. Os três principais modelos de serviço são Software como um Serviço (SaaS), Plataforma como um Serviço (PaaS) e Infraestrutura como um Serviço (IaaS). (FEDOSEENKO, 2018)

#### 3.1.2.1 Software as a Service (SaaS)

O SaaS é um modelo de serviço que oferece aplicações de software hospedadas na infraestrutura de nuvem e disponíveis para os consumidores via diversos dispositivos, como navegadores da web ou software cliente. O usuário não precisa gerenciar a infraestrutura subjacente, incluindo servidores, sistemas operacionais e armazenamento. A única exceção pode ser configurações específicas de aplicativos para usuários individuais. Esse modelo é altamente conveniente, pois os usuários podem acessar aplicativos de qualquer lugar com uma conexão à Internet. Exemplos de serviços SaaS incluem Salesforce e o Google Docs.

#### 3.1.2.2 Platform as a Service (PaaS)

O modelo PaaS fornece aos usuários uma plataforma de desenvolvimento baseada na nuvem, onde eles podem criar, testar, executar e gerenciar aplicativos. Isso elimina a necessidade de se preocupar com a

infraestrutura subjacente, como servidores e sistemas operacionais. Os provedores PaaS oferecem linguagens de programação, bibliotecas e ferramentas de desenvolvimento, permitindo que os desenvolvedores se concentrem na criação de aplicativos em vez de gerenciar a infraestrutura. Além disso, os usuários têm controle sobre as aplicações implantadas e possíveis configurações do ambiente de hospedagem. Exemplos de serviços PaaS incluem o Google App Engine e o Microsoft Azure.

#### 3.1.2.3 Infrastructure as a Service (IaaS)

O IaaS é a camada mais fundamental dos modelos de serviço em nuvem. Ele fornece aos usuários recursos de computação fundamentais, como processamento, armazenamento e rede, que podem ser usados para implantar sistemas operacionais e aplicativos. Nesse modelo, os usuários têm um maior controle sobre a infraestrutura, incluindo sistemas operacionais e aplicativos, mas não precisam se preocupar com a gestão da infraestrutura subjacente, como servidores físicos e dispositivos de rede. Os serviços IaaS são altamente escaláveis, permitindo que os usuários aumentem ou diminuam seus recursos de acordo com as necessidades, pagando apenas pelo que usam. Exemplos de serviços IaaS incluem a *Amazon Elastic Compute Cloud (EC2)* e o *Eucalyptus*. Esses modelos de serviços em nuvem representam uma evolução das formas tradicionais de fornecimento de recursos de TI, como a gestão de data centers locais ou o uso de provedores de hospedagem. Com a migração para a nuvem, a responsabilidade e o custo total de propriedade (TCO) são transferidos dos clientes para os provedores de serviços, aliviando as organizações das preocupações com a manutenção, atualização e operação de equipamentos de TI.

A figura 3.1, ilustra como a divisão de responsabilidades varia entre os modelos de serviço em nuvem, com os consumidores assumindo diferentes níveis de controle sobre a infraestrutura:

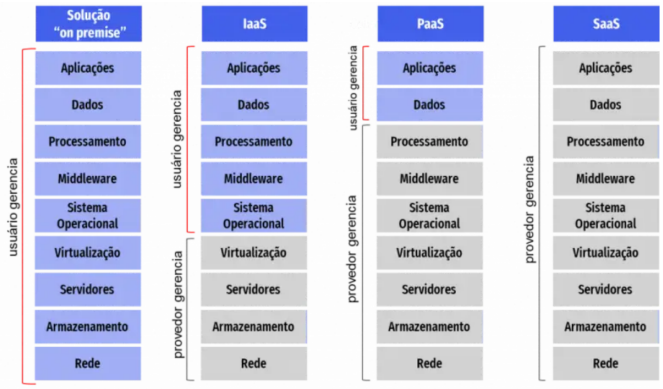


Figura 3.1: Ilustração da Divisão de Responsabilidade da nuvem, Fonte: ArtBackup

Em resumo, os modelos de serviço em nuvem revolucionaram a forma como as organizações consomem recursos de TI, oferecendo maior flexibilidade, escalabilidade e conveniência. Os consumidores podem escolher o modelo que melhor atende às suas necessidades e se beneficiar da transferência de responsabilidades e custos para os provedores de serviços em nuvem.

### 3.1.3 Modelos de Implementação em Nuvem

A computação em nuvem, uma tecnologia revolucionária que transformou a maneira como as empresas e organizações gerenciam e acessam recursos de TI, oferece uma série de modelos de implantação para atender às diversas necessidades dos consumidores. Esses modelos são definidos com base no público consumidor dos serviços e na localização dos recursos de computação em nuvem. Neste artigo, exploraremos em detalhes os quatro principais modelos de implantação de acordo com o NIST (Instituto Nacional de Padrões e Tecnologia) e outras fontes de referência. (MELL; GRANCE, 2011) - (SURBIRYALA; RONG, 2019)

#### 3.1.3.1 Nuvem Privada

A nuvem privada é um dos modelos de implantação de computação em nuvem e é definida como uma infraestrutura de nuvem provisionada para uso exclusivo de uma única organização. Isso significa que todos os recursos, como servidores, armazenamento e aplicativos, são dedicados exclusivamente a essa organização. Há várias características distintivas desse modelo:

- Controle Total: Na nuvem privada, a organização tem total controle sobre sua infraestrutura de TI. Isso permite personalização e configuração de acordo com as necessidades específicas da organização.
- Segurança Aprimorada: A natureza dedicada dos recursos torna a nuvem privada altamente segura, pois os dados não são compartilhados com outras entidades. Isso é especialmente importante para organizações que lidam com informações sensíveis.
- Escalabilidade Controlada: Embora os recursos sejam dedicados, a nuvem privada ainda oferece escalabilidade, permitindo que a organização dimensione sua infraestrutura conforme necessário.
- Baixa Latência: A infraestrutura da nuvem privada está localizada nas instalações da organização ou em um ambiente protegido, o que resulta em baixa latência de rede.

A nuvem privada é frequentemente a escolha preferida para organizações que precisam manter o controle total sobre seus recursos e dados, especialmente aquelas que operam em setores que têm regulamentações rigorosas de segurança e conformidade.

#### 3.1.3.2 Nuvem Pública

A nuvem pública é o oposto da nuvem privada, pois fornece infraestrutura de recursos e serviços de computação em nuvem para uso aberto pelo público em geral. Essa infraestrutura é de propriedade, gerenciada e operada por provedores de serviços de nuvem. As principais características da nuvem pública incluem:

- Compartilhamento de Recursos: Na nuvem pública, os recursos são compartilhados entre diversos

clientes. Isso resulta em economia de custos, pois as despesas são compartilhadas entre muitos usuários.

- Escalabilidade Ilimitada: A nuvem pública é altamente escalável, permitindo que as organizações acessem recursos adicionais conforme necessário, sem investimentos significativos em infraestrutura.
- Manutenção Terceirizada: Os provedores de serviços de nuvem são responsáveis pela manutenção e gerenciamento da infraestrutura, o que alivia as organizações dessas tarefas.
- Confiabilidade: Devido à grande quantidade de recursos, a nuvem pública oferece alta confiabilidade e redundância, reduzindo os riscos de falhas.

A nuvem pública é atraente para empresas de todos os tamanhos, especialmente aquelas que desejam reduzir custos operacionais, acessar recursos facilmente escaláveis e não desejam gerenciar a infraestrutura internamente.

#### 3.1.3.3 Nuvem Híbrida

O modelo de nuvem híbrida é uma composição de duas ou mais infraestruturas de nuvem distintas, que podem ser privadas, públicas ou comunitárias. Essas infraestruturas permanecem como entidades exclusivas, mas são unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos. As principais vantagens da nuvem híbrida incluem:

- Controle e Flexibilidade: A organização pode escolher quais cargas de trabalho e dados são mantidos internamente na nuvem privada e quais são movidos para a nuvem pública, proporcionando um alto nível de controle e flexibilidade.
- Reaproveitamento de Investimentos: As empresas podem aproveitar os investimentos já feitos em infraestrutura local, evitando a necessidade de migrar todos os recursos para um provedor de nuvem.
- Custo-Benefício: A nuvem híbrida permite que as organizações usem recursos de nuvem pública apenas quando necessário, pagando conforme o uso, o que pode resultar em economia de custos.
- Maior Segurança para Dados Críticos: Dados críticos podem ser mantidos localmente na nuvem privada, oferecendo maior segurança e controle.

A nuvem híbrida é uma opção popular para empresas que desejam combinar o melhor dos dois mundos: a flexibilidade da nuvem pública e o controle da nuvem privada.

#### 3.1.3.4 Nuvem Comunitária

A nuvem comunitária é definida como uma infraestrutura de nuvem compartilhada por diferentes organizações que têm interesses e requisitos comuns, como missão, segurança, políticas e conformidade. As principais características da nuvem comunitária incluem:

- Compartilhamento de Recursos Financeiros: Os custos da nuvem comunitária são compartilhados entre as organizações participantes, resultando em economia de recursos financeiros.
- Economia de Recursos como Energia e Resfriamento: Uma infraestrutura compartilhada diminui o custo de energia e resfriamento, uma vez que vários usuários compartilham o mesmo ambiente.
- Maior Investimento Conjunto: As organizações podem se beneficiar do poder de compra coletiva, adquirindo recursos computacionais de alta qualidade a preços acessíveis.

A nuvem comunitária é uma escolha adequada quando várias organizações colaborativas precisam armazenar e compartilhar dados e funcionalidades em um ambiente compartilhado.

### 3.1.4 Principais provedores

Os provedores de nuvem pública adotam a virtualização de sua infraestrutura, plataforma e aplicações a partir de hardware proprietário, oferecendo serviços e recursos a múltiplos clientes simultaneamente através da Internet (HAT, 2021). Assim, oferecem serviços em nuvem para o público em geral, disponibilizando armazenamento e processamento a preços acessíveis.

Anualmente, o Instituto Gartner (MEINARDI, 2019) conduz estudos em diferentes mercados para avaliar o desempenho das principais empresas em suas áreas de atuação. O "Quadrante Mágico" é um relatório anual que resume esses estudos, destacando as empresas líderes, visionárias, concorrentes de nicho e desafiantes em um determinado mercado, conforme ilustrado na Figura 3.2:

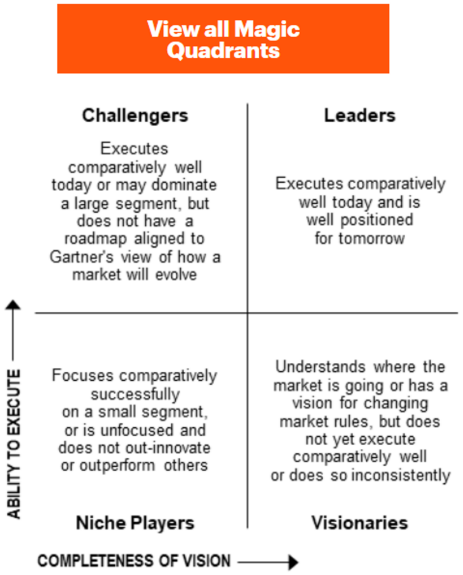


Figura 3.2: Quadrante Mágico, Fonte: Gartner (MEINARDI, 2019).

Assim, tem-se que:

- Líderes: Competidores que executam bem sua visão de mercado e estão bem posicionados para o futuro.

- Visionários: Competidores com uma visão de futuro do mercado, mas enfrentam desafios na execução.
- Concorrentes de Nicho: Competidores que atuam bem em um segmento pequeno de mercado ou não têm um foco específico e inovam menos ou têm desempenho inferior.
- Desafiantes: Competidores que têm uma boa execução ou domínio em um segmento grande do mercado, mas carecem de uma visão de futuro.

À medida que a computação em nuvem ganha popularidade entre empresas, desenvolvedores e organizações, observa-se o surgimento de vários provedores de serviços. No entanto, três se destacam: Google Cloud Platform (GCP) (CLOUD, 2023), Amazon Web Services (AWS) (AWS Partner Network (APN) Blog, 2022) e Microsoft Azure (MARTINEKUAN, 2023).


Figura 3.3: Quadrante Mágico do Gartner para Serviços de Infraestrutura e Plataforma em Nuvem, Fonte: Gartner (CLOUD, 2023)

Assim, a Figura 3.3 revela que, comparado aos anos anteriores, os gigantes do mercado – AWS, Microsoft Azure e GCS – continuam a dominar, enquanto antigos concorrentes de nicho, como Alibaba Cloud e Oracle, demonstram crescimento contínuo no cenário da computação em nuvem, alcançando até a classificação de visionários. A Amazon, ao longo de um período de quatro anos, sustenta uma liderança sólida no *Market Share*. Paralelamente, Microsoft e Google também expandem sua presença, consolidando-se como as três principais empresas fornecedoras de serviços em nuvem em escala global. Vale ressaltar a ascensão de novos concorrentes de nicho, a exemplo do Tencent Cloud e Huawei Cloud, que conquistam espaço significativo no mercado.

Segundo Kenneth (SURKSUM, 2014), uma vez que cada usuário paga pelo que consome dos recursos e serviços, é possível dividir o custo de manutenção, suporte e operação para os diversos clientes que usufruem da infraestrutura em nuvem. Logo, com o surgimento de provedores baseados em nuvem e o fato de que a maioria das empresas esteram adaptadas a este novo sistema, a importância dos SLAs se multiplicou. Os SLAs, se tornaram cruciais para estabelecer padrões de serviço, gerenciar expectativas, explicar responsabilidades e criar estruturas para lidar com suporte ao cliente e reparos pontuais quando ocorrem falhas.

Assim sendo, são comumente utilizadas *Service Level Agreements* (SLAs) – Acordos de Nível de Serviço (MALATHI, 2011) para determinar a relação do provedor de serviço e o cliente. No SLA são redigidos os requisitos de entrega de serviços, tal como percentual de garantia de disponibilidade. Cada provedor utiliza um SLA com termos próprios, e caso não haja o cumprimento dos termos redigidos, o cliente pode ter direito a ressarcimento de custos, ou em outros casos acarretar multas ao provedor, dependendo dos termos do contrato. Quando muitas operações de missão crítica dependem da confiabilidade e da qualidade desses serviços — seja a Internet, infraestrutura de TI, hospedagem na nuvem, telecomunicações ou suporte de TI, entre outros —, ter um bom SLAs é inegociável.

#### 3.1.4.1 Amazon Web Services (AWS)

Amazon Web Services (AWS) é um dos mais antigos e experientes provedores do mercado de nuvem. Ela foi lançada publicamente em 2006, é o setor tecnológico da empresa Amazon, e com isso estabeleceu uma base maior de usuários, bem como maiores fatores de confiabilidade em sua plataforma de computação em nuvem.

Atualmente, este provedor mantém várias regiões geográficas, incluindo regiões na América do Norte, África do Sul, América do Sul, Europa, China, Ásia-Pacífico e Oriente Médio, fornecendo mais de 200 tipos de serviços em nuvem para 245 países e territórios (AWS Partner Network (APN) Blog, 2022).

A infraestrutura da AWS é composta por regiões e zonas de disponibilidades. O conceito de zona de disponibilidade (do inglês, *Availability Zone* — AZ) é a composição de um ou mais *datacenters* distintos com energia, rede e conectividade redundantes em uma região da AWS. As AZs proporcionam aos clientes a capacidade de operar plataformas distribuidas com alta disponibilidade, tolerância a falhas e escalabilidade (AWS Partner Network (APN) Blog, 2022).

O provedor AWS opera em 80 zonas de disponibilidade, distribuídas em 25 regiões geográficas espalhadas pelo Mundo, e anunciou planos de lançamento de mais 5 regiões, conforme apresentado na Figura 2.3. Como citado anteriormente, existe uma quantidade considerável de serviços ofertados pelo provedor AWS. Os principais são (AWS Partner Network (APN) Blog, 2022):


Figura 3.4: Infraestrutura Global do AWS, Fonte: AWS (AWS Partner Network (APN) Blog, 2022)

A AWS também oferece diversos serviços e produtos de computação em nuvem que estão disponíveis para o público em geral, os principais produtos e serviços são:

1. Elastic Compute Cloud (EC2): serviço web que fornece capacidade de computação redimensionável,

basicamente prove máquinas virtuais escaláveis sob demanda; serviço de IaaS, ofertando máquinas virtuais e toda uma estrutura de infraestrutura em nuvem;

2. Serviços de Armazenamento: os serviços de armazenamento disponíveis pelo provedor serão detalhados no Capítulo 3, pois é o foco deste trabalho;

3. Elastic Beanstalk:plataforma destinada para upload de códigos desenvolvidos em Java, .NET, PHP, Node.js, Python, Ruby, Go e Docker. Este serviço automa ticamente se encarrega da implementação, desde o provisionamento de capacidade, o balanceamento de carga e a escalabilidade automática, até o monitoramento da saúde do aplicativo;

4. AWS Lambda: proporciona a possibilidade de executar códigos sem que seja necessário gerenciar ou provisionar servidores. Dessa forma, o usuário só paga pelo tempo de computação que for utilizado, é a chamada computação "*serverless*" ;

5. Amazon RDS: permite a fácil configuração, operação e escalabilidade de bancos de dados relacionais em nuvem, tais como MySQL, PostgreSQL, Oracle, SQL Server e MariaDB;

6. Amazon Aurora: banco de dados relacional de alta performance, proprietário da Amazon;

7. Amazon DynamoDB:serviço de DBaaS, banco de dados não relacional (NoSQL), proprietário da Amazon;

8. Amazon Redshift:*data warehouse* ágil para análise de dados. Esse serviço realiza suas funções por meio de ferramentas como SQL padrão, além de recursos de BI (*Business Intelligence*);

9. Virtual Private Cloud (VPC): serviço que permite o provisionamento de uma seção da nuvem AWS isolada, de modo lógico. Com esse serviço, os recursos da AWS só podem ser executados em uma rede virtual que o próprio usuário define;

10. Amazon CloudFront: rede de entrega de conteúdo global, que oferece dados de conteúdo aos usuários de maneira segura, em alta velocidade de transferência e com baixa latência.

11. Amazon Lightsail:serviço de PaaS que oferece servidores, armazenamento, banco de dados e arquitetura de rede totalmente virtuais a fim do cliente desenvolver, implementar e executar aplicações em nuvem;

12. Amazon S3:o Amazon Simple Storage é um serviço de armazenamento de dados do tipo armazenamento por objeto, em nuvem;

A AWS oferece soluções para diversas áreas, tais como publicidade e *marketing*, serviços financeiros, tecnologia de jogos e órgãos governamentais(AWS, 2020). A AWS também oferece soluções em nuvem para as áreas de análises de *datalakes*, *machine learning*, computação em nuvem sem servidor e armazenamento (AWS Partner Network (APN) Blog, 2022).

#### 3.1.4.2 Microsoft Azure

O Microsoft Azure foi lançado em 2010, é a principal plataforma de nuvem oferecida pela empresa Microsoft (MICROSOFT, 2023), com a intenção de fornecer uma plataforma de computação em nuvem competente para empresas, e desde então tem obtido sucesso, tornando-se, atualmente, a maior concorrente da gigante AWS. Sendo, a maior vantagem que o Azure tem sobre seus concorrentes é oferecer os produtos da Microsoft em nuvem para uso do público em geral, como por exemplo os produtos da OpenAI.

Assim como o GCP e a AWS, a sua infraestrutura também é dividida em regiões e zonas de disponibilidade (MICROSOFT, 2023). Ao todo são 56 regiões, mas com planos anunciados de expanção de mais 17 como pode ser visto na Figura 2.5. Isso tornará a Microsoft Azure a maior infraestrutura de nuvem computacional do Mundo, com mais regiões globais do que qualquer outro provedor em nuvem.

Figura 3.5: Infraestrutura Global do Microsoft Azure, Fonte: Microsoft (MARTINEKUAN, 2023)

A plataforma de nuvem do Microsoft Azure consiste em mais de 200 produtos e ser viços, dentre estes, destacam-se (MICROSOFT, 2023):

1. Máquinas Virtuais: serviço de provisionamento de máquinas virtuais (VMs) Linux e Windows, escalável sob demanda;
2. Serviços de Armazenamento: os serviços de armazenamento disponíveis pelo provedor serão detalhados no Capítulo 3, pois é o foco deste trabalho;
3. Azure SQL banco de dados SQL em nuvem, gerenciado e fornecido como parte do Microsoft Azure;
4. Azure Cosmo DB: um serviço de banco de dados NoSQL totalmente gerenciado para o desenvolvimento de aplicativos modernos;
5. Azure Kubernetes Service (AKS): implantação e gerenciamento de aplicativos em contâiners, que fornece Kubernetes sem servidor;
6. Azure Functions: uma plataforma de computação sem servidor orientada a eventos que também pode resolver problemas complexos de orquestração;
7. Azure Cognitive: uma coleção de APIs hospedadas na nuvem que permite aos desenvolvedores adicionarem facilmente recursos de inteligência artificial para visão, fala, linguagem, conhecimento e pesquisa em aplicativos, em dispositivos e plataformas, como iOS, Android e Windows;

8. App Service:uma plataforma totalmente gerenciada para construir, implantar e dimensionar seus aplicativos da *web*;

9. Rede Virtual: serviço de rede privada na nuvem.

10. Azure OpenAI Service: serviço de geração de modelos de inteligência artificial oferecidos pela OpenAI;

11. Azure Cognitive Service for Vision:serviço de análise de imagem e pesquisa visual computacional, utilizando inteligência artificial e OCR;

12. Azure Machine Learning: serviço de MLaaS (*Machine Learning as a Service*), aprendizado de máquina como serviço para utilização corporativa;

13. Container Instances: serviço de PaaS que oferece soluções em *container* para desenvolvimento e execução de aplicativos;

14. Microsoft Defender for Cloud: soluções de segurança e proteção de dados para serviços em nuvem.

#### 3.1.4.3 Google Cloud Platform (GCP)

O Google Cloud Platform (GCP) começou sua jornada em 2008, é a plataforma de nuvem da Google Ċom o objetivo de competir diretamente com outros concorrentes como AWS e Azure, a GCP oferece diversos serviços em nuvem para seus clientes. A intenção inicial do Google Cloud era fortalecer os próprios produtos do Google, como o mecanismo de pesquisa do Google e o YouTube. Atualmente, eles também introduziram seus serviços empresariais para que qualquer pessoa possa usar o GCP, que compartilha a mesma infraestrutura de Pesquisa Google ou do YouTube.

A GCP também oferece mais de 150 produtos, dentre eles, diversos produtos gratuitos para diferentes áreas, tais como infraestrutura em nuvem, armazenamento em nuvem, inteligência artificial, aprendizado de máquina, banco de dados em nuvem, análise de dados, infraestrutura de rede e ferramentas para desenvolvedores.

Ainda mais, os serviços do GCP estão disponíveis na América do Norte, América do Sul, Europa, Ásia e Austrália. Esses locais estão divididos em regiões e zonas. É possível escolher onde localizar os aplicativos para atender aos requisitos de latência, disponibilidade e durabilidade (GOOGLE, 2010). Atualmente, o Google Cloud Platform está disponível em 24 regiões e 73 zonas, fornecendo serviços em nuvem para um pouco mais de 200 países e territórios, e possuem previsão de implantação em mais 9 regiões, como pode ser visto na Figura 3.6.


Figura 3.6: Infraestrutura Global do GCP, Fonte: GCP (CLOUD, 2023)

A lista completa de serviços que compõem o portifólio do GCP oferece mais de 100 produtos , dentre eles os serviços que mais se destacam são (CLOUD, 2023):

1. Compute Engine: componente que ofereceo serviço de Infraestrutura como Serviço do GPC, o qual permite que os usuários iniciem máquinas virtuais sob demanda;
2. Serviços de Armazenamento: os serviços de armazenamento disponíveis pelo provedor serão detalhados no Capítulo 3, pois é o foco deste trabalho;
3. App Engine: uma plataforma de computação em nuvem para desenvolver e hospedar aplicações *web* na infraestrutura do Google;
4. Google Cloud Functions: funções como serviço (FaaS) escalonáveis e de pagamento por utilização para executar seu código, sem a necessidade de gerenciar servidores;
5. Cloud SQL: serviço de banco de dados relacional, totalmente gerenciado, para MySQL, PostgreSQL e SQL Server;
6. Big Query: serviço de *data warehouse*, sem necessidade de servidor, que oferece análises em escala de petabytes para facilitar consultas SQL;
7. Nuvem Privada Virtual (VPC): serviço de rede gerenciada, uma versão virtual de uma rede física, implementada dentro da rede de produção do Google;
8. Cloud CDN: serviço que utiliza balanceamento de cargas e a rede de borda global do Google para exibir conteúdo mais relevante aos usuários, o que acelera seus sites e aplicativos;
9. Cloud Run: permite o desenvolvimento e a implantação de aplicativos em contêineres altamente escalonáveis em uma plataforma totalmente gerenciada e sem servidor.

## 3.2 GRC - GOVERNANÇA, RISCO E CONFORMIDADE

O conceito de integração do GRC, abrangendo governança, gerenciamento de riscos e conformidade, ganhou importância nos últimos anos. Isso ressalta a necessidade de as organizações não apenas atenderem

às regulamentações governamentais, mas também impulsionarem o crescimento, apoiarem a tomada de decisões informadas por riscos, aprimorarem a eficiência, garantirem transparência e promoverem agilidade nos negócios.(MAHENDRA; AL., 2022)

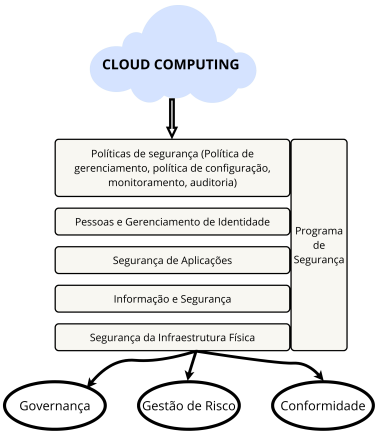


Figura 3.7: Infraestrutura Global do GRC, Fonte: Al-Anzi (AL-ANZI; YADAV; SONI, 2014)

O GRC, consiste em um conjunto de três iniciativas interligadas com o propósito de criar valor para agências públicas e corporativas. Elas operam de maneira coordenada para assegurar a realização de metas, lidar eficazmente com as incertezas e fomentar a integridade (OCEG, 2015).

O principal propósito de uma organização é estabelecer uma estrutura robusta para a Governança, Gestão de Riscos e Conformidade (GRC), por meio da implementação de procedimentos, controles e uma estrutura organizacional que fomente a eficiência na governança, gerenciamento de riscos e cumprimento das regulamentações. A governança envolve o desenvolvimento de políticas, conformidade legal e estruturas tecnológicas que fornecem uma direção clara para atingir objetivos de segurança. Isso envolve a avaliação do risco de acesso de provedores de serviços de nuvem, a proteção de dados sensíveis, o entendimento de questões legais, a gestão do ciclo de vida da informação e a garantia de portabilidade e interoperabilidade (AL-ANZI; YADAV; SONI, 2014). Dessa forma, a organização pode estabelecer um quadro para o gerenciamento eficiente de riscos, que pode ser medido por meio de métricas específicas. Além disso, acordos de nível de serviço (SLAs) desempenham um papel fundamental na garantia do cumprimento dos requisitos de segurança (BRERETON et al., 2007)

A governança, de forma simples, é como uma organização é administrada e controlada. Ela envolve a forma como as pessoas que dirigem a empresa (gerentes), as pessoas que são donas da empresa (acionistas) e outras pessoas envolvidas (*stakeholders*) interagem para garantir que os gerentes façam o que é melhor para os donos e para todas as partes envolvidas. Isso é feito para garantir que a empresa funcione bem e siga as regras corretamente. (VIEIRA; BARRETO, 2019)

A gestão de riscos é um conjunto de protocolos que as empresas seguem para lidar com situações incertas que podem afetar seus objetivos de forma negativa. É como um plano para identificar, entender, avaliar, lidar e ficar de olho em problemas que podem surgir. Essa abordagem ajuda as empresas a aprimorar seus negócios, ao encontrar oportunidades e reduzir a probabilidade e/ou o impacto dos riscos. Também ajuda a garantir que todos sigam princípios éticas e normas legais. (VIEIRA; BARRETO, 2019)

Integridade, ou seja, fazer as coisas certas e de acordo com as regras, é como o "pilar" que mantém uma organização funcionando da maneira correta. Envolve garantir que todos na empresa/órgãos governamentais, sigam as diretrizes éticas e legais, evitando problemas. É um trabalho contínuo que inclui descobrir quais são as normas administrativas e legais, fazer análises técnicas na prevenção de riscos de não conformidade e implementação de medidas necessárias para prevenir e corrigir o sistema fora da conformidade. (VIEIRA; BARRETO, 2019)

Para aprimorar ainda mais o GRC, as organizações estão focando fortemente na automação das atividades de GRC, muitas vezes dependendo da tecnologia da informação para gerenciá-las de forma eficiente. No entanto, há uma lacuna na pesquisa acadêmica nessa área, destacando a necessidade de mais estudos e pesquisas para desenvolver um robusto framework de tecnologia da informação para a implementação bem-sucedida do GRC integrado em vários âmbitos (WIBOWO; AL., 2022).

Além disso, em uma sociedade democrática, a boa governança pública envolve a resposta às partes interessadas que trabalham na solução de problemas públicos, garantindo cooperação entre setores público, social e privado. Isso requer a definição de procedimentos para estabelecer e alcançar objetivos, incentivos apropriados para funcionários públicos e avaliação de desempenho e conformidade. (Bao et al.,2012)

Assim, a boa governança combina desempenho e conformidade, onde o desempenho refere-se à criação de valor para a comunidade e a conformidade implica em cumprir requisitos éticos e legais. Por princípios, as decisões baseadas nos fundamentos essenciais da governança pública incluem dimensões estratégicas, éticas e legais, abrangendo a dedicação à solução de questões públicas, a adoção de decisões éticas e a observância das leis e regulamentos. Consequentemente, os mecanismos de governança, gestão de riscos e integridade (GRC) devem assegurar que os funcionários públicos alcancem os objetivos das agências governamentais, melhorem o desempenho e atendam a princípios éticos e legais, garantindo a eficácia das decisões em benefício das partes envolvidas na solução de problemas públicos. (VIEIRA; BARRETO, 2019)

### 3.2.1 Governança

No mundo atual, rápido e interconectado, a governança eficaz de TI (Tecnologia da Informação) é essencial para organizações, sejam elas públicas ou privadas, formais ou informais. Esse tipo de gestão, implica na especificação dos direitos de decisão e responsabilidades para incentivar comportamentos desejáveis no uso da tecnologia da informação. Os autores Weill e Ross, definem a governança de TI como a especificação dos direitos de decisão e o quadro de responsabilidade para incentivar comportamentos desejáveis no uso da TI (WEILL; ROSS, 2004).

Na área da governança de TI, vários modos de coordenação entram em jogo, incluindo hierarquias e redes. As hierarquias dependem da autoridade centralizada e do controle formal, com linhas claras de comando e funções especializadas. É uma abordagem estruturada e sistemática para a governança, garantindo que as tarefas sejam realizadas de forma eficiente e em conformidade com as regras e regulamentos estabelecidos. No entanto, as hierarquias tendem a se tornar rígidas e insensíveis às demandas externas e às necessidades dos clientes.

Em contraste, as redes dependem da confiança e cooperação entre atores interconectados. Elas envol-

vem várias partes que colaboram de forma autônoma, mas interdependente, compartilhando recursos para benefício mútuo. As redes constroem relacionamentos de confiança ao longo do tempo, o que leva a uma maior colaboração e objetivos compartilhados. Esse modo de governança é mais igualitário e cooperativo em comparação com hierarquias.

É importante observar que cada modo de governança tem suas vantagens e desvantagens, e a abordagem de governança mais eficaz muitas vezes envolve uma combinação desses modos. Hierarquias podem se tornar burocráticas e inflexíveis. A escolha do modo de governança deve ser adaptada às circunstâncias e metas exclusivas de uma organização. Hierarquias e redes, quando usadas de maneira complementar, podem proporcionar um equilíbrio entre a estrutura e a flexibilidade necessárias para uma governança eficaz de TI (SUICIMEZOV; GEORGESCU, 2014).

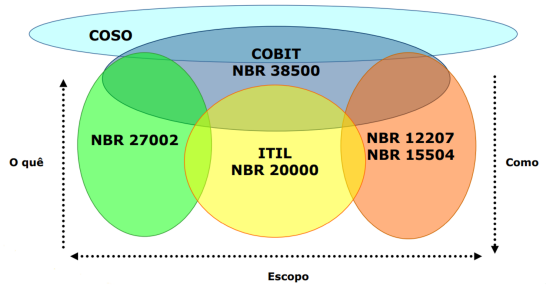


Figura 3.8: Diversos modelos e padrões de governança para metas exclusivas de uma organização, Fonte: Isaca (5, 2012)

Além disso, a governança de TI desempenha um papel fundamental na harmonização da TI com a estratégia geral de uma organização. Quando as estratégias de TI e de negócios estão alinhadas, isso leva a um melhor desempenho da organização, como demonstrado em inúmeros estudos. Portanto, as organizações analisam e implementam uma variedade de modelos, padrões e melhores práticas de tecnologia, visando alcançar objetivos específicos da própria empresa. A importância de compreender esses elementos, conforme ilustrado na Figura 3.8, reside na necessidade de explorar suas possíveis integrações para atender às exigências corporativas. O COBIT (Control Objectives for Information and Related Technologies) desempenha um papel unificador ao fornecer diretrizes de boas práticas para a gestão, controle e garantia da Tecnologia da Informação, auxiliando as organizações no cumprimento de requisitos regulatórios e na garantia de conformidade (5, 2012) - (JOSHI et al., 2018).

Esse conjunto de iniciativas levou à definição de um padrão para a governança de TI, resultando na criação de um modelo de governança para metas exclusivas de uma organizaçã ISO38500:2008 em maio de 2008. Este padrão foi fortemente influenciado pelo Padrão Australiano para Governança Corporativa de Tecnologia da Informação e Comunicação AS8015-2005, publicado em janeiro de 2005. A ISO38500:2008 representa um framework que inclui três tarefas diferentes para a governança de TI, a saber: (1) a avaliação do uso da TI, (2) a preparação e implementação de planos e políticas, (3) e o monitoramento da conformidade com as políticas e o desempenho em relação aos planos. Estruturas como o COBIT (Objetivos de Controle para Informação e Tecnologias Relacionadas) e o ISO38500 fornecem diretrizes para a implementação das melhores práticas na governança de TI, garantindo que os recursos de TI sejam gerenciados, controlados e usados de forma eficaz para atender aos objetivos organizacionais

(BRANDIS; AL., 2019).

Em conclusão, a governança de TI é uma parte integrante das operações comerciais modernas. Envolve a tomada de decisões estratégicas, o estabelecimento de estruturas de responsabilidade e garantia de que os recursos de TI sejam usados para incentivar comportamentos desejáveis. Seja uma organização baseada em estruturas hierárquicas, forças de mercado ou redes de colaboração, a escolha do modo de governança deve estar alinhada com os objetivos e circunstâncias da organização. Ao gerenciar eficazmente os recursos de TI e alinhá-los com as estratégias corporativas, as organizações podem melhorar seu desempenho geral e atender melhor às demandas do cenário digital em constante evolução.

#### 3.2.1.1 No setor público

A governança de Tecnologia da Informação (TI) tem se tornado cada vez mais relevante no setor público, à medida que a dependência da tecnologia cresce e a busca por eficiência e transparência se intensifica (MELO; JR, 2018).

Como foi dito, no tópico anterior, a governança de TI é um campo da governança corporativa que estabelece estruturas e diretrizes para a tomada de decisões e a prestação de contas na utilização da TI. Isso engloba questões como liderança, estrutura organizacional e processos, todos destinados a assegurar que a TI esteja alinhada com a estratégia e os objetivos da organização (SUICIMEZOV; GEORGESCU, 2014).

No Tribunal de Contas da União, foram identificados desafios na implementação da governança de TI, incluindo desafios como redesenho inadequado, falta de princípios de negócios para gerenciar conflitos, ausência de um procedimento para situações excepcionais e restrição na ênfase dada à avaliação de desempenho dos sistemas. No entanto, também foram destacados fatores facilitadores, como o engajamento ativo na governança, um processo decisório bem estruturado, a definição clara de responsabilidades em TI, a promoção da transparência, o investimento em educação e uma comunicação eficaz. Além disso, observou-se que a cultura organizacional do TCU, composta por valores, crenças, ritos, tabus, mitos, normas e comunicações formais e informais, desempenha um papel fundamental no estabelecimento da governança de TI em organizações públicas, com a participação de comitês e a utilização de frameworks reconhecidos, como Cobit 5, ITIL, ISO 17799 e PMBok, segundo (BORBOREMA; SANTOS, 2018).

A Política de Governança de TI (PGTI/TCU), conforme a Resolução TCU nº 247/2011, define a Governança de TI como um conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam a garantir que as decisões e ações relacionadas à gestão e uso de Tecnologia da Informação (TI) estejam alinhadas com as necessidades da instituição, contribuindo para o cumprimento da missão e o alcance dos objetivos organizacionais (TCU, 2011).

Assim, a Resolução-TCU nº 320, de 12 de agosto de 2020, trata da política de governança organizacional do Tribunal de Contas da União (TCU). Esta política tem como objetivo estabelecer mecanismos e estruturas para avaliar, direcionar e monitorar a atuação da gestão, visando melhorar o desempenho, embasar o processo decisório com evidências, orientar estrategicamente a organização a longo prazo e avaliar as ações. A resolução define funções, princípios e diretrizes da governança no TCU, bem como os mecanismos de liderança, estratégia e controle para seu exercício. As diretrizes incluem transparência, probidade, confiabilidade, prestação de contas, responsabilidade organizacional, legitimidade, equidade,

eficácia, eficiência, efetividade e capacidade de resposta (TCU, 2020).

Pela Resolução nº 284 de 2016, foi estabelecido o CGTI (Comitê de Governança de Tecnologia da Informação) é um órgão colegiado permanente com responsabilidades estratégicas e executivas. Seu objetivo principal é coordenar a elaboração de propostas de políticas, objetivos, estratégias, investimentos e prioridades em tecnologia da informação e serviços digitais. O Comitê Gestor de TI (CGTI) e a Comissão de Coordenação Geral (CCG) são atores-chave nesse contexto. O CGTI atua na intermediação entre governança e gestão de TI, coordenando propostas de políticas, diretrizes, objetivos e estratégias, bem como participando da avaliação de demandas relacionadas a TI. Por sua vez, a CCG desempenha um papel central na Governança de TI, avaliando e decidindo sobre as propostas submetidas pelo CGTI, além de monitorar o desempenho e a situação de TI no TCU (TCU, 2015).

Falhas na realização dessas atividades de Governança de TI podem resultar em políticas desalinhadas, iniciativas de TI não adequadas à estratégia e objetivos do TCU, atrasos nas ações corretivas, falta de comunicação e transparência, e decisões equivocadas. Tais falhas podem afetar o desempenho operacional, a realização de objetivos estratégicos e a reputação e as finanças da instituição. Portanto, a correta implementação da Governança de TI é crucial para o TCU. (MURAMAKI; GARTNER, 2018).

### 3.2.2 Gestão de Risco

O gerenciamento de projetos implica na aplicação integrada de conhecimentos, habilidades, ferramentas e técnicas para atender aos requisitos do projeto, envolvendo a identificação de requisitos, atendimento às necessidades das partes interessadas, comunicação eficaz e o equilíbrio entre diversas restrições, como escopo, qualidade, cronograma, orçamento, recursos e riscos. As mudanças em um desses fatores podem afetar os outros, e as divergências das partes interessadas podem ser desafiadoras. A equipe de projeto deve ser capaz de avaliar a situação, equilibrar demandas e manter comunicação proativa para alcançar o sucesso do projeto. O desenvolvimento do plano de gerenciamento do projeto é uma atividade iterativa e progressiva, permitindo ajustes à medida que informações mais detalhadas se tornam disponíveis, conforme relata o PMI (INSTITUTE, 2014).

O gerenciamento de riscos na nuvem é essencial para lidar com questões críticas de segurança da informação durante a contratação de serviços em nuvem. Principais riscos incluem a escolha do provedor, responsabilidade pela informação, localização dos data centers, acesso de terceiros, invasões por hackers, segregação de dados, recuperação de dados e suporte à investigação. Um modelo eficaz de gerenciamento de risco envolve a identificação e avaliação de ativos, análise de ameaças e vulnerabilidades, determinação de níveis de risco, desenvolvimento de planos de tratamento e integração nos SLAs (Acordo de Nível de Serviço) (FARRELL, 2010).

O autor (Gatewood,2009) propõe que organizações que estejam avaliando soluções de computação em nuvem criem uma lista de verificação que aborde os riscos relacionados a contratos e Acordos de Nível de Serviço (SLAs), incluindo serviços, responsabilidades de gerenciamento, conformidade de registros, controles de segurança, destruição de dados, períodos de retenção por classificação de dados, opções de destruição segura, backups, replicação, failover e garantias de disposição nos acordos.

Assim, os requisitos para uma gestão eficaz incluem uma estrutura organizacional de segurança, adoção

de melhores práticas, definição/adaptação de metodologia de análise de risco, desenvolvimento de políticas e procedimentos, estabelecimento de estrutura de gerenciamento de riscos, planos de remediação de vulnerabilidades, procedimentos de resposta a incidentes e um plano de continuidade de negócios, adaptando-se às necessidades e regulamentações específicas de cada organização (CASTRO; SOUSA, 2010).

O emprego da computação em nuvem proporciona vantagens consideráveis, contudo, não está livre de riscos significativos que afetam tanto usuários quanto organizações. Os riscos de segurança da informação, ressaltados por especialistas, abarcam desde aspectos contratuais até desafios técnicos e jurídicos, ressaltando a importância de uma abordagem cautelosa nesse cenário dinâmico e complexo.

Dentre os riscos identificados na computação em nuvem, destaca-se a falta de atendimento dos requisitos contratuais, que pode não alinhar-se completamente com as necessidades específicas da organização, incluindo políticas de retenção de dados e controle de acesso. A visibilidade limitada dos controles de segurança, vazamento de informações devido à vulnerabilidade a ataques DDoS, falta de compatibilidade entre ferramentas de diferentes provedores e a ausência de rastreamento em casos de fraude também são preocupações críticas. O acesso privilegiado de usuários desconhecidos, não conformidade com regulamentações, políticas de recuperação de dados e tempos de resposta inadequados devido ao tráfego online são desafios adicionais que requerem atenção na gestão de serviços em nuvem (ARATA; RODRIGUES; FARRAGONI, 2018).

De acordo com as recomendações da OWASP para segurança em nuvem, essas preocupações são expandidas para cobrir também aspectos adicionais relacionados à segurança da infraestrutura, abrangendo a falta de interoperabilidade e as vulnerabilidades em aplicativos web e infraestrutura, além da exposição do ambiente de não produção. Além disso, foram registrados riscos extras, como a ausência de processos seguros de desenvolvimento de software e o potencial aprisionamento pelo fornecedor, especialmente no contexto do nível de plataforma como serviço (OWASP, 2009).

O documento "Orientação de Segurança para Áreas Críticas de Foco em Computação em Nuvem V2.1" da CSA explora desde a arquitetura até a escolha de controles com base em infraestrutura, serviços de segurança e requisitos regulatórios. O documento aconselha as empresas a analisarem as lacunas nos modelos de serviço e implantação em nuvem, mapeando-as em relação a controles de segurança e modelos de conformidade; essas "lacunas" identificadas representam os riscos de segurança que a empresa deve gerenciar, influenciando a escolha de fornecedores de nuvem conforme suas necessidades específicas.

Em um modelo de SaaS (*Software as a Service*), o provedor de nuvem disponibiliza instalações, infraestrutura e ambiente de aplicativos hospedado para que o pessoal da empresa utilize software cliente, geralmente por meio de um navegador. A empresa tem controle apenas sobre as configurações específicas do aplicativo, não gerenciando a infraestrutura, sistema operacional ou outros aplicativos. Neste modelo, o provedor de nuvem assume a responsabilidade por uma solução integrada de ambiente em nuvem, incluindo controles de segurança, tecnologias em todas as camadas, governança, conformidade e possíveis responsabilidades em caso de perda ou violação. O provedor pode implementar controles em diversos níveis, como físico, computação e armazenamento, computação confiável, rede, gerenciamento, informação e aplicativo. Além disso, são aplicados controles relacionados à segurança nos níveis de pessoas (separação de funções) e processos (gerenciamento de mudanças), de acordo com (FARRELL, 2010).

#### 3.2.2.1 Gestão de riscos no setor público

O gerenciamento de riscos no setor público é crucial para aprimorar os resultados, dada a evolução na administração pública. A decisão sobre equilibrar benefícios e perdas no interesse público é responsabilidade dos formuladores de políticas públicas pois, essas decisões envolvem escolhas morais relacionadas ao risco imposto à sociedade, exigindo que os gerentes ponderem interesses conflitantes para encontrar soluções ótimas e aceitáveis, frequentemente de natureza política. Uma abordagem sistemática ajuda a reconhecer, atacar, decidir, administrar e monitorar riscos de forma eficaz. O objetivo é reduzir custos de atividades incertas e aumentar benefícios sociais e econômicos nas funções governamentais (ÁVILA, 2014).

Conforme mencionado anteriormente, o risco é um conceito associado às escolhas feitas por indivíduos e ao impacto de eventos sobre os ativos. Assim, não é determinado apenas pelo tamanho do risco, mas pelo equilíbrio entre as consequências esperadas e inesperadas. Nesse sentido, organizações frequentemente se envolvem em atividades de alto risco sem compreender completamente os custos envolvidos, o que leva à necessidade de programas de gestão de riscos (PAQUETTE; JAEGER; WILSON, 2010).

No caso das organizações, a gestão de riscos não é apenas defensiva, mas envolve o desenvolvimento de uma estratégia que equilibra oportunidades e consequências. Para isso, é necessário compreender, calcular e gerenciar de forma eficiente a variabilidade nos resultados financeiros das empresas. Uma vez que o objetivo é selecionar e implementar medidas de mitigação para manter o risco em um nível aceitável a um custo aceitável (IBGP, 2019).

Dessa forma, visando uma padronização mais eficiente, a ABNT (Associação Brasileira de Normas Técnicas), fundada em 1940, é responsável pela normalização técnica no Brasil, sendo uma entidade privada e sem fins lucrativos. No âmbito da gestão de riscos e segurança da informação, diversas normas foram desenvolvidas, com destaque para a ABNT, NBR ISO/IEC 27005 “Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação”.A norma ABNT NBR ISO/IEC 27005:2008, relacionada à tecnologia da informação e gestão de riscos de segurança da informação, baseada nos estudos da ISO 31000:2009. Essa norma faz parte da série ISO/IEC 27000, que inclui também as normas ISO/IEC 27001 e ISO/IEC 27002. A norma ABNT NBR ISO/IEC 27005:2008 fornece diretrizes para o gerenciamento de riscos de segurança da informação, empregando conceitos da norma ABNT NBR ISO 27001:2005. O documento descreve o processo necessário para a gestão de riscos de segurança da informação, seguindo a abordagem cíclica e contínua desse processo. O documento está dividido em um total de 12 sessões. As sessões de 1 a 4 abordam as referências e a estrutura da norma, enquanto as sessões 5 e 6 oferecem uma visão geral do processo de gestão de riscos. As sessões a partir da 7 são dedicadas especificamente ao processo de gestão de riscos. Adicionalmente, há seis anexos identificados de A a F, fornecendo informações adicionais e exemplos (BEZERRA, 2013).

É notório, que a adoção de computação em nuvem pelo governo é complexa e traz diversos riscos. Esses riscos incluem mudanças de política, implementação dinâmica de aplicativos e segurança em um ambiente dinâmico.

Segundo Paquette (PAQUETTE; JAEGER; WILSON, 2010), os riscos específicos associados à computação em nuvem no governo podem ser categorizados em:

- Riscos tangíveis/conhecidos incluem:
  - Acesso: Garantir a segurança de dados privados e evitar acesso não autorizado em um ambiente de nuvem apresenta desafios além da segurança de rede tradicional, como segregação de dados e leis de privacidade em diferentes países.
  - Disponibilidade: Os serviços em nuvem prometem alta disponibilidade, mas interrupções inesperadas, sobrecargas e falhas podem ocorrer, impactando as funções do governo e incorrendo em custos financeiros e de reputação.
  - Infraestrutura: A infraestrutura em nuvem deve ser flexível, escalável e interoperável, mas desafios incluem migração de dados, vida útil da tecnologia e a falta de padrões universais e APIs proprietárias.
  - Integridade: Manter a precisão e a segurança dos dados é essencial, e a responsabilidade pela integridade dos dados, responsabilidade e direitos de propriedade intelectual devem ser claramente definidos nos acordos de nível de serviço (SLAs).
- Riscos intangíveis/desconhecidos incluem:
  - Acesso e Uso da Nuvem: Poder usar a nuvem sempre que necessário, sem interrupções do fornecedor ou terceiros.
  - Confiabilidade da Nuvem: A capacidade da nuvem de executar aplicativos críticos sem problemas.
  - Serviço Contínuo: Evitar a perda de serviço, que poderia afetar as funções governamentais.
  - Segurança de Acesso: Prevenir o acesso não autorizado a dados e código.
  - Mecanismos de Segurança: Restringir o provedor de monitorar informações do governo na nuvem.
  - Confidencialidade e Privacidade dos Dados: Proteger informações pessoais e dados sensíveis nas agências governamentais.
  - Preservação de Informações: Atender às leis sobre retenção e preservação de registros federais.
  - Responsabilidade em Problemas Graves: Definir claramente quem é responsável em crises graves.
  - Proteção de Propriedade Intelectual: Garantir que dados patenteados estejam seguros na nuvem.
  - Regulação e Controle das Informações: Regular e controlar informações criadas usando serviços em nuvem.
  - Interoperabilidade de Tecnologia: Garantir que diferentes tecnologias possam funcionar juntas.
  - Portabilidade de Dados e Recursos: Mover dados e coisas entre partes diferentes da nuvem.
  - Capacidade de Auditoria: Permitir auditorias conforme regulamentações governamentais.
  - Localização Jurídica: Determinar a jurisdição legal em caso de reclamações contra o provedor de nuvem.(PAQUETTE; JAEGER; WILSON, 2010)

A iniciativa de implantar a gestão de riscos no setor público no Brasil é recente, inspirada por ações em países como o Reino Unido desde os anos 1990. Assim, no contexto brasileiro, a Emenda Constitucional nº 19 de 1998 introduziu o conceito de eficiência na administração pública, buscando reorientar a ação estatal em direção à eficiência e qualidade dos serviços prestados ao cidadão.

Dessa maneira, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) e a Controladoria-Geral da União (CGU) emitiram instruções normativas e manuais para promover a gestão de riscos no Poder Executivo Federal. Além disso, o Decreto nº 9.203 de 2017 tratou da política de governança na administração pública federal, incluindo a gestão de riscos (TCU, 2018).

Além disso, o Tribunal de Contas da União (TCU) também desempenha um papel crucial na promoção da gestão de riscos. Iniciou o mapeamento da situação da gestão de riscos em 2012 e, em 2017, avaliou todas as entidades do setor público no âmbito do Índice Geral de Governança do Setor Público (IGG). O TCU lançou um Roteiro de Auditoria de Gestão de Riscos para avaliar a maturidade da gestão de riscos das organizações públicas. Logo, a resolução TCU nº 287, de 12 de abril de 2017, trata da política de gestão de riscos do Tribunal de Contas da União (TCU) e faz alterações em resoluções anteriores relacionadas à estrutura, competências e funções do TCU. O objetivo é melhorar a capacidade do TCU em lidar com incertezas e riscos que possam afetar seus objetivos e missão, bem como a imagem e segurança da instituição. Em decorrência disso, é definido que a alta administração é responsável por liderar, apoiar e monitorar a gestão de riscos, enquanto várias unidades e gestores desempenham papéis específicos no processo. O Presidente do Tribunal está autorizado a emitir regulamentos e resolver casos omissos, e a resolução entrou em vigor na data de sua publicação (TCU, 2017).

A resolução estabelece princípios, diretrizes, competências e responsabilidades na gestão de riscos, definindo um processo que inclui o estabelecimento do contexto, identificação, análise, avaliação, tratamento, comunicação, consulta, monitoramento e melhoria contínua dos riscos. Com isso, a análise de risco envolve a compreensão e determinação do nível de risco, seguindo os passos a seguir:

1. Avaliar o impacto do risco no objetivo/resultado, considerando o potencial comprometimento (alto, médio, baixo, etc.).
2. Avaliar a probabilidade de ocorrência do risco (alta, média, baixa, etc.).
3. Definir o nível de risco com base em uma matriz de probabilidade x impacto, onde as escalas podem variar de acordo com o objeto de gestão.
4. Utilizar escalas qualitativas de probabilidade (raro, pouco provável, provável, muito provável, praticamente certo) e de impacto (muito baixo, baixo, médio, alto, muito alto).
5. O nível do risco é atribuído a cada evento com base na matriz, não por fórmulas matemáticas, com 25 possíveis níveis de risco.
6. O impacto é mais relevante do que a probabilidade; riscos com alto impacto e baixa probabilidade devem ser priorizados.
7. A escolha dos participantes na avaliação dos riscos é importante, pois o conhecimento aprofundado melhora a avaliação.

8. Pode-se usar matrizes com diferentes escalas (3x3, 5x5, etc.) para aprimorar a tomada de decisão.

9. Avaliar os riscos considerando a situação real com os controles em funcionamento (risco residual).

Lembrando que não há uma escala padrão para matrizes de avaliação de risco, e o gestor deve escolher a análise que agregue valor à tomada de decisão (TCU, 2017).

É importante ressaltar que, segundo o estudo de Omar Ali (2020), destaca que para garantir o sucesso da adoção da computação em nuvem e construir confiança, é essencial criar regras específicas que abordem a segurança e privacidade dos serviços em nuvem. Tanto o governo nacional quanto os governos locais devem implementar regulamentações econômicas para garantir a qualidade dos serviços em nuvem. As organizações governamentais locais precisam desenvolver planos claros sobre quais serviços serão movidos para a nuvem e quando. Para atrair mais empresas de serviços em nuvem, o governo deve estabelecer condições favoráveis tanto do ponto de vista governamental quanto empresarial. (ALI; OSMANAJ, 2020).

### 3.2.3 *compliance*

A origem do conceito de *compliance* remonta à década de 1970 nos Estados Unidos, inicialmente como uma resposta à necessidade de coibir e sancionar práticas desleais de empresas americanas no exterior, incluindo suborno para obtenção de contratos. Além disso, tinha como objetivo salvaguardar os cidadãos contra práticas irregulares das empresas e os efeitos prejudiciais decorrentes (CARARETTO, 2021). O termo *compliance*, derivado do verbo em inglês *to comply* (cumprir), refere-se à ação de agir conforme as regras e está vinculado a um conjunto de normas e diretrizes que orientam as organizações em relação à sua conduta e conformidade com padrões específicos em seus setores. A relevância desse conceito nos Estados Unidos foi notadamente destacada a partir de 1991, com a publicação das "Diretrizes Federais para a Condenação de Organizações", que estabeleceram elementos específicos para programas eficientes de *compliance*, proporcionando a redução de penas para empresas que os adotassem em casos de condenação (MARASCHIN, 2017).

Atualmente, empresas ao redor do mundo, independentemente de sua origem, devem observar conjuntos específicos de regras em cada país. Isso faz com que a prática do *compliance* seja fundamental, especialmente para aquelas que mantêm relações com órgãos públicos. A essência do termo "*compliance*" reside em agir em conformidade com as regras estabelecidas, buscando aderir às normas internas e cumprir os comandos, promovendo, dessa forma, uma conduta ética alinhada aos padrões regulatórios vigentes.

Os programas de conformidade são essenciais, embora não eliminem todos os riscos organizacionais, sua implementação consistente e adequada pode resultar em uma considerável redução de riscos. Não há um modelo fixo para esses programas, mas é crucial que estejam integrados à estrutura da empresa, conectando-se naturalmente com diversas áreas.

O conceito de *compliance* na tecnologia, diz respeito à conformidade nos sistemas de TI com políticas, procedimentos, regulamentos e requisitos legais, conforme descrito por (SINGH et al., 2015). Portanto, é essencial compreender o significado do *compliance* e por que ele é de extrema importância, especialmente em ambientes de computação em nuvem. A abrangência do conceito de *compliance* é diversificada e engloba várias dimensões, desde a conformidade com regulamentações e políticas internas até a garantia

da manutenção da segurança e privacidade dos dados.

Conforme (BRANDIS; AL., 2019), a conformidade na tecnologia, envolve atender a vontades, demandas, propostas, regulamentos ou restrições, e cumprir requisitos oficiais para a área. Assim, Na literatura científica, é possível encontrar uma descrição mais precisa de conformidade, que se refere à concordância dos sistemas de tecnologia da informação corporativos com políticas, procedimentos, padrões, orientações, especificações predefinidas ou legislações citekim2007.

Deste modo, a computação em nuvem lida com uma vasta quantidade de dados, muitos dos quais podem ser sensíveis, é necessário cumprir com regulamentações de proteção de dados, como a GDPR na Europa, HIPAA nos EUA e agora LGPD no Brasil. (YIMAM; FERNANDEZ, 2016)

Como mencionado anteriormente, as empresas que operam em vários países devem cumprir com leis locais e internacionais, e para o setor de *cloud* não seria diferente. Percebe-se então, que as implicações legais e regulatórias relacionadas aos dados armazenados na nuvem tornam-se cada vez mais proeminentes. Estas questões originam-se predominantemente em quatro domínios principais: contratos, segurança de dados, cumprimento da lei e medidas de proteção específicas para áreas especialmente delicadas.

Os contratos entre usuários, locatários, provedores de nuvem e subfornecedores estabelecem obrigações e responsabilidades em relação aos fluxos de dados. É fundamental auditar esses contratos para garantir o cumprimento e detectar violações. De tal forma que, a proteção de dados é uma dimensão crítica da conformidade em ambientes de *cloud computing*, pois muitos dados pessoais são armazenados e processados na nuvem. Consequentemente, a conformidade com leis de proteção de dados é fundamental pois, a conformidade também envolve a garantia de que a segurança e privacidade dos dados sejam mantidas. Isso inclui a detecção e prevenção de ameaças cibernéticas e a manutenção de políticas de privacidade.

Logo, as empresas devem estar preparadas para relatar demandas governamentais por dados, especialmente em contextos de segurança nacional e aplicação de leis. (SINGH et al., 2015)

#### 3.2.3.1 Normas e Legislação Brasileiras

No Brasil, a implementação de práticas de *compliance* teve início com bancos e grandes empresas globais, sendo gradualmente adotada por empresas do agronegócio. O foco principal do *compliance* é garantir que as empresas estejam em conformidade com normas internas e externas, notadamente a Lei nº 12846, conhecida como lei anticorrupção de 2013. Essa legislação impõe penalidades a gestores e empresas envolvidos em práticas criminosas, destacando a importância do *compliance* na prevenção de penalidades mais severas. (**??**)

Paralelamente, o Instituto Brasileiro de Governança Corporativa (IBGC) define governança como a direção, monitoramento e incentivo nas empresas, transformando princípios em práticas para proteger e melhorar o valor da organização. O Decreto 9203/17 estabelece diretrizes para a governança na administração pública federal, enfatizando princípios como capacidade de resposta, integridade e transparência. A Governança Pública, com base em transparência, integridade e prestação de contas, é vital para uma gestão eficiente dos recursos públicos, envolvendo programas de *compliance* nas Controladorias Internas. (BRANDIS; AL., 2019)

No entanto, no cenário brasileiro, não há uma lei específica para regular a computação em nuvem. Embora uma proposta de lei tenha sido apresentada em 2013, ela foi arquivada sem votação. Entre 2013 e 2016, o governo promulgou várias leis relacionadas à tecnologia, sem abordar diretamente a computação em nuvem. Em 2016, a discussão sobre a imposição de limites à internet fixa gerou controvérsias, levando a Agência Nacional de Telecomunicações (Anatel) a proibir permanentemente esse modelo, considerando seu impacto na acessibilidade e custo dos serviços de computação em nuvem. Assim, a partir de janeiro de 2016, entrou em vigor a ABNT NBR ISO/IEC 17788/2015, uma norma que serve como guia para a computação em nuvem. Adaptada ao contexto brasileiro, essa norma, desenvolvida em colaboração com organizações internacionais, busca esclarecer como a computação em nuvem pode ser utilizada no país, promovendo o crescimento do mercado nacional. (ABNT, 2016)

Decretos como nº 8.771/2016 e nº 8.135/2013, juntamente com a Portaria Interministerial nº 141/2014, desempenham papéis cruciais na regulamentação governamental. O primeiro regulamenta o Marco Civil da Internet, definindo aspectos relevantes para a governança da rede. O segundo, em conjunto com a Portaria Interministerial, surge em resposta às preocupações sobre a vigilância de dados pessoais pelos EUA, assegurando o uso seguro de serviços de comunicação e exigindo que a administração pública federal utilize redes e serviços de TI fornecidos por órgãos governamentais. (FERREIRA; ANDRADE, 2016)

O Acórdão nº 1739/2015 do Tribunal de Contas da União estabeleceu regras para fiscalizar os gastos do governo em serviços de computação em nuvem, alinhado aos objetivos do Programa TI Maior e da Estratégia de Governança Digital (EGD) de melhorar a área de tecnologia no Brasil.

Por fim, a Portaria MP/STI nº 20 de 2016 oferece orientações para a contratação de serviços de Tecnologia da Informação (TI), alinhadas a regras e leis, fornecendo direções específicas para órgãos do governo ao contratar serviços de nuvem. Essas medidas visam garantir a segurança nacional, a privacidade dos dados e a eficiência na gestão dos recursos públicos. (FERREIRA; ANDRADE, 2016)

#### 3.2.3.2 *compliance* e sua Importância na nuvem

Os serviços em nuvem envolvem uma série de relações diretas (tipicamente contratuais) entre usuários e locatários, locatários e provedores de nuvem e provedores de nuvem e subfornecedores. Normalmente, os fluxos de dados correspondem a essas relações. As considerações legais e regulatórias para fluxos de dados na nuvem giram em torno de quatro dimensões principais. A primeira dimensão são as obrigações contratuais. Os serviços em nuvem envolvem diversos contratos, como acordos de nível de serviço e políticas de privacidade. Esses documentos impõem obrigações para as quais seria valioso auditar os fluxos de dados e, portanto, verificar o cumprimento, detectar violações e atribuir responsabilidades.

Em segundo lugar, leis de proteção de dados, adotadas em muitos países, impõem obrigações e responsabilidades aos locatários e provedores para a gestão de dados pessoais. A premissa fundamental da proteção de dados é que todos os usos de informações identificáveis a um indivíduo devem ser estritamente regulamentados e controlados, com diversos mecanismos de auditoria, restrições de fluxo e finalidade, e penalidades (pelo menos, teoricamente) para o não cumprimento.

A terceira dimensão é o acesso de aplicação da lei para crimes/segurança nacional. Para empresas globais com clientes internacionais, há uma pressão crescente para relatar as demandas do governo por

dados.

Por fim, existem proteções regulatórias e de direito comum para domínios particularmente sensíveis, como saúde, finanças, relações médico-paciente e advogado-cliente, bem como, em um contexto comercial, proteção de segredos comerciais e outros ativos de propriedade intelectual.

O tipo de oferta de serviço em nuvem determina a capacidade de gerenciamento. As ofertas em nuvem tendem a ser descritas em termos de um modelo de serviço, que reflete as partes da pilha em nuvem que são gerenciadas pelo provedor. Ou seja, o tipo de modelo de serviço está relacionado ao grau de controle que um locatário tem sobre o serviço. Geralmente, os locatários têm meios limitados (se houver) para influenciar ou visualizar os aspectos gerenciados pelo provedor.

Conforme visualizado na Figura 3.1, Ilustração da Divisão de Responsabilidade da nuvem, o software como serviço (SaaS) está no extremo oposto do espectro, onde a aplicação inteira é oferecida e gerenciada pelo provedor. Isso pode ser um serviço de e-mail universitário administrado por um grande provedor de webmail, por exemplo. Os locatários de SaaS têm muito menos liberdade, porque qualquer gerenciamento é determinado pela funcionalidade de configuração oferecida pela aplicação. (SINGH et al., 2015)

O artigo (YIMAM; FERNANDEZ, 2016) relata que, a falta de uma Arquitetura de Referência (RA) de conformidade padrão e independente de fornecedor é um desafio fundamental para provedores de serviços, intermediários de serviços, consumidores e auditores. Assim, uma Arquitetura de Referência (AR) enfatiza a necessidade de começar a partir de uma visão conceitual da semântica das regulamentações, sem se envolver prematuramente em detalhes de implementação.

Além disso, em (FERNANDEZ; MONGE; HASHIZUME, 2015), o autor apresenta o valor de uma AR como uma maneira de enumerar ameaças e indicar onde devem ser implementadas contramedidas. Como a conformidade está fortemente baseada em medidas de segurança e políticas relacionadas, fica claro que uma AR aceita que descreva regulamentações específicas proporcionaria uma maneira de facilitar a construção de sistemas que estejam em conformidade com as regulamentações correspondentes. Consideraremos o uso ou a ausência de ARs como critério para avaliar as publicações que analisamos em nossa pesquisa. As ARs podem ser construídas usando padrões e o uso de padrões é outra maneira de tornar explícita a conformidade com as políticas. Um padrão é uma solução para um problema recorrente em um contexto específico, normalmente expresso usando modelos UML (Linguagem de Modelagem Unificada).

Um padrão encapsula uma solução para um problema recorrente em um contexto específico. Padrões podem ser usados para analisar sistemas complexos, capturar decisões de design, pressupostos e experiências. Eles podem melhorar a qualidade do software ao promover a reutilização, escalabilidade e consistência. As soluções de padrões geralmente são representadas usando linguagens de modelagem, como a Linguagem de Modelagem Unificada (UML), talvez combinada com linguagens formais, como a Linguagem de Restrições de Objetos (OCL). Os padrões podem incluir diagramas de classes, diagramas de sequência correspondentes a casos de uso e diagramas de estado, e são descritos usando modelos.

A eeferência (ELGAMMAL et al., 2016) propôs uma Linguagem de Solicitação de Conformidade que pode ser usada para especificar padrões de conformidade que podem ser aplicados a processos de negócios. Eles construíram um framework de gerenciamento de conformidade em tempo de design que pode ser usado para automatizar a validação e verificação da conformidade. Eles não fizeram nenhuma

tentativa de definir um modelo preciso para seu framework.

O autor (FERNANDEZ; MONGE; HASHIZUME, 2015) desenvolveram uma arquitetura de referência de segurança (SRA) para sistemas em nuvem a partir de casos de uso, modelagem de ameaças e padrões; eles mapeiam componentes identificados em padrões abstratos usando um catálogo. Propusemos uma abordagem de cinco etapas para construir ARs usando metamodelos, padrões e melhores práticas (YIMAM; FERNANDEZ, 2016). Primeiro, analisamos as fontes de entrada do AR a partir de requisitos funcionais, requisitos não funcionais, partes interessadas, regulamentações e padrões. Identificamos componentes a partir de casos de uso, ontologias, modelagem de ameaças, políticas e melhores práticas. Segundo, construímos um modelo conceitual (RM) analisando componentes de domínio, partes interessadas e suas interações. Usamos UML para analisar a natureza estática e dinâmica dos componentes identificados. Terceiro, mapeamos os componentes identificados em padrões usando padrões abstratos. Quarto, construímos ARs combinando os resultados das etapas 1, 2 e 3. Quinto, avaliamos a arquitetura validando seus atributos de qualidade, como precisão, completude, modularidade, reutilização, flexibilidade e legibilidade.

O texto aborda desafios relacionados à conformidade em serviços de nuvem, destacando várias questões. Inicialmente, destaca-se a complexidade das regulamentações, que são muitas vezes redigidas de maneira extensa e difícil de compreender. O foco é na necessidade de identificar padrões para tornar essas regulamentações mais claras e precisas, especialmente no contexto do Health Insurance Portability and Accountability Act (HIPAA). Outro ponto abordado é a sobreposição de regulamentações, evidenciando que empresas de serviços em nuvem devem cumprir várias normativas, o que pode levar a custos elevados e inconsistências. A falta de arquiteturas de referência padrão (ARs) também é discutida, destacando a diversidade de abordagens na construção dessas arquiteturas e a ausência de um metamodelo abrangente. A falta de controle completo e transparência na nuvem pública é identificada como um desafio adicional, especialmente no que diz respeito à replicação de dados em diferentes regiões. Além disso, são apontadas ameaças à segurança na computação em nuvem, destacando a necessidade de mais pesquisas para construir a confiança dos consumidores e identificar possíveis ameaças. Finalmente, destaca-se a sobreposição entre conformidade e segurança, indicando que, embora esses dois aspectos estejam inter-relacionados, muitas vezes são tratados por grupos distintos, resultando em abordagens ingênuas e insuficientes para garantir uma arquitetura altamente segura. (SINGH et al., 2015)

## 3.3 TAGS

### 3.3.1 Definição de tags

Marcar algo não é uma prática recente; ao contrário, essa ação tem sido parte integrante do nosso cotidiano por bastante tempo. A palavra *tag*, originária do inglês e traduzida como etiqueta, tem o papel de organizar informações ao agrupar conteúdos marcados com a mesma palavra-chave. (ASSIS, 2009)

Nas bibliotecas, as palavras-chave eram cuidadosamente classificadas por meio de etiquetas nas estantes, representando os resultados dessa classificação. Se alguém buscasse um livro sobre “Receita de Bolo”, as palavras-chave relevantes seriam, por exemplo, “Confeitaria”, “Culinária” ou “Bolo”. Esse sistema, aplicado há muito tempo nas bibliotecas, foi adaptado para a era digital, onde as *tags* são palavras-chave

utilizadas em artigos, fotos, vídeos e outros tipos de conteúdo online. (ASSIS, 2009)

A definição de *tag* transcende sua aplicação nas bibliotecas, abrangendo diversos campos. No universo digital, uma etiqueta é uma peça de informação que descreve dados ou conteúdos aos quais é atribuída. É crucial destacar que, por si só, um identificador não carrega semântica ou informação significativa.(ROUSE, 2017)

A marcação desempenha várias funções, incluindo:

- Classificação
- Marcação de propriedade
- Descrição do tipo de conteúdo
- Identidade online;

A marcação, além de funções como classificação e marcação de propriedade, encontra aplicação na nuvem. As etiquetas, nesse contexto, são identificadores de recursos que representam a propriedade e associação de elementos na nuvem, respondendo a perguntas cruciais sobre gerenciamento, clientes, aplicativos e ambientes. (SASI, 2023)

A governança de nuvem deve liderar o processo de definição das *tags*, pois elas devem ser aplicadas de forma consistente para todas as equipes da empresa. Aplicações individuais também podem adicionar essas etiquetas para atender às suas necessidades específicas. (ADTSYS, 2022)

Na ausência de uma política de marcação, é comum que equipes ou indivíduos da mesma empresa usem variações da mesma *tag*, tornando extremamente difícil obter relatórios precisos. Para utilizar as etiquetas de maneira eficaz para fins de relatórios e controle, é essencial criar uma política que defina convenções de nomenclatura consistentes, incluindo ortografia, maiúsculas/minúsculas e espaçamento. (ADTSYS, 2022)

Conheça alguns exemplos de *tags*:

Tabela 3.1: Descrição das *tags* para gerenciamento de recursos

| **Tipo de *tag*** | **Propósito** | **Exemplos** |
|---|---|---|
| Ambiente | Identificar os recursos de cada ambiente | ambiente = teste |
| | | ambiente = dev |
| | | ambiente = prod |
| Custo | Alocar uma ou mais marcadores para custos | custo = região |
| | | custo = projeto |
| Aplicação | *tags* para servidores e serviços | db = database |
| | | srv = jenkins |
| *compliance* | Alocar etiquetas conforme regras de *compliance* | *compliance* = soc |
| | | *compliance* = hipaa |
| Agendamento | Alocar *tags* para start/stop dos recursos | time = 12x05 |

Há muitas práticas de otimização de custos no mundo da computação em nuvem, e a marcação (*tagging*) é uma das mais eficazes. Existem algumas razões para isso que podem ser acompanhadas a seguir.

No âmbito empresarial, a prática de marcação desempenha um papel fundamental ao possibilitar que as empresas organizem, visualizem e gerenciem eficientemente uma variedade de recursos compartilhados entre diferentes departamentos, projetos e unidades de negócios. Esse método não apenas promove a otimização da estrutura interna, mas também contribui significativamente para a economia de custos.

Assim, em uma perspectiva financeira, a prática de marcação concede às organizações, uma visão abrangente dos gastos totais relacionados aos recursos em nuvem em toda a organização. Isso possibilita uma análise minuciosa dos custos associados a funções e serviços específicos, promovendo, assim, uma gestão mais eficaz dos recursos disponíveis. Essa abordagem estratégica não apenas promove a eficiência operacional, mas também impulsiona a tomada de decisões embasadas em dados concretos.

Outro benefício crucial da marcação reside na capacidade de rotular e agrupar ativos em nuvem. Essa prática simplifica substancialmente a criação de relatórios de custos e a realização de auditorias financeiras, tornando essas atividades menos complexas e mais acessíveis para as empresas. Ao facilitar a categorização e organização dos ativos, a marcação emerge como uma ferramenta indispensável para a transparência e conformidade financeira.(SASI, 2023)

Em resumo, as *tags* constituem uma ferramenta valiosa na era digital, contribuindo para a organização eficaz e a recuperação de informações em meio à vastidão da internet. Acredita-se que ao adotar corretamente as práticas de marcação, as empresas poderão não apenas aprimorar a eficiência operacional, mas também maximizar o retorno sobre os investimentos em recursos em nuvem.

### 3.3.2 Definição de *tags* em Computação em Nuvemm

As *tags* desempenham um papel fundamental na organização e gestão eficaz de recursos em ambientes de computação em nuvem. Esses rótulos de metadados, compostos por chaves e valores, são designados a aplicativos, recursos e outros serviços disponíveis em ambientes de nuvem, possibilitando uma abordagem flexível para a categorização técnica e de negócios. (WILLIS, 2023)

A ferramenta de *tags*, embora por vezes subestimada, se destaca na gestão eficiente da infraestrutura em nuvem, possibilitando a filtragem de recursos e a execução de tarefas com base nos valores atribuídos às etiquetas. Além disso, a sua aplicação, desempenha um papel crucial na representação e nomeação precisa de recursos, contribuindo para a segurança e governança. As empresas implementam essa marcação pública em nuvem por muitas razões, mas a mais prática é a disposição de alcançar uma maior visibilidade nas taxas de utilização e custos dos recursos em nuvem em equipes e departamentos. (GUTNIK, 2022)

Sem uma estratégia adequada de gerenciamento de marcadores, as empresas podem cometer os seguintes erros: implementar *tags* incorretamente e, como resultado, falhar em relatórios e otimização de custos, ou seja, as organizações correm o risco de se deparar com contas em nuvem enormes a serem pagas. Um exemplo relacionado à ausência de aplicação de *tags* é que, em caso de incidente de segurança, é necessário identificar rapidamente os sistemas afetados, as funções que esses sistemas suportam e o impacto potencial nos negócios. As etiquetas contribuem para realizar essa identificação de maneira ágil e eficiente. (KUPERMAN, 2023)

Como mencionado anteriormente, as *tags* consistem em duas partes: uma “chave” e um “valor” associado a essa chave. A chave representa o nome único usado para identificar a *tag*, enquanto o valor pode ser os dados identificados ou um indicador da localização desses dados. Para ilustrar, imagine o seguinte exemplo: ao usar etiquetas para rastrear ativos por projeto, a “chave” seria “Projeto” e o “valor” seria o projeto específico, como “Sun”. Dessa forma, rotula-se o ativo “Sun” como (Chave=Projeto, Valor=Sun). Posteriormente, poderia correlacionar informações sobre quais projetos implementam quais ativos, filtrando os ativos com base nos metadados da *tag* associada à chave “Projeto”. (GUTNIK, 2022)

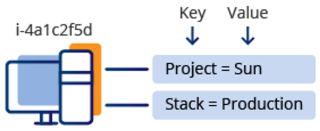


Figura 3.9: Exemplo de *tags*, Fonte: AWS (AWS Partner Network (APN) Blog, 2022).

Vale a pena mencionar que existem dois tipos diferentes de *tags*. O primeiro tipo de marcação é aquele criado pela AWS ou Azure. Eles são gerados automaticamente e não podem ser alterados. Geralmente, contêm longas cadeias de letras e números e se parecem com isso:

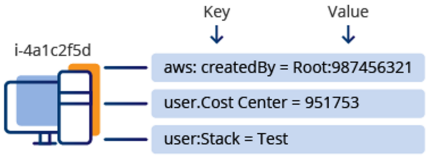


Figura 3.10: *tags* criadas pelo provedor e pelo usuário, Fonte: AWS (AWS Partner Network (APN) Blog, 2022).

Outro tipo de *tag* são as etiquetas definidas pelo usuário, conforme a Figura 3.9 exibe. Neste artigo, vamos nos concentrar principalmente nelas. Esses indicadores podem ser rotuladas da maneira que uma empresa preferir. (GUTNIK, 2022)

No entanto, a compreensão de que as *tags* têm significado apenas para a equipe da organização e são independentes da arquitetura do código é essencial para a aplicação funcione corretamente. Para os provedores de nuvem, são simplesmente sequências de caracteres sem significado semântico. Elas são completamente separadas da arquitetura do código. Ao anexar etiquetas aos recursos,é possível filtrá-los facilmente com base nas *tags* que foram utilizadas para mantê-los logicamente organizados(WILLIS, 2023). É importante lembrar que, no contexto da nuvem, um único recurso pode ter diversas etiquetas, proporcionando uma flexibilidade extensa e abrangente para a gestão e entendimento dos ativos na nuvem.(SASI, 2023)

Assim, alterar os nomes dos recursos mais tarde pode ser difícil, então estabelecer uma convenção abrangente de nomenclatura antes de iniciar uma implantação extensa na nuvem é fundamental. Uma estratégia de nomenclatura e etiquetagem fornece uma base sólida para qualquer projeto na nuvem, incluindo migração para a nuvem.(KUPERMAN, 2023)

#### 3.3.2.1 Benefícios

Entende-se que as etiquetas são úteis para lidar com questões técnicas específicas, Ddo mesmo modo, elas desempenham um papel crucial ao abordar questões mais abrangentes relacionadas às estratégias, planos e retorno sobre investimentos de uma organização. Os benefícios mais destacados decorrentes do emprego das etiquetas incluem:

- **Gerenciamento de grupo de recursos:** Os provedores de nuvem pública geralmente organizam os recursos por serviço como configuração padrão. No entanto, a marcação oferece aos administradores a flexibilidade de escolher como desejam organizar esses recursos na empresa (GUTNIK, 2022). Dessa forma, as equipes de Tecnologia da Informação podem utilizar etiquetas para identificar de maneira eficiente recursos associados a cargas de trabalho específicas, configurações, grupos de propriedade e outras informações cruciais (KUPERMAN, 2023). A filtragem por etiquetas proporciona uma forma ágil de diminuir a busca por recursos no seu console. Adicionalmente, algumas plataformas possibilitam a criação de consoles personalizados, levando em consideração etiquetas parciais ou uma combinação de uma ou mais etiquetas (HAVA, 2022).

- **Alocação de Custos:**A atribuição de custos muitas vezes é a principal razão pela qual as empresas valorizam a marcação de recursos na nuvem. Isso é particularmente benéfico para provedores de serviços gerenciados que monitoram o uso de vários clientes na mesma infraestrutura. Com relatórios de custos facilmente acessíveis, as empresas podem implementar políticas de recuperação de custos para rastrear o uso de recursos em nuvem por diferentes departamentos, atribuir esses recursos a equipes e projetos e realocá-los conforme necessário (GUTNIK, 2022). Além disso, é possível gerar relatórios de despesas recorrentes como parte de estratégias de redução de custos (KUPERMAN, 2023), promovendo uma cultura de conscientização sobre custos na nuvem (HAVA, 2022) e identificando a análise de causa raiz (RCA) para anomalias de custo (SASI, 2023). Isso permite que as empresas relatem métricas de custo pertinentes ao seu negócio.

- **Automação:** A automação na computação em nuvem é uma ferramenta eficaz para economizar tempo e esforço para os proprietários de negócios, pois reduz significativamente o trabalho manual e o risco de erros humanos (GUTNIK, 2022). Assim, esses processos automáticos de tarefas de infraestrutura geralmente se baseia em *tags* específicas de recursos ou serviços, indicando o que se deve fazer com esses elementos de *cloud*. Além disso, ao contar com uma estrutura organizacional bem estabelecida, é possível explorar a automação na nuvem para criar recursos, implementar processos de DevOps (KUPERMAN, 2023), monitorar operações e até mesmo realizar a inicialização ou encerramento automático de instâncias conforme as necessidades (NETAPP, 2021). Um exemplo prático da eficácia da automação é a capacidade de programar o desligamento automático de todos os recursos marcados com a mesma etiqueta todas as noites(ESTRIN, 2021). Dessa forma, a utilização de *tags* facilita a organização de todos os recursos relevantes (computação, rede, armazenamento, etc.) em um único local, possibilitando a aplicação de ferramentas ou scripts de automação de forma ágil.

- **Controle de Acesso:**Implementar o controle de acesso por meio de *tags* é uma prática amplamente adotada. Restrições rigorosas são aplicadas àqueles que têm autorização para criar, excluir ou modificar as etiquetas, o que deve ser tratado com seriedade ao gerenciar políticas de controle de acesso em sua empresa (GUTNIK, 2022). Além disso, permissões atribuídas a usuários ou funções podem utilizar *tags* para restringir ou permitir o acesso a ambientes ou VPCs específicos (HAVA, 2022), possibilitando o controle sobre quem pode acessar recursos específicos. Por exemplo, determinando quem tem permissões para visualizar um painel de recursos atualmente em uso em um projeto específico (ESTRIN, 2021).

- **Gerenciamento de Operações:** A equipe responsável pela administração das operações precisa ficar de olho nos acordos comerciais e nos SLAs que foram definidos. Para gerenciar as operações de forma eficaz, é crucial contar com uma maneira fácil de avaliar a importância de recursos específicos, e é aí que as etiquetas se tornam essenciais. (KUPERMAN, 2023) Além disso, a equipe tem a capacidade de agendar backups para recursos específicos, levando em consideração as informações associadas às etiquetas. (NETAPP, 2021).

- **Gestão de Riscos de Segurança:** Ao criar recursos, é possível aplicar *tags* para identificar aqueles que lidam com dados sensíveis ou confidenciais, demandando atenção especial do ponto de vista da segurança (HAVA, 2022). O monitoramento desses recursos também simplifica a identificação de possíveis violações de políticas de segurança, como a exposição pública indevida de um contêiner de armazenamento fundamental no serviço utilizado (NETAPP, 2021). Em situações de violações ou outros problemas de segurança, é crucial categorizar os dados afetados e compreender seu impacto na segurança, o que facilita operações mais seguras (KUPERMAN, 2023).
- **Governança e conformidade:** Assegurar consistência entre os recursos é crucial na prática de governança e conformidade. Logo, o uso de etiquetas oferece a capacidade de aplicar padrões para avaliar a conformidade regulatória (KUPERMAN, 2023). Essa abordagem também contribui para a aplicação consistente de políticas de segurança em todo o conjunto de recursos na nuvem. Por exemplo, ao implementar uma etiqueta de ambiente com valores como dev/test/prod (SASI, 2023).
- **Alertas:**A implementação de uma estratégia de marcação na nuvem oferece uma maneira eficaz de gerenciar os alertas, permitindo a decisão de escaloná-los ou até mesmo eliminá-los. Isso ajuda a mitigar a "fadiga de alerta", que ocorre quando o sistema gera numerosos alertas que não são essenciais (KUPERMAN, 2023). Ou seja, impede que caso os alertas não são pertinentes para a equipe, não ocorra o risco de eles começarem a ignorá-los ou a responder de forma seletiva.

Diante desses benefícios mencionados, é evidente que a introdução de um sistema de marcação visa simplificar o monitoramento de ativos, reduzindo a complexidade e facilitando a tomada de decisões com base nos requisitos operacionais da organização. Dessa maneira, é considerável investir tempo no desenvolvimento e manutenção de padrões de marcação alinhados aos objetivos da empresa. Esse investimento pode estabelecer uma relação direta entre o valor comercial de um ativo e seus custos operacionais, alterando a percepção da Tecnologia da Informação de um simples centro de custos para um elemento estratégico, reconhecido pelo seu impacto positivo (KUPERMAN, 2023).

# 4 PROPOSTA DE FRAMEWORK

A prova de conceito viabiliza a demonstração prática da metodologia, dos conceitos e das tecnologias fundamentais empregadas na concepção do projeto, apresentando uma lista de tecnologias pertinentes (frameworks, padrões, arquiteturas, etc.) e esboçando um modelo conceitual para a solução proposta.

## 4.1 CENÁRIO SEM UTILIZAÇÃO DE *TAGS*

Com o avanço contínuo das implementações em nuvem, as equipes enfrentam desafios cada vez mais complexos na gestão de recursos implantados que estão constantemente sendo alterados ou acrescentados nos projetos de diversos setores de uma empresa. É evidente que, conforme a infraestrutura em nuvem se expande, a complexidade no monitoramento eficaz dos recursos alocados aumenta simultaneamente. (AWS Partner Network (APN) Blog, 2022)

Uma reclamação constante dos profissionais de TI é devido à dificuldade em ter uma visibilidade de forma clara de seus recursos na nuvem, sendo que muitas vezes isso acontece devido a falta de organização da tecnologia por parte do seu uso. Sem uma boa organização, é fácil usar a nuvem de forma incorreta, gastando tempo e dinheiro em coisas que não são realmente importantes no momento. Portanto, é importante organizar o uso da nuvem, dividindo os recursos em grupos e usando *tags* para identificá-los mais facilmente. (CHAGAS, 2022)

Se um projeto não utiliza *tags* adequadamente ou se os recursos não são marcados corretamente, isso pode resultar em vários problemas:(AWS Partner Network (APN) Blog, 2022)

1. Dificuldade de Organização: Quando não se usa as etiquetas para marcar os recursos, pode ficar difícil organizar tudo, especialmente em ambientes com vários projetos em andamento simultaneamente. Isso pode causar confusão na hora de identificar e organizar os ativos.(AWS Partner Network (APN) Blog, 2022)

2. Dificuldade de Rastreamento de Custos: Usar marcadores é como colocar preço em recursos específicos para saber quanto estão custando no projeto. Sem as *tags*, pode ser complicado descobrir quais projetos estão gastando mais dinheiro, e isso pode acarretar em perda do controle de gastos. (AWS Partner Network (APN) Blog, 2022)

3. Problemas de Segurança: *Tags* podem ser usadas para implementar políticas de segurança, como restringir o acesso a recursos específicos com base em etiquetas. A falta de marcação pode expor dados a riscos, aumentando a possibilidade de acesso não autorizado.(AWS Partner Network (APN) Blog, 2022)

4. Dificuldade de Automação: *Tags* são frequentemente usadas em processos automatizados para identificar e agir sobre recursos específicos. Sem *tags*, a automação pode se tornar mais complicada e menos eficiente.(AWS Partner Network (APN) Blog, 2022)

5. Problemas de Conformidade: Em ambientes que requerem conformidade com regulamentações específicas, a falta de *tags* pode dificultar a demonstração e auditoria de práticas de conformidade.(AWS Partner Network (APN) Blog, 2022)

Muitas empresas adotam a tecnologia em nuvem com a expectativa principal de economizar dinheiro. Segundo um relatório da Flexera, uma empresa especializada em soluções de gerenciamento em nuvem, aproximadamente 73% delas planejam utilizar a nuvem de forma mais eficiente para reduzir despesas (ZANIN, 2021). No entanto, um problema sério, identificado pela Gartner, é que 80% das empresas acabarão gastando mais do que o planejado na nuvem, devido à falta de controle e gestão de custos. A previsão é que até 2024, quase todas as antigas aplicações migradas para a nuvem pública precisarão de ajustes para serem financeiramente eficientes. Dessa forma, a explicação para esse cenário reside na ausência de implementação de um plano de gestão de gastos com a nuvem por parte das organizações, onde o erro não está na migração em si, mas na falta de um plano que poderia trazer benefícios financeiros imediatos (MARKETING, 2021).

Assim, torna-se um desafio para as empresas monitorarem seus gastos na nuvem, o que é surpreendente, uma vez que a tecnologia promete eficiência financeira, gerando até mesmo uma aparente contradição. Contrariamente aos antigos data centers, onde usar os recursos eficientemente nem sempre significava gastar menos, a nuvem proporciona uma visibilidade aprimorada dos custos de tecnologia da informação. Além disso, atualmente, os provedores de nuvem oferecem diversas ferramentas e APIs para auxiliar os gestores na empresa a controlar o que estão utilizando na nuvem, facilitando o cálculo dos custos (MARKETING, 2021).

A Gartner proporciona algumas explicações sobre como a falta de uma gestão adequada de custos com a nuvem acontece: (MARKETING, 2021)

- Não conseguem identificar o custo com o local do gasto: Ao serem cobradas pelo consumo, e não de uma vez só, as organizações têm dificuldades de compreender todos os possíveis itens responsáveis pelo seu gasto e, consequentemente, de fazer estimativas, bem como selecionar a melhor opção de preço para cada caso de uso.(MARKETING, 2021)

- Contratam recursos desnecessários: A facilidade e a segurança de implementar recursos com poucos cliques, dada sua natureza on demand, torna comum a extensão desnecessária e sem uma análise prévia, assim como o esquecimento dessa ação, o que gera um média de 35% de taxa de subutilização de serviços cloud, de acordo com a RightScale. Além disso, O custo dos recursos parece baixo e assim a lgumas funcionalidades custam centavos. Para o colaborador que consome, o valor parece irrisório. Contudo, no final do mês, a conta fecha alta.(ZANIN, 2021)

- Muitas opções de produtos dos provedores: A variedade e a mudança constantes das ofertas dos provedores, que adicionam serviços, funcionalidades e modelos de precificação diferentes a seu portfólio de produtos, e a consequente falta de estandardização dos produtos das grandes plataformas , é outra fonte de dificuldade para as organizações.(MARKETING, 2021)

- Muitas possibilidades de combinação: Derivado do ponto anterior vem a possibilidade de construir a mesma aplicação por meio de várias arquiteturas, serviços e componentes distintos, que também

resultam em custos diferentes. As organizações têm dificuldade de identificar todas essas possibilidades e de selecionar a mais adequada em termos de custo-benefício.(MARKETING, 2021)

- Descentralização do consumo dos recursos de cloud: Além da TI, colaboradores de outros departamentos, como marketing, podem adquirir recursos para a nuvem. Com a compra descentralizada, o consumo tende a aumentar.(ZANIN, 2021)
- Falta de governança em TI: A ausências de processos, regras e orçamentos bem definidos pode levar ao cenário de descontrole. É comum, por exemplo, identificar empresas pagando por recursos subutilizados. Uma política de governança de TI consistente pode evitar desperdícios como esse.(ZANIN, 2021)

Os próximos tópicos apresentam as abordagens das *tags* em ambientes de GRC na nuvem, juntamente com uma proposta de framework para a implementação dessas *tags*. Incluiu-se também as melhores práticas recomendadas pelos principais provedores e os desafios enfrentados nesse contexto.

## 4.2 *TAGS* PARA FINS DE GRC

Nesta seção, apresenta-se a importâcia da aplicação de *tags* dentro do contexto de Governança, Gerenciamento de Riscos e Conformidade, para uma melhor compreensão de como o uso das marcações pode influenciar na gestão e tomadas de decisões importantes para uma empresa. Logo, para alcançar o sucesso, é crucial adotar plataformas que facilitem a gestão dos aspectos relacionados à Governança, Risco e Conformidade empresarial, assegurando o acesso contínuo aos serviços essenciais para a empresa. Logo, implementar o método de marcação de recursos na nuvem é essencial para aprimorar a gestão. Portanto, é fundamental manter um conjunto consistente de rótulos, assegurando uniformidade e facilitando a organização para todos na empresa. Esses rótulos desempenham um papel crucial ao fornecer informações sobre a empresa, simplificando a organização dos recursos para monitorar custos, gerar relatórios, garantir precisão e promover a segurança dos dados.(ADTSYS, 2022)

A Figura 4.1 mostra o conjunto de ferramentas que podem ser realizadas dentro de GRC em uma nuvem:

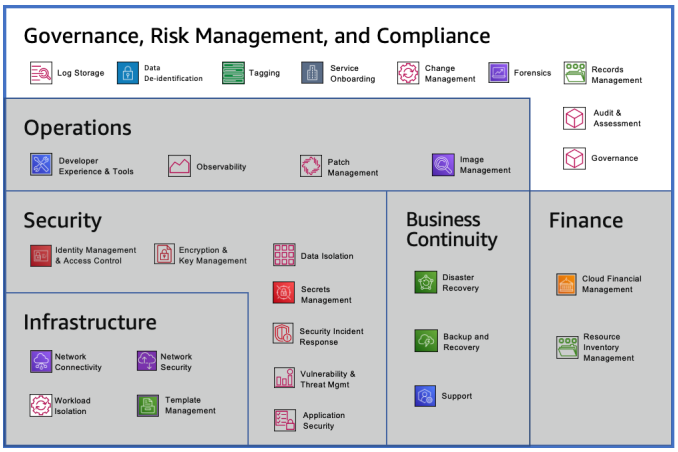


Figura 4.1: Categoria Governança, Gestão de Riscos e Conformidade, Fonte: AWS (AWS, 2020)

A Figura 4.1, ilustra as capacidades de Governança, Gerenciamento de Riscos e Conformidade, que abrangem: A marcação, o armazenamento de logs, a investigação forense, a incorporação de serviços, a desidentificação de dados, a Governança, auditoria e avaliação, gestão de mudanças e gestão de registros.

Dessa forma, as *tags* são essenciais para a aplicação e monitoramento da governança em nuvem e devem apoiar os objetivos da empresa, que normalmente incluem gerenciar efetivamente as operações em nuvem, abrangendo desempenho, automação, gerenciamento de custos, segurança e conformidade.

A implementação eficaz da higiene de *tags* é fundamental para estabelecer a base do framework de governança em nuvem, envolvendo a identificação de pontos críticos, como o provisionamento de novos recursos, e a definição de parâmetros para garantir consistência, visibilidade, segurança e conformidade. A busca pela simplicidade na governança é crucial, visto que o framework deve servir como um guia claro e específico para todos os envolvidos. (YORK, 2022)

Uma organização usufrui de diversas vantagens ao implementar um framework concreto de governança em nuvem, apoiado por uma eficiente marcação de recursos. Estes incluem reforço na segurança, reduzindo a probabilidade de violações de dados e negando acesso não autorizado. Além disso, há aprimoramento na visibilidade, possibilitando a todos visualizar seus dados, melhor gestão de custos com dimensionamento adequado e eliminação de recursos inativos, e maior eficiência operacional para um melhor desempenho. A governança em nuvem estabelece padrões para as operações na nuvem, e a abordagem abrangente de marcação harmoniza interesses divergentes entre várias partes interessadas, considerando cuidadosamente cada uma delas sem perder de vista os objetivos gerais do negócio. Isso garante que a marcação e a utilização de recursos estejam alinhadas com as prioridades empresariais. (ADTSYS, 2022)

No contexto da Gestão de Risco de Projetos, o uso de *tags* revela-se crucial, especialmente ao monitorar recursos que demandam uma camada adicional de segurança. A nuvem, muitas vezes, serve como ambiente para a execução de fluxos de trabalho contendo informações altamente confidenciais, as quais necessitam de proteção constante. Diversas organizações implementam cargas de trabalho que envolvem dados sensíveis sujeitos a regulamentações rigorosas, como HIPAA ou GDPR. Além disso, as etiquetas de segurança desempenham um papel estratégico ao possibilitar a concessão ou restrição de acesso a recursos específicos. Dessa forma, os usuários podem empregar condições fundamentadas em *tags* para regular per-

missões com base em valores e *tags* específicas, proporcionando um controle refinado sobre a segurança e o acesso aos recursos.(AWS Partner Network (APN) Blog, 2022)

Outro ponto a ser considerado na parte de gerenciamento de riscos, é que a classificação de dados e a avaliação do impacto de segurança, especialmente no contexto de violações ou outros incidentes de segurança, são essenciais em empresas que precisam cumprir as normas. Para operar de maneira segura, torna-se fundamental incorporar a prática de atribuir *tags* para a classificação adequada dos dados nos recursos e serviços associados aos dados sensíveis. (MARTINEKUAN, 2023)

Para garantir a conformidade por meio de *tags*, o Azure Policy é empregado para impor regras e padrões de marcação. Ao formular uma política, evita-se a ocorrência em que recursos são implantados na assinatura sem as marcações esperadas pela organização. Em lugar de realizar manualmente a aplicação de *tags* ou procurar por recursos em desacordo, cria-se uma política que automaticamente atribui as *tags* necessárias durante o processo de implantação. Além disso, é possível aplicar etiquetas a recursos já existentes usando o novo efeito "Modificar" e uma tarefa de remediação. (MARTINEKUAN, 2023)

## 4.3 PROPOSTA DE FRAMEWORK

Nesta seção, apresenta-se uma proposta de framework para a implementação e validação de *tags* em cloud computing, especificamente voltado para a gestão de Governança, Risco e Conformidade (GRC). O intuito é simplificar e padronizar a atividade de marcação, visando otimizar o uso da nuvem, com o conhecimento das informações e explicações fornecidas nas seções anteriores.

Conforme mencionado anteriormente, as empresas possuem a oportunidade de desenvolver uma estratégia personalizada para marcação, simplificando os processos em diversos setores. Assim, o diagrama proposto neste estudo tem o propósito de guiar as equipes de tecnologia na marcação de recursos de aplicativos e infraestrutura na nuvem. Ele proporciona o contexto essencial para gerenciar, operar e proteger esses recursos de maneira eficiente, sem acarretar custos adicionais.

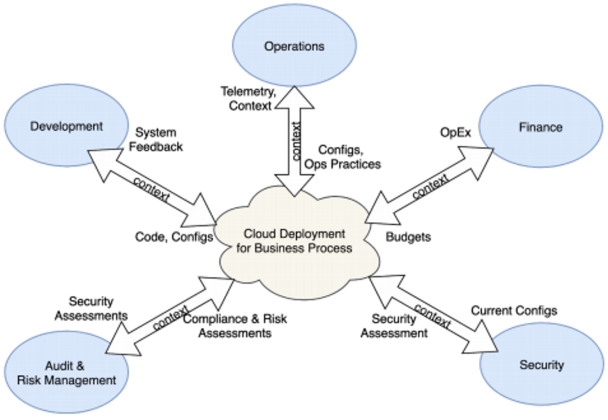


Figura 4.2: Implantação na Nuvem e Funções de Suporte, Fonte: AWS (AWS Partner Network (APN) Blog, 2022)

Portanto, este documento é direcionado primariamente aos profissionais responsáveis pelo planejamento, execução e operação de implementações de aplicativos em plataformas de nuvem. Esses papéis

englobam as seguintes categorias profissionais:

- Engenheiros e tecnólogos que atuam em organizações que fazem uso de plataformas de nuvem.
- Arquitetos e líderes encarregados de impulsionar os esforços arquitetônicos em suas organizações.
- Executivos sêniores, analistas de negócios e colegas em toda a empresa que possuam metas e requisitos críticos de negócios, demandando suporte de TI, especialmente nas áreas de Finanças, Segurança e Gerenciamento de Riscos.
- Fornecedores de ferramentas que desenvolvem soluções especializadas para aprimorar a eficiência, desempenho e segurança nas implantações de nuvem de seus clientes.

Seguindo o diagrama na Figura 4.3, as empresas podem criar sua própria maneira de usar *tags* e facilitar a organização dos ativos em toda a empresa. Foi dividido em 4 fases: Modelagem, Definição de políticas, Implementação e Resultados.

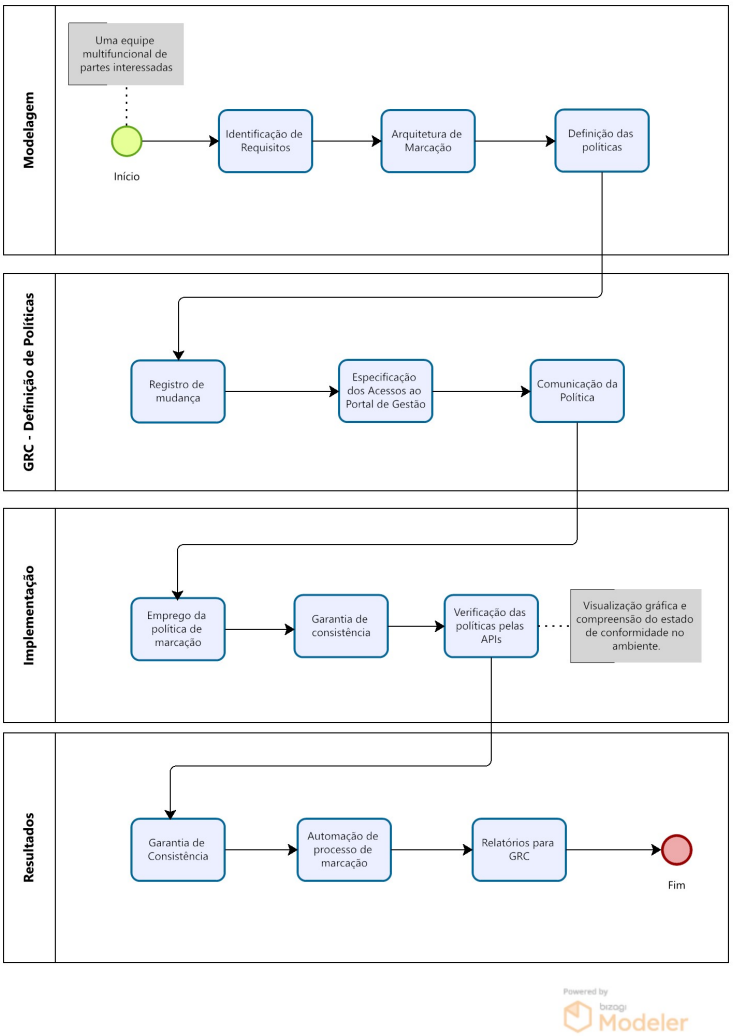


Figura 4.3: Diagrama de processos proposto.

Temos então as seguintes etapas para cada fase:

Etapa 1: Identificar e discutir requisitos

É recomendado que as empresas iniciem a definição de uso das *tags* com uma equipe multifuncional de partes interessadas, com profissionais que realmente utilizarão as *tags* para algum propósito de análise e gerenciamento de recursos. Cabe ressaltar que a equipe pode incluir não apenas membros do departamento de TI, mas também funcionários de finanças, vendas, marketing ou qualquer outro departamento que implante recursos em nuvem.

Etapa 2: Arquitetura de marcação

É importante criar uma estrutura que integre-se eficientemente com sistemas já em uso, como gerenciamento de acesso, monitoramento de segurança e plataformas GRC. Essa arquitetura visa garantir uma etiquetagem integrada e sem interrupções nos processos existentes. Além disso, é importante se atentar na capacidade de escalonamento, para assegurar que o sistema possa lidar com o aumento do volume de dados na nuvem sem comprometer a eficácia ou a consistência das etiquetas.

Etapa 3: Definir as políticas

Na elaboração da taxonomia de marcação, é aconselhável optar por *tags* obrigatórias e, adicionalmente, incluir *tags* opcionais. Estabelecer o formato de par chave/valor, mantendo uniformidade, seja utilizando camelcase, letras maiúsculas ou minúsculas.

Para iniciar, é fundamental estabelecer o contexto necessário para desempenhar funções essenciais de gerenciamento operacional e de custos. Assim, as *tags* propostas desempenham um papel crucial ao identificar e delimitar recursos dentro das fronteiras organizacionais e dos processos-chave. As perguntas a seguir auxiliarão na determinação das etiquetas primordiais para otimizar o GRC.

- Quem é o proprietário deste recurso? A qual aplicativo ele pertence?
- Quem devemos chamar quando o aplicativo está com problemas?
- Quem deve pagar por este recurso? Quais aplicativos estão impulsionando nossos custos?
- Os controles de acesso garantem a segurança apropriada deste recurso?
- Quanto risco nossa implantação na Nuvem tem? Onde está concentrado esse risco?
- Quais melhorias de segurança reduzem mais o risco?

Além disso, uma análise de projetos já implementados nas empresas, proporcionou uma ideia de sugestão do conjunto principal de *tags* a serem utilizadas no mapeamento de recursos na Nuvem, que pode ser visualizado na Tabela 4.1.

Etapa 4: Registro das mudanças

É indispensável a elaboração de registros detalhados de todos os temas discutidos durante as reuniões com a equipe multifuncional. Isso engloba a definição das *tags*, com uma descrição precisa de como e em

que contextos serão utilizadas. Além disso, é de suma importância documentar as razões que motivaram a escolha da empresa em adotar determinadas etiquetas. Essa documentação desempenha um papel inevitável como uma fonte de referência, proporcionando clareza e transparência quanto às decisões tomadas durante o processo de implementação das etiquetas.

Etapa 5: Comunique a política

Compartilhe as decisões referênte as *tags* e divulgue a política de marcação de maneira centralizada para todas as equipes envolvidas. Equipes frequentemente utilizam wikis internos, como Confluence ou Notion, ou até mesmo ferramentas que já possuem acesso com os provedores para esse propósito. Isso promove uma comunicação transparente e eficiente sobre a política de marcação, facilitando a integração desse processo em toda a organização.

É importante reforçar que a eficácia da implementação é maximizada quando é proveniente de uma equipe central, que colabora de forma interfuncional com as equipes de engenharia, garantindo uma implementação coesa e alinhada aos objetivos globais da empresa.

Tabela 4.1: Descrição das *tags* para recursos na nuvem

| **Orientação de tag** | **Descrição** | **Exemplo** |
|---|---|---|
| Proprietário | Identificar a equipe/unidade responsável pelo recurso e seu emprego nos processos de negócios. | ENE = Departamento de Engenharia Elétrica |
| | | ENC = Departamento de Engenharia Civil |
| | | EPR = Departamento de Engenharia de Produção |
| Aplicação | Identificar os recursos que são necessários para uma implantação específica de um aplicativo | AD = Active Directory |
| | | srv = Jenkins |
| Nome | Identifica um recurso com uma designação compreensível para os usuários. | rg-connect-001 = Resource group |
| | | vm-connect-01 = Máquina virtual |
| Ambiente | Indica o estágio do aplicativo e é útil para análise de custos, operações e segurança. | teste = Ambiente de teste |
| | | dev = Ambiente de desenvolvimento |
| | | prod = Ambiente de produção |
| Função | Define a função de um recurso em um aplicativo, auxiliando os engenheiros na operação e monitoramento. | BD = BancoDeDados |
| | | WebSvr = ServiçoWeb |
| Unidade de Negócios | Identifica a principal divisão organizacional proprietária do recurso ou conta na nuvem. | RH = Recursos Humanos |
| | | Financa = Controle de finanças |
| | | mkt = Marketing |

Continua na próxima página

**Tabela 4.1 – Continuação da página anterior**

| Orientação de tag | Descrição | Exemplo |
|---|---|---|
| Processo de Negócios | Indica a função ou processo principal que um recurso na nuvem suporta, facilitando o rastreamento de custos, monitoramento da saúde e avaliação de riscos para a entrega de relatórios. | Primários = Core Business |
| | | Apoio = Pessoal de apoio técnico |
| | | Gerencial = Equipe de gestão |
| Centro de Custos | Vincula um recurso a um centro de custos específico, facilitando a contabilização e gestão de custos para os gerentes responsáveis por um processo de negócios. | CC1 = Centro de Custos 1 |
| | | CC2 = Centro de Custos 2 |
| Esquema de Conformidade | Identifica o padrão regulatório para a configuração do recurso, usado por ferramentas de análise de configuração para verificar a conformidade e auxiliar em auditorias. | ISO27001 = padrão de segurança da informação |
| | | LGPD = Lei Geral de Proteção de Dados |
| Esquema de Conformidade | | HIPAA = Lei de Portabilidade e Responsabilidade do Seguro Saúde |

Etapa 6: Emprego da política de marcação

A implementação das *tags* selecionadas varia de acordo com as recomendações e orientações fornecidas pelo provedor de serviços utilizado. No tópico 4.3.1 deste estudo, serão apresentadas algumas diretrizes recomendadas pelos próprios sites dos provedores.

Adicionalmente, a equipe encarregada da administração dos provedores de nuvem deve apresentar relatórios semanais contínuos para evidenciar o grau de abrangência das *tags*. Esses relatórios não apenas refletem o estado atual, mas também registram melhorias na cobertura das *tags* ao longo do tempo.

Etapa 7: Garantia de consistência

Se houver inconsistência na capitalização e nas convenções de nomenclatura entre as funções, as empresas correm o risco de criar *tags* duplicadas, o que pode resultar na incapacidade de visualizar relatórios de custos precisos e dados estatísticos.

Portanto, é crucial que as empresas estejam cientes de que cada provedor de nuvem adota uma abordagem ligeiramente diferente para a marcação e possui suas próprias restrições. Além disso, é importante observar que, para cada recurso, cada chave de *tag* deve ser única e ter apenas um valor. Então, a tabela abaixo apresenta alguns dos parâmetros de marcação para fornecedores de nuvem como AWS, Azure e GCP:

Etapa 8: Visualização da aplicação

Com o tempo, a estrutura do sistema de marcação em nuvem pública dentro da organização natural-

mente evoluirá, integrando a marcação como um componente inicial em grande parte dos processos de negócios. Recomenda-se, no entanto, começar esse processo criando e implementando um conjunto inicial de *tags* que satisfaça as demandas imediatas da empresa.

Adicionalmente, é crucial configurar alertas automatizados por e-mail diariamente ou semanalmente para os recursos que não possuem as *tags* necessárias. Algumas organizações podem optar por encerrar o processo na Etapa 6 se já tiverem alcançado a adoção desejada das *tags*. É essencial também estabelecer alertas para os recursos que permaneceram sem marcação por um período específico (por exemplo, 24 horas). Caso não sejam devidamente marcados, esses recursos podem ser encerrados (apenas para ambientes não produtivos) ou gerar notificações por e-mail ao gestor da área.

Etapa 9: Automatizar processos de marcação

*tags* bagunçadas e inconsistentes podem ser organizadas; recursos marcados erroneamente podem ser remarcados. Recursos em nuvem sem *tags* podem ser marcados com base em outros dados contextuais. Novos recursos em nuvem podem ser marcados automaticamente com base em políticas definidas. E as *tags* podem ser agrupadas em hierarquias.

Etapa 10: Prepare o terreno para o futuro

Marque desde o início e marque regularmente, mesmo que haja alguns recursos que não são comumente usados hoje, eles podem se tornar uma parte essencial de planos e projetos futuros. Quanto mais cedo marcar os recursos, mais fácil será acompanhá-los e lidar com os processos de gerenciamento.

Após a implementação, espera-se que as *tags* facilitem às equipes na Nuvem a identificação de recursos de aplicativos e seus respectivos proprietários. Isso se revela crucial tanto para a contabilidade de custos quanto para a análise de riscos. Adicionalmente, a delimitação dos recursos envolvidos na operação de um aplicativo ou ambiente se torna essencial, proporcionando um meio eficiente para abordar questões relacionadas ao desempenho e disponibilidade.

### 4.3.1 Implementação de *tags* em Provedores de Nuvem

É importante se atentar que cada provedor de nuvem possui limites e restrições distintos em relação às *tags*. Na tabela abaixo, são apresentados alguns dos parâmetros de marcação para fornecedores mencionados anteriormente, tais como AWS, Azure e GCP:

Embora esses limites existam e, às vezes, compliquem o processo de marcação, desempenham um papel suficiente, pois ajudam as organizações a criar um sistema de marcação em nuvem coordenado.

#### 4.3.1.1 Como Usar a Função de Editor de *tags* da AWS

Conforme foi mencionado, existem duas categorias de *tags* na AWS, a saber:

- *Tags* Geradas pela AWS: São etiquetas automaticamente geradas pela AWS e, portanto, não estão sujeitas a modificações por parte do usuário. Normalmente, elas iniciam com o prefixo “aws:” (por exemplo, aws:createdBy) e são compostas por uma sequência alfanumérica. Ao examinar a *tag*

Tabela 4.2: Comparação de *tags* entre Google, AWS e Azure

| | **Google** | **AWS** | **Azure** |
|---|---|---|---|
| *tag* por recursos | 64 | 50 | 64 |
| Caracteres da chave | 63 | 127 | 512 |
| Caracteres do valor | 63 | 256 | 256 |
| Case sensitive | Somente letras minúsculas | Sim (chave e valor) | Não |
| Caracteres permitidos | Letras minúsculas, caracteres numéricos, sublinhados e traços. | Letras, espaços e caracteres especiais | Alfanumérico |
| Observações | As chaves devem começar com uma letra minúscula. As *tags* são chamadas de "Labels" no GCP. Existem "*tags* de rede" no GCP usadas para aplicar regras de firewall. Estas são separadas dos rótulos. | Não use "aws" como prefixo, pois isso é reservado para a AWS. Ative determinadas *tags* para alocação de custos para que elas apareçam nos relatórios de faturamento. Chaves de *tag* para relatórios de gerenciamento de faturamento e custos: Máximo 500. | *Tag* no nível do Grupo de Recursos ou do Recurso. Sugerir nível de recurso para melhor alocação de custos. Combine *tags* ou use a string JSON se exceder o limite de 15 *tags*. |
| Recursos tagueados | Compute Instance, Cloud SQL e outros | EC2, RDS e outros | Todos os recursos do ARM podem utilizar *tags*. |

"createdBy", torna-se possível identificar o responsável pela criação do recurso. Exemplos típicos de *tags* geradas pela AWS abrangem IDs de sub-rede e IDs de instância.

- *Tags* Geradas pelo Usuário: São *tags* que podem ser criadas, personalizadas e implementadas conforme necessário para atender aos requisitos específicos. A AWS permite a adição de até 50 *tags* a um único recurso, proporcionando flexibilidade para organizar e categorizar os recursos de acordo com as necessidades do usuário.

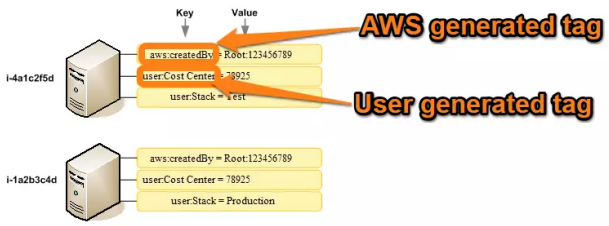


Figura 4.4: Duas categorias de *tags*, Fonte: Documentação da AWS (AWS, 2022)

Dessa forma, é importante observar que um recurso pode ter, no máximo, 50 *tags* atribuídas pelo usuário, conforme outras orientações. E a adição de novas etiquetas a um recurso pode ser impedida quando se aproxima desse limite de marcações definido pelo usuário. Entretanto, as *tags* geradas automaticamente pela AWS não entram no limite das 50 marcações. Além disso, as chaves das *tags* devem ser exclusivas

nos recursos selecionados, impedindo a adição de uma nova *tag* com uma chave já existente nos recursos escolhidos.

Com esse entendimento, uma ferramenta que permite adicionar e editar *tags* para qualquer recurso na Amazon Web Services, é o Editor de *Tags*. Essa ferramenta, possibilita a inclusão de etiquetas nos recursos selecionados, os quais podem ser identificados nos resultados da busca por "Encontrar recursos para marcar". Após localizar os recursos desejados, o editor oferece funcionalidades como adição, visualização, edição e exclusão das *tags* conforme necessário.

A AWS em (AWS, 2023), recomenda os seguintes passos para adicionar marcações:

1. 1. Acesse o Console de Gerenciamento da AWS. Em seguida, opte pelo Editor de Tags.

2. Na tabela de resultados da consulta Localizar recursos para marcar, assinale as caixas de seleção ao lado dos recursos aos quais se deseja adicionar *tags*. Insira uma sequência de texto em Filtrar recursos na parte superior da tabela para realizar um filtro com base em parte do nome, ID, chaves de *tag* ou valores de etiqueta do recurso. Na coluna *tags*, observe que os recursos nos resultados já possuem marcações atribuídas a eles. Como ilustração, na instância do EC2 fornecida como exemplo, já existem duas etiquetas aplicadas.

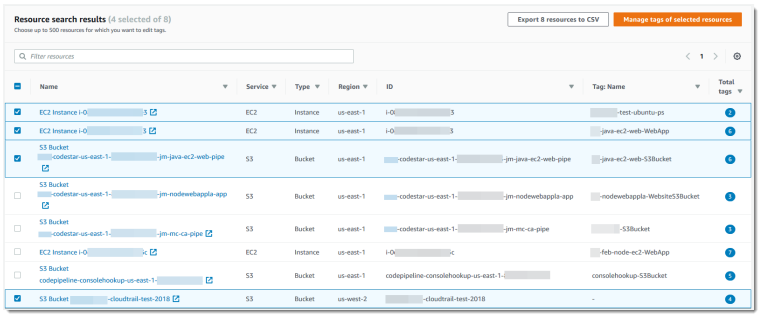


Figura 4.5: Página de Resultados da pesquisa de recursos, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

3. Marque a caixa de seleção de um ou mais recursos e opte por Gerenciar *tags* dos recursos selecionados.

4. Na página Gerenciar tags, apresentada a seguir, examine as *tags* nos recursos que foram selecionados. Apesar de sua consulta original ter retornado mais recursos, a adição de etiquetas está sendo realizada exclusivamente nos recursos escolhidos na etapa 1. Escolha Adicionar tag

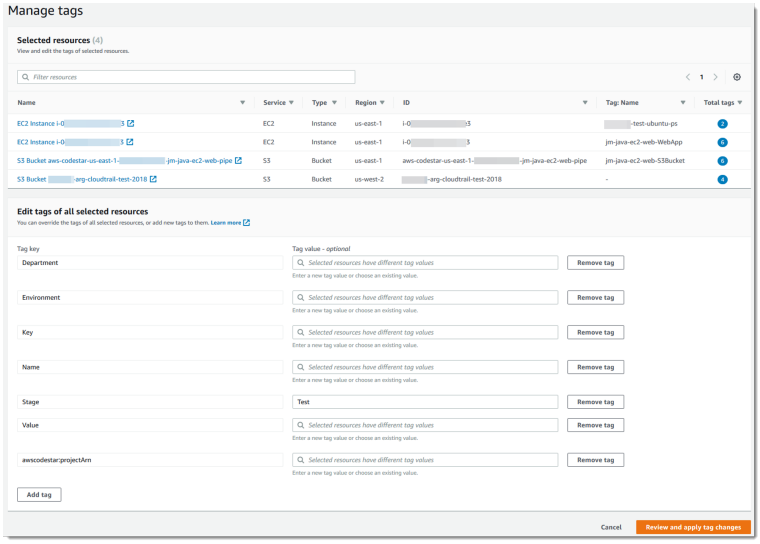


Figura 4.6: Página de gerenciamento de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

5. Inclua uma chave de *tag* e um valor de *tag* opcional. No exemplo a seguir, para esse procedimento, foi adicionada a chave da *tag* “Team” e o valor da *tag* “Development”.

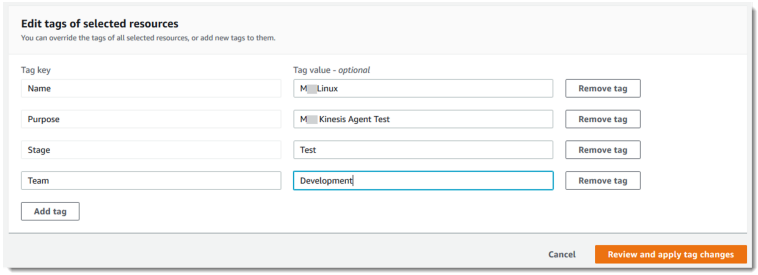


Figura 4.7: Página de edição de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

6. Ao concluir a adição de *tags*, opte por Revisar e aplicar as alterações.

7. Caso concorde com as alterações, selecione Aplicar alterações a todos os selecionados.

8. Dependendo do número de recursos escolhidos, a aplicação das novas *tags* pode demandar alguns minutos. Evite sair da página ou abrir outra página na mesma guia do navegador. Se as alterações forem bem-sucedidas, um banner de sucesso verde será exibido na parte superior da página. Aguarde até que um banner de sucesso ou falha apareça na página antes de prosseguir.

Além da adição, o Editor de *Tags* exibe as *tags* existentes nos recursos escolhidos que surgem nos resultados da consulta. E assim, visualizar as *tags* e exportar os resultados (WILLIS, 2023), recomenda-se as instruções a seguir:

1. 1. Nos resultados da sua consulta Encontrar Recursos para Marcar, selecione um número na coluna Total de *Tags* para qualquer recurso, para visualizar as etiquetas existentes. Observação: recursos que têm um traço na coluna Total de *Tags* não têm marcações existentes.

2. Visualize as *tags* existentes em *Tags* de Recurso. Esta janela também pode ser aberta na página gerenciamento.

3. Para exportar os resultados da pesquisa para um arquivo de valores separados por vírgula (CSV) a fim de auxiliar no desenvolvimento de uma estratégia de marcação para recursos na organização ou identificar sobreposições ou inconsistências na marcação na nuvem entre aplicativos e recursos.

4. Nos resultados da pesquisa, opte por Exportar Recursos para CSV.

5. Ao ser solicitado pelo navegador, escolha abrir o arquivo CSV ou salvá-lo em uma localização conveniente.

A modificação de uma *tag* implica na alteração do valor dessa *tag* em todos os recursos selecionados que possuem a mesma chave de tag. Não é viável renomear uma chave de *tag*; no entanto, é possível excluir uma *tag* e criar uma nova com um nome diferente para substituir a chave original. Destaca-se que essa ação resulta na exclusão de todas as *tags* com essa chave nos recursos selecionados. Assim, as instruções a seguir demonstram como excluir uma *tag* para ser substituída ou excluída permanentemente:

1. Nos resultados da consulta "Encontrar recursos para marcar", figura 4.5, assinale as caixas de seleção adjacentes aos recursos nos quais deseja alterar *tags* existentes. Insira uma sequência de texto em "Filtrar recursos" para realizar um filtro com base em parte do nome ou do ID do recurso. Na coluna "*Tags*", observe que os recursos nos resultados já possuem marcações atribuídas a eles. Na ilustração, na instância do EC2 selecionada no exemplo, já existem duas etiquetas.

2. Opte por "Gerenciar *tags* dos recursos selecionados".

3. Na página "Gerenciar *tags*", em "Editar *tags* de recursos selecionados", observe as etiquetas no recurso selecionado. Apesar de sua consulta original poder ter retornado mais recursos, a alteração das marcações ocorre exclusivamente nos recursos escolhidos na etapa 1.

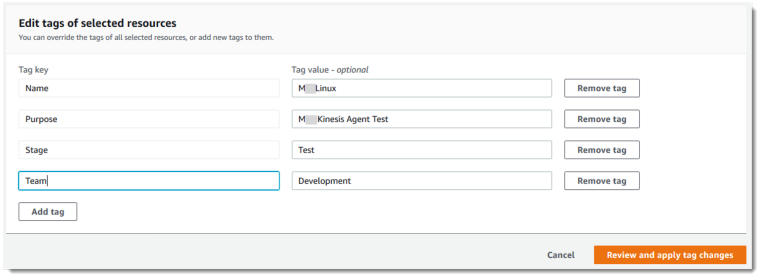


Figura 4.8: Página de edição de *tags* de recursos selecionados, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

4. Altere, adicione ou exclua os valores das *tags*. As etiquetas devem possuir uma chave, sendo os valores opcionais. Como exemplo, neste procedimento, o valor da *tag* "Team" foi alterado para "QA".

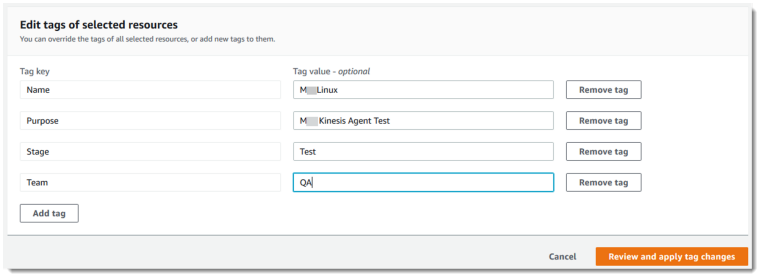


Figura 4.9: Alteração de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

Se os recursos na seleção apresentarem valores distintos para a mesma chave, será exibida a lista dos diferentes valores de *tag* no campo "Valor da tag" quando os recursos selecionados possuírem valores diferentes. Nessa situação, ao posicionar o cursor na caixa, será aberta uma lista suspensa contendo todos os valores disponíveis para essa chave de *tag* nos recursos selecionados.

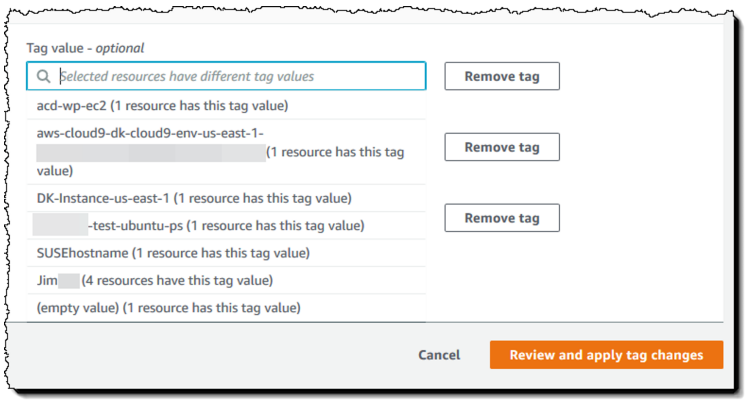


Figura 4.10: Valores de *tags*, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

Se os recursos na seleção contiverem o valor desejado para a tag, o próprio valor será destacado à medida que for digitado. Por exemplo, se os recursos na seleção já possuírem o valor da *tag* "QA", esse valor será realçado à medida que seja inserida a letra "Q". Os valores disponíveis na lista suspensa auxiliam na manutenção da consistência dos valores das *tags* em todos os recursos. A alteração no valor da *tag* reflete em todos os recursos selecionados. Neste exemplo, o valor da *tag* é modificado para "QA" em todos os recursos selecionados que possuíam a chave de *tag* "Team". Para recursos selecionados sem a *tag* "Team", é adicionada a *tag* "Team" com o valor "QA".

5. Ao concluir a alteração das *tags*, opte por "Revisar e aplicar as alterações".

6. Caso aceite as alterações, selecione "Aplicar alterações a todos os selecionados".

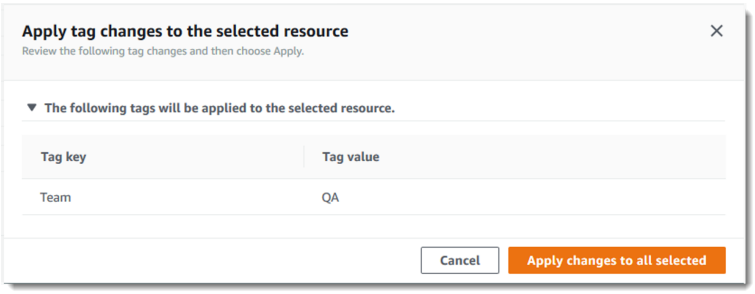


Figura 4.11: Aplicar alterações a todos os selecionados, Fonte: Documentação da AWS (AWS Partner Network (APN) Blog, 2022)

Para o caso de não obter sucesso em algumas ou todas as alterações de *tags* mencionadas anteriormente, recomenda-se a consulta do guia de "Solução de problemas de alterações de *tags*". Após abordar as causas fundamentais de alterações mal sucedidas nas marcações, como permissões insuficientes, é possível repetir as alterações das etiquetas nos recursos para os quais as tentativas anteriores falharam. (AWS, 2023).

Conforme abordado na seção 4.1 deste estudo, muitas empresas adotam a tecnologia em nuvem com a expectativa principal de economia financeira. Nesse contexto, a Amazon Web Services oferece diretrizes com o intuito de simplificar e acelerar o acompanhamento e a compreensão dos gastos na plataforma, especialmente durante a fase completa de implementação. Essas orientações fazem uso das "*tags* de alocação de custos", desempenhando um papel crucial para alcançar a meta principal de administração orçamentária. Considere essas *tags* como rótulos especiais que devem ser associados aos seus recursos na AWS, possibilitando uma organização mais eficiente e um rastreamento aprimorado dos custos associados. Assim, destacam-se em (AWS, 2021) as seguintes considerações:

- Ativação Específica: Ao contrário das *tags* comuns, é preciso especificamente designar uma ou mais marcações como "*tags* de alocação de custos" na AWS. Isso ajuda a garantir que seus gastos sejam categorizados corretamente.
- Transferência de Contas: Mover uma conta para outra organização, é necessário reativar as *tags* de alocação de custos para essa conta.
- Acesso Restrito: Apenas uma conta de gerenciamento ou uma conta independente (que não é membro de uma organização) pode acessar as *tags* de alocação de custos no Billing and Cost Management.
- Habilitação Necessária: Para ver suas *tags* de alocação de custos no Billing and Cost Management, é necessário ter habilitado recursos como AWS Cost and Usage Reports, AWS Cost Explorer, relatórios legados ou AWS Budgets.
- Recursos Antigos: Se houve a criação de recursos antes de começar a usar *tags*, esses recursos não terão etiquetas associadas a eles e não podem ser retroativamente marcados.
- Recursos sem Medição: Recursos que não geram custos, mesmo que possam ser marcados, não aparecerão nos relatórios de Gerenciamento de Custos.

- Marcação Manual: O Billing and Cost Management não faz a marcação automaticamente. Será preciso marcá-los manualmente para começar a acompanhar e entender seus gastos na AWS. Pense nessas marcações como rótulos que ajudam a organizar e compreender seus custos de maneira mais clara.(AWS, 2021)

#### 4.3.1.2 Como Marcar Aplicações na Nuvem no Azure

Nesta seção, será abordado o processo de marcação de recursos utilizando o portal do Azure para marcação de *tag* no ambiente de nuvem.

Para adicionar *tags*, a Microsoft sugere que:

1. Para visualizar as *tags* de um recurso ou de um grupo de recursos, procure por *tags* existentes na visão geral. Se ainda não tiver aplicado etiquetas anteriormente, a lista estará vazia.

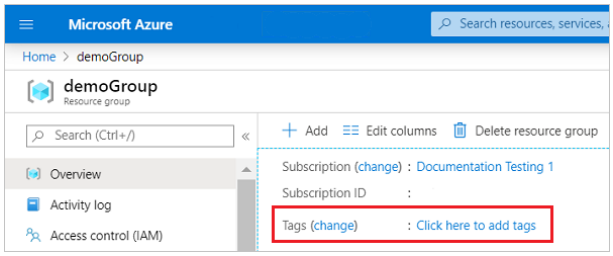


Figura 4.12: Lista de *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

2. Para adicionar uma tag, selecione “Clique aqui para adicionar *tags*”.
3. Forneça um nome e um valor.

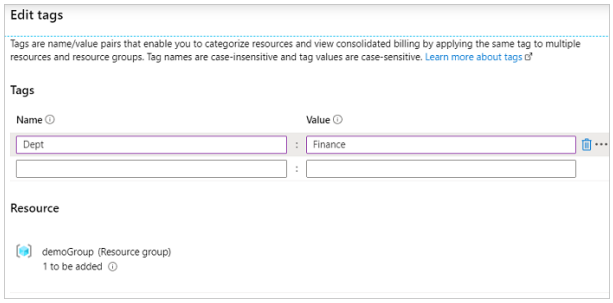


Figura 4.13: Página de edição de *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

4. Continue adicionando *tags* conforme necessário. Quando terminar, selecione Salvar.
5. As *tags* agora são exibidas na visão geral.

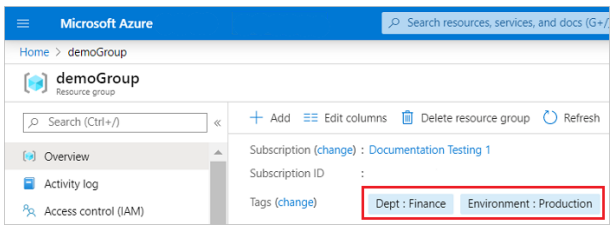


Figura 4.14: Lista com as *tags* criadas, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

Para editar as *tags*, recomenda-se que siga as instruções abaixo:

1. Para adicionar ou excluir uma tag, selecione alterar.
2. Para excluir uma tag, selecione o ícone da lixeira. Em seguida, salve.

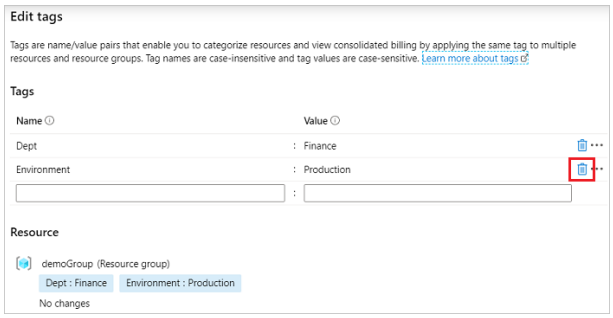


Figura 4.15: Editar as *tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

Para aplicar *tags* em larga escala a diversos recursos:

1. Em qualquer lista de recursos, selecione a caixa de seleção dos recursos aos quais deseja atribuir a tag. Em seguida, selecione Atribuir *tags*.

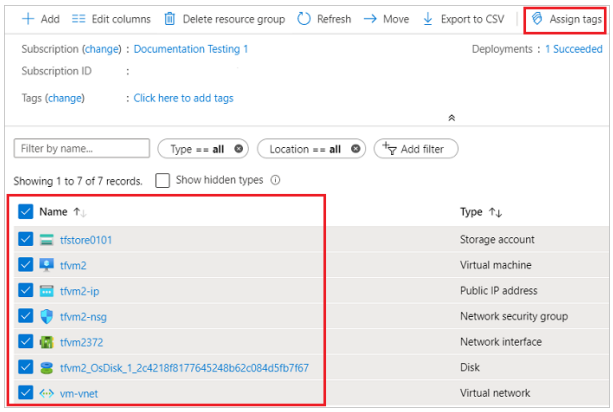


Figura 4.16: Lista de recursos, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

2. Adicione nomes e valores. Quando terminar, selecione Salvar.

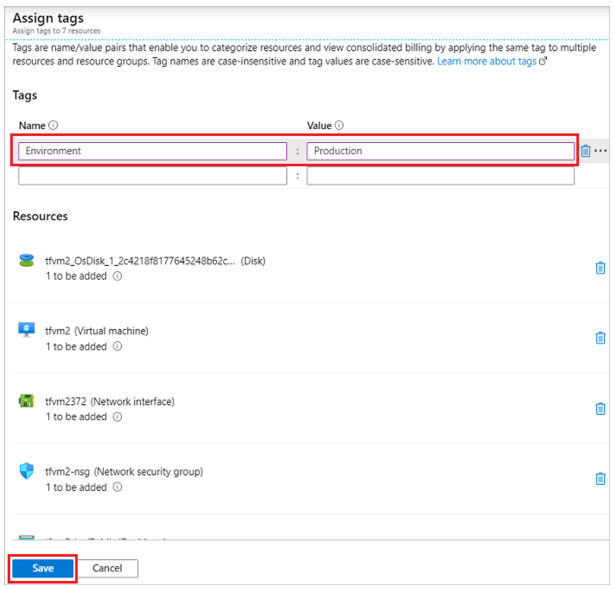


Figura 4.17: Atribuir etiquetas, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

Para visualizar todos os recursos com uma tag:

1. No menu do portal do Azure, pesquise por *tags*. Selecione essa opção disponível.
2. Selecione a *tag* para visualizar os recursos.

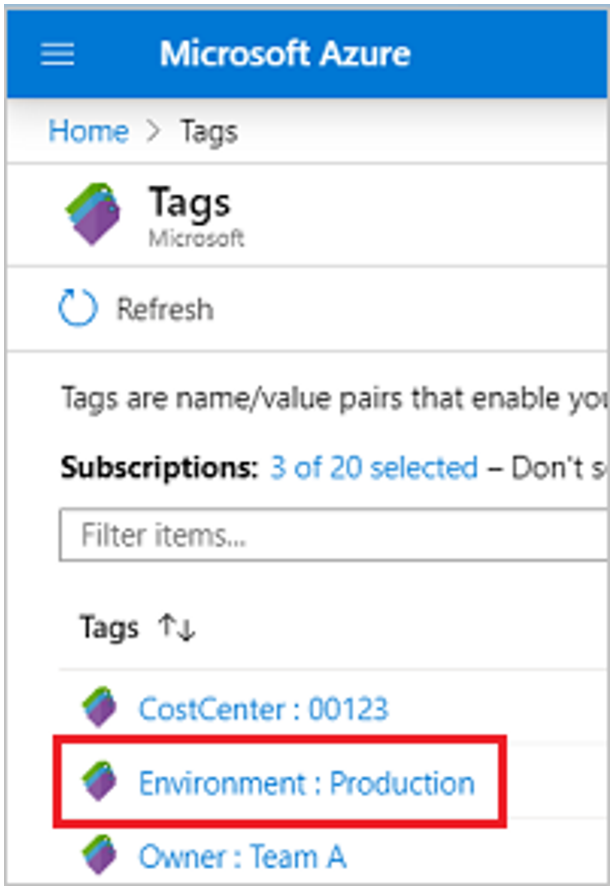


Figura 4.18: *Tags*, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

3. Todos os recursos com essa *tag* são exibidos.

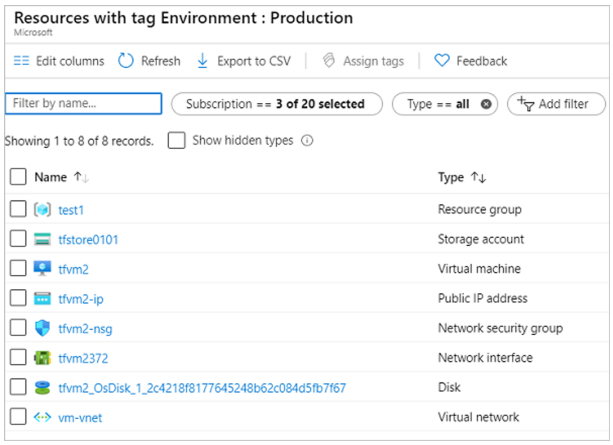


Figura 4.19: Recursos com a etiqueta ambiente: Produção, Fonte: Learn Microsoft (MARTINEKUAN, 2023)

O objetivo principal é assegurar uma estrutura organizacional mais coesa, simplificando a categorização, identificação e rastreamento eficaz dos recursos disponíveis. Nesse contexto, torna-se viável estabelecer a obrigatoriedade do uso de *tags* como uma prática fundamental na administração de recursos em ambientes de nuvem, como é o caso do Azure. A seguir, apresentam-se alguns passos recomendados para implementar essa abordagem:


Figura 4.20: Aplicando políticas para *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

Após selecionar a política destacada na imagem, o próximo passo é atribuir (Assign) de acordo com o escopo desejado.

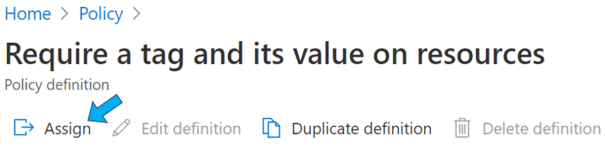


Figura 4.21: Atribuição de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

E quando se trata de políticas, no Azure é possível atribuir em três níveis:

- Management Group - Subscription - Resource Group Neste caso, vamos aplicar ao Resource Group: RG-

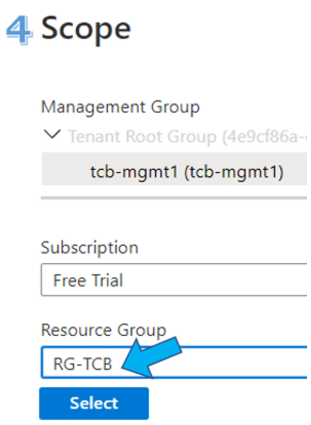


Figura 4.22: Grupo de recursos, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

No último estágio, é imperativo fornecer tanto o nome (*Tag Name*) quanto o valor da etiqueta (*Tag Value*) na guia denominada “Parameters”:

Para finalizar, clique em “Review + create” e, em seguida, em “Create”!

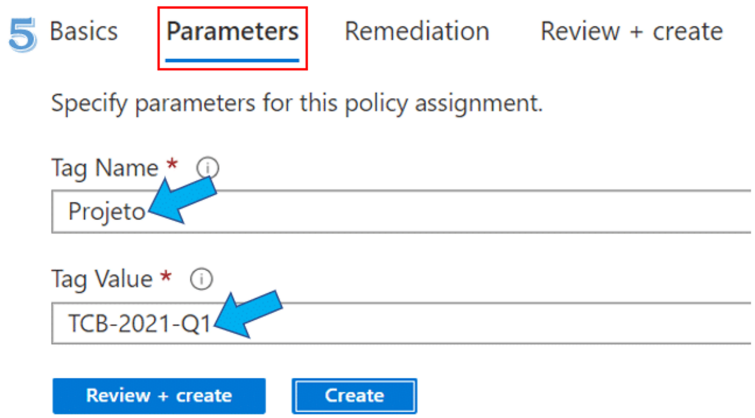


Figura 4.23: *Tag Name* e *Tag Value*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

A Microsoft recomenda aguardar por um tempo entre 5 e 15 minutos para que uma política seja efetivada. Assim, passado o tempo, vamos ao teste, que consiste na tentativa de criação do recurso Storage Account, dentro do Resource Group: RG-TCB , sem informar uma *tag* e seu respectivo valor.

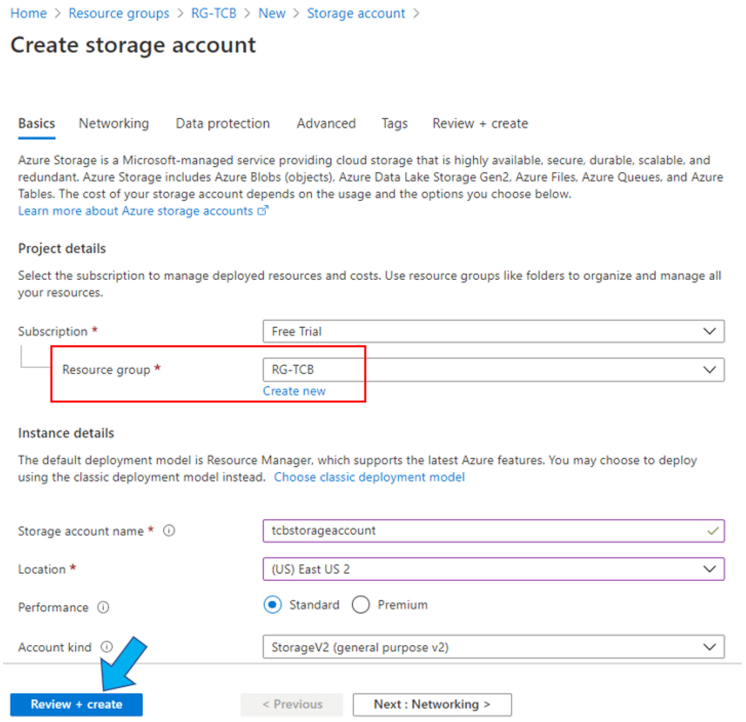


Figura 4.24: Criando a Política de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

Na etapa de validação, é importante clicar em "Revisar + Criar" para dar continuidade ao processo. Caso encontre um erro, recomenda-se obter informações detalhadas clicando para visualizar os detalhes correspondentes. De acordo com a mensagem fornecida, é necessário observar uma política específica que requer a inclusão de uma *tag* e seu respectivo valor no recurso para que a criação seja bem-sucedida.

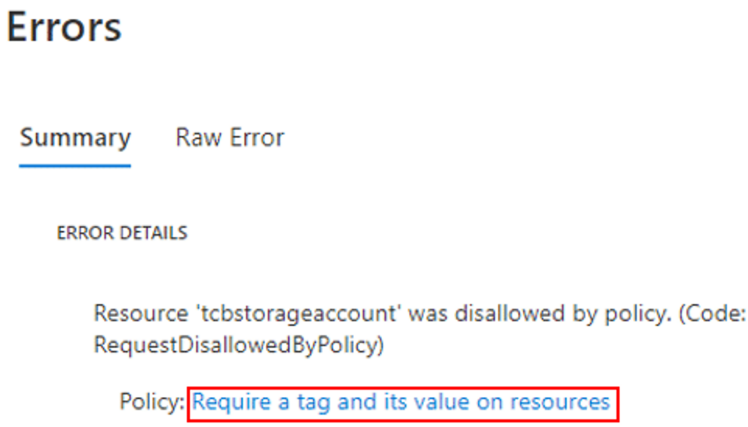


Figura 4.25: Erro de criação da política de *tags*, Fonte: The Cloud Boot Camp (PEREIRA, 2023)

Importante frisar que, as *tags* não são herdadas, ou seja, caso uma *tag* tenha sido aplicada à um "Resource Group", não significa que os recursos contidos neste, herdarão sua respectiva marcações. Mas existem políticas que altere essa funcionalidade, alguns exemplos podem ser vistos na tabela:

Tabela 4.3: Políticas para a marcação de recursos na nuvem

| **Name** | **Descrição** | **Effect(s)** | **Version (GitHub)** |
|---|---|---|---|
| Add or replace a *tag* on resources | Adiciona ou substitui a etiqueta e valor especificados quando um recurso é criado ou atualizado. Recursos existentes podem ser corrigidos acionando uma tarefa de correção. Não modifica as etiquetas dos grupos de recursos. | modify | 1.0.0 |
| Append a *tag* and its value to resource groups | Acrescenta a etiqueta e valor especificados quando um grupo de recursos que está sem essa etiqueta é criado ou atualizado. Não modifica as etiquetas dos grupos de recursos criados antes da aplicação desta política até que esses grupos de recursos sejam alterados. Novas políticas de efeito 'modificar' estão disponíveis para suporte à correção de etiquetas em recursos existentes. | append | 1.0.0 |
| Inherit a *tag* from the resource group | Adiciona ou substitui a etiqueta e valor especificados do grupo de recursos pai quando um recurso é criado ou atualizado. Recursos existentes podem ser corrigidos acionando uma tarefa de correção. | modify | 1.0.0 |
| Inherit a *tag* from the resource group if missing | Adiciona a etiqueta especificada com seu valor do grupo de recursos pai quando um recurso que está sem essa etiqueta é criado ou atualizado. Recursos existentes podem ser corrigidos acionando uma tarefa de correção. Se a etiqueta existir com um valor diferente, ela não será alterada. | modify | 1.0.0 |
| Require a *tag* and its value on resource groups | Impõe uma etiqueta e seu valor obrigatórios nos grupos de recursos. | deny | 1.0.0 |
| Require a *tag* on resource groups | Impõe a existência de uma etiqueta nos grupos de recursos. | deny | 1.0.0 |

#### 4.3.1.3 Como usar *tags* no GCP

No Google Cloud Platform, a organização de recursos no Cloud Storage é realizada através das *tags* do Google Cloud e dos rótulos de bucket do Cloud Storage. As etiquetas podem ser aplicadas em níveis mais altos da hierarquia de recursos e em todo o ambiente do Google Cloud. Gerenciadas pelo Resource Manager, elas podem ser referenciadas nas vinculações de políticas do IAM (Gerenciamento de Identidade e Acesso) para conceder acesso condicional a recursos. Os rótulos de bucket, por sua vez, são gerenciados por meio das ferramentas específicas do Cloud Storage. É relevante ressaltar que *tags* e rótulos operam independentemente um do outro, possibilitando a utilização simultânea de ambos em um mesmo bucket.

Um recurso de chave de *tag* pode ser criado nos recursos da organização ou do projeto, e os valores de *tag* são recursos anexados a uma chave. É possível criar no máximo 1.000 chaves em uma determinada organização ou projeto, com um total de 1.000 valores criados para cada chave. Por fim, é possível anexar esses valores a recursos na sua hierarquia, que têm a associação do par de chave-valor. Então, para começar, é preciso criar uma chave de tag.

Para criar uma nova tag, primeiro é necessário criar uma chave que descreva a *tag* está sendo criada. Assim, o "*shortName*" da chave de *tag* pode ter no máximo 256 caracteres. O conjunto de caracteres permitidos inclui caracteres Unicode codificados em UTF-8, exceto aspas simples (’), aspas duplas (”) e barras invertidas (\), e barras normais (/).

Depois de criado, o "*shortName*" não pode ser alterado e precisa ser exclusivo no mesmo namespace. Assim, para criar uma chave de tag, faça o seguinte:

1. Abra a página *tags* no console do Google Cloud.
2. No Seletor de escopo na parte de cima da página, escolha a organização ou o projeto que usará para criar uma chave de tag.
3. Clique em Criar.
4. Na caixa Chave da tag, insira o nome de exibição da chave. Isso se torna parte do nome de namespace da tag.
5. Na caixa Descrição da chave da tag, insira uma descrição da sua chave.
6. Para adicionar valores da *tag* a essa chave, clique em add Adicionar valor para cada valor de *tag* que quiser criar.
7. Na caixa Valor da tag, insira o nome de exibição do valor da sua tag. Isso se torna parte do nome de namespace da tag.
8. Na caixa Descrição do valor da tag, insira uma descrição.
9. Quando terminar de adicionar valores de tag, clique em Criar chave de tag.

Depois de criar a chave, é possível encontrar o nome de exibição legível exclusivo chamado ”namespacedName”, que tem namespace no recurso pai e um ID permanente, exclusivo globalmente, chamado ”name”.

Quando um par de chave-valor de *tag* é anexado a um recurso, todos os descendentes desse recurso herdam a tag. É possível modificar uma *tag* herdada em um recurso descendente. Para isso, aplique uma *tag* usando a mesma chave da herdada, mas com um valor diferente.

Por exemplo, considere a atribuição da identificação “ambiente: desenvolvimento” a uma pasta, que possui duas subpastas denominadas “equipe-a” e “equipe-b”. É igualmente possível associar uma identificação distinta, como “ambiente: teste”, à subpasta “equipe-b”. Isso implica que os projetos e demais itens contidos na “equipe-a” adotarão a identificação “ambiente: desenvolvimento”, enquanto os projetos e demais itens da “equipe-b” adotarão a identificação “ambiente: teste”.

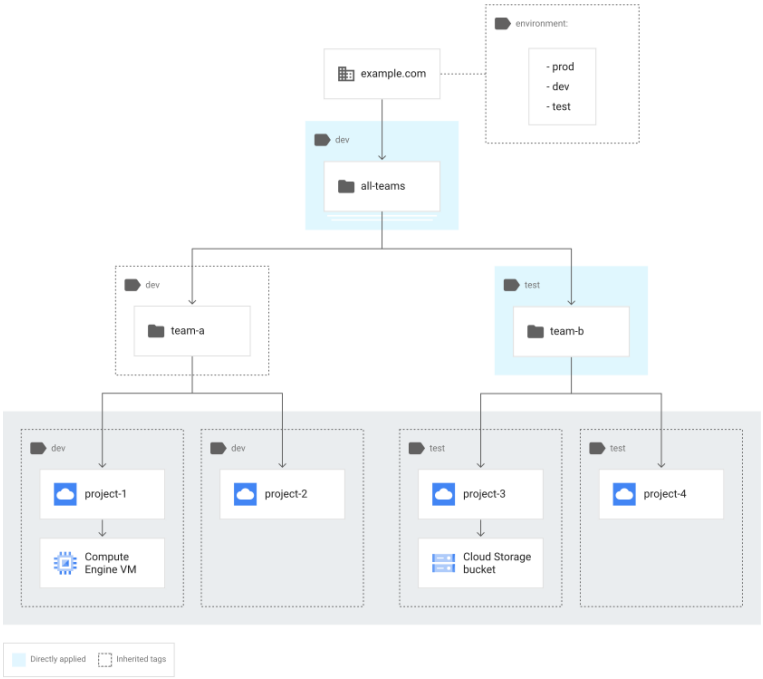


Figura 4.26: Estrutura de herança no Google Cloud Plataform, Fonte: GCP (CLOUD, 2023)

Ao remover a identificação “ambiente: teste” da pasta “equipe-b”, a pasta e seus recursos passarão a herdar a identificação “ambiente: desenvolvimento”.

No Google Cloud Platform (GCP), as identificações atribuídas a um recurso, sejam elas diretas ou herdadas de seus ancestrais na hierarquia, são coletivamente referidas como “identificações efetivas”. Essas identificações efetivas resultam da combinação das identificações diretamente associadas ao recurso e das identificações associadas a todos os ancestrais do recurso em toda a hierarquia.

É possível obter informações sobre uma determinada chave de identificação usando o ID permanente ou o nome do “namespace” atribuído durante a criação. Para visualizar uma identificação criada:

1. Abra a página *tags* no console do Google Cloud.
2. No Seletor de escopo na parte superior da página, escolha a organização ou o projeto que contém a identificação.
3. Todas as identificações na organização ou projeto selecionados aparecerão na lista. Clique na identificação relacionada à chave que deseja verificar.

Ao referenciar identificações usando a Google Cloud CLI, pode-se utilizar o nome com "*namespace*" ou o ID permanente para chaves e valores de identificações. Chamadas para a API, exceto "*getNamespaced*", devem usar apenas o ID permanente.

Além disso, é possível modificar uma identificação existente atualizando a chave ou os valores associados a ela. É viável também, atualizar a descrição de uma identificação, mas não o nome curto.

Para atualizar a descrição da chave de identificação, siga estas etapas:

1. Abra a página *tags* no console do Google Cloud.
2. No Seletor de escopo na parte superior da página, escolha a organização ou o projeto que contém a chave de identificação.
3. Clique em Ações ao lado da chave de identificação que deseja atualizar e clique em Visualizar detalhes.
4. Clique em Editar ao lado de Descrição, na parte superior da tela.
5. Atualize a descrição da chave de identificação.
6. Clique em Salvar.

Também é possível alterar a descrição dos valores da identificação.

Para listar todas as chaves de identificação associadas a uma organização ou recurso de projeto específico usando o console do Google Cloud, a CLI gcloud ou uma chamada para a API. O mesmo se aplica à listagem de todos os valores de identificação associados a uma chave de identificação específica. Assim, visualizar todas as identificações, as instruções são:

1. Abra a página *tags* no console do Google Cloud.
2. No Seletor de escopo na parte superior da página, escolha a organização ou o projeto que contém as identificações.
3. Todas as identificações criadas nessa organização ou projeto aparecerão na lista.

Ao remover uma chave ou definição de valor, se a identificação estiver associada a um recurso, a remoção não será bem-sucedida. É necessário eliminar as associações existentes, chamadas de vínculos de identificação, antes de excluir a definição da identificação em si. Para oferecer uma camada adicional de proteção aos valores de identificação, é possível vincular uma retenção de identificação a um valor específico. Essa retenção, semelhante a um vínculo de identificação, impede que um usuário exclua o valor associado. Alguns recursos automaticamente estabelecem uma retenção de identificação para cada valor vinculado ao recurso. Remover essa retenção é necessário para permitir que um usuário exclua o valor da identificação.

Após a criação de uma *tag* e a concessão do acesso apropriado à *tag* e ao recurso, é possível anexar a *tag* a um recurso no Google Cloud como um par de chave-valor. Cada recurso pode ter, no máximo, um

valor anexado para uma determinada chave. Por exemplo, se a *tag* "environment: development" estiver anexada, as *tags* "*environment: production*" ou "environment: test" não poderão ser anexadas. O número máximo de pares de chave-valor anexados a um recurso é 300.

Além disso, as *tags* são associadas aos recursos por meio da criação de um recurso de vinculação de etiquetas, que vincula o valor ao recurso do Google Cloud. O seguinte fluxo de trabalho descreve como anexar uma *tag* a um recurso em uma organização, pasta ou projeto:

1. Acesse a página Gerenciar recursos no console do Google Cloud.
2. Selecione a organização, pasta ou projeto no qual deseja associar uma tag.
3. Clique em *tags*.
4. No painel de *tags*, clique em Selecionar escopo.
5. Escolha a organização ou projeto que contém as *tags* e clique em Abrir.
6. No painel de *tags*, selecione Adicionar tag.
7. No campo Chave, escolha a chave da *tag* que deseja associar na lista. Para filtrar a lista, digite palavras-chave.
8. No campo Valor, escolha o valor da *tag* que deseja associar na lista. Para filtrar a lista, digite palavras-chave.
9. Se desejar associar mais *tags*, clique em Adicionar *tag* e selecione a chave e o valor de cada uma.
10. Clique em Salvar.
11. Na caixa de diálogo Confirmar, clique em Confirmar para associar a tag.
12. A notificação confirma que as *tags* foram atualizadas, e as novas etiquetas são exibidas na coluna *Tags* na página Gerenciar recursos.

É possível consultar uma lista de todas as *tags* associadas a um recurso, incluindo aquelas herdadas ou diretamente associadas. E para verificar todas as etiquetas associadas ou herdadas por um recurso, as instruções são:

1. Acesse a página **Gerenciar recursos** no console do Google Cloud.
2. Localize a organização, pasta ou projeto na lista de recursos.
3. As *tags* associadas ao recurso são exibidas na coluna *Tags*, e as etiquetas herdadas são marcadas como "Herdadas".

Por fim, é possível desassociar uma *tag* de um recurso excluindo o recurso de vinculação de *tags*. E para desassociar uma etiqueta de um recurso em uma organização, pasta ou projeto, as etapas são descritas como:

1. Acesse a página Gerenciar recursos no console do Google Cloud.
2. Selecione a organização, pasta ou projeto do qual deseja remover uma tag.
3. Clique em *tags*.
4. No painel de *tags*, ao lado da etiqueta que deseja remover, clique em Excluir item.
5. Clique em Salvar.
6. Na caixa de diálogo Confirmar, clique em Confirmar para remover a tag.
7. A notificação confirma que as *tags* foram atualizadas, e a lista atualizada de *tags* é exibida na coluna *tags* da página Gerenciar recursos.

## 4.4 MELHORES PRÁTICAS NO USO DE *TAGS*

Conforme discutido anteriormente, a associação de *tags* a recursos na nuvem oferece uma abordagem flexível e organizada para categorizar, rastrear e controlar os elementos fundamentais de uma infraestrutura virtual.

Nesse contexto, compreender e aplicar os métodos eficazes para o uso de *tags* em cloud computing é essencial para otimizar a eficiência operacional dessa tecnologia. Tomando isso em consideração, neste tópico apresenta-se uma visão abrangente e de alto nível de algumas das melhores práticas que podem ser adotadas para aprimorar significativamente a estratégia de marcação.

Uma prática recomendada é revisar o conjunto mínimo de etiquetas sugerido pelo provedor de nuvem escolhido para o seu projeto antes de começar. Avalie cada etiqueta quanto à sua importância e aplicabilidade ao seu negócio pois, algumas das etiquetas sugeridas pelo provedor podem não ser necessárias para o conjunto principal. (KUPERMAN, 2023)

Assim, o resultado do exercício de revisão descrito no ponto anterior é uma lista de etiquetas e suas descrições a serem usadas em seu projeto na nuvem. Inclua informações sobre a fonte dos dados para essas etiquetas, pois a falta de consistência nas marcações pode complicar e atrasar o processo. Por exemplo, se muitos recursos implantados não tiverem *tags* de alocação de custos, a análise de custos que depende dessas *tags* será imprecisa. (AWS Partner Network (APN) Blog, 2022)

Com foco econômico, a Azure recomenda o uso de um código de cobrança interno ou número de pedido como identificador de faturamento para o grupo de recursos, correspondendo a uma linha de diário geral. Algumas sugestão podem ser vistas na tabela 4.4, são *tags* específicas que facilitam a determinação do uso de faturamento para VMs em execução na produção (TFITZMAC, 2023).

Tabela 4.4: *Tags* com foco econômico

| **Nome da Tag** | **Estado** | **Descrição** | **Valor da Tag** | **Exemplo** |
|---|---|---|---|---|
| AppTaxonomy | Obrigatório | Fornece informações sobre quem é o proprietário do grupo de recursos e qual o propósito dele dentro de sua aplicação | Org | USOPS |
| MaintenanceWindow | Opcional | Fornece uma janela durante a qual podem ser realizadas manutenções de patch e outras impactantes | Janela em UTC "dia:hora:minuto-dia:hora:minuto" | Ter:04:00-Ter:04:30 |
| EnvironmentType | Obrigatório | Fornece informações sobre para que serve o grupo de recursos (útil para manutenção, aplicação de políticas, rateio, etc.) | Dev, Test, UAT, Prod | Test |
| BillingIdentifier | Obrigatório | Fornece um código de cobrança ou centro de custo para atribuir a fatura dos recursos | Centro de custo | 34821 |
| ExpirationDate | Opcional | Fornece uma data em que o ambiente deverá ser removido, para que relatórios possam confirmar se um ambiente ainda é necessário | Data de Expiração em UTC | 2016-06-15T00:00 |

Outra etapa inteligente, consiste em automatizar o processo de reconciliação de etiquetas. Estabelecer uma única fonte de verdade para as etiquetas e configurar um processo automatizado periódico que mantenha a sincronização entre todos os recursos e grupos na nuvem com essa fonte central. (KUPERMAN, 2023) É desaconselhável utilizar *tags* para armazenar dados confidenciais, como informações pessoais, devido ao amplo uso das *tags* em diversos serviços da nuvem, o que poderia resultar no compartilhamento desprevenido de informações sensíveis. (AWS, 2021)

Outra dica, é o uso de notificações automáticas para identificar etiquetas incorretas ou ausentes. Pois, configurar alertas e sistemas de detecção de anomalias é uma prática essencial para garantir que sua equipe seja prontamente informada sobre qualquer irregularidade. No entanto, é recomendável limitar o número de alertas recebidos para evitar a fadiga de alertas, assegurando que as notificações sejam eficazes e relevantes. (KUPERMAN, 2023)

Utilize uma plataforma que atenda ao ponto em que se encontra em a jornada de marcação, e que

possa fornecer insights de custo mesmo que a marcação não esteja perfeita.(AWS, 2021) Dado que, utilizar uma planilha para gerenciar e decodificar um grande volume de recursos marcados não é a abordagem recomendada. Uma plataforma de gerenciamento de custos na nuvem possibilita o processamento de *tags* em análises acionáveis, e algumas plataformas são capazes de corrigir erros de digitação e variações de ortografia para manter as *tags* organizadas. Engajar uma plataforma de gerenciamento de custos na nuvem em seu processo de marcação o mais cedo possível é altamente benéfico. Algumas plataformas de gerenciamento de custso recomendados, foram o Cass information System (SYSTEMS, 2018), Binadox (BINADOX, 2015) e Cloudability (CLOUDABILITY, 2019), segundo (WILLIS, 2023)

## 4.5 DESAFIOS

A computação em nuvem apresenta uma complexidade considerável, envolvendo a utilização de centenas de milhares de serviços em diversas plataformas. No entanto, contar apenas com marcação manual pode se tornar falha em alguns momentos, especialmente em ambientes que mudam constantemente, com novos projetos todos os dias, equipes dinâmicas e a importância de detalhes como maiúsculas e minúsculas em identificadores (SASI, 2023)

Em última análise, é difícil alcançar a perfeição nas etiquetas, e é provável que sempre existam alguns recursos sem marcação. Em muitos casos, esses recursos não marcados não pertencem exclusivamente a uma única equipe, o que complica a atribuição. Uma abordagem inicial para enfrentar esse desafio é associar serviços a equipes ou aplicativos com base em compartilhamento proporcional ou diretamente às equipes quando uma única equipe consome o serviço. (SASI, 2023)

Ainda assim, quando um recurso não está marcado, é possível rastrear seu custo agrupando sob a categoria “não alocados” em relatórios de custo até que recebam marcações apropriadas. (SASI, 2023)

Outros obstáculo comum para implementar uma marcação, é a adoção tardia. Pode ser desafiador desenvolver uma estratégia abrangente de marcação, que requer contribuições de diversas partes da organização, após o início do uso da nuvem. Muitas empresas ainda não passaram por esse processo ou estão tentando fazê-lo à medida que o uso da nuvem cresce.

Além disso, pode ocorrer a governança inadequada e falta de aplicação/consistência pois, à medida que as organizações se expandem e adicionam novas equipes e serviços em nuvem, quaisquer estruturas de marcação existentes inevitavelmente se desfazem sem esforço para mantê-las no lugar.

Finalmente, outro desafio enfrentado reside na falta de familiaridade com as ferramentas e plataformas disponíveis. A marcação pode se tornar complexa, especialmente para aqueles que não têm experiência com esse tipo de aplicação. Se a empresa utiliza uma abordagem de multi-nuvem, ou seja, envolve diversos provedores, como mencionado anteriormente, cada provedor de nuvem adota um método de marcação distinto, o que pode causar confusão.(AWS, 2021)

# 5 CONCLUSÃO

Neste trabalho, evidenciou-se que a computação em nuvem transformou significativamente a paisagem da Tecnologia da Informação, proporcionando flexibilidade e eficiência. Tornando assim, uma escolha estratégica para organizações globais, impulsionada por líderes como Oracle, Microsoft, Amazon e Google. No entanto, sua implementação requer uma abordagem cuidadosa para gerenciar riscos e garantir conformidade, destacando a importância da Governança, Gerenciamento de Riscos e Conformidade (GRC). Esse conjunto integrado de práticas visa não apenas atender a regulamentações, mas também promover crescimento, eficiência e transparência nos negócios.

Analisando cenários que não usam marcação de recursos ou fazem uma implementação de um plano de gestão de gastos na nuvem resulta em empresas gastando mais do que o planejado, conforme alertado pela Gartner (GARTNER, 2018). A falta de governança em TI e a descentralização do consumo de recursos são desafios adicionais, enquanto as ferramentas e APIs dos provedores de nuvem oferecem meios para controle e cálculo preciso de custos. O cenário destaca a necessidade de estratégias robustas e uma abordagem organizada para maximizar os benefícios da computação em nuvem.

A proposta de um framework para implementação e validação de tags em cloud computing, com ênfase em GRC, visa simplificar e padronizar a marcação de recursos na nuvem. O objetivo central é otimizar o uso desses recursos, garantindo eficiência operacional e evitando custos adicionais. O diagrama de processo sugerido, guia equipes de tecnologia na marcação de recursos, proporcionando contexto essencial para gerenciar, operar e proteger eficientemente esses recursos. O público-alvo inclui profissionais de TI, arquitetos, líderes, executivos e fornecedores de ferramentas. As etapas abrangem desde identificar requisitos até automatizar processos de marcação, visando garantir consistência, visualização eficaz e preparação para o futuro, destacando a importância da comunicação transparente da política de marcação.

Além disso, são apresentadas sugestões de tags para diferentes categorias e a inclusão do registro detalhado sobre as mudanças, destacando a necessidade de garantir consistência na capitalização e nas convenções de nomenclatura, além de alertar para limites e restrições específicos de provedores de nuvem, como AWS, Azure e Google Cloud. O intuito do framework é facilitar a identificação e gestão de recursos, contribuindo para a contabilidade de custos, análise de riscos e eficiência operacional na nuvem.

Assim, compreender e aplicar métodos eficazes para o uso de tags é crucial para otimizar a eficiência operacional. Nas melhores práticas destaca-se a necessidade de revisão contínua da estratégia de etiquetagem, enfatizando a importância da consistência e da utilização de plataformas de gerenciamento de custos na nuvem para análises acionáveis e correção de erros.

Ao adotar essas ideias, é possível criar uma estrutura sólida para a Governança, Risco e Conformidade em projetos de Cloud Computing. É importante que as organizações controlem cuidadosamente seus gastos, projetos e recursos, especialmente em órgãos públicos, onde a gestão eficiente desses elementos é quase sempre preferencialmente prioritário. Pois, nestas situações, as empresas devem operar de forma transparente e eficaz, dada a natureza dos recursos públicos com os quais lidam, muitas vezes exigindo prestações de contas detalhadas sobre suas despesas.

## 5.1 TRABALHOS FUTUROS

Considerando a crescente adoção de ambientes multi-cloud por parte de diversas empresas, faz-se necessário aprimorar o framework proposto, incorporando a integração de plataformas de gerenciamento de custos e a realização de comparações entre essas plataformas. Tal aprimoramento proporcionaria uma seleção mais informada e criteriosa, alinhada às necessidades específicas de cada organização.

Empresas como Cloudability (CLOUDABILITY, 2019), Flexera(FLEXERA, 2022), Binadox(BINADOX, 2015) e Cass information System (SYSTEMS, 2018), destacam-se no mercado ao oferecer ferramentas especializadas para monitorar e administrar uma ampla gama de recursos em nuvem. Isso abrange desde aplicativos SaaS até serviços em nuvem, conforme mencionado por Willis (WILLIS, 2023). Além disso, uma análise mais aprofundada e comparativa de outras empresas foi apresentada em (REDACAO, 2023), proporcionando uma visão mais abrangente sobre soluções dessa natureza.

Por estas plataformas terem como objetivo simplificar a análise e comparação de dados de custos na nuvem ao longo de períodos definidos. Elas destacam-se por identificar recursos não utilizados, subutilizados e ociosos, proporcionando às empresas uma visão mais clara sobre a eficiência do uso de seus recursos em nuvem. Além disso, essas plataformas oferecem recomendações de dimensionamento com base em cargas de trabalho previstas, permitindo uma alocação mais eficiente de recursos na nuvem. Logo, espera-se que uma proposta de adaptação do framework proposto, sera realizado com a integração dessas plataformas em estratérgias de utilizar serviços de nuvem de mais de um provedor simultaneamente.

# REFERÊNCIAS BIBLIOGRÁFICAS


5, C. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. 2012. Disponível online. Acesso em: 06 set. 2023. Disponível em: <http://www.isaca.org/cobit/>.

ABNT. *NBR ISO/IEC 17788:2015 (2016) - Tecnologia da informação - Computação em nuvem - Visão geral e vocabulário*. 2016. Disponível online. Acesso em: 28 jun. 2023.

ADTSYS. *Definição de TAGs e governança em cloud - ADTsys*. 2022. Disponível online. Acesso em: 28 jun. 2023. Disponível em: <https://www.adtsys.com.br/definicao-de-tags-e-governanca-em-cloud/>.

AL-ANZI, F. S.; YADAV, S. K. R.; SONI, J. Cloud computing: Security model comprising governance, risk management and compliance. *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, Sep 2014.

ALI, O.; OSMANAJ, V. The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law  Security Review*, v. 36, p. 105396, 2020. ISSN 0267-3649. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364920300017>.

ARATA, E. P.; RODRIGUES, C. F.; FARRAGONI, R. Análise de vulnerabilidades em cloud computing. *Revista FATEC SEBRAE em Debate: Gestão, Tecnologias e Negócios*, v. 05, n. 09, 2018. ISSN 2358-9817.

ASSIS, P. de. *O que é "tag"?* 2009. Disponível online. Acesso em: 29 set. 2023. Disponível em: <https://www.tecmundo.com.br/navegador/2051-o-que-e-tag-.htm>.

ÁVILA, M. D. G. Gestão de riscos no setor público - controle estratégico para um processo decisório eficiente. *Revista Controle: Doutrinas e Artigos*, v. 12, n. 2, p. 179–198, 2014. ISSN 1980-086X.

AWS. *Governance, Risk Management, and Compliance - Establishing Your Cloud Foundation on AWS*. 2020. Disponível online. Acesso em: 20 out. 2023. Disponível em: <https://docs.aws.amazon.com/whitepapers/latest/establishing-your-cloud-foundation-on-aws/governance.html>.

AWS. *AWS Tagging Strategy*. 2021. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://www.cloudzero.com/blog/aws-tagging-strategy/>.

AWS. *Best Practices for Tagging AWS Resources*. 2022. Disponível em: <https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/tagging-best-practices.html>.

AWS. *Como gerenciar tags de tags com o editor de tags - Marcar recursos do AWS*. 2023. Disponível online. Acesso em: 20 out. 2023. Disponível em: <https://docs.aws.amazon.com/pt_br/tag-editor/latest/userguide/tagging-resources.html>.

AWS Partner Network (APN) Blog. *How Better Tagging Can Help Organizations Optimize Expenses and Improve ROI*. 2022. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://aws.amazon.com/pt/blogs/apn/how-better-tagging-can-help-organizations-optimize-expenses-and-improve-roi/>.

BARROS MAISA CRUZ BRAGA, J. S. d. S. Conceição de M. P. Cloud computing. Instituto de Computação - Universidade Estadual de Campinas, 2012.

BEZERRA, E. K. *Gestão de riscos de TI: NBR 27005*. Rio de Janeiro: RNP/ESR, 2013. 138 p. ISBN 978-85-63630-32-2.

BINADOX. 2015. Disponível em: <https://www.binadox.com/>.

BORBOREMA, E. A.; SANTOS, R. R. dos. A cultura organizacional e a adoção de metodologias de governança em tecnologia da informação pelo tribunal de contas da união. p. 31–35, 2018. Disponível em: <http://portal.tcu.gov.br/biblioteca-digital/>.

BRANDIS, K.; AL. et. Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, v. 9, n. 2, p. 320, 2019.

BRERETON, P.; KITCHENHAM, B. A.; BUDGEN, D.; TURNER, M.; KHALIL, M. Lessons from applying the systematic literature review process within the software engineering domain. *J Syst Softw*, v. 80, n. 4, p. 571–583, 2007.

CARARETTO, V. *A importância do compliance nas instituições públicas*. 2021. Disponível online. Acesso em: 21 set. 2023. Disponível em: <https://www.tcm.go.gov.br/escolatcm/artigo-a-importancia-do-compliance-nas-instituicoes-publicas/>.

CASTRO, R. C. C.; SOUSA, V. L. P. de. Segurança em cloud computing: Governança e gerenciamento de riscos. Fortaleza-CE, 2010.

CHAGAS, B. *6 problemas enfrentados em uma gestão de custos em cloud ruim*. 2022. Disponível online. Acesso em: 11 nov. 2023. Disponível em: <https://sumus.com.br/6-problemas-que-voce-provavelmente-enfrenta-em-sua-gestao-de-custos-em-cloud/>.

CLOUD, G. *Criar e Gerenciar Tags*. 2023. <https://cloud.google.com/resource-manager/docs/tags/tags-creating-and-managing?hl=pt-br>. Disponível online. Acesso em: 18 out. 2023.

CLOUD, S. *Why Should You Tag All Your Cloud Resources?* 2017. <https://successive.cloud/importance-tagging-cloud-resource/>. Disponível online. Acesso em 28 jun. 2023.

CLOUDABILITY. *Cloudability - Cloud Cost Management & Optimization - Apptio*. 2019. Disponível em: <https://www.apptio.com/products/cloudability/>.

DOUGLAS, F. P. *The Challenge to Computer Utility*. 4. ed. [S.l.]: Addison-Wesley, 1966.

DUTTA, N.; SARKER, M. M. A tracking solution of it assets and resources management. *Zenodo (CERN European Organization for Nuclear Research)*, jul. 2022.

ELGAMMAL, A.; TUREKTEN, O.; HEUVEL, W.-J. van der; PAPAZOGLOU, M. Formalizing and applying compliance patterns for business process compliance. *Journal of Software and Systems Modeling*, v. 15, p. 119–46, 2016.

ESTRIN, E. *Tags for Cloud Resources: Tips and Best Practices*. 2021. Disponível online. Acesso em: 18 out. 2023. Disponível em: <https://www.iucc.ac.il/en/blog/tags-for-cloud-resources-tips-and-best-practices/>.

FARRELL, R. Securing the cloud—governance, risk, and compliance issues reign supreme. *Information Security Journal: A Global Perspective*, v. 19, n. 6, p. 310–319, novembro 2010. Disponível em: <https://doi.org/10.1080/19393555.2010.514655>.

FEDOSEENKO, V. *What is XaaS? IaaS vs SaaS vs PaaS: what's the difference. Examples*. 2018. Cyprus. [Acesso em 20 mai. 2023]. Disponível em: <https://www.ispsystem.com/ru/node/2650>.

FERNANDEZ, E. B.; MONGE, R.; HASHIZUME, K. Building a security reference architecture for cloud systems. *Requirements Engineering*, 2015.

FERREIRA, M.; ANDRADE, C. Edição 12 - dezembro de 2016: Cloud computing - normas, leis e orientações do governo brasileiro. *Journal/Periodical Title*, 2016.

FLEXERA. *IT and Cloud Management, Optimization and Solutions*. 2022. Disponível em: <https://www.flexera.com/>.

GOOGLE. *Locais Globais: Regiões e Zonas*. 2010. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://cloud.google.com/about/locations?hl=pt-br>.

GUTNIK, I. *How to Implement a Cloud Tagging Strategy*. 2022. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://medium.com/@Igal_Gutnik_Binadox/how-to-implement-a-cloud-tagging-strategy-9b0f5228d430>.

HAT, R. *O que são provedores de nuvem?* 2021. Disponível online. Acesso em: 23 set. 2023. Disponível em: <https://www.redhat.com/pt-br/topics/cloud-computing/what-are-cloud-provider>.

HAVA, T. *Leveraging Tags and Labels for AWS, GCP, and Azure Documentation*. 2022. Disponível online. Acesso em: 2 out. 2023. Disponível em: <https://www.hava.io/blog/leveraging-tags-and-labels-for-aws-gcp-and-azure-documentation>.

IBGP. *Benefícios e Riscos na adoção de Serviços em Nuvem*. 2019. Disponível online. Acesso em: 21 set. 2023. Disponível em: <https://forum.ibgp.net.br/beneficios-e-riscos-na-adocao-de-servicos-em-nuvem/>.

INSTITUTE, P. M. *Um guia do conhecimento em gerenciamento de projetos (Guia PMBOK). Quinta edição.* [S.l.]: Project Management Institute, 2014.

JHONNYE, R. *Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança*. 2010. <https://www.academia.edu>.

JOSHI, A.; BOLLEN, L.; HASSINK, H.; HAES, S. D.; GREMBERGEN, W. V. Explaining it governance disclosure through the constructs of it governance maturity and it strategic role. *Information Management*, v. 55, p. 368–380, 2018.

KUPERMAN, L. *Build A Cloud Tagging Strategy In 5 Steps*. 2023. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://cast.ai/blog/build-a-cloud-tagging-strategy-in-5-steps/>.

LOUIS, M. Tag aggregation across public/private clouds. 2023. Technical Disclosure Commons, September 26, 2023. Disponível em: <https://www.tdcommons.org/dpubs_series/6278>.

MAHENDRA, I.; AL. et. Information technology challenges for integrated governance, risk and compliance (grc). *1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS)*, Aug 23 2022.

MALATHI, M. Cloud computing concepts. In: IEEE. *2011 3rd International Conference on Electronics Computer Technology*. [S.l.], 2011. v. 6.

MARASCHIN, G. M. R. Compliance no setor público. Porto Alegre, 2017. Especialização em Advocacia de Estado e Direito Público.

MARKETING, S. *Como monitorar gastos com cloud*. 2021. Disponível online. Acesso em: 11 nov. 2023. Disponível em: <https://www.supero.com.br/blog/monitorar-gastos-com-cloud/>.

MARTENS, B.; TEUTEBERG, F. Risk and compliance management for cloud computing services: Designing a reference model. 2011. Paper 228. Disponível em: <http://aisel.aisnet.org/amcis2011_submissions/228>.

MARTINEKUAN. *Resource Naming and Tagging Decision Guide - Cloud Adoption Framework*. 2023. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming-and-tagging-decision-guide?toc=%2Fazure%2Fazure-resource-manager%2Fmanagement%2Ftoc.json>.

MEINARDI, M. *Implementing a Tagging Strategy for Cloud IaaS and PaaS*. 2019. ID G00451072. Disponível online. Acesso em: 18 set. 2023.

MELL, P. M.; GRANCE, T. The nist definition of cloud computing. n. 800-145, 2011. Disponível em: <https://doi.org/10.6028/NIST.SP.800-145>.

MELO, G. P. F. de; JR, C. D. dos S. Os impactos das iniciativas de governança de ti nos objetivos organizacionais em instituições públicas federais. p. 43–47, 2018. Disponível em: <http://portal.tcu.gov.br/biblioteca-digital/>.

MICROSOFT. *Tag resources, resource groups, and subscriptions with Azure portal - Azure Resource Manager*. 2023. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources-portal>. Disponível online. Acesso em: 20 out. 2023.

MURAMAKI, G. A.; GARTNER, I. R. Proposição de modelo para suporte à priorização de iniciativas estratégicas de ti do tcu. p. 55–58, 2018. Disponível em: <http://portal.tcu.gov.br/biblioteca-digital/>.

NETAPP. *How to Develop a Public Cloud Tag Management Strategy*. 2021. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://spot.io/blog/how-to-develop-a-public-cloud-tag-management-strategy/#:~:text=Publiccloudtaggingservesmany>.

OWASP, O. W. A. S. P. *OWASP Cloud Top 10*. 2009. Disponível em: <https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf>.

PAQUETTE, S.; JAEGER, P. T.; WILSON, S. C. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, v. 27, n. 3, p. 245–253, 2010.

PEREIRA, H. *Azure: como tornar obrigatório o uso das Tags?* 2023. <https://thecloudbootcamp.com/pt/blog/microsoft-azure/azure-como-tornar-obrigatorio-o-uso-das-tags/>. Disponível online. Acesso em: 20 out. 2023.

REDACAO. *Veja quais as 10 melhores ferramentas para gestão da nuvem - IT Forum*. 2023. Disponível online. Acesso em: 15 dez. 2023. Disponível em: <https://itforum.com.br/noticias/veja-quais-as-10-melhores-ferramentas-para-gestao-da-nuvem/>.

ROUSE, M. *Tag Metadata*. 2017. Disponível online. Acesso em: 2 out. 2023. Disponível em: <https://www.techopedia.com/definition/5240/tag-metadata>.

SASI, K. *Cloud Tagging Part 1: Tagging 101*. 2023. Disponível online. Acesso em: 2 out. 2023. Disponível em: <https://bootcamp.uxdesign.cc/cloud-tagging-part-1-tagging-101-a38325a1f3e1>.

SINGH, J.; POWLES, J.; PASQUIER, T.; BACON, J. Data flow management and compliance in cloud computing. *IEEE Cloud Computing*, v. 2, n. 4, p. 24–32, 2015.

SUICIMEZOV, N.; GEORGESCU, M. R. It governance in cloud. *Procedia Economics and Finance*, v. 15, p. 830–835, 2014. ISSN 2212-5671. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2212567114005310>.

SURBIRYALA, J.; RONG, C. Cloud computing: History and overview. IEEE, p. 1–7, 2019. Disponível em: <https://doi.org/10.1109/CloudSummit47114.2019.00007>.

SURKSUM, K. van. Gartner releases its magic quadrant for cloud infrastructure as a service. In: . [s.n.], 2014. Disponível em: <https://api.semanticscholar.org/CorpusID:107648879>.

SYSTEMS, C. I. *Cloud Cost Optimization Services*. 2018. Disponível em: <https://www.cassinfo.com/cloud-management/services/cloud-cost-optimization-services>.

TCU, T. de Contas da U. *Política de Governança de TI (PGTI/TCU), conforme a Resolução TCU nº 247/2011*. 2011. Resolução. Disponível online. Acesso em: 14 set. 2023.

TCU, T. de Contas da U. *Comitê Gestor de Tecnologia da Informação (CGTI) | Portal TCU*. 2015. Disponível online. Acesso em: 14 set. 2023. Disponível em: <https://portal.tcu.gov.br/governanca/governanca-de-ti/comite-gestor-de-tecnologia-da-informacao-cgti/>.

TCU, T. de Contas da U. *Resolução - TCU Nº 287, de 12 de abril de 2017*. 2017. Diário Oficial da União, Brasília, DF. Seção 1.

TCU, T. de Contas da U. *Referencial Básico de Gestão de Riscos*. [s.n.], 2018. 160 p. Disponível em: <https://repositorio.cgu.gov.br/handle/1/33144>.

TCU, T. de Contas da U. Política de governança (resolução-tcu, nº 320 de 12 de agosto de 2020). n. 320, 2020.

VIEIRA, J. B.; BARRETO, R. T. d. S. *Governança, gestão de riscos e integridade*. Brasília: Enap, 2019. 240 p. ISBN 978-85-256-0107-0.

WEILL, P.; ROSS, J. W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA, USA: Harvard Business School Press, 2004. ISBN 978-1591392538.

WERFF, L. V. D. et al. Building consumer trust in the cloud: An experimental analysis of the cloud trust label approach. *Journal of Cloud Computing*, v. 8, n. 1, p. 6, dezembro 2019. Disponível em: <https://doi.org/10.1186/s13677-019-0129-8>.

WIBOWO, S.; AL. et. Integrated governance, risk, and compliance (grc) and combined assurance: A comparative institutional study. *Indonesian Journal of Business and Entrepreneurship*, 2022.

WILLIS, M. *How to Tag Cloud Applications and Resources*. 2023. Disponível online. Acesso em: 10 out. 2023. Disponível em: <https://www.cassinfo.com/cloud-management-blog/how-to-tag-cloud-resources>.

YIMAM, D.; FERNANDEZ, E. B. A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, v. 7, n. 5, p. 5, 2016. Disponível em: <https://doi.org/10.1186/s13174-016-0046-8>.

YORK, F. *Tag Management Governance*. 2022. Disponível em: <https://www.cloudsaver.com/resources/articles/tag-management-governance/>.

ZANIN, S. *Gestão de custos em cloud computing: como reduzir despesas e otimizar nvestimentos*. 2021. Disponível online. Acesso em: 11 nov. 2023. Disponível em: <https://blog.compass.uol/tech/gestao-de-custos-em-cloud-computing-como-reduzir-despesas-e-otimizar-investimentos/>.