DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal

Fábio Galvão Ferreira Tabosa

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal

Assessment of the post-pandemic evolution of the propensity to face cloud computing risks by managers of the federal public administration

Fábio Galvão Ferreira Tabosa

Orientador: Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB
Coorientador: Prof. Dr. William Ferreira Giozza, ENE/FT/UnB

PUBLICAÇÃO: PPEE.MP.021
BRASÍLIA-DF, 22 DE SETEMBRO DE 2022.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal

Fábio Galvão Ferreira Tabosa

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB _____
Orientador

Prof. Dr. Demétrio A. da S. Filho, ENE/FT/UnB _____
Examinador Interno

Prof. Dr. Sérgio A. S. de Moraes, UNIATENAS _____
Examinador Externo

Prof. Dr. Rafael Timóteo de Sousa Jr, ENE/FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

TABOSA, FÁBIO GALVÃO FERREIRA
Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal [Distrito Federal] 2022.
xvi, 82 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Computação em Nuvem	2. Riscos
3. Setor Público	4. Governo Eletrônico
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

TABOSA, F.G.F. (2022). *Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 82 p.

CESSÃO DE DIREITOS

Fábio Galvão Ferreira Tabosa
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho a Santíssima Trindade e a Nossa Senhora Aparecida, a minha esposa Danielle Alves de Oliveira Tabosa, a minhas filhas Maria Clara Alves Tabosa e Isabel Alves Tabosa e aos meus pais Iracema Christiane Galvão Tabosa e Pedro José Ferreira Tabosa e a todos os meus familiares.

AGRADECIMENTOS

Agradeço sobretudo a Deus por ter me dado saúde, paciência e perseverança para a condução e a conclusão desta pesquisa.

Agradeço aos professores Rafael Rabelo Nunes (Orientador), William Ferreira Giozza (Coorientador) e Rafael Timóteo de Sousa Júnior (Coordenador do PPEE) pela oportunidade, pela confiança depositada e pelos conselhos que foram indispensáveis. Ao competente time de professores do ENE/UnB que contribuiu para minha formação acadêmica. Ao professor Daniel Alves, por todo o incentivo que foi essencial para iniciar esta jornada.

Agradeço o apoio técnico e computacional do Laboratório de Tecnologias para Tomada de Decisão - LATITUDE, da Universidade de Brasília, que conta com apoio do CNPq - Conselho Nacional de Pesquisa (Outorgas 312180/2019-5 PQ-2 e 465741/2014-2 INCT em Cibersegurança), da Advocacia Geral da União (Outorga AGU 697.935/2019), do Ministério da Justiça e Segurança Pública (Outorga MJSP 01/2019) e dos Decanatos de Pesquisa e Inovação e de Pós-Graduação da Universidade de Brasília (Outorga 7129 FUB/EMENDA/DPI/COPEI/AMORIS).

RESUMO

Este trabalho teve como objetivo avaliar o enfrentamento dos riscos ao se implantar serviços de computação em nuvem sob a ótica dos gestores de órgãos públicos federais no Brasil. Para alcançar o objetivo proposto, foram realizadas entrevistas semiestruturadas com servidores de nível estratégico, tático e operacional, envolvidos com a gestão de tecnologia da informação de vinte e três órgãos da Administração Pública Federal por meio de um estudo longitudinal pré e pós-pandemia de COVID-19. Os dados foram analisados com base nas recomendações de entidades internacionais para enfrentamento de riscos dessa natureza, fundamentados em nove dimensões: legislação e regulamentações; governança de TIC; privacidade e proteção de dados; segurança das operações e comunicações; isolamento de cliente em nuvem; gestão de identidade e de acessos; resposta a incidentes; continuidade dos negócios; e conformidade e auditoria. Os resultados demonstraram que ainda há um caminho a ser percorrido para a completa implementação desses serviços na Administração Pública Federal, principalmente no que se refere a questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis, governança e segurança. Em complemento, para se implementar o serviço de computação em nuvem como proposto pela Lei de Governo Digital, os achados sugerem a necessidade de enfrentar riscos de transposição complexa que ainda não foram superados por completo, uma vez que o momento atual demonstra que a implantação já ocorreu e a fase agora é de operação dos serviços em computação em nuvem.

ABSTRACT

This work aimed to evaluate the risks faced when deploying cloud computing services from the perspective of managers of federal public agencies in Brazil. To obtain the proposed objective, semi-structured interviews were conducted with strategic, tactical, and operational level servers involved in information technology management in twenty-three federal public administration agencies through a longitudinal pre- and post-pandemic study of COVID-19. The data were analyzed based on the recommendations of international entities for dealing with risks of this nature, based on nine dimensions: legislation and information security. The data were analyzed based on the advice of international organizations to address such risks, based on nine measurements: legislation and regulations; ICT governance; data privacy and protection; operations and communications security; cloud client isolation; identity and access management; incident access management; incident response; business continuity; and compliance and auditing. The results showed that there is still a way to go for the complete implementation of these services in the Federal Public Administration, especially when it comes to questions about the risks linked to their use, with attention to the treatment of sensitive data, governance, and security. In addition, to implement the cloud computing service as proposed by the Digital Government Law, the findings suggest the need to face complex transposition risks that have not yet been fully overcome since the current moment shows that the deployment has already occurred, and the phase now is the operation of cloud computing services.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLA

Siglas

ABNT	Associação Brasileira de Normas Técnicas
API	*Application Programming Interface* (Interface de Programação de Aplicação)
CASB	*Cloud Access Security Broker* (Agente de Segurança de Acesso à Nuvem)
CE	Critério de Exclusão
CGI.BR	Comitê Gestor da Internet no Brasil
CIA	*Confidentiality, Integrity e Availability* (Confidencialidade, Integridade e Disponibilidade)
CI	Critério de Inclusão
COBIT	*Control Objectives for Information and related Technology* (Controle de Objetivos para Informação e Tecnologias Relacionadas)
COVID-19	Corona Vírus Doença
CRM	*Customer Relationship Management* (Gestão de Relacionamento com o Cliente)
CSA	*Cloud Security Aliance* (Aliança de Segurança em Cloud)
CSC	*Cloud Service Customer* (Cliente de Serviço de Cloud)
CSP	*Cloud Service Provider* (Provedor de Serviço de Cloud)
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
ENISA	*European Union Agency for Cybersecurity* (Agência Europeia para a Segurança das Redes e da Informação)
EUA	Estados Unidos da América
FMI	*International Monetary Fund* (Fundo Monetário Internacional)
IaaS	*Infrastructure as a Service* (Infraestrutura como Serviço)
IBM	*International Business Machines* (Maquinas de Negócios Internacional)
IEC	*International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)
IEEE	*Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos)
ISACA	*Information Systems Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação)
ISO	*International Organization for Standardization* (Organização Internacional para Padronização)
ITRC	*Identity Theft Resource Center* (Centro de Recursos de Roubo de Identidade)
LGPD	Lei Geral de Proteção de Dados

MFA	*Multi Factor Authentication* (Autenticação Multifator)
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
PaaS	*Platform as a Service* (Plataforma como Serviço)
PAM	*Privilege Account Management* (Gerenciamento de acesso privilegiado)
PCI-DSS	*Payment Card Industry Data Security Standard* (Padrão de Segurança de Dados da Indústria de Pagamento com Cartão)
PF	Polícia Federal
PII	*Personally Identifiable Information* (Informações de Identificação Pessoal)
PRISMA	*Preferred Reporting Itens for Systematic reviews and Meta Analysis* (Itens preferenciais de relatórios para revisões sistemáticas e metanálises)
SaaS	*Software as a Service* (Software como Serviço)
SLA	*Service Level Agreement* (Acordo de Nível de Serviços)
SOC	*Secutiry Operation Center* (Centro de Operações de Segurança)
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UEBA	*User Entity and Behavior Analytics* (Análise do Comportamento de Usuários e Entidades)

1 INTRODUÇÃO

Com a adoção de estratégias de transformação digital brasileira dos serviços públicos em 2019, o processo de digitalização, na era do governo eletrônico, ganhou uma importância social e econômica para o País atualmente. Os serviços já atendem a um universo de 81,2 milhões de pessoas no Brasil e atingiram a marca de 1.639 serviços digitalizados [1][2].

Mais da metade dos serviços públicos *on-line* foram disponibilizados após o início da crise sanitária causada pela pandemia de COVID-19, que evidenciou a importância do acesso e do uso das tecnologias de informação e comunicação (TIC) como uma dimensão chave do acesso à informação, educação, saúde, cultura, trabalho e, em geral, a todas as esferas de participação econômica e social.

Observa-se que todos os seguimentos de serviços públicos *on-line* tiveram um crescimento no seu uso e a maior impulsionadora foi a crise sanitária, a qual tem forçado governos e sociedades a voltarem-se para as tecnologias digitais para responder à crise em um curto prazo de tempo, resolver as repercussões socioeconômicas a médio prazo e reinventar as políticas e ferramentas existentes a longo prazo [3].

Atrelado a tudo isso, temos o rápido avanço na área de TIC e o avanço da digitalização de serviços, os quais vem impulsionando o intenso uso do espaço cibernético na cadeia produtiva e, por consequência, nas mais variadas atividades adjacentes por todo o mundo. Entretanto, como resultado, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade [4].

Em ataques cibernéticos recentes, grupos de *hackers* têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional; o descrédito da população nos serviços públicos; a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas; a desconfiança nos processos eleitorais; e o descontentamento da população com relação à administração pública [4].

Segundo a área de segurança da IBM [5], o custo com mega vazamento de dados, aqueles com mais de 1 milhão de registros comprometidos, tem um impacto negativo nos consumidores e nas indústrias. As informações pessoalmente identificáveis (PII) de cliente foram a categoria de registro perdido ou roubado mais comum no ano de 2021. O custo médio de um mega vazamento de dados foi de 401 milhões de dólares para as maiores violações (50 a 65 milhões de registos) e foram necessárias uma média de 212 dias para identificar o incidente e uma média de 75 dias para conter o mesmo, com um ciclo de vida total de 287 dias. Assim, se uma violação ocorresse em 1 de janeiro de 2021 e levasse 287 dias para identificar e conter, a mesma violação não seria contida antes de 14 de outubro de 2021.

Em todo o mundo, as organizações governamentais têm modificado suas infraestruturas computacionais de serviços localmente mantidos para serviços ofertados por meio da computação em nuvem, para reduzir o custo total com os investimentos em infraestrutura de TI e aproveitar os benefícios desse novo paradigma de computação [6]. No Brasil não é diferente, haja vista a meta prevista na Estratégia Brasileira de Governo Digital de migrar para nuvem, até 2022, serviços de pelo menos 30 órgãos federais, conforme

Lei n.º 14.129 de Governo Digital [7][8].

A computação em nuvem tem colaborado para o trabalho de segurança cibernética, produtividade e economia de gastos, pois com as cargas de trabalho em nuvem habilitam-se recursos tecnológicos que possibilitam a implantação do escritório em qualquer lugar, além de prover serviços públicos *on-line* de forma ágil. Em contrapartida, o risco cibernético envolvido, segundo o Fundo Monetário Internacional (FMI), é a nova ameaça à estabilidade financeira global. O número de ciberataques triplicou na última década à medida que nos tornamos cada vez mais dependentes dos serviços financeiros digitais, que continuam a ser o setor mais visado. Obviamente, os riscos cibernéticos tornaram-se uma ameaça à estabilidade financeira [9].

Segundo a *Cloud Security Aliance* - CSA [10], uma organização sem fins lucrativos que visa promover as melhores práticas para garantir segurança no ambiente de computação em nuvem, as falhas de configurações, tais como políticas de senhas inadequadas, visibilidade limitada da utilização de recursos e configurações inadequadas de barreira de seguranças e servidores, são constantemente as principais preocupações das organizações na utilização de computação em nuvem no modelo de implantação pública. Tais falhas (i) conduzem a vazamento de dados, (ii) permitem a eliminação ou modificação de recursos, (iii) causam interrupções de serviço, e (iv) provocam estragos nas operações comerciais.

Em 2019, antes da crise sanitária, a categoria de serviço de computação em nuvem mais utilizada pelos órgãos públicos federais e estaduais brasileiros foi o correio eletrônico, contratado por pouco mais de um terço dos órgãos (36%), proporção que era de 25% em 2017. O principal crescimento ocorreu entre órgãos do Poder Judiciário (aumento de 15% para 40% entre 2017 e 2019) e órgãos federais do Poder Executivo (de 19% para 40%), seguido pelos serviços de armazenamento de arquivos ou banco de dados (24%), software de escritório (20%) e capacidade de processamento (18%) [7].

Em 2021, o governo brasileiro, por meio do Ministério da Economia, realizou a 2.ª licitação centralizada para contratação de serviços em nuvem para 52 órgãos da administração pública, incluindo órgãos dos poderes executivo e judiciário, tanto federal como estadual. Nessa contratação, que teve um custo de R$ 66 milhões de reais ao ano, o governo informa que foi adotado como referência o padrão do *National Institute of Standards and Technology* - NIST para conformidade do contratado [11].

Nesse contexto, é notória a utilização, pelas organizações públicas brasileiras, de computação em nuvem. Este trabalho tem o objetivo de contribuir com o gerenciamento de risco no uso desse ambiente pela administração pública federal, no desenvolvimento de um estudo longitudinal com pesquisa quantitativa e qualitativa perante os gestores de TIC dos órgãos do executivo, do legislativo e do judiciário para avaliação da evolução da propensão ao enfrentamento de riscos de computação em nuvem pós-pandemia.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Atualmente os serviços públicos digitais cobrem uma parcela da população considerável, sendo responsáveis por gerenciar serviços de saúde pública, segurança pública, ensino, regulação de serviços privados, dentre outros diversos. A indisponibilidade desses serviços pode ocasionar um colapso nos serviços públicos.

Conforme a pesquisa TIC Governo Eletrônico realizada pelo NIC.BR [12], os processos de gerenciamento de risco em TIC foram os menos mencionados pelos órgãos federais. É importante salientar que a existência desses processos é fundamental para identificar, monitorar e controlar vulnerabilidades que podem comprometer a segurança da informação nos órgãos públicos e também a segurança e privacidade dos dados dos cidadãos. Os processos de gestão de tecnologia mencionados pelos entrevistados foram: (i) Gestão de infraestrutura em TI (87%), (ii) Gestão de contratos (86%), (iii) Tratamento de incidentes (85%), (iv) Acompanhamento de projetos (82%), (v) Gerenciamento de serviços (80%) e (vi) Gestão de riscos (68%). As boas práticas mundiais recomendam que os processos de Gestão de Riscos devem ocorrer antes dos processos de Gestão de TIC.

A digitalização dos serviços públicos é uma realidade em todo o mundo há anos, pois reduz a burocracia e auxilia a economia. No Brasil é algo recente. Com o processo de digitalização ocorre uma série de problemas de disponibilidade no acesso aos serviços públicos. Serviços esses utilizados por pessoas ativas economicamente como também por pessoas inativas, sejam elas aposentados e dependentes de previdência social, em estado de extrema pobreza e dependentes de alguma forma de auxílio prestado pelos governos.

A necessidade de uma avaliação baseada em um estudo longitudinal para conhecer o panorama atual pré e pós-pandemia de COVID-19 torna-se, portanto, importante do ponto de vista acadêmico e profissional visto que estudos com essa linha de pesquisa são novos e desconhecidos pela academia.

Nesse sentido, se faz necessário investigar quais foram as ações de mitigação aplicada aos riscos em ambiente de computação em nuvem pela administração pública brasileira e identificar os problemas enfrentados com a adoção e migração para esse ambiente, que às vezes podem ser com planejamento, com planejamento precário do ponto de vista de gestão de risco ou até mesmo sem o devido planejamento.

1.2 PROBLEMA DE PESQUISA

Este trabalho foca nas questões relacionadas ao enfrentamento pós-pandemia dos riscos associados a computação em nuvem pelos gestores da Administração Pública Brasileira. Conforme relatado no capítulo introdutório, existe um problema que só repercute com a digitalização dos serviços públicos, que é o aumento de incidentes cibernéticos com a modernização dos ataques, causando comprometimento de dados aos serviços públicos *on-line* e a consequente baixa ou até ausência de maturidade de um processo de gestão de risco de segurança da informação para adoção de computação em nuvem pelas organizações, contribuindo para que essas ameaças se amplifiquem.

Antes da crise sanitária, já existia um movimento de adoção de computação em nuvem, porém com algumas resistências por parte dos gestores e profissionais, conforme evidenciado em um dos trabalhos resultante da pesquisa "Riscos de Computação em Nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil" [13].

Neste trabalho, durante a 1ª coleta de dados em 2019, período pré-pandemia, observou-se que ainda havia um caminho a ser percorrido para a implementação desses serviços na Administração Pública, principalmente no que se refere a questionamentos acerca dos riscos atrelados ao uso de computação em nuvem, com atenção especial ao tratamento de dados sensíveis considerando a publicação da Lei Geral de Proteção

de Dados Pessoais - LGPD em 2018 [14].

Dessa forma, foi estabelecido como problema de pesquisa deste trabalho a seguinte hipótese:

Problema 1 (P1): *Os riscos evidenciados em 2019 e atrelados a adoção de computação em nuvem pelos órgãos federais brasileiros foram tratados e/ou mitigados depois da pandemia de COVID-19?*

Considerando o **Problema 1** exposto, formula-se duas hipóteses;

Hipótese 1 (H1): *Considerando que a crise sanitária global motivou ações imediatas de gestão em TIC com a disponibilização de serviços públicos on-line, os gestores públicos do governo federal não fizeram a gestão de risco antes da adoção de computação em nuvem devido ao momento atual.*

Hipótese 2 (H2): *Devido a ausência de processos de gestão de risco para adoção de computação de nuvem, os órgãos públicos federais sofreram ataques cibernéticos em razão da inexistência de controles que foram evidenciados na 1º coleta em 2019, quando da migração e implantação de serviços em nuvem.*

1.3 OBJETIVO GERAL

O objetivo geral deste trabalho é identificar e analisar a evolução, pós-pandemia de COVID-19, da propensão ao enfrentamento de riscos no uso de computação em nuvem pelos gestores públicos da administração pública federal.

1.4 OBJETIVOS ESPECÍFICOS

Partindo do objetivo geral deste trabalho, definiram-se os seguintes objetivos específicos:

OBJ1: realizar uma revisão da literatura em relação aos riscos na adoção de computação em nuvem pelas organizações governamentais ao redor do mundo;

OBJ2: identificar quais são as percepções dos gestores públicos de TI da administração pública federal quanto ao enfrentamento dos riscos na adoção de computação em nuvem e a prontidão dos provedores de serviços em nuvem durante o período de três anos investigado (pre-pandemia e pós-pandemia);

OBJ3: verificar quais são as influências das expectativas de computação em nuvem, da preparação para a nuvem e dos fatores de valor do negócio TI, isoladamente e como um modelo multi-nuvem sobre o seu desempenho;

OBJ4: analisar as mitigações ou aceitação dos riscos pelos gestores públicos de TI na adoção de computação em nuvem durante o período da pandemia; e

OBJ5: observar quais são os modelos de serviços de computação em nuvem em uso pela administração pública federal.

1.5 METODOLOGIA DE PESQUISA

Em relação aos parâmetros de classificação, o objetivo da pesquisa é descritivo, porque descreve as características de determinadas populações ou fenômenos, e exploratório, pois envolve levantamento bibliográfico e entrevistas com pessoas experientes no problema pesquisado [15].

Para alcançar o objetivo, foi utilizada a abordagem de pesquisa quantitativa e qualitativa com procedimentos técnicos de pesquisa de campo por meio da aplicação de entrevistas semiestruturadas, com gestores de organizações da administração pública federal que possuem contratos de serviços em nuvem, cuja temporalidade é longitudinal. O trabalho baseou-se nas seguintes etapas metodológicas:

1. Pesquisar se houve mudança na maturidade das organizações dos entrevistados quanto à propensão, pós-pandemia de COVID-19, no uso de computação em nuvem;
2. Investigar se a resistência a adoção de computação em nuvem e/ou o que a ela está associada afeta o sucesso do uso de computação em nuvem e os profissionais envolvidos na gestão de riscos;
3. Analisar a presença e as causas de resistência de gestores ou grupos de gestores diante do uso de computação em nuvem e diante das mudanças decorrentes da adoção da tecnologia de serviços em nuvem;
4. Avaliar formas de superação, mitigação e ou eliminação dos riscos e seus efeitos no uso de computação em nuvem;
5. Explorar a existência de mudanças no trabalho em decorrência de transferência de serviços para um provedor de computação em nuvem;
6. Estudar a existência e a caracterização de riscos em decorrência do uso de computação em nuvem e suas respectivas ações de gestão de riscos; e
7. Obter eventuais contribuições espontâneas dos participantes.

1.6 PUBLICAÇÕES RESULTANTES DESSE TRABALHO

Título 1: ***Riscos da Computação em Nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil*** [13].

Autores:	Andrio de A. Alves, Carlos André de M. Alves, Fábio G. F. Tabosa e Rafael Rabelo Nunes
RIS:	Qualis A4.
Publicação:	Navus: Revista de Gestão e Tecnologia; Vol 11 - 2021.
url:	<https://navus.sc.senac.br/index.php/navus/article/view/1513/pdf>
DOI:	<http://dx.doi.org/10.22279/navus.2021.v11.p01-18.1513>

Título 2:	***Fatores de Riscos que Influenciam em uma Infraestrutura de Data Center utilizando o método TEMAC*** [16].
Autores:	Fábio G. F. Tabosa, Daniel A. da Silva, Rafael T. Sousa Jr, Flavio Elias G. de Deus e Rafael Rabelo Nunes
Conferência:	16th Iberian Conference on Information Systems and Technologies (CISTI) - 2021.
Publicação:	IEEE
url:	<https://ieeexplore.ieee.org/document/9476286>
DOI:	<https://doi.org/10.23919/CISTI52073.2021.9476286>

1.7 ESTRUTURA DA DISSERTAÇÃO

Essa dissertação está dividida em 5 capítulos, incluindo este capítulo introdutório:

1. Capítulo 2 - Referencial Teórico: destinado a apresentar os principais trabalhos acadêmicos correlatos, dividindo o tema em quatro linhas de pesquisa:
    - Computação em nuvem: principais conceitos e modelos de prestação de serviço;
    - Conformidade em computação em nuvem: análise dos principais normativos nacionais e internacionais;
    - Gestão de Riscos de Segurança e Privacidade em computação em nuvem;
    - *Frameworks* de Defesa Cibernética.
2. Capítulo 3 - Metodologia: Abordagem do método utilizado no trabalho.
3. Capítulo 4 - Resultados: Apresentação e análise dos resultados coletados e analisados.
4. Capítulo 5 - Conclusão: Apresentação das conclusões e sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este Capítulo apresenta os principais conceitos de computação em nuvem e suas normas de Conformidade, Gestão de Riscos e *Frameworks* utilizadas na segurança cibernética aplicados no contexto de gestão de riscos em computação em nuvem. Além disso, este capítulo apresenta os principais trabalhos relacionados, discutindo suas limitações e destacando o principal diferencial da proposta desta dissertação.

2.1 COMPUTAÇÃO EM NUVEM

O conceito de computação em nuvem utilizado neste trabalho baseia-se no *National Institute of Standards and Technology* - NIST fundado em 1901, responsável pelo desenvolvimento de normas e orientações de segurança da informação, incluindo requisitos mínimos para os sistemas de informações federais do Governo dos Estados Unidos. A conceitualização de computação em nuvem apresentada pelo NIST é também utilizada pelo Tribunal de Contas da União [17] no país.

2.1.1 Aspectos conceituais e modelos de serviços

Os conceitos de nuvem abrangem cinco características essenciais, três modelos de serviço e quatro modelos de implantação, ilustrados na Figura 2.1. O NIST [18] descreve, de maneira abrangente, as cinco características essenciais de computação em nuvem da seguinte forma:

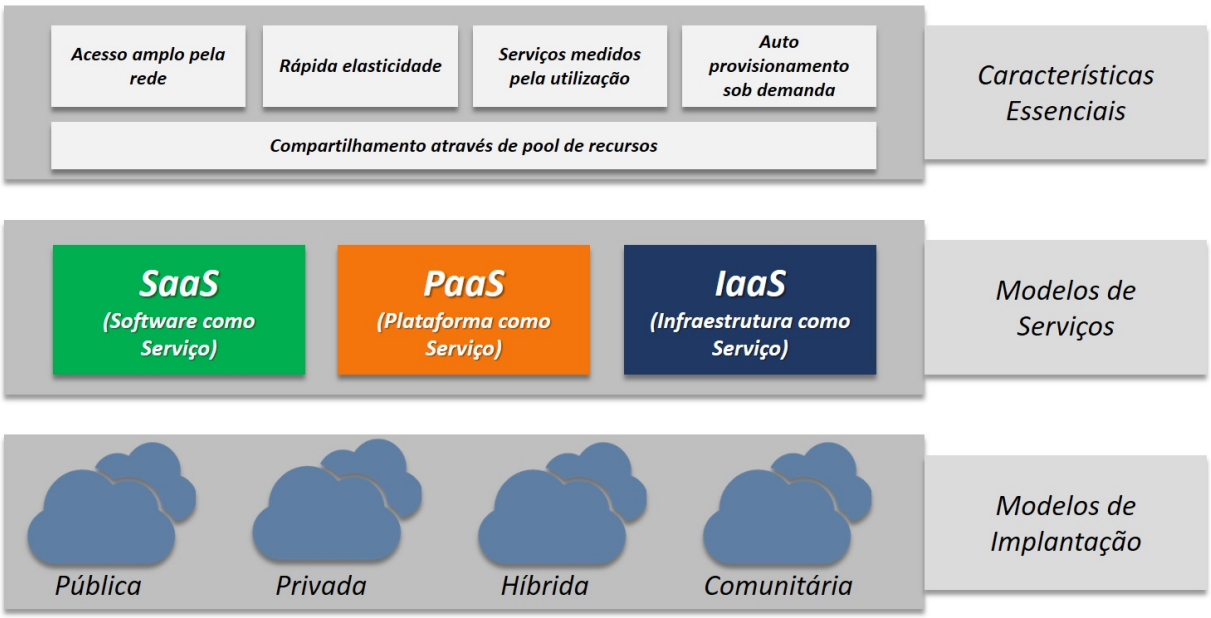

Figura 2.1: Forma visual dos conceitos de nuvem.
Fonte: Adaptado da NIST [18] e CSA [19].

- **Acesso amplo pela rede**: os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (estações de trabalho, tablets, smartphones etc.) através de mecanismos padrões.
- **Rápida elasticidade**: os recursos computacionais podem ser elasticamente provisionados e liberados e, em alguns casos, de maneira automática, adaptando-se à demanda.
- **Serviços medidos por utilização**: os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado como armazenamento, processamento, largura de banda e contas de usuário ativas.
- **Autoprovisionamento sob demanda**: o consumidor pode ter a iniciativa de provisionar recursos na nuvem e ajustá-los conforme as suas necessidades no decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços.
- **Compartilhamento através de *pool* de recursos**: os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo multi-tenant) com recursos físicos e virtuais, sendo alocados e realocados dinamicamente conforme a demanda dos seus consumidores.

Os três principais modelos de serviços de nuvem ilustrados na Figura 2.1, são baseados numa arquitetura em camadas hierárquicas, em que os serviços da camada superior são provisionados pela camada inferior subsequente [18] [17] [20], a saber:

- **Infraestrutura como um serviço**(*Infrastructure as a Service* - IaaS): é a capacidade oferecida ao consumidor de fornecer processamento, armazenamento, redes e outros recursos fundamentais de computação, nos quais se pode implementar e executar softwares arbitrários, podendo incluir sistemas operacionais e aplicativos, tais como: Armazenamento e Backup (EMC, Symantec, RainStor, Amazon S3) e Computação (Amazon EC2, JitScale, Rackspace, Uniserver, Microsoft Azure, Google Compute Engine).
- **Plataforma como um serviço** (*Platform as a Service* - PaaS): é a capacidade oferecida ao consumidor de implementar os aplicativos criados ou adquiridos na infraestrutura em nuvem, tais como: Desenvolvimento de Aplicações Genéricas (Google App Engine, Microsoft Azure) e Desenvolvimento de Aplicações Especificas (Salesforce Force.com, SaaSPlaza, SAP Business ByDesign).
- **Software como um serviço** (*Software as a Service* - SaaS): possibilidade de usar os aplicativos do provedor em execução em uma infraestrutura de nuvem. Os aplicativos são acessíveis a partir de vários dispositivos, como um navegador da Web (por exemplo, e-mail baseado na Web) ou uma interface de programa, tais como: Supply Chain Management - SCM (Descartes, Ariba, Ketera, JDA Software), Sistema integrado de gestão empresarial - ERP (NetSuite, Exact Online, Twinfield, SAP Business ByDesing, Infor), Gestão de Relacionamento com o Cliente - CRM (Salesforce.com, PerfectView CRM Online, AccountView CRM Online), Produtividade de escritório (Google Apps, Microsoft Office 365) e Comunicação e colaboração - (Cisco Webex, Microsoft Lync, IBM Lotusphere).

Independentemente do modelo de serviço, é necessário considerar também os modelos de implantação da nuvem [18] [17]. A implantação representa como a computação em nuvem será estruturada no que tange ao compartilhamento e controle de recursos físicos e virtuais [18] [20] [21] [22]. Os modelos de implantação citados na Figura 2.1 podem ser assim descritos:

- **Nuvem Privada**: a infraestrutura de nuvem privada está disponível para uso exclusivo de uma única organização.
- **Nuvem Comunitária**: a infraestrutura de nuvem comunitária está disponível para uso exclusivo de uma comunidade específica, formada por organizações que possuem interesses e preocupações em comum.
- **Nuvem Pública**: a infraestrutura de nuvem pública está disponível para uso aberto do público e fica nas instalações do provedor.
- **Nuvem Híbrida**: a infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem (privada, comunitária ou pública).

Com a evolução da adoção de computação em nuvem, surgiu a necessidade de se conseguir que dois ou mais provedores de serviço em nuvem interajam, ou colaborem entre si. Nesse sentido, criou-se o termo "federação de nuvem" (*cloud federation*). Os princípios básicos da federação de nuvens podem ser descritos através das interações dos atores em uma representação em camadas de confiança, segurança, e compartilhamento e utilização de recursos [23].

Em dezembro de 2021, o Conselho do IEEE (do inglês,*Institute of Eletrical and Electronics Engineers*), uma organização profissional sem fins lucrativos fundada nos Estados Unidos, sendo a mais relevante organização profissional do mundo dedicada ao avanço da tecnologia em benefício da humanidade, aprovou a norma IEEE 2302-2021 *Standard for Intercloud Interoperability and Federation*. A norma 2301-2021 baseia-se também na Publicação Especial NIST 500-332 - Arquitetura de referência da NIST Cloud Federation. Essa abordagem atinge a interoperabilidade da nuvem utilizando um conjunto de características e funcionalidades. Esse modelo permite uma gama de topologias de implantação e gestão. Como norma, deve ser aplicada a muitos domínios mesmo utilizando diferentes abordagens de implementação [23] [24].

2.1.2 Serviços Públicos Digitalizados

De acordo com o Comitê Gestor da Internet no Brasil - CGI.BR [25], após o início da pandemia, registrou-se um aumento expressivo (18%) na utilização de serviços públicos por parte dos usuários de Internet (57%) no país se comparado com o ano de 2018. Os serviços públicos *on-line* mais buscados ou realizados desde o início da pandemia foram aqueles relacionados ao direito do trabalhador ou previdência social (72%), documentos pessoais (46%), saúde pública (45%) e educação pública (37%), conforme apresentado na Figura 2.2.

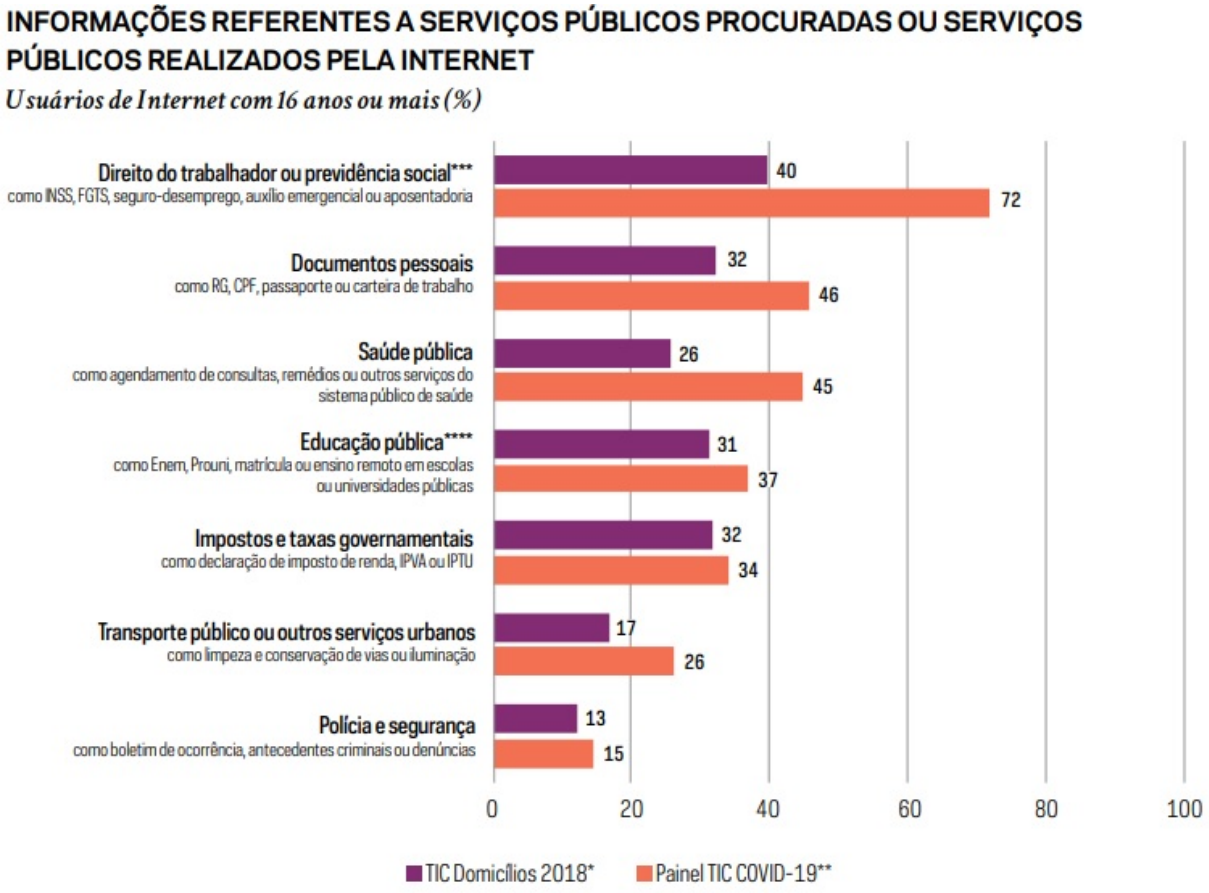

Figura 2.2: Serviços Púbicos on-line mais procurados no Brasil em 2020.
Fonte: Painel TIC COVID-19 CGI-BR [25].

A inovação, a produtividade e o trabalho não são exceções, dado que o crescimento econômico e a inclusão social serão cada vez mais influenciados pela capacidade dos países em manter um ecossistema digital dinâmico e altamente conectado. Aliado a esse movimento, tem-se o trabalho remoto que se mostrou eficaz para diversas organizações, tanto pelo lado da qualidade do trabalho e produtividade, como pelo lado dos custos econômicos de operação [26].

A crise sanitária acelerou esse processo da nova forma de trabalhar, criando o "escritório em qualquer lugar". A presente situação combinada com a necessidade humana de computação onipresente, com acesso imediato para consumo e prestação de serviços on-line, tem gerado uma demanda por investimento para serviços com cada vez mais alta Confidencialidade, Integridade e Disponibilidade (tríade CIA), que em muitos casos não são implementados da forma miníma adequada, o que força a todos a assumir riscos cibernéticos sem o devido tratamento de mitigação e até eliminação.

2.1.3 Adoção de Computação em Nuvem no Setor Público

A adoção da computação em nuvem pelas organizações constitui mais uma área chave da literatura sobre computação em nuvem, em que os benefícios mais difundidos atribuídos à nuvem estão relacionados à oportunidade de reduzir os custos e a complexidade, e ainda oferecer nova, e às vezes desconhecida, oportunidade de inovação [27].

As organizações do setor público tradicionalmente dispõem de sistemas de TIC mantidos em ambiente próprio. Nos EUA, o Governo Federal voltou-se para serviços em nuvem para melhorar a eficiência da TI, mantendo elevados padrões de segurança e reduzindo despesas extremamente elevadas. Foi criado o Programa Federal de Gestão de Autorizações de Risco denominado FedRAMP em 2011, que representa um passo importante para a garantia da informação em nuvem. O programa baseia-se em procedimentos de inspeção, avaliação e autorização para garantir a segurança e a privacidade das informações das Agências Federais Americanas em Nuvem Pública. O programa diferencia três linhas de base de segurança (baixa, moderada, alta) segundo a sensibilidade dos dados processados nos sistemas de computação em nuvem, e conta com uma seleção de controles baseados no NIST SP 800-53 [28].

Ainda nos EUA, o Governo Federal atualizou a Estratégia Federal de computação em nuvem do Governo (*Cloud First*), desenvolvendo uma nova estratégia para acelerar a adoção de soluções baseadas em nuvem pelas agências: *Cloud Smart* [29].

No Brasil, O Governo Federal editou a Lei 14.129 de 29 de março de 2021 [8], a qual dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Essa lei determinou que a Administração Pública participará de forma integrada e colaborativa, da consolidação da Estratégica Nacional de Governo Digital [7], editada pelo poder executivo. A Estratégia tem como objetivo a adoção de tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal.

Segundo o Objetivo 16 - Otimização das infraestruturas de tecnologia da informação da Estratégia de Governo Digital, o Governo Brasileiro definiu que os órgãos públicos têm como meta a Iniciativa 16.5. Migração de serviços de, pelo menos, trinta órgãos para a nuvem até 2022. Acredita-se que a presente iniciativa foi atingida ainda em 2021, com o auge da crise sanitária, conforme apresentado no capítulo introdutório desse trabalho [2].

Em agosto de 2021, o poder executivo publicou a Instrução Normativa N.º 05 do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal [30]. No Poder Judiciário houve a mesma estratégia com a publicação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário denominada ENTIC-JUD [31], ambas com o propósito de promover a adoção de computação em nuvem considerando o custo-benefício e seus aspectos de segurança.

2.2 GESTÃO DE RISCO DE SEGURANÇA E PRIVACIDADE

O conceito de risco - quando considerado no contexto da tecnologia da informação e cibersegurança - faz referência a um extenso vocabulário, incluindo ameaças e vulnerabilidades, apetite de risco, tolerância, impacto, priorização e resposta, entre muitos outros termos essenciais às disciplinas de governança de risco, gestão e avaliação da tecnologia da informação [32].

Já no contexto nacional, o Gabinete de Segurança Institucional da Presidência da República publicou uma Portaria com o Glossário de Segurança da Informação [33], que define "RISCO no conceito geral é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade". Nessa mesma Portaria é definido também o "RISCO de Segurança da Informação como sendo um potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação, ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização".

Ainda de acordo com a ABNT NBR/ISO 31.000 – Gestão de Riscos - Diretrizes [34], risco é o efeito da incerteza nos objetivos, onde o efeito é um desvio em relação ao esperado podendo ser positivo e/ou negativo.

2.2.1 Incidentes em Computação em Nuvem

O Governo Brasileiro, através do Centro de Prevenção, Tratamento e Resposta a Incidentes de Governo - CTIR Gov, registrou 4.984 incidentes confirmados em 2021, sendo 2.015 de Abuso de Sítio Web, 1.041 de Fraudes, 595 de Scan, 388 de Malware, 196 de Vazamentos de Dados e 744 outros incidentes [35].

Em 2021, por exemplo, houve um incidente de indisponibilidade no Brasil que ocasionou a paralisação do sistema de notificação de casos de COVID-19, do Programa Nacional de Imunização e do ConectaSUS [36]. Segundo a nota da Polícia Federal, o incidente de segurança cibernético ocorreu no ambiente de nuvem pública contratado pelo Ministério da Saúde através de licitação realizada pelo Ministério da Economia.

Em decorrência ao incidente no ConectaSUS do Ministério da Saúde, o CTIR Gov emitiu o Alerta 08/2021 [37] para ambientes em computação em nuvem utilizados pela administração pública brasileira, informando que estavam sendo observadas diversas ações maliciosas, como intrusões, *defacement* e exclusão de dados, dentre outras ações de ataque nesses ambientes.

Observa-se que a quantidade de cada tipo de incidente não está diretamente relacionada com o tamanho do estrago proporcionado à organização. Desses incidentes, o vazamento de dados, considerado pela CSA como a principal ameaça mais relevante em ambientes de computação em nuvem, possui um impacto muito maior se comparado com o abuso de sítio web. O número de 196 incidentes de Vazamento de Dados talvez pareça baixo no ano 2021, mas isso pode ser explicado pelo fato dos incidentes de vazamentos de dados levarem uma média de 212 dias para serem identificados [5].

No relatório *The 2021 Data Breach* do *Identity Theft Resource Center* - ITRC [38] de 2021, houve mais comprometimentos de dados comunicados ao Governo Americano por organizações públicas e privadas

americanas do que em qualquer ano desde que a primeira lei de notificação de violação de dados estatais entrou em vigor em 2003. Isso representa um aumento de 68% sobre 2020, chegando a um total de 1.862 incidentes relacionados a comprometimento de dados conforme mostrado na Figura 2.3. Os principais vetores de ataques identificados pelo relatório estão distribuídos da seguinte forma: (i) 87% Cyberataques, (ii) 9,6% Erros humanos e de sistemas, (iii) 2,7% Ataques físicos e (iv) 0,7% desconhecidos.

Figura 2.3: Número de comprometimento de dados nos EUA em 2021.
Fonte: The 2021 Data Breach Report [38].

2.2.2 Riscos em Computação em Nuvem

A preservação da confidencialidade dos dados sensíveis do governo ganhou importância após a publicação de documentos secretos por Edward Snowden, particularmente sobre o programa de vigilância PRISM da NSA [39]. Muitos governos duvidam da política de contratação de serviços de sistemas de informação externos como os serviços baseados na nuvem, fornecidos principalmente por empresas americanas [40].

Os riscos da computação em nuvem trazem relação com o modelo de serviço e o modelo de sua implantação citados na Seção 2.1 desta dissertação. A norma ABNT NBR 27017:2016, intitulada "Tecnologia da Informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem", fornece diretrizes que apoiam a implementação de controles de segurança para clientes e provedores de serviços em nuvem [21].

Os principais riscos elencados pela ABNT encontram-se evidenciados em variados artigos e relatórios, entre eles: *Guidelines on Security and Privacy in Public Cloud Computing* do NIST [41] e *Cloud Computing: benefits, risks and recommendations for information security* da ENISA [42]. Este último consolida as classes de riscos da computação em nuvem em três dimensões, conforme descrito na Tabela 2.1, a saber: (i) riscos organizacionais e de políticas; (ii) riscos técnicos; e (iii) riscos legais e regulatórios.

Tabela 2.1: Riscos de Computação em Nuvem.

Dimensão dos Riscos	**Riscos**
Riscos Organizacionais e de Políticas - ROP	ROP01. Bloqueio de dados e serviços em *Cloud* (*Lock-in*)
	ROP02. Perda de governança e controle (*Loss of governance*)
	ROP03. Falha na cadeia de suprimentos (*Suppy Chain Failure*)
	ROP04. Conflitos entre os procedimentos de proteção do cliente e do ambiente de nuvem
	ROP05. Ataques de Engenharia Social
Riscos Técnicos - RTC	RTC06. Exaustão de recursos (sub ou super provisionamento)
	RTC07. Falha de isolamento
	RTC08. Informante malicioso interno ao Provedor de nuvens - abuso de privilégios elevados
	RTC09. Comprometimento da interface de gestão (manipulação, disponibilidade de infraestrutura)
	RTC10. Intercepção de dados em trânsito
	RTC11. Eliminação insegura ou ineficaz dos dados
	RTC12. Negação de serviço distribuída (DDoS)
	RTC13. Negação financeira de serviço (EDoS)
	RTC14. Comprometimento da Plataforma de Nuvem
	RTC15. Perda de Chaves Criptográficas
	RTC16. Falhas técnicas ou ataques relacionada a redes não especificas da nuvem
	RTC17. Perda de *Backups*
	RTC18. Desastres naturais
Riscos Legais e Regulatórios - RLR	RLR19. Intimação e e-descoberta
	RLR20. Risco de mudança de jurisdição
	RLR21. Riscos da proteção de dados
	RLR22. Questões de Licenciamento
	RLR23. Questões de Propriedade Intelectual

Fonte: Adaptado da ENISA [42].

A CSA, em 2020, classificou 11 ameaças, como riscos e vulnerabilidades mais relevantes em ambientes de nuvem, conforme apresentado na Tabela 2.2.

Tabela 2.2: *Ranking* de Ameaças em Computação em Nuvem

	Ranking de Ameaças
1.	Vazamentos de dados
2.	Configurações erradas ou inadequadas
3.	Falta de Arquitetura e Estratégia de Segurança na Nuvem
4.	Identidade, Credenciais, Acesso e Gestão de Chaves Insuficientes
5.	Sequestro de conta
6.	Ameaça interna
7.	Interfaces inseguras de APIs
8.	Plano de Controle Fraco
9.	Falhas na infraestrutura e na estrutura de aplicações
10.	Visibilidade limitada da utilização da Nuvem
11.	Abuso e Uso Nefasto dos Serviços de Nuvem

Fonte: Adaptado da CSA [10]

De forma a enfrentar esses riscos, algumas recomendações sobre gerenciamento de riscos foram propostas. O gerenciamento de riscos da computação em nuvem deve ser flexível o suficiente para lidar com

um cenário em constante evolução e mudança, principalmente no que se trata de tecnologias [41]. O NIST, a Agência da União Europeia para a Segurança Cibernética (ENISA) e a *Cloud Security Alliance* (CSA), instituições que contribuem para o fortalecimento de políticas de segurança cibernéticas, elencam pontos de relevância no que tange ao uso de nuvem pelas organizações, incluindo recomendações para a gestão de tais riscos. Essas recomendações foram utilizadas como base para a construção da norma ABNT NBR ISO/IEC 27017 [21] e estão estruturadas em nove dimensões, resumidas na Tabela 2.3.

Tabela 2.3: Domínios de recomendação para gestão de riscos em nuvem.

Domínio	Descrição
Governança de TIC - GTIC	Conjunto de práticas, políticas e padrões, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos e otimizar o desempenho das atividades de TI.
Legislação e Regulamentações - LEG	Leis e regulamentos que impõem obrigações de segurança e privacidade à organização e, potencialmente, impactam as iniciativas de computação em nuvem.
Auditoria e Conformidade - ACF	Mecanismos e ferramentas de auditoria para determinar como os dados são armazenados, protegidos e usados para validar os serviços e para verificar a aplicação das políticas, garantindo que as práticas organizacionais sejam seguidas durante todo o ciclo de vida dos sistemas.
Continuidade dos Negócios - CNG	Assegurar que, durante uma interrupção intermediária ou prolongada ou um desastre grave, as operações críticas possam ser imediatamente retomadas e que todas as operações possam ser eventualmente reinstituídas de maneira oportuna e organizada.
Segurança das Operações e Comunicações - SOC	Medidas para garantir a disponibilidade, integridade, confidencialidade e a autenticidade da informação. Inclui avaliações de vulnerabilidade e testes de penetração, revisando regularmente certificações e atestados de conformidade específicos do setor, de forma a obter garantia de que o provedor está seguindo as práticas recomendadas e os regulamentos da infraestrutura em nuvem.
Isolamento de Clientes em Nuvem - ICN	Entender a virtualização e outras técnicas de isolamento lógico que o provedor de nuvem emprega em sua arquitetura de software e avaliar os riscos envolvidos à organização, como também configurar adequadamente os serviços de virtualização de acordo com as orientações do provedor e outras práticas recomendadas em padrões e certificações do setor.
Gestão de Identidades e Acessos - GIA	Proteger as funções de autenticação, autorização, auditoria e outras funções de gerenciamento de identidade e acesso que sejam adequadas à organização.
Privacidade e Proteção de Dados - PPD	Utilizar a opção de criptografia apropriada com base nos modelos de gestão de riscos para os dados, negócios e requerimentos técnicos, e, sempre que possível, utilizar chaves gerenciadas pela organização. Não confiar e depender completamente dos controles de acesso e criptografia fornecidas pelo provedor.
Resposta a Incidentes - RIC	Certificar-se de que a organização possa responder aos incidentes de maneira coordenada com o provedor de nuvem, de acordo com suas respectivas funções e responsabilidades para o ambiente de computação.

Fonte: Adaptado da NIST [41] e CSA [43].

Em contraste com a aplicabilidade genérica dos processos de gestão de riscos de segurança da informação, a computação em nuvem possui fontes de riscos de segurança próprios, derivadas de suas características, que diferem da computação tradicional, tais como: rede, escalabilidade e elasticidade do sistema, compartilhamento de recursos, provisionamento por autosserviço, administração sob demanda, provisionamento de serviços através de diversas jurisdições e visibilidade limitada sobre a implementação de controles [21].

No tocante à legislação e à regulamentação citadas na Tabela 2.3 e buscando minimizar riscos, é útil mencionar que a contratação dos serviços de nuvem pode ser normatizada em diferentes setores.

Como, por exemplo, no setor financeiro brasileiro, a contratação desses serviços é regulamentada para instituições financeiras, com base na Resolução do Conselho Monetário Nacional n.º 4.658, de 26 de abril de 2018 [44], e para as instituições de pagamento, tal regulamentação baseia-se na Circular n.º 3.909, de 16 de agosto de 2018 do Banco Central do Brasil [45]. Acrescenta-se que a referida resolução é aplicável inclusive a bancos com controle público federal.

Por fim, ainda no contexto da legislação e da regulamentação elencadas na Tabela 2.3, podem ser lembradas recomendações direcionadas às organizações da Administração Pública Federal Brasileira a respeito dos riscos na computação em nuvem, citando-se os seguintes exemplos: as orientações do Acórdão n.º 1.739/2015-TCU, pelo Tribunal de Contas da União, a respeito dos riscos mais relevantes na contratação de serviços de nuvem [17]; os pontos apresentados pela Portaria do Gabinete de Segurança Institucional - GSI n.º 9/2018 [46], que orienta as entidades governamentais a apenas trafegarem informações não sigilosas por meio da nuvem; e a Instrução Normativa n.º 01/2019 divulgada pela Secretaria de Governo Digital do Ministério da Economia [47], que fomenta o uso de serviços de nuvem entre organizações públicas, referendada pela Lei n.º 14.129 de Governo Digital [8].

Em complemento, relativo às dimensões citadas na Tabela 2.3 'Legislação e regulamentações' como também 'Proteção de Dados', pode ser lembrada a Lei n.º 13.709, de 14 de agosto de 2018, também chamada de Lei Geral Proteção de Dados Pessoais - LGPD [14]. Essa lei, embora não esteja relacionada diretamente a serviços de nuvem, traz obrigações quanto ao tratamento de dados pessoais sensíveis, a serem consideradas por organizações públicas que usem tais serviços.

2.3 *FRAMEWORKS* DE SEGURANÇA CIBERNÉTICA EM COMPUTAÇÃO EM NUVEM

Os *Frameworks* de Segurança Cibernética em Computação em Nuvem são ferramentas para ajudar a orientar as decisões de segurança. A *Cloud Security Alliance* (CSA) é uma organização sem fins lucrativos e líder mundial dedicada à definição e sensibilização das melhores práticas para ajudar a garantir um ambiente seguro de computação em nuvem [19].

Em 2017, a CSA revisou e recomendou os seguintes *frameworks* no que tange a ambiente de computação em nuvem:

1. CSA *Enterprise Architecture* [48].
2. CSA *Cloud Controls Matrix* [49].
3. O projeto de Arquitetura de Referência de Segurança de Computação em NIST (Publicação Especial NIST 500-299 [50].
4. ISO/IEC 27017 Tecnologia da Informação - Técnicas de segurança - Código de prática para controles de segurança da informação baseado na ISO/IEC 27002 para serviços na nuvem conforme versão ABNT NBR [21].

Publicado em 2011 na sua primeira versão, o *framework* Arquitetura Empresarial CSA foi adotada em 2013 pelo Instituto Nacional de Normas e Tecnologias no documento NIST SP 500-299 e NIST SP 500-292 [51] e descontinuado em 2018 [50].

2.3.1 CSA *Enterprise Architecture*

O *framework* CSA *Enterprise Architecture*, atualizado em 2021 e destinado à área de governança e estratégia, é tanto uma metodologia quanto um conjunto de ferramentas que permitem aos arquitetos de segurança, arquitetos de empreendimentos e profissionais de gerenciamento de risco alavancar um conjunto comum de soluções e controles. Essas soluções e controles atendem a um conjunto de requisitos comuns que os gestores de risco devem avaliar com relação ao status operacional da segurança interna de TI e aos controles dos provedores de nuvem. Os controles são expressos em termos de capacidades de segurança e projetados para criar um roteiro comum para atender às necessidades de segurança de seus negócios [51].

A Figura 2.4 representa a composição do *framework* CSA *Enterprise Architecture* com 4 domínios no primeiro nível. No segundo nível, os domínios são segmentados em grupos de componentes, no terceiro nível, os componentes possuem subgrupos de componentes e no último nível, os componentes possuem contêiner.

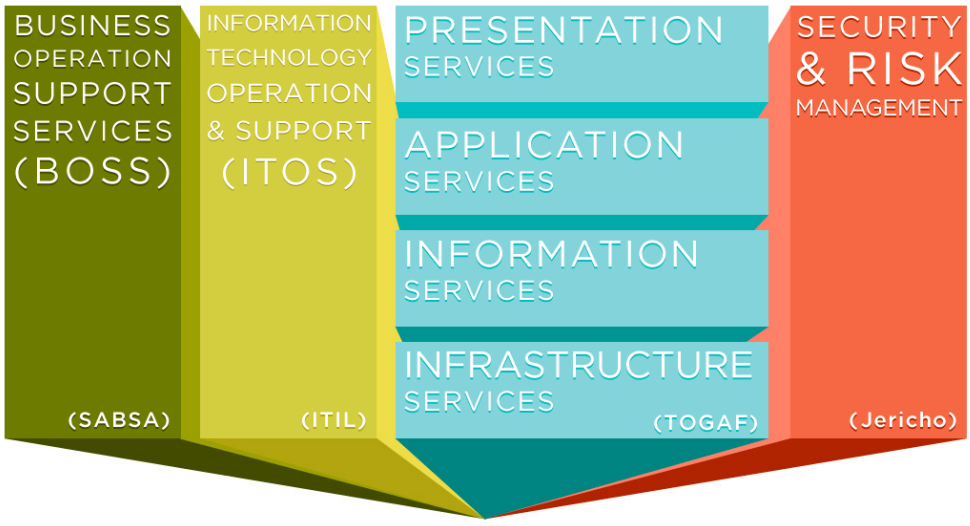

Figura 2.4: CSA Enterprise Architecture.
Fonte: Cloud Security Alliance [51].

2.3.2 CSA *Cloud Controls Matrix*

O *framework Cloud Controls Matrix* (CCM), atualizado também em 2021, é uma estrutura de controle de segurança que se destina à gestão do risco em computação em nuvem. Foi desenvolvido para responder à falta de um *framework* de segurança e conformidade para computação em nuvem, uma vez que a gestão do risco estava apenas centrada na abordagem da infraestrutura de informática tradicional. O CCM surgiu então para preencher essa lacuna, ajudando os provedores de computação em nuvem e seus clientes a

avaliar os riscos globais de segurança dos serviços na nuvem [52].

Os controles do CCM consistem em uma especificação de controle que descreve uma melhor prática para melhorar a segurança de um serviço oferecido. O CCM mapeia os controles de segurança na nuvem do CSA para as principais normas internacionais e padrões tais como: ISO/IEC 27001/27002/27017/27018, NIST SP 800-53, PCI DSS, e ISACA COBIT [19] [52].

Os controles cobertos pelo CCM são preventivos, com o propósito de evitar a ocorrência de um incidente, notificar um incidente e corrigir e limitar os danos causados pelo incidente. Os controles estão no âmbito dos controles legais (políticas), controles físicos (controles de acesso físico), controles processuais (treinamento de pessoal) e controles técnicos (uso de criptografia ou *firewalls*) de acordo com os domínios segurança do CCM, conforme mostrado na Tabela 2.4.

Tabela 2.4: Domínios de Segurança CCM

	Domínios de Segurança	# Controles
AIS	Segurança de Aplicação & Interface	7
A&A	Auditoria & Confiança	6
BCR	Gestão da Continuidade dos Negócios e Resiliência Operacional	11
CCC	Controle de Mudança e Gerenciamento de Configuração	9
CEK	Criptografia, Encriptação e Gerenciamento de Chaves	21
DSP	Segurança de Dados e Gerenciamento do Ciclo de Vida de Privacidade	19
DCS	Segurança do Datacenter	15
GRC	Governança, Risco e Conformidade	8
HRS	Recursos Humano	13
IAM	Gestão de Identidade e Acesso	16
IVS	Segurança de Infraestrutura e Virtualização	9
IPY	Interoperabilidade e Portabilidade	4
LOG	Registro e Monitoramento	13
SEF	Gestão de Incidentes de Segurança, E-Discovery, & Cloud Forensics	8
STA	Gestão da Cadeia de Fornecimento, Transparência e Prestação de Contas	14
TVM	Gestão de Ameaças e Vulnerabilidades	10
UEM	Gestão Universal de Endpoints	14
	Quantidade Total de Controles	197

Fonte: Adaptado da CSA [19].

2.4 TRABALHOS CORRELATOS

No decorrer da pesquisa bibliográfica, utilizando repositórios internacionais de pesquisa acadêmica, foram identificados trabalhos de pesquisa, os quais abrangem pesquisas semelhantes de avaliação de riscos na adoção de serviços de computação em nuvem por organizações governamentais. Na Tabela 2.5 são descritos os trabalhos relacionados com objetivos semelhantes aos desta dissertação.

Tabela 2.5: Trabalhos correlatos

Autor	Ano	País	Abordagem				
			COVID-19	Framework de Controle	Método de pesquisa	Fatores Influenciadores	Dim. dos Riscos
[53]	2021	AUS	×	✓	Qualitativo e Quantitativo	14	Organizacionais
[40]	2021	IDN	×	✓	Qualitativo	5	Técnicos
[54]	2020	KOR	×	×	Quantitativo	2	Organizacionais e Técnicos
[55]	2020	SAL	×	×	×	5	Técnicos
[56]	2020	USA e GBR	×	✓	×	7	Técnicos e Legais
[57]	2020	GRC	×	×	Quantitativo	4	Técnicos
[58]	2020	SAL	×	✓	Quantitativo	8	×
[6]	2019	GBR	×	✓	Qualitativo	18	Organizacionais Técnicos Legais
[59]	2019	SAL	×	✓	×	5	Organizacionais Técnicos
[60]	2019	MYS	×	✓	×	12	Técnicos
[61]	2019	OMN	×	✓	Qualitativo	3	Organizacionais
[62]	2019	AUS	×	×	×	×	×
[63]	2018	NAM	×	×	Qualitativo	7	×
[64]	2018	NAM	×	✓	×	21	Organizacionais Técnicos Legais
[65]	2018	SAL	×	✓	Quantitativo	29	Organizacionais Técnicos Legais
Este trabalho	2022	BRA	✓	CCM	Qualitativo e Quantitativo	9	Organizacionais Técnicos Legais

2.4.1 Método de seleção e resultados

Este trabalho utilizou uma revisão sistemática para assegurar que tanto a investigação como o processo de recuperação fossem focados na precisão, imparcialidade e relevância. Uma revisão sistemática é definida como uma técnica de investigação que tenta recolher todas as provas empíricas num determinado campo, avaliá-las criticamente e obter conclusões que resumem a investigação [66]. Esta revisão sistemática seguiu o conjunto de diretrizes definido pelo guia *Preferred Reporting Itens for Systematic reviews and Meta-Analysis* (PRISMA) que consiste em um *checklist* com vinte e sete itens de verificação juntamente com um fluxograma dividido em quatro partes (identificação, rastreio, elegibilidade e inclusão) [67].

Foi examinado um conjunto de direcionadores de modelos conceituais que podem ser utilizados por clientes de computação em nuvem (*Cloud Service Customer - CSC*) para avaliar os riscos de provedores de serviços de computação em nuvem (*Cloud Services Provider - CSP*). Uma revisão sistemática para identificar modelos conceituais propostos para a avaliação dos riscos de aprovisionamento de nuvens que também poderiam servir de referência para a administração pública foi realizada em janeiro e fevereiro de 2022.

2.4.1.1 Questões de Investigação

Estabelecer as questões de investigação certas é uma fase chave de qualquer revisão sistemática, uma vez que é de importância primordial para identificar os principais objetivos da análise. A revisão deste trabalho foi conduzida com a seguinte pergunta principal de investigação (PPI):

PPI: Quais são as ações de gestão de riscos para enfrentamento dos riscos possíveis e suas mitigações na adoção de computação em nuvem enfrentado pelos seus gestores de governo brasileiro quando da migração de suas cargas de trabalho de seus ambientes locais para nuvem?

Esta principal questão é genérica, e assim, foi dividida nas seguintes questões de busca (QB):

QB1: Quais são as dimensões/categorias de riscos enfrentados por clientes de CSP? Esta questão de investigação permite identificar quais são as categorias ou dimensões de riscos associados à adoção de computação em nuvem.

QB2: Quais são as ações de controles para mitigar os riscos identificados na adoção de computação em nuvem? Esta questão de investigação permite identificar e selecionar os principais controles de mitigação efetivos para os riscos associados à adoção de computação em nuvem.

2.4.1.2 Palavras-Chaves

A quantidade de estudos de investigação aumentou exponencialmente ao longo dos anos. Assim, é importante definir consultas e estratégias de pesquisa claras para identificar as publicações mais relevantes

relacionadas com o tema investigado. Em particular, é preciso identificar as palavras-chaves relacionadas com o tema de investigação e os seus objetivos. As palavras-chaves foram escolhidas de acordo com os tipos de infraestrutura, contexto e administração conforme mostrado na Tabela 2.6.

O padrão *wildcard* (* nas consultas) significa qualquer número de caracteres, tendo sido introduzido para identificar alguns termos relacionados que têm o mesmo prefixo (por exemplo; *cloud, risk, government,* etc.).

Tabela 2.6: Palavras-chaves relacionadas com a investigação do tema

Infraestrutura	**Contexto**	**Administração**
*cloud**	*risk**	*public sector*
intra-cloud	*threat*	*government**
multi-cloud	*security*	
cloud-based	*privacy*	
IaaS	*assessment*	
PaaS	*governance*	
SaaS	*standards*	
	model	
	services	
	provider	
	platforms	

Asterisco Wildcard (*) representa qualquer grupo de caracteres.

2.4.1.3 Consulta

Uma vez definidas as palavras-chaves de investigação, o próximo passo foi dar forma à consulta de pesquisa a ser utilizada para encontrar obras relevantes. Esta consulta foi realizada em duas bases científicas notadamente reconhecidas, *Web of Science* e *SCOPUS* utilizando a pesquisa avançada de cada ferramenta conforme descrito a seguir:

a) Consulta na base *Web of Science*:

```
TI=(cloud* OR intra-cloud OR multi-cloud OR cloud-based OR IaaS OR PaaS OR
SaaS) AND TS=(risk* OR threat OR security OR privacy OR assessment OR
governance) AND TS=(standards OR model OR services OR provider OR
platforms) AND ALL=("public sector" OR government*) AND DOP=(2018/2022)
```

b) Consulta na base *SCOPUS*:

```
(TITLE (cloud* OR intra-cloud OR multi-cloud OR cloud-based OR iaas OR paas
OR saas) AND TITLE-ABS-KEY (risk* OR threat OR security OR privacy OR
assessment OR governance) AND TITLE-ABS-KEY (standards OR model OR services
OR provider OR platforms) AND TITLE-ABS-KEY ("public sector" OR
government*)) AND PUBYEAR > 2017 AND PUBYEAR < 2023
```

Ambas as consultas devolveram uma lista de obras (artigos de conferência, artigos de jornal, livros, entre outros). Apesar do fato de muitos dos registros recuperados estarem relacionados com a investigação, alguns deles não atenderam aos requisitos desta revisão sistemática.

2.4.1.4 Seleção das obras

Os resultados recuperados da pesquisa nas bases de dados passaram por um processo descrito no diagrama PRISMA e *checklist* de verificação. Esse processo inclui a identificação de todos os estudos, remoção de registros duplicados, e definição de critérios de inclusão e exclusão. Os critérios de inclusão e exclusão constituíram a base para a decisão final quanto às obras a incluir na síntese qualitativa e quantitativa.

O processo de seleção de obras nas bases *Web of Science* e *SCOPUS* foi realizado segundo as seguintes etapas:

Etapa 1: Identificação

Tanto o *SCOPUS* como a *Web of Science* são bases de dados importantes que indexam trabalhos de diferentes fontes tais como IEEE Xplore, ACM Digital Library, SpringerLink, ArXiv, Wiley Online Library, Mdpi e outras. A fusão dos resultados de ambos os conjuntos de dados conduz à duplicação de registros que devem ser removidos. Assim, os registros recuperados, juntamente com a sua bibliografia e metadados, são armazenados utilizando software de gestão de referência "*Mendeley Desktop*". Este software é utilizado para remover registros duplicados e classificar os estudos obtidos a partir dos motores de busca.

Etapa 2: Rastreio

Uma vez removidos os registros duplicados, obtém-se vários registros únicos, que precisam ser filtrados para restarem apenas publicações relevantes para a revisão sistemática pretendida. Neste trabalho foram definidos os seguintes critérios de inclusão (CI) e critérios de exclusão (CE):

CI1: Artigos escritos no idioma inglês.
CI2: Artigos propondo análise de riscos na adoção de computação em nuvem para governo.

CE1: Artigos sem lidar com qualquer relação de contexto de *Cloud* e Risco.
CE2: Artigos não publicadas em revistas internacionais ou anais de conferências com revisão por pares.
CE3: Artigos que não tem relação com áreas de pesquisa de engenharia e ciência da computação.

Embora o termo "Computação em Nuvem" tenha surgido em meados de 2007 [27], esta revisão sistemática foi delimitada aos artigos publicados nos últimos 5 anos (a partir de 2018). A decisão de selecionar estudos publicados nesse espaço de tempo baseia-se no período pré-pandemia e pós pandemia de COVID-19.

Com o objetivo de selecionar apenas os artigos que preencham os requisitos estabelecidos para esta revisão sistemática, aplicou-se os critérios de inclusão (CI) e critérios de exclusão (CE) na análise dos títulos e resumos através das bases de dados *Web of Science* e *SCOPUS*. Ao final, foram selecionado cerca de 31% do número total de artigos obtidos na etapa anterior.

Etapa 3: Elegibilidade

Nesta etapa, observou-se atentamente cada estudo remanescente sob a consideração do objetivo prin-

cipal desta revisão e dos CI e CE estabelecidos. Se o artigo revisto não cumpriu os requisitos estabelecidos em etapas anteriores, o mesmo foi excluído desta revisão sistemática.

Etapa 4: Inclusão

Os artigos são categorizados de acordo com as suas conclusões e contribuições dentro do campo da pesquisa (avaliação de riscos na adoção de serviços de computação em nuvem por organizações governamentais). Esta etapa foi o último filtro a fim de selecionar apenas publicações relevantes para esta revisão sistemática.

2.4.1.5 Processo PRISMA

A Figura 2.5 mostra o diagrama de fluxo e os resultados depois de todo o processo ter sido seguido. Um total de 655 artigos foram recuperados das bases de dados científicos *Web of Science* (355) e *Scopus* (300) após a execução das consultas definidas.

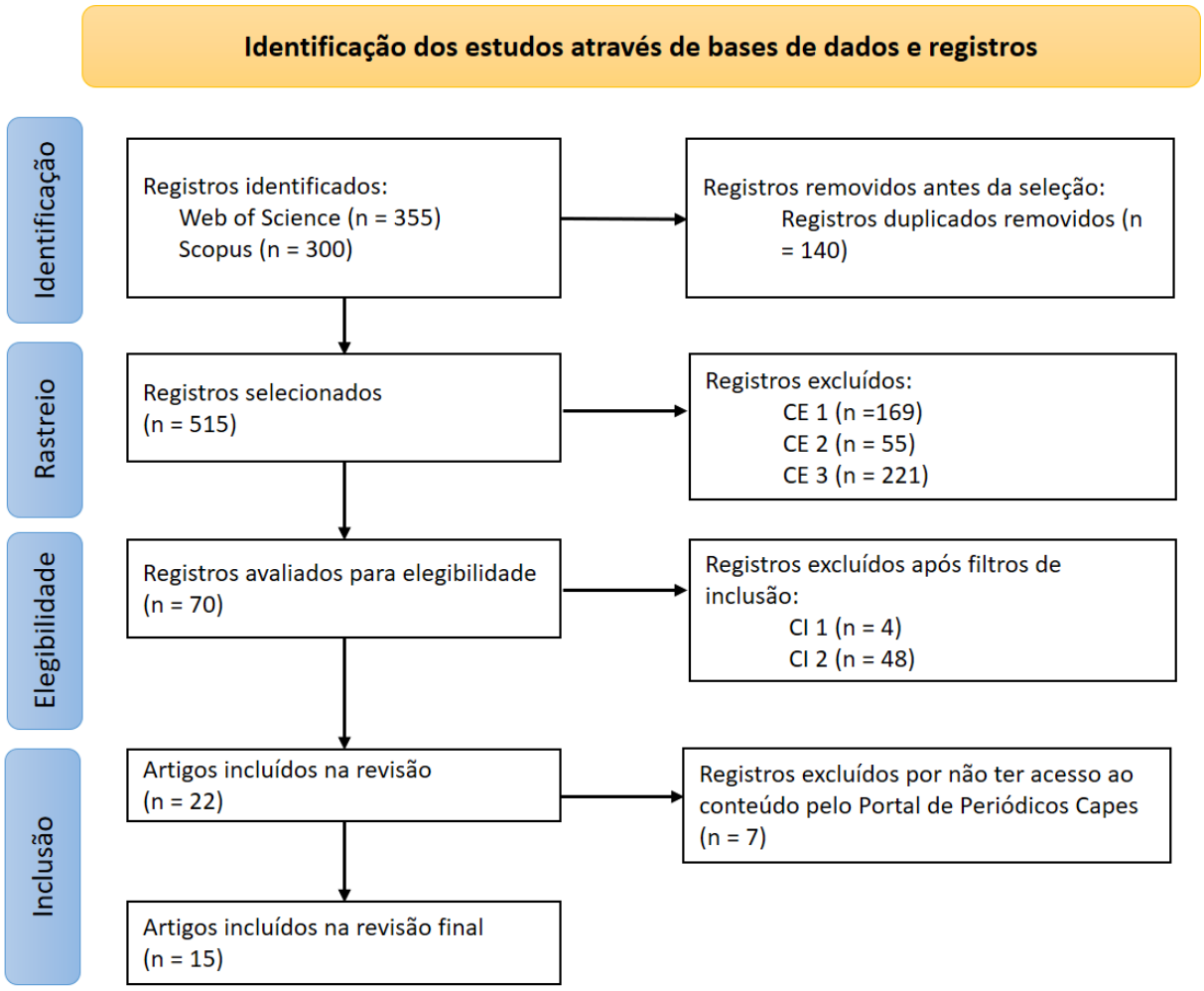

Figura 2.5: Resultados da aplicação do processo PRISMA

Em primeiro lugar, 515 registros únicos foram obtidos após a remoção de registros duplicados. Apesar

da sobreposição entre as duas bases de dados científicos, houve um número significativo de trabalhos publicados em conferências ou em revistas que foram indexados apenas por uma base de dados. No entanto, esta lista de trabalhos de pesquisa incluiu, na sua maioria, estudos não relacionados - quer não lidando com contexto de *Cloud* e Risco (CE1) - quer não sendo publicado em revistas internacionais ou anais de conferências com revisão por pares (CE2) - quer não tendo relação com áreas de pesquisa de engenharia e ciência da computação (CE3) - e assim, foram excluídos durante a etapa de seleção, o que significou 86% dos artigos selecionados. Além disso, foram filtrados durante a seleção - quer sendo escrito no idioma inglês - quer propondo análise de riscos na adoção de computação em nuvem para governo - o que significou também quase 75% dos artigos avaliados para elegibilidade com a leitura de títulos e resumos.

Foram incluídos um total de 22 artigos após a triagem dos critérios de inclusão/exclusão sobre os títulos e resumos, porém, apenas em 15 artigos foi possível realizar o acesso ao conteúdo através do Portal de Periódicos CAPES [68]. Após acesso e uma avaliação completa dos 15 artigos, foram concluídos todos os requisitos para esta revisão sistemática e, por conseguinte, os 15 artigos foram incluídos na análise.

2.4.1.6 Visão geral dos estudos selecionados

Os autores Ali *et al*. [53] avaliam a complexidade na adoção de computação em nuvem pelo Governo Australiano com a realização entrevistas com gerentes de TI para identificar os fatores críticos na adoção da tecnologia. O trabalho destaca-se pela proposta de um modelo de avaliação de complexidade de computação em nuvem, onde foram utilizados os métodos de pesquisa qualitativo e quantitativo na dimensão dos riscos organizacionais.

No Governo Indiano, os autores Nugraha e Martin [40] propõem um *framework* de acordo de nível de segurança. Nesse estudo foram encontrado achados que indicam que os níveis discretos de garantia de segurança desempenham um papel essencial no apoio à definição e inclusão dos requisitos de confidencialidade de dados do Governo em um SLA.

Segundo Lee *et al* [54], o Governo Coreano lançou o seu Plano de Adoção de Computação em Nuvem em 2009 e em 2015 a lei de desenvolvimento de computação em nuvem. Os autores nesse estudo buscaram avaliar a eficácia das políticas governamentais coreanas e compreender o nível de utilização da "nuvem computacional" no sector público, o desempenho do sistema e o desempenho empresarial e benefícios econômicos relacionados, concluindo que a utilização da nuvem pública melhorou o desempenho dos negócios e proporcionou benefícios financeiros.

Mudawi *et al* [55] propõem recomendações para o desenvolvimento de sistemas de TI focados na confiança ao adotar a computação em nuvem nos serviços de governo eletrônico. De acordo com os autores, os governos ainda enfrentam muitos desafios em sua implementação de serviços de governo eletrônico em geral, incluindo a Arábia Saudita, como uma infraestrutura de TI pobre, falta de financiamento e segurança de dados insuficiente.

Os autores Kushwaha, Roguski e Watson [56] abordam em seu estudo questões legais de como os Governos dos Estados Unidos e do Reino Unido protegeram seus dados em computação em nuvem contra o acesso da aplicação da lei estrangeira e sugere métodos que os governos poderiam empregar para garantir a soberania dos dados.

O estudo de Kyriakou, Euripides e Paraskevi [57] investiga empiricamente a extensão do uso da forma mais simples de serviços de Computação em Nuvem e Armazenamento em Nuvem pelos Municípios Gregos, bem como os fatores que a afetam na adoção de serviços em nuvem.

Para Al-Ruithe e Benkhelifa [58], a computação em nuvem traz novas questões de governança de dados, onde a perda de dados é um dos maiores riscos associados. Segundo os autores, antes de adotar a computação em nuvem as organizações devem desenvolver um programa de governança de dados em nuvem. Este estudo é focado em um caso aplicado no setor público da Arabia Saudita e foi realizado com o intuito de diagnosticar e comprovar, com evidências, que a implementação de governança de dados em computação em nuvem influenciará fortemente a eficiência e colaboração entre organizações sauditas como consumidores e fornecedores de serviços na nuvem.

Em seu trabalho, Jones *et al*. [6] demonstram como as implantações de computação em nuvem podem complementar e melhorar as abordagens existentes à implementação de TI. Nesse estudo de pesquisa, destacaram-se as experiências de implantação de uma solução de computação em nuvem implementada para três organizações do setor público no Reino Unido. A descoberta empírica salientou classificações de vantagens (estratégicas, táticas e operacionais) e evidenciou riscos a que se sujeitam a organização adotante da solução.

Ainda no governo da Arabia Saudita, Alannsary e Hausawi [59] afirma que a utilização de computação em nuvem é mínima. Apesar do governo ter oficializado a adoção, a tecnologia não foi devidamente implementada. Em seu trabalho é proposta uma metodologia de implantação de computação em nuvem focada em Plataforma e Software como serviço.

Hamid *et al*. [60] definiram um modelo de requisitos de segurança de tecnologia da informação que é implantado na plataforma de computação em nuvem como Software as a Service (SaaS) para o governo da Malásia. Primeiro foi feito um levantamento de objetivos e políticas de segurança, depois o mapeamento das principais ameaças e controles, considerando as referências [49] e [10], e tendo como resultado o modelo conceitual denominado OTPAF que é *Security Objective* (Objetivos de Segurança), *Threats* (Ameaças), *Policy* (Politicas), *Assumption* (Assunção) e *Security Functionality* (Funcionalidade de Segurança).

Alzadjali e Elbanna [61] apresentam a seguinte questão em seu estudo: “Como podem as instituições influenciar positivamente a adoção de serviços de computação em nuvem?”. Nesse estudo de caso, os autores examinam o caso da adoção da computação em nuvem pelo governo de Omã: como as forças coercivas como as miméticas estão a desempenhar papéis proeminentes na promoção da adoção e migração para a frente das nuvens, aliviando a resistência potencial das forças normativas.

O estudo de Pursultani e Sinnott [62] avalia a migração de um sistema de 15.000 usuários do governo Australiano para computação em nuvem no modelo privado, considerando questões técnicas de performance para sustentar a decisão dos gestores. Dentre os achados técnicos, a limitação técnica de armazenamento em disco foi o principal gargalo. Nesse sentido, os autores apresentam o seu *framework* que não tem o foco em custos, mas em performance técnica.

No governo da Namíbia, os autores Nghihalwa e Shava [63] avaliam a prontidão quanto a adoção de serviços de computação em nuvem pelo setor público. O estudo revelou que os gestores estão prontos para adotarem os serviços uma vez que têm percebido os benefícios associados a produtividade governamental,

mas o ceticismo quanto a questões de segurança da informação é um limitador que deve ser superado.

Dessa forma, os autores no estudo [64] publicam o segundo estudo que apresenta um *framework* de adoção segura de computação em nuvem para o governo da Namíbia. Nesse segundo estudo de caso, o *framework* consiste em quatro componentes: fatores organizacionais, habilitadores tecnológicos, fatores ambientais e características de usuários. O trabalho revelou que o *framework* proposto pode seguramente ser o guia para adoção de computação pelo governo com riscos mínimos de segurança da informação.

Na era da Transformação Digital pelos governos do mundo todo, os autores Al-Ruithe, Benkhelifa e Hameed [65] abordam em seu estudo que a computação em nuvem é o pilar principal para o ecossistema de tecnologia para transformação digital. No governo da Arabia Saudita, através do estudo empírico, os autores examinaram as preocupações quanto aos obstáculos para a adoção de computação em nuvem, e segurança, privacidade e perda de governança foram as principais alegações identificadas.

3 METODOLOGIA

Este trabalho baseia-se em um estudo descritivo e exploratório com uma abordagem qualitativa focado no estudo de caso longitudinal de adoção de computação em nuvem pela administração pública federal brasileira. A abordagem longitudinal possui um carácter confirmatório para a nossa abordagem dedutiva de forma a definir com precisão as fases, para que se possa medir os riscos no momento apropriado. O seu objetivo é compreender o resultado de um fenômeno através da definição de três elementos-chave: contexto, ações, e a interligação temporal entre ações [69].

Ao estudar campos como risco e segurança, os pesquisadores tendem a confiar em métodos subjetivos que exigem a entrada de respondentes bem qualificados para obter dados [70].

Para coletar os dados, foram utilizadas entrevistas semiestruturadas - às vezes chamadas de entrevistas informais - tratando de conversar com pessoas, mas de maneira que sejam autoconscientes, organizadas e parcialmente estruturadas [71]. Entrevistas são tipicamente usadas quando os objetivos do estudo são complexos e difíceis de explicar concisamente em um formulário de pesquisa e quando informações detalhadas são necessárias [72].

A seleção de participantes para entrevistas semiestruturadas é de grande importância. Tradicionalmente as pessoas são escolhidas com base em sua experiência relacionada ao tema da pesquisa [73].

O critério para selecionar o gestor público entrevistado de cada organização foi a necessidade de que esse fizesse parte de departamentos relacionados a Tecnologia da Informação, Infraestrutura, Segurança ou equivalentes e estivesse incluído em um ou mais dos seguintes perfis:

1. **Perfil Profissional Estratégico**: Posições de tomadores de decisões a respeito de Tecnologia da Informação ou equivalentes (Diretor, Chefe de divisão, *Chief Information Officer*, entre outros).
2. **Perfil Profissional Tático**: Posições de influência em coordenações de Segurança da Informação das instituições (analistas, gerentes, coordenadores-geral, entre outros).
3. **Perfil Profissional Operacional**: Posições de influência na coordenação de infraestrutura relacionada à Tecnologia da Informação das instituições (analistas, gerentes, coordenadores, entre outros).

As entrevistas foram iniciadas abordando questões relativas ao uso de tecnologias baseadas em nuvem, a fim de avaliar a ótica dos participantes quanto à gestão dos riscos no contexto de cada organização. Para isso, os entrevistados foram perguntados a respeito das circunstâncias presentes, passadas e futuras quanto à utilização de recursos em nuvem pelas suas organizações.

3.1 ESTUDO LONGITUDINAL E AMOSTRA DE ENTREVISTADOS

Este trabalho empregou um estudo longitudinal, quando os entrevistados são estudados em um período determinado, neste caso, compreendendo duas etapas, a primeira coleta pré-pandemia de COVID-19, em

abril de 2019 [13] e a segunda em maio, junho e julho de 2022, pós-pandemia conforme descrito na Tabela 3.1.

Tabela 3.1: Coleta de Dados

Coleta	Objetivos	Perfil Profissional	Coleta de Dados	Análise de Dados
1.º Coleta (abril 2019)	Avaliar os riscos ao se implantar serviços de computação em nuvem	Estratégico Tático Operacional	Entrevista Semi-estruturada com questões fechadas e abertas	Análise de Conteúdo
2.º Coleta (maio-julho 2022)	Identificar e avaliar a evolução da propensão ao enfrentamento de riscos no uso de computação em nuvem pelos gestores públicos, pós-pandemia de COVID-19.	Estratégico Tático Operacional	Entrevista Semi-estruturada com questões fechadas e abertas	Análise de Conteúdo

A amostra da pesquisa diz respeito a um recorte sociodemográfico da população para criar um grupo específico que corresponda ao público-alvo e assim poder entender seu comportamento. A amostra analisada na presente pesquisa foi composta por 23 organizações públicas do nível federal (10%) do universo de 232 organizações possíveis de serem entrevistadas, considerando ainda a esfera de poder a qual pertence para se ter um equilíbrio na escolha dos respondentes. A Figura 3.1 representa a amostra analisada.

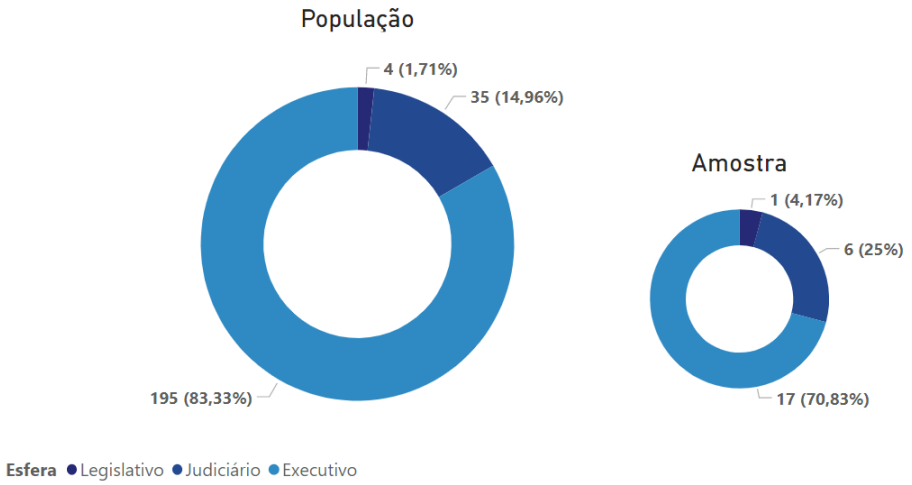

Figura 3.1: Amostra analisada.

Para avaliar a adoção de computação em nuvem na administração pública, na 1ª Coleta, em abril de 2019, foram entrevistados gestores de 10 diferentes organizações do Governo Federal, incluindo o Poder Judiciário e Executivo. Na 2ª Coleta, no período de maio, junho e julho de 2022, foram entrevistados gestores de 15 diferentes organizações das três esferas de poder. Duas organizações participaram das duas coletas. A Tabela 3.2 resume o quadro de organizações públicas entrevistadas.

Tabela 3.2: Organizações públicas entrevistadas

Esfera de Poder	Organizações	Total	1º Coleta [13]		2º Coleta	
			Quant.	(%)	Quant.	(%)
Executivo	Administração direta	28	4	14%	3	10%
	Administração indireta	167	5	3,5%	5	3,5%
Legislativo	Congresso e Órgãos administrativos	4	-	-	1	25%
Judiciário	Tribunais Superiores	5	-	-	4	75%
	Justiça Comum - TJs	27	-	-	1	3%
	Conselhos de Justiça	3	1	33%	1	33%
Total		**232**	**10**	**4,3%**	**15**	**6,4%**

Passados dois anos de pandemia de COVID-19 no Brasil, houve o aumento da quantidade de serviços digitalizados pelo governo brasileiro, e realizou-se a segunda coleta para identificar a interligação temporal entre as ações de adoção de computação em nuvem pelos gestores de TI governamentais. Nesta etapa foram entrevistados 16 gestores de 15 diferentes organizações de administração pública federal, no período de maio, junho e julho de 2022, três anos após a primeira coleta, conforme mostrado na Figura 3.2.

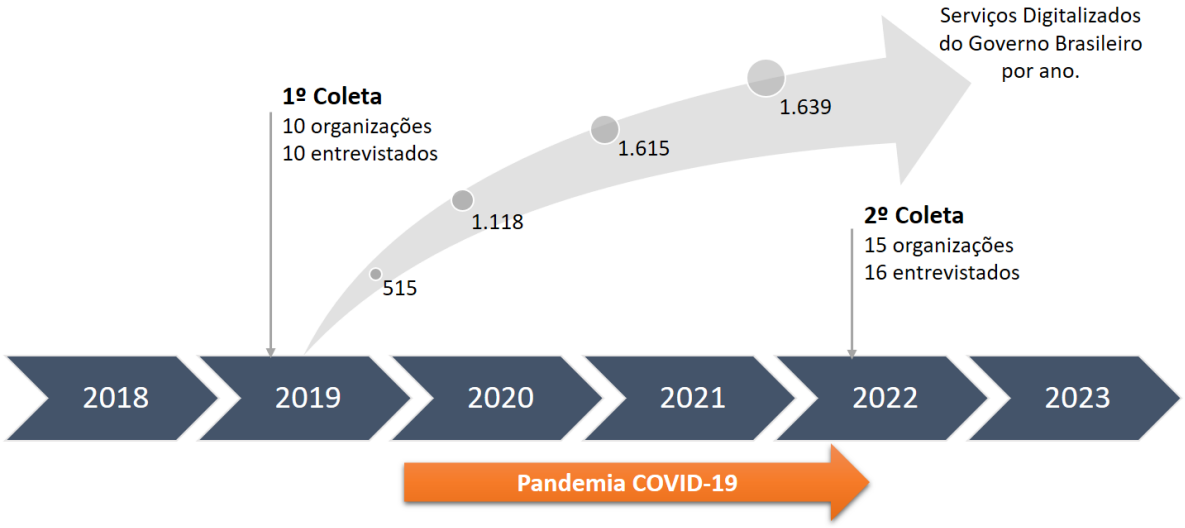

Figura 3.2: *Timeline* do Estudo Longitudinal

Os dados levantados com as entrevistas foram utilizados para compor a descrição e as análises dos resultados relativos à ótica dos entrevistados, em relação à gestão de riscos no uso da computação em nuvem nos órgãos públicos em que atuavam durante a pandemia de COVID-19. Na segmentação dessa análise, foram consideradas, inclusive, as dimensões descritas na Tabela 2.3.

3.2 ENTREVISTA SEMIESTRUTURADA E O ROTEIRO

Uma vez delimitado o problema de pesquisa e realizado o levantamento exploratório para o conhecimento da temática, o pesquisador seleciona o público-alvo e determina qual proporção dele pretende

abordar por meio de entrevistas pessoais [74]. Ao conduzir as entrevistas semiestruturadas, é possível fazer anotações ou gravar áudio da discussão, permitindo concentrar-se totalmente na interação [75]. Logo após a entrevista, documentam-se os principais temas que surgiram e qualquer assunto que possa ter valor para agregar à pesquisa, qualificando esse procedimento como análise de dados qualitativos [76] [77].

A pesquisa quantitativa e qualitativa contribui para isso, pois permite considerar os dados em totalidade, de modo subjetivo e objetivo, no sentido de ampliar o significado das experiências e aprofundar a compreensão do discurso [74].

Ao escolher a entrevista semiestruturada, o pesquisador deve garantir que o roteiro de perguntas lhe servirá de norte para conduzir o entrevistado, no momento oportuno, ao abordar ou retomar o assunto de interesse da pesquisa. Por outro lado, o pesquisador deverá ser suficientemente flexível para permitir que o entrevistado derive suas reflexões para temáticas ou questões relacionadas, ou aborde outros ângulos do problema que lhe haviam escapado [74] [78].

Para atingir os objetivos propostos neste estudo, não se fez necessário identificar os entrevistados. A fim de proteger dados de identificação pessoal, bem como resguardar o sigilo das organizações entrevistadas, optou-se por segmentar as respostas de maneira anônima, utilizando uma numeração para fazer remissão a cada entrevistado, incluindo siglas como, por exemplo, E01, E02 em diante.

O roteiro de entrevista semiestruturada foi elaborado baseado na "Gestão de Risco de Segurança e Privacidade em computação em nuvem da ENISA" [42], nas "Dimensões de recomendação para a gestão de riscos em computação em nuvem do NIST" [41] e, também, no "*Framework* de *CSA Cloud Controls Matrix*" [19], realizando a correlação entre as perguntas do roteiro e os domínios de segurança em computação em nuvem apresentado no *framework* CCM da CSA. Para tanto, definiu-se 4 (quatro) instrumentos a serem aplicados na entrevista semiestruturada conforme ilustrado na Figura 3.3.

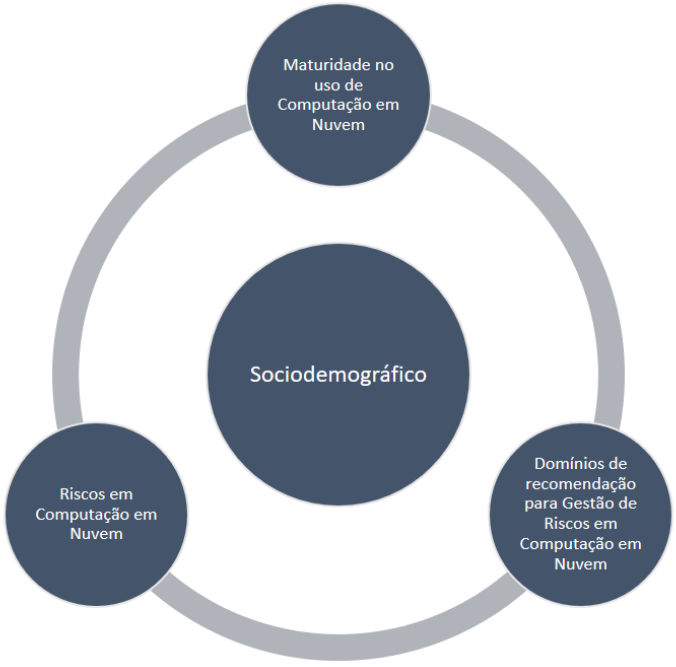

Figura 3.3: Instrumentos do trabalho

O primeiro instrumento aplicado ao entrevistado foi o Sociodemográfico composto por dois conjuntos de perguntas, duas relativas a organização do entrevistado e três relativas ao perfil do entrevistado (Tab. 3.3). Desse modo, foram coletadas informações para posicionar e categorizar a organização no âmbito da administração pública federal, bem como identificar a área de atuação profissional do entrevistado dentro de sua organização.

Tabela 3.3: Instrumento - Sociodemográfico

ID	Perguntas
P01-DEM	Esfera de Poder: ( ) Executivo ( ) Judiciário ( ) Legislativo
P02-DEM	Quantidade de usuários finais de TI: ( ) 1-500 ( ) 501-2000 ( ) 2001-10000 ( ) +10001
P03-DEM	Atuação profissional de TI na organização é na área de: ( ) Governança (Avaliar, Dirigir e Monitorar); ( ) Gestão (Planejar, Executar, Controlar e Agir).
P04-DEM	Em qual etapa no processo de tomada de decisão na área de TIC você atua? ( ) Não atua ( ) Concepção ( ) Planejamento ( ) Aprovação ( ) Execução ( ) Fiscalização
P05-DEM	Qual é o seu tempo de experiência em TIC? ( ) 1 a 4 anos ( ) 5 a 9 anos ( ) 10 a 15 anos ( ) + 15 anos

O segundo instrumento é denominado de "Maturidade no uso de Computação em Nuvem" composto por 6 (seis) perguntas (Tab. 3.4) de forma a atingir o objetivo especifico 2 (Seção 1.4) do presente trabalho que é a identificação de quais são as percepções dos gestores públicos de TI da administração pública federal quanto ao enfrentamento dos riscos na adoção de computação em nuvem e a prontidão dos provedores de serviços em nuvem durante o período de três anos investigado (pré-pandemia e pós-pandemia).

Tabela 3.4: Instrumento - Maturidade no uso de Computação em Nuvem

ID	Perguntas
P06-MAN	Atualmente, quais são os serviços ou soluções baseadas em Computação em Nuvem que são utilizados pela sua organização?
P07-MAN	Há quanto tempo os serviços em nuvem são utilizados pela organização?
P08-MAN	Percentualmente, quantos serviços internos já foram transferidos para nuvem e qual é a topologia adotada?
P09-MAN	Qual seria a percentual de usuários internos que utilizam serviços ou soluções em nuvem?
P10-MAN	Existe algum serviço nuvem que a sua organização deixou de utilizar?
P11-MAN	A sua organização pretende contratar mais serviços em nuvem?

O instrumento "Domínios de recomendação para gestão em risco em Computação em Nuvem" possui 9 perguntas (Tab. 3.5) relativas aos 9 domínios (Tab. 2.3) extraídos do NIST [41] e CSA [43], e correlacionados aos Domínios de Segurança do CCM, com intuito de contribuir para o alcance dos objetivos específicos 3, 4 e 5 (Seção 1.4) propostos neste trabalho.

Tabela 3.5: Instrumento - Domínios de recomendação para gestão de riscos em Computação em Nuvem

Domínio	ID	Perguntas	Referência CCM [19]
Legislação e Regulamentações	P12-LEG	Em quais aspectos você acredita que a legislação brasileira vigente pode prejudicar ou promover o avanço tecnológico do Governo quanto ao uso de serviços em nuvem?	A&A e GRC
	P13-LEG	Quais são os riscos (negativos ou positivos) implicados à sua organização pela legislação brasileira quanto ao uso de serviços em nuvem? Quais são as medidas ou controles que a sua organização tem tomado para se adequar à legislação?	A&A e GRC
Governança de TIC	P14-GTI	A sua organização estabeleceu uma política ou norma para decidir em quais casos é apropriado o uso de serviços em nuvem? Quais são as medidas ou controles aplicados de governança de TIC sobre o uso de serviços em nuvem?	GRC, SEF, STA e TVM
Privacidade e Proteção de Dados	P15-PPD	Quais são as preocupações quanto aos riscos relacionados aos dados institucionais armazenados (sensíveis e não sensíveis) associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	DSP, DCS, IVS, LOG e TVM
Gestão de Identidade e Acessos	P16-GIA	Quais são as preocupações quanto aos riscos de gestão e identidade e acessos associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	IAM, BCR, A&A, DSP, IAM e TVM
Isolamento de Clientes em Nuvem	P17-ICN	Quais são as preocupações quanto aos riscos de isolamento de clientes em nuvem associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	AIS, CEK, DCS, HRS, IVS e TVM
Segurança das Operações e Comunicações	P18-SOC	Quais são as preocupações quanto aos riscos de segurança das operações e comunicações associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	AIS, DSP, IVS, STA, GRC, LOG e TVM
Resposta a Incidentes	P19-RIC	Quais são as preocupações quanto aos riscos a resposta a incidentes associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	GRC, SEF, TVM e LOG
Continuidade de Negócios	P20-CNG	Quais são as preocupações quanto aos riscos de continuidade de negócio associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	BCR, CCC e GRC
Auditoria e Conformidade	P21-ACF	Quais são as preocupações quanto aos riscos de auditoria e conformidade associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	A&A e GRC

Por último, o instrumento de "Riscos no uso de Computação em Nuvem" formula uma pergunta (Tab. 3.6) com o propósito de complementar o objetivo especifico 2 (Seção 1.4).

Tabela 3.6: Instrumento - Riscos no uso de Computação em Nuvem

ID	Perguntas
P22-RIS	De maneira geral, quais seriam os maiores riscos associados ao uso de nuvem entendido pela sua organização?

3.3 FLUXO DA PESQUISA

Após a elaboração do roteiro, foi dado inicio à coleta dos dados de testes por meio de entrevistas remotas com gravação e transcrição dos áudios utilizando a ferramenta Microsoft Teams. O fluxo da pesquisa até a análise dos dados está sumarizado na Figura 3.4.

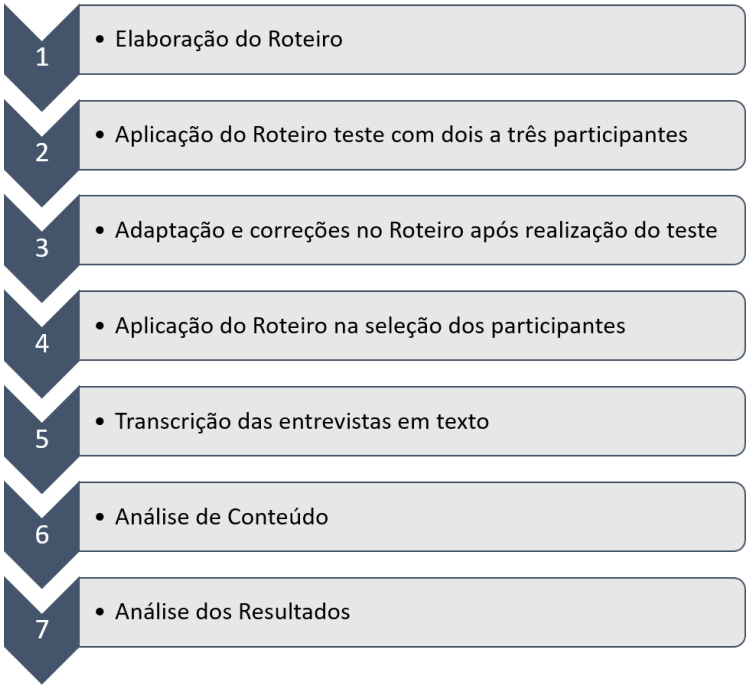

Figura 3.4: Fluxo da Pesquisa

Durante a aplicação do roteiro de teste com 3 (três) entrevistados pertencentes à população pesquisada, observou-se que o tempo de entrevista com os 4 (quatro) instrumentos da pesquisa variou de 25 a 50 minutos. A finalidade desta prova, geralmente designada como pré-teste, é evidenciar possíveis falhas na redação do questionário, tais como: complexidade das questões, imprecisão na redação, desnecessidade das questões, constrangimentos ao informante, exaustão etc [15]. As sugestões obtidas durante o pré-teste e sua avaliação para uso nos instrumentos são apresentadas na Tabela 3.7 de acordo com o foco.

Tabela 3.7: Contribuições do pré-teste

FOCO	Contribuições
Clareza e precisão dos termos	Sem modificações
Quantidade de perguntas	Sem modificações
Ordem das perguntas	Sem modificações
Introdução do questionário	- Adição do Termo de Consentimento Livre e Esclarecido (TCLE)
Conteúdo das questões	- Adicionar exemplos de riscos e tecnologia para melhor situar o entrevistado quanto a questão abordada - Consolidar as questões do instrumento Domínios de recomendação para gestão de riscos em nuvem

3.4 ANÁLISE DE CONTEÚDO

Para realizar a análise dos dados obtidos através dos instrumentos de pesquisa, utilizou-se a análise de conteúdo segundo Bardin [79], que apresenta três diferentes etapas para a análise de conteúdo: (i) pré-análise; (ii) exploração do material; e (iii) tratamento dos resultados, inferência e interpretação, conforme Figura 3.5.

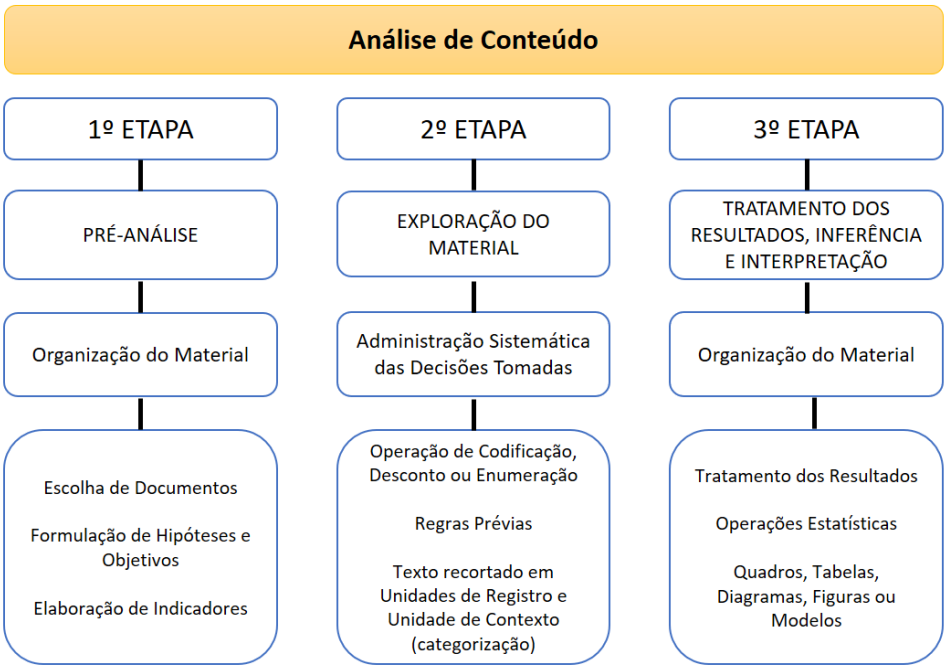

Figura 3.5: Etapas para a análise de conteúdo

A análise de conteúdo visa extrair dos textos narrados, a partir de características metodológicas objetivas e sistematizadas, a inferência do conhecimento e o sentido que reverbera das mensagens daquilo que é verbalizado [79].

A análise dos dados permite organizá-los de modo que forneçam respostas para o problema de pesquisa. Neste sentido, os dados coletados a partir do modelo de informações pessoais permitem compreender o universo dos participantes e fornecem dados quantitativos que possibilitam conhecer o perfil sociodemográfico [74].

Na análise de conteúdo podem ser utilizadas diferentes técnicas, tais como: (i) Análise Categorial, (ii) Análise de Avaliação, (iii) Análise de Enunciação, (iv) Análise Proposicional do Discurso, e (v) Análise de Expressão. No presente trabalho, optou-se por utilizar a técnica de Análise Categorial, que funciona por operações de desmembramento do texto em unidades, em categorias segundo reagrupamento analógicos. A técnica de Análise Categorial apresenta bons resultados em pesquisa qualitativa, devido à possibilidade de realizar interpretações embasadas por inferências [79].

3.4.1 Procedimentos de Análise de Conteúdo

Com a coleta dos dados por meio das entrevistas semiestruturadas, prosseguiu-se com as etapas seguintes para obter os resultados quanto à Análise de Conteúdo conforme o protocolo de Bardin [79]. Destaca-se que os resultados são apresentados em categorias, estabelecidas antes e depois, com base nos objetivos da pesquisa e no protocolo de Análise Categorial de acordo com as fases a seguir:

(i)[**Pré-análise:**] A pesquisa iniciou com a escolha e identificação do tema de pesquisa a ser abordado, a Adoção de Computação em Nuvem pelo setor público pós-pandemia. Após uma leitura flutuante utilizando das regras de exaustividade, representatividade, homogeneidade, pertinência e exclusividade. Observou-se pouca literatura disponível sobre o assunto, isto é, literatura escassa e não científica. Com isso, constatou-se a necessidade de pesquisas científicas sobre o tema.

Nesse sentido, foi realizada uma revisão sistemática de literatura para analisar a relevância da pesquisa quanto ao objeto escolhido e verificar até que ponto o tema é abordado na literatura. Os resultados são apresentados na Tabela 2.5, o que confirmou a relevância e pertinência do assunto, além da escassez de produção científica no país.

Considerando o levantamento realizado em 2019 com gestores da administração pública, período anterior a pandemia de COVID-19, foi possível definir este trabalho como um estudo longitudinal, com duas coletas de dados, uma em 2019 e outra em 2022.

Por fim, fez-se a elaboração de indicadores num corpo teórico de revisão de literatura para fundamentar a interpretação final com a criação e elaboração de um roteiro de entrevista semiestruturada e aplicação deste junto aos gestores da administração pública federal.

O contato com os órgãos federais foi realizado primeiramente com alunos mestrandos do programa de Pós-graduação Profissional em Engenharia Elétrica (PPEE) do Departamento de Engenharia Elétrica da Universidade de Brasília (UnB). Em seguida, com indivíduos provenientes de indicações dos próprios entrevistados, conforme aconteciam as entrevistas. A Figura 3.6 sumariza os passos e procedimentos dessa etapa.

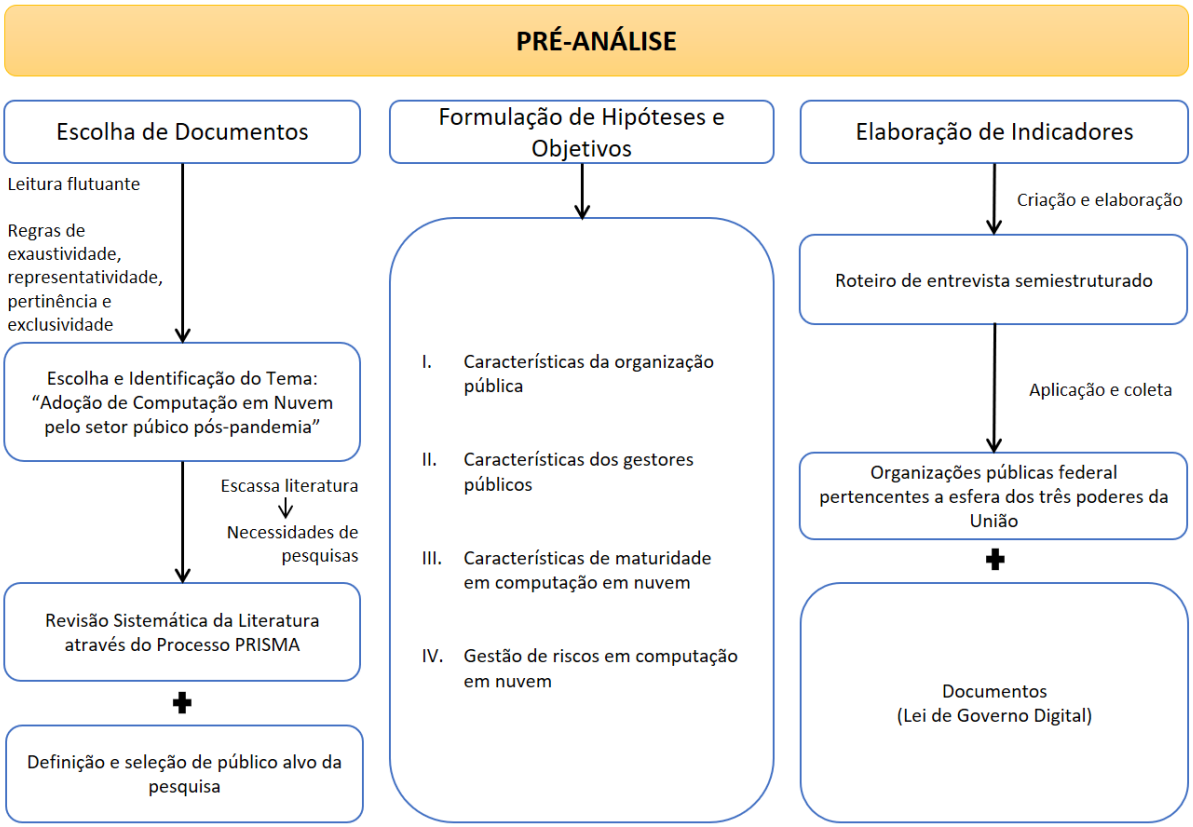

Figura 3.6: Aplicação da etapa Pré-Análise.

(ii) Exploração do material: O material coletado e selecionado foi recortado em unidades de registro e unidades de contexto com caracterização temática *a priori* e *posteriori*, por meio de quatro categorias (blocos):

(a) Categoria 1: Características da organização pública;
(b) Categoria 2: Características dos gestores públicos:
(Subcategoria 2.1: Especificidades de atuação profissional;
Subcategoria 2.2: Experiência profissional);
(c) Categoria 3: Características de maturidade no uso de computação em nuvem e
(d) Categoria 4: Gestão de riscos em computação em nuvem:
(Subcategoria 4.1: Legislação e Regulamentações;
Subcategoria 4.2: Governança de TIC;
Subcategoria 4.3: Privacidade e Proteção de Dados;
Subcategoria 4.4: Gestão de Identidade e Acessos;
Subcategoria 4.5: Isolamento de Clientes em Nuvem;
Subcategoria 4.6: Segurança das Operações e Comunicações;
Subcategoria 4.7: Resposta a Incidentes;
Subcategoria 4.8: Continuidade de Negócio;
Subcategoria 4.9: Auditoria e Conformidade e

Subcategoria 4.10: Riscos no uso de Computação em Nuvem).

A categorização *a priori* foi usada, pois já se tinha um conhecimento prévio ou interesse nessas categorias pré-estabelecidas. Nesse sentido, optou-se por categoria *posteriori* neste trabalho com subsequente elaboração de subcategorias quando necessário. A unidade de contexto são as organizações da administração pública da União. A categorização é temática, uma vez que os domínios de recomendação para gestão de riscos em computação em nuvem já foram definidos.

Dessa forma, trata-se de uma categorização temática *a priori* e *posteriori* por meio de blocos conforme ilustrado na Figura 3.7.

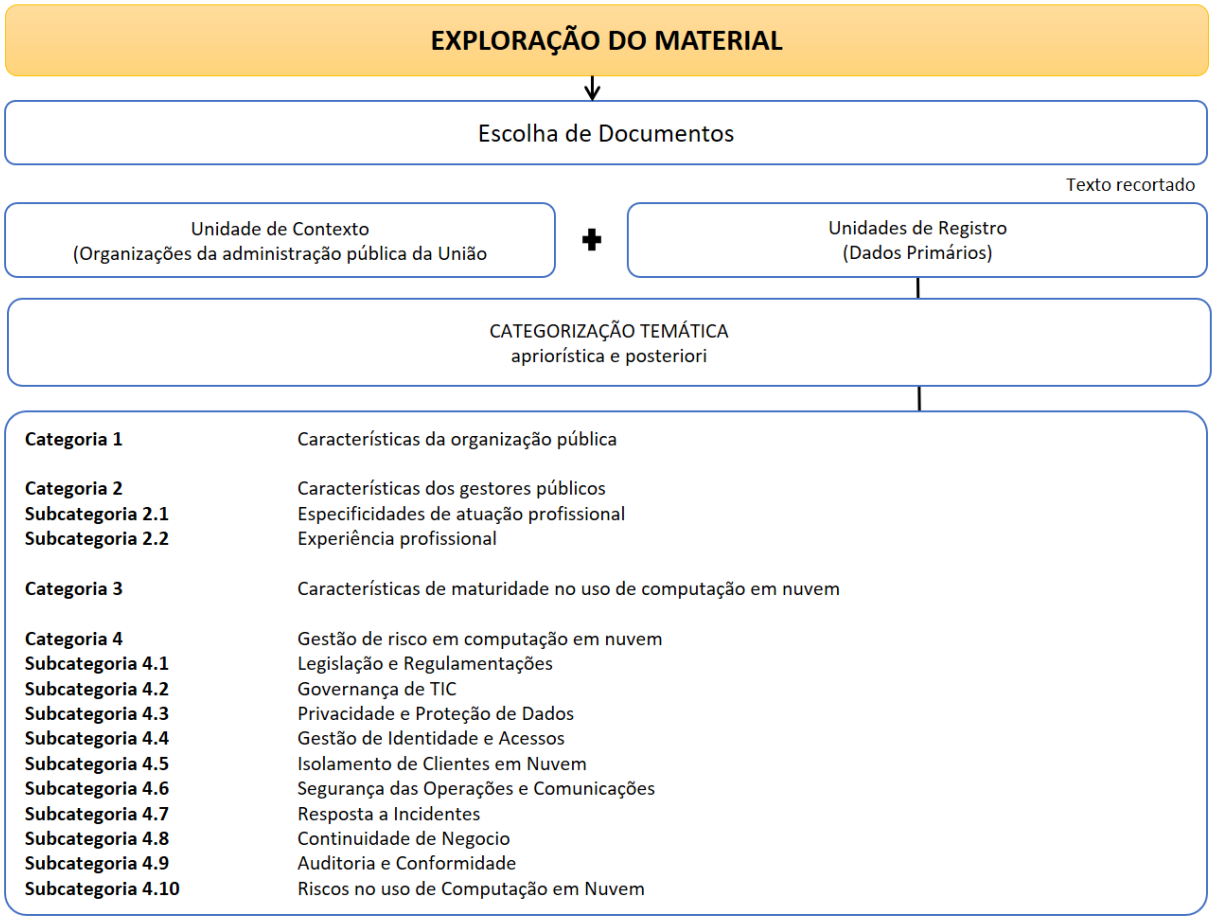

Figura 3.7: Aplicação da etapa de Exploração de Material.

(iii)Tratamento dos resultados, inferência e interpretação: Nesta última fase, os resultados foram tratados de forma expressiva e confirmados com a transcrição das entrevistas. Foram elaboradas figuras, quadros e tabelas que puderam

mostrar e destacar as informações a fim de alcançar os objetivos propostos.

Por fim, os dados obtidos com a pesquisa foram tratados, inferidos e interpretados por meio de categorização temática a *priori-posterior* e discutidos conforme será descrito no próximo capítulo.

A Figura 3.8 sumariza os passos e procedimentos dessa fase.

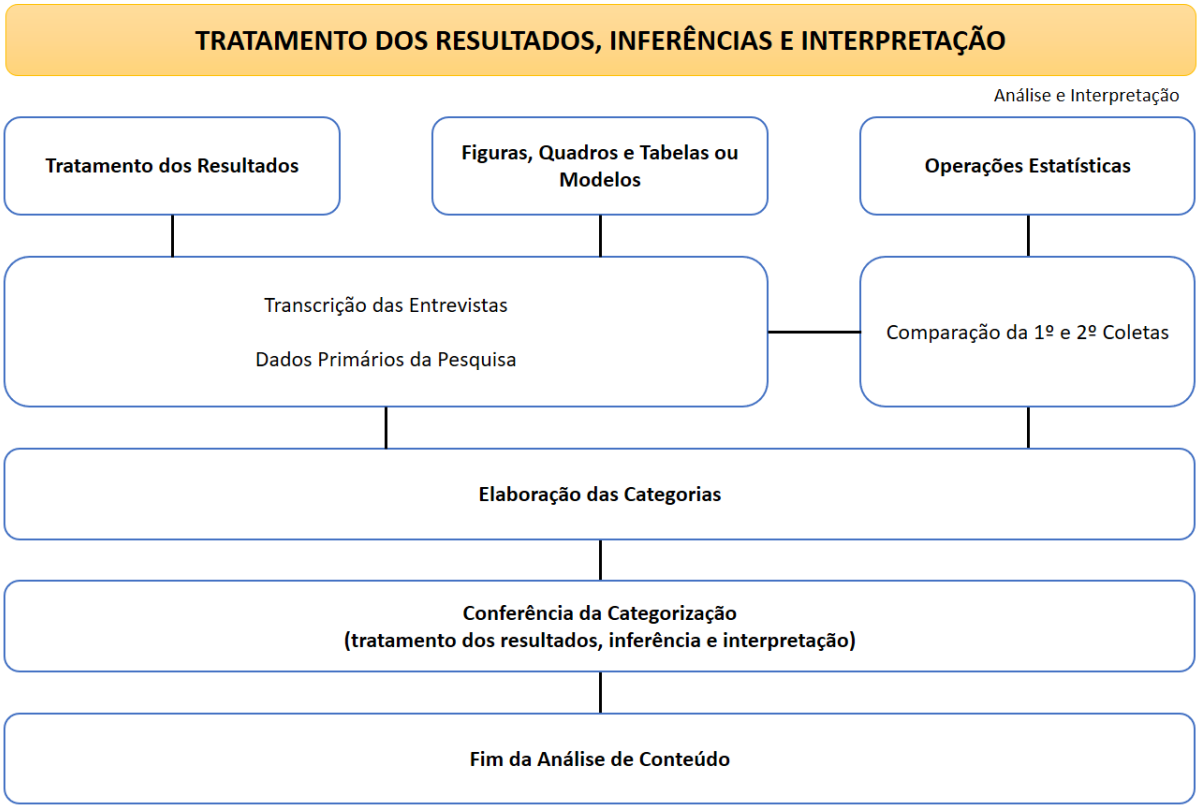

Figura 3.8: Aplicação da etapa de Exploração de Material.

Ressalta-se que os entrevistados neste estudo foram denominados como Entrevistado 01 com a sigla (EE01), Entrevistado 02 - (EE02), assim por diante, de forma a preservar a identidade do entrevistado assim como da organização a qual pertence.

4 RESULTADOS

Neste Capítulo apresenta-se a análise dos dados obtidos, segundo a metodologia apresentada no Capítulo 3 (Seção 3.4.1) e a fundamentação teórica no Capítulo 2. Os resultados descritos a seguir seguem os métodos e técnicas já expostos.

4.1 CATEGORIA 1: CARACTERÍSTICAS DA ORGANIZAÇÃO PÚBLICA

A Categoria 1, Características da Organização Púbica, tem por objetivo identificar e caracterizar a organização pública seguindo o roteiro de entrevista mostrado pela Tabela 4.1. Os dados dessa categoria são mais gerais, de forma a apresentar as organizações públicas federais.

Tabela 4.1: Roteiro sobre a caracterização da organização pública

Itens	Caracterização do Núcleo de Sentido
Esfera de Poder	Organização
Quantidade de usuários internos de TIC	Organização quanto ao perfil de dimensão da organização baseado no quantitativo de usuários internos de TIC

A Tabela 4.2 apresenta a caracterização das organizações públicas dos entrevistados em termos de esfera de poder (Executivo, Legislativo e Judiciário) e quantidade de usuários internos de TIC (Micro, 1 a 500), (Pequeno, 501 a 2.000), (Médio, 2.001 a 10.000) e (Grande, + 10.001).

De maneira a mitigar possíveis vazamentos de dados sensíveis ou não, os participantes e suas instituições foram preservados e anonimizados conforme já mencionado anteriormente.

Tabela 4.2: Caracterização da organização pública

Organização	Entrevistado	1º Coleta [13]	2º Coleta	Esfera de Poder	Quantidade de usuários
ORG01	EE01	✓		Executivo	501-2.000
ORG02	EE02	✓		Executivo	501-2.000
ORG03	EE03	✓		Executivo	1-501
ORG04	EE04	✓		Executivo	501-2.000
ORG05	EE05	✓		Executivo	1-501
ORG06	EE06	✓		Executivo	501-2.000
ORG07	EE07	✓		Executivo	+ 10.001
ORG08	EE08	✓		Executivo	+ 10.001
ORG09	EE09 e EE09.1	✓	✓	Judiciário	501-2.000
ORG10	EE10 e EE10.1	✓	✓	Executivo	+ 10.001
ORG11	EE11		✓	Executivo	501-2.000
ORG12	EE12		✓	Executivo	+ 10.001
ORG13	EE13		✓	Executivo	2.001-10.000
ORG14	EE14		✓	Executivo	501-2.000
ORG15	EE15		✓	Executivo	+ 10.001
ORG16	EE16		✓	Executivo	+ 10.001
ORG17	EE17		✓	Executivo	+ 10.001
ORG18	EE18 e EE18.1		✓	Judiciário	2.001-10.000
ORG19	EE19		✓	Judiciário	2.001-10.000
ORG20	EE20		✓	Legislativo	2.001-10.000
ORG21	EE21		✓	Judiciário	2.001-10.000
ORG22	EE22		✓	Judiciário	2.001-10.000
ORG23	EE23		✓	Judiciário	+ 10.001
23	**26**	**10**	**15**	69,6% Executivo 26,1% Judiciário 4,3% Legislativo	35% +10.001 26% 2.001-10.000 31% 501-2.000 8% 1-501

A Tabela 4.2 inclui informações que possibilitam a categorização, como o codinome da organização, do(s) entrevistado(s), a participação do entrevistado na respectiva coleta, podendo ser em uma ou em ambas, a esfera de poder que compõe a organização do Estado Brasileiro e a quantidade de usuários internos de TIC de maneira a classificar o tamanho e porte da organização.

Durante um mês na primeira coleta, em abril de 2019, foram entrevistados 10 gestores, enquanto que na segunda coleta, em maio, junho e julho de 2022, foram entrevistados 16 gestores. Desse total, apenas duas organizações participaram das duas coletas e uma terceira teve dois entrevistados durante a segunda coleta, situação essa que não afetou no resultado da pesquisa, uma vez que os dados obtidos foram mesclados para a mesma organização na execução do protocolo de Análise de Conteúdo. Paralelamente, observa-se que a distribuição das organizações ficou equilibrada entre as duas coletas, considerando o somatório das quantidades de usuários internos de TIC das organizações.

A esfera de poder que apresentou maior representatividade na amostra foi o Executivo com 16 organizações (69,6%), seguido pelo Judiciário com 6 organizações (26,1%) e, por último, o Legislativo com 1 organização (4,3%), conforme apresentado na Figura 4.1, refletindo o mesmo resultado considerando o porte de usuários internos de TIC por esfera de poder.

Esse cenário apresentado das organizações entrevistadas por esfera de poder e porte das organizações

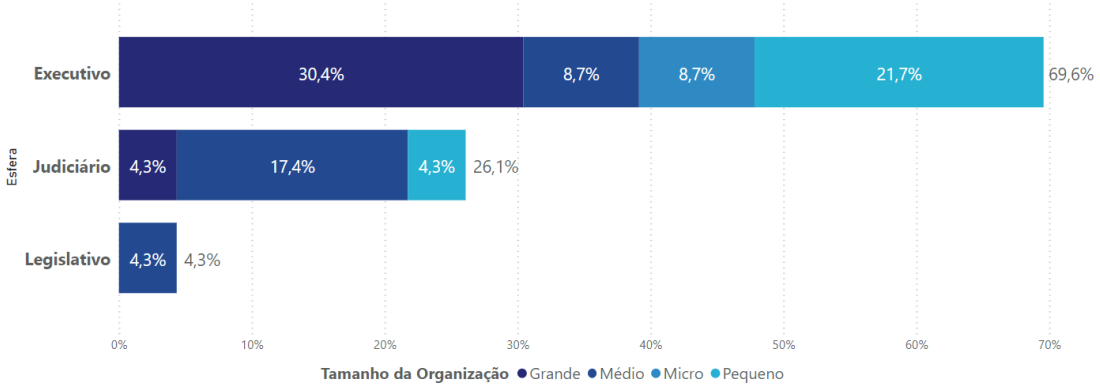

Figura 4.1: Disposição por esfera de poder e porte das organizações.

denota os aspectos quanto à utilização de computação em nuvem e suas peculiaridades no que tange ao comportamento relacionado a gestão de riscos praticado pelos gestores da administração pública federal brasileira.

Essa categoria de análise de conteúdo atingiu o objetivo de caracterizar a distribuição das organizações entrevistadas em todas as esferas de poder da administração pública federal com as coletas das amostras realizadas de maneira proporcional quanto à participação de cada uma no estado brasileiro, conforme a seguir:

(i): caracterização da esfera de atuação no poder da união do estado brasileiro: a atuação pode variar de uma organização para outra conforme esfera de poder (executivo, judiciário e legislativo).

(ii): caracterização do tamanho da organização: o tamanho pode variar de uma organização para outra conforme o porte da organização (micro, pequeno, médio e grande).

4.2 CATEGORIA 2: CARACTERÍSTICAS DOS GESTORES PÚBLICOS

A Categoria 2, Características dos gestores públicos, tem por objetivo identificar e caracterizar o gestor público seguindo o roteiro de entrevista mostrado pela Tabela 4.3. Os dados dessa categoria são mais gerais, de forma a definir o perfil dos gestores entrevistados.

Tabela 4.3: Roteiro sobre a caracterização da organização pública

Itens	Caracterização do Núcleo de Sentido
Atuação profissional em TIC dentro da organização	Perfil profissional do entrevistado
Atuação no processo de tomada de decisão na área de TIC	Perfil profissional quanto a atuação no processo de tomada de decisão
Tempo de experiência em TIC	Perfil profissional quanto ao tempo de experiência

A Tabela 4.4 apresenta as características profissionais dos gestores públicos quanto à atuação, incluindo área, processo decisório e experiência profissional em TIC conforme as seguintes opções: Governança (Avaliar, Dirigir e Monitorar) e Gestão (Planejando, Executando, Controlando e Agindo) para Atuação profissional em TIC dentro da organização. As opções: Não atua; Concepção; Planejamento; Aprovação; Execução e Fiscalização para Atuação no processo de tomada de decisão na área de TIC. E por último, as opções de 1 a 4 anos, 5 a 9 anos, 10 a 15 anos e mais de 15 anos para tempo de experiência profissional em TIC.

Tabela 4.4: Características profissionais

Entrevistado	**Características profissionais Atuação: Área, Processo decisório e Experiência**									
	Governança	Gestão	Governança e Gestão	Não atua	Concepção	Planejamento	Aprovação	Execução	Fiscalização	Experiência
EE01			✓		✓	✓	✓		✓	10 a 15 anos
EE02	✓				✓		✓		✓	10 a 15 anos
EE03			✓		✓	✓	✓			+ de 15 anos
EE04			✓		✓	✓	✓			+ de 15 anos
EE05		✓				✓		✓	✓	10 a 15 anos
EE06			✓		✓	✓	✓		✓	+ de 15 anos
EE07			✓		✓	✓	✓		✓	+ de 15 anos
EE08		✓			✓	✓	✓			10 a 15 anos
EE09			✓		✓	✓	✓		✓	5 a 9 anos
EE09.1			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE10			✓		✓	✓	✓		✓	10 a 15 anos
EE10.1			✓		✓	✓	✓	✓		+ de 15 anos
EE11			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE12		✓			✓			✓		+ de 15 anos
EE13			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE14			✓		✓	✓	✓			+ de 15 anos
EE15			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE16			✓		✓	✓		✓	✓	+ de 15 anos
EE17			✓			✓			✓	10 a 15 anos
EE18			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE18.1			✓		✓	✓	✓	✓	✓	+ de 15 anos
EE19		✓			✓	✓	✓	✓	✓	+ de 15 anos
EE20		✓			✓	✓		✓		10 a 15 anos
EE21			✓		✓	✓		✓	✓	+ de 15 anos
EE22			✓		✓	✓	✓	✓		5 a 9 anos
EE23	✓					✓	✓		✓	+ de 15 anos
										8% 5 a 9 anos
100%	8%	19%	73%	0%	88%	92%	77%	54%	77%	27% 10 a 15 anos
										65% + de 15 anos

Esta categoria atingiu o objetivo de caracterizar o perfil profissional dos gestores da administração pública federal entrevistados com as coletas das amostras realizadas de maneira proporcional quanto à

participação de cada uma no estado brasileiro, conforme a seguir:

(i): caracterização do perfil profissional dos entrevistados: a atuação pode variar de uma organização para outra conforme esfera de poder e a área de atuação (governança, gestão e governança e gestão).

(ii): caracterização da atuação no processo de tomada de decisão dos entrevistados: a quantidade de processos em que atua pode variar de um entrevistado para o outro de acordo com o tempo de experiência.

(iii): caracterização do tempo de experiência profissional dos entrevistados: o tempo pode variar de um entrevistado para outro conforme o tamanho da organização (Grande, Média, Pequena e Micro).

4.2.1 Subcategoria 2.1: Especificidades de atuação profissional

Observa-se na Figura 4.2, com dados extraídos da Tabela 4.4, que 7 entre 10 entrevistados possuem perfil de governança e gestão acumuladamente perante a sua organização, fato notado apenas nas esferas do executivo e judiciário.

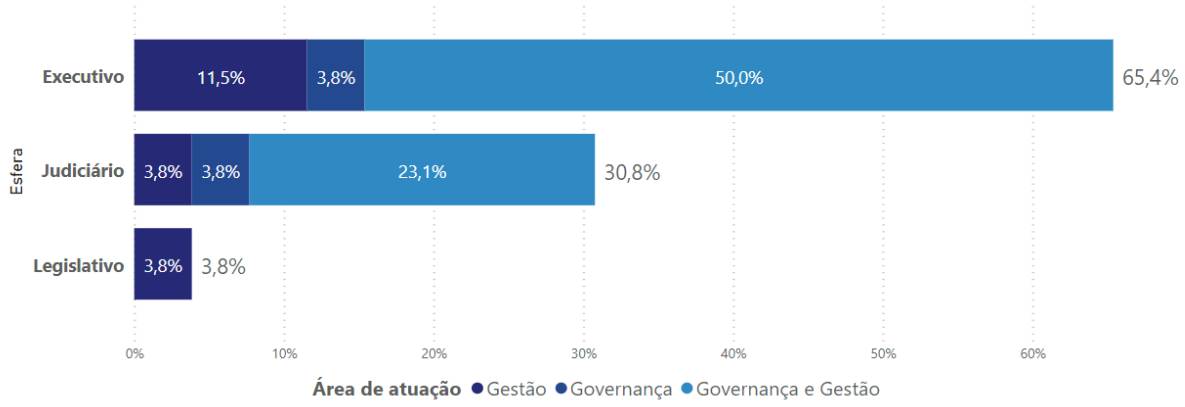

Figura 4.2: Área de atuação por esfera de poder.

Quanto as atuações dos gestores entrevistados nas etapas do processo de tomada de decisão em TIC (Fig. 4.3), as etapas de concepção, planejamento, aprovação, execução e fiscalização são realizados por 26,92% dos entrevistados e 42,31% desempenham quatro etapas do processos mencionados, de tal forma que 69,26% dos entrevistados executam pelo menos 4 etapas.

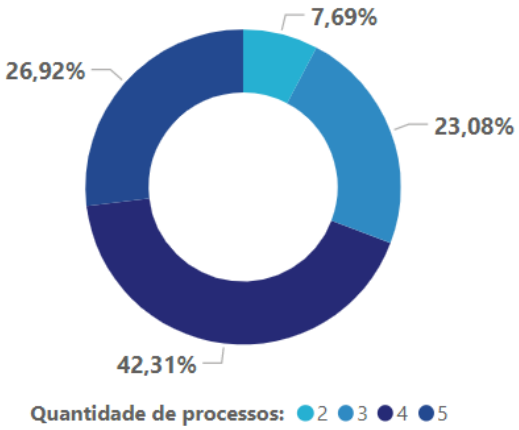

Figura 4.3: Quantidade de processos realizados paralelamente.

Do ponto de vista em relação ao tamanho da organização (Fig. 4.4), apenas as instituições com tamanho micro desempenham duas etapas, as demais realizam 3 ou mais etapas do processo de tomada de decisão.

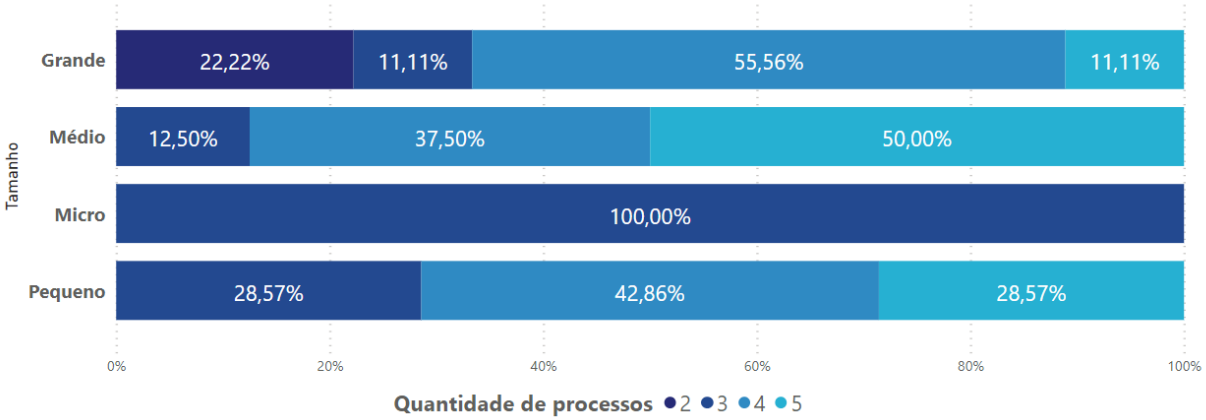

Figura 4.4: Quantidade de processos realizados paralelamente.

Essa subcategoria atingiu o objetivo de caracterizar as especificidades de atuação profissional dos gestores entrevistados, uma vez que as coletas das amostras possibilitaram identificar as áreas de atuação do gestores de cada esfera de poder, conforme a seguir:

(i): caracterização das especificidades de atuação profissional dos entrevistados: a área de atuação pode variar de uma esfera de poder para outra conforme a área (governança, gestão, e governança e gestão).

(ii): caracterização das especificidades de atuação profissional dos entrevistados: a amostra possui uma proporção maior de gestores que atuam nas duas áreas de governança e gestão, possibilitando uma qualidade das respostas apresentadas para o estudo.

(iii): caracterização das especificidades de atuação profissional dos entrevistados: a amostra

possui uma proporção maior de gestores que atuam em quatro ou mais processos de tomada de decisão, possibilitando uma qualidade das respostas apresentadas para o estudo.

4.2.2 Subcategoria 2.2: Experiência profissional

Um fator relevante observado na Tabela 4.4 foi o tempo de experiência profissional dos gestores entrevistados. Conforme mostrado na Figura 4.4, 65% possuem mais de 15 anos trabalhando com TIC, o que representa uma maturidade profissional dos gestores quanto à realização dos processos de governança e gestão.

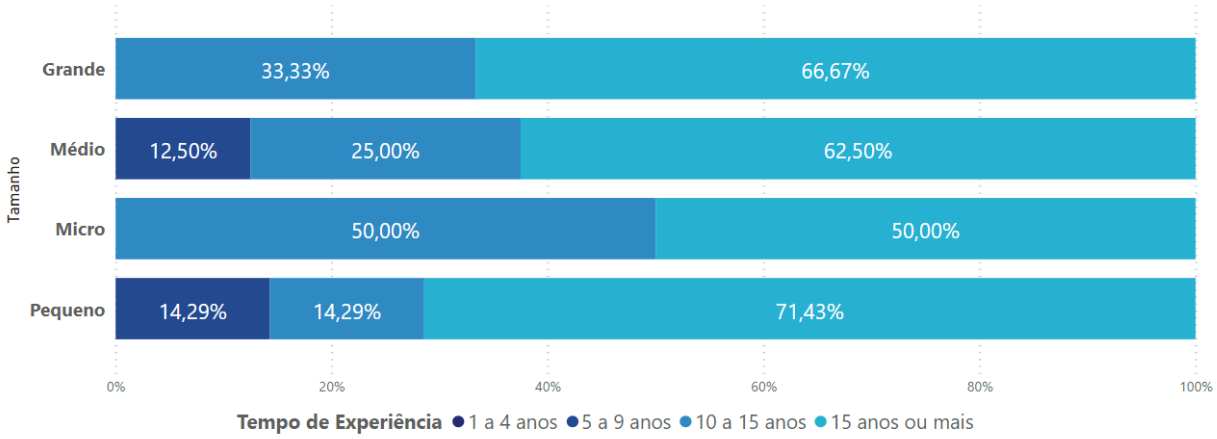

Figura 4.5: Tempo de experiência profissional.

Esta subcategoria atingiu o objetivo de caracterizar o tempo de experiência profissional dos gestores entrevistados, conforme a seguir:

(i): caracterização da experiência profissional dos entrevistados: o tempo pode variar de acordo com o tamanho da organização (micro, pequeno, médio e grande).

(ii): caracterização das especificidades de atuação profissional dos entrevistados: a amostra possui uma proporção maior de gestores que atuam nas duas áreas de governança e gestão, possibilitando uma qualidade das respostas apresentadas para o estudo.

(iii): caracterização das especificidades de atuação profissional dos entrevistados: a amostra possui uma proporção maior de gestores que atuam em quatro ou mais processos de tomada de decisão, possibilitando uma qualidade das respostas apresentadas para o estudo.

4.3 CATEGORIA 3: CARACTERÍSTICAS DE MATURIDADE NO USO DE COMPUTAÇÃO EM NUVEM

A Categoria 3, Características de maturidade no uso de computação em nuvem, tem por objetivo identificar e caracterizar a maturidade no uso de computação em nuvem seguindo o roteiro de entrevista mostrado

pela Tabela 4.5. Os dados dessa categoria têm o objetivo de identificar o uso de computação em nuvem nas organizações entrevistadas.

Tabela 4.5: Roteiro sobre a caracterização da maturidade no uso de computação em nuvem pela organização pública

Itens	Caracterização do Núcleo de Sentido
Atualmente, quais são os serviços ou soluções baseadas em computação em nuvem que são utilizados pela sua organização?	Modelos de serviços de computação em nuvem
Há quanto tempo os serviços em nuvem são utilizados pela organização?	Tempo de utilização de computação em nuvem
Percentualmente, quantos serviços internos já foram transferidos para nuvem e qual é a topologia adotada?	Experiência de computação em nuvem
Qual seria a percentual de usuários internos que utilizam serviços ou soluções em nuvem?	Adoção de serviços de computação em nuvem
Existe algum serviço em nuvem que a sua organização deixou de utilizar?	Adoção de serviços de computação em nuvem
A sua organização pretende contratar mais serviços em nuvem?	Adoção de serviços de computação em nuvem

Cumprindo-se os objetivos deste estudo, foram analisados os dados coletados, explorando os aspectos mais relevantes relacionados à maturidade quanto ao uso de nuvem nas óticas dos entrevistados, além de suas percepções quanto aos riscos inerentes ao uso da computação em nuvem pelo governo e as maiores tendências de práticas de gestão de riscos. Na Tabela 4.6 é apresentada uma consolidação das respostas de acordo com o tipo de modelo de serviço adotado, experiência no uso de computação em nuvem, percentual de serviços internos migrados para computação em nuvem, público interno da organização para a 1º coleta feita em abril de 2019.

Tabela 4.6: Características profissionais - 1º Coleta

Entrevistado 1º Coleta - 2019 [13]	**Características de maturidade no uso de computação em nuvem**								
	SaaS - Software como Serviço	PaaS - Plataforma como Serviço	IaaS - Infraestrututa como Serviço	Tempo de utilização (anos)	Serviços internos migrados	Usuários internos em nuvem	Topologia adotada	Deixou de utilizar nuvem	Pretende contratar mais nuvem
EE01	✓			1	-	Parcial	Híbrida	Não	Sim
EE02	✓		✓	2	-	Integral	Híbrida	Sim	Sim
EE03	✓	✓	✓	5	-	Integral	Híbrida	Não	Sim
EE04	✓			0,58	-	Parcial	Híbrida	Sim	Sim
EE05	✓	✓	✓	3	-	Parcial	Híbrida	Sim	Sim
EE06	✓	✓	✓	1,5	-	Integral	Híbrida	Não	Sim
EE07	✓			3	-	Integral	Híbrida	Não	Sim
EE08				0	-	Nenhum	-	Sim	Não
EE09	✓			3	-	Parcial	Híbrida	Não	Sim
EE10	✓			1,5	-	Integral	Híbrida	Não	Sim
10	90%	30%	40%	2		50% Integral 40% Parcial 10% Nenhum	100% Híbrida	60% Não 40% Sim	90% Sim 10% Não

Na Tabela 4.7 é apresentada uma consolidação das respostas de acordo com o tipo de modelo de serviço adotado, experiência no uso de computação em nuvem, percentual de serviços internos migrados para computação em nuvem, público interno da organização para a 2º coleta realizada em maio, junho e julho de 2022.

Tabela 4.7: Características profissionais - 2º Coleta

Entrevistado 2º Coleta 2022	**Características de maturidade no uso de computação em nuvem**								
	SaaS - Software como Serviço	PaaS - Plataforma como Serviço	IaaS - Infraestrutura como Serviço	Tempo de utilização (anos)	Serviços internos migrados	Usuários internos em nuvem	Topologia adotada	Deixou de utilizar nuvem	Pretende contratar mais nuvem
EE09.1	✓			6	25%	Integral	Híbrida	Sim	Sim
EE10.1	✓	✓		4,5	25%	Integral	Híbrida	Não	Sim
EE11	✓			2	10%	Integral	Híbrida	Não	Sim
EE12	✓		✓	5	5%	Parcial	Multi-cloud	Não	Sim
EE13	✓			3	30%	Integral	Híbrida	Não	Sim
EE14	✓	✓	✓	2	40%	Integral	Multi-cloud	Não	Sim
EE15	✓	✓		3	20%	Integral	Híbrida	Sim	Sim
EE16	✓	✓	✓	9	40%	Integral	Multi-cloud	Sim	Sim
EE17	✓	✓	✓	5	70%	Integral	Híbrida	Não	Sim
EE18 e EE18.1	✓	✓	✓	4	10%	Integral	Multi-cloud	Não	Sim
EE19	✓	✓		4	15%	Integral	Pública	Não	Sim
EE20	✓	✓		5	15%	Integral	Híbrida	Não	Sim
EE21	✓	✓		1,5	10%	Integral	Híbrida	Não	Sim
EE22	✓		✓	2,5	40%	Integral	Multi-cloud	Não	Sim
EE23	✓	✓		2	50%	Integral	Híbrida	Não	Sim
16	100%	73%	33%	3,9	27%	94% Integral 6% Parcial	60% Híbrida 33% Multi-cloud 7% Pública	18% Sim 82% Não	100% Sim

Ao analisar as óticas dos entrevistados quanto à maturidade no uso de computação em nuvem em relação as duas coletas, é possível apontar que houve um aumento de 90% para 100% das instituições que passaram a utilizar essa tecnologia e a média de tempo de utilização subiu de 2 para 3,9 anos. Complementando a questão, os entrevistados relataram que as instituições ainda enfrentam dificuldades quanto à carência de mão de obra especializada para exercer as atividades de gestão dos ambientes de computação em nuvem, sendo um dos fatores característicos da fase de transformação digital em que o governo se encontra.

De acordo com o critério ”Deixou de utilizar nuvem”, os relatos positivos mencionados durante a entrevista não se tratam de fatores relacionados aos riscos de segurança, mas sim do uso da tecnologia, em sua maioria pertencente ao modelo *SaaS*, onde o serviço testado foi descartado pela organização, sendo que ora não atendia a demanda de negócio, ora era muito além tecnicamente do que se estava buscando. A diferença observada entre as duas Coletas, onde na 1ª existiam 40% de respostas ”Sim” e na 2ª Coleta, uma redução para 18%, demonstra que as organizações estão maduras quanto a tecnologia de computação em nuvem.

Os entrevistados relataram que estes estão hospedando diversos sistemas e utilizando ostensivamente as funcionalidades oferecidas pela nuvem na modalidade de software como um serviço (Software as a Service - SaaS), de forma a tornar a gestão de TI mais eficiente quando se trata de custos, performance e

segurança (Fig. 4.6). Também foi apontado que os usuários dessas instituições estão familiarizados com as plataformas, fazendo uso delas em seu dia a dia, como nos casos em que há a possibilidade do uso dessas plataformas para fins de teletrabalho considerando a pandemia de COVID-19.

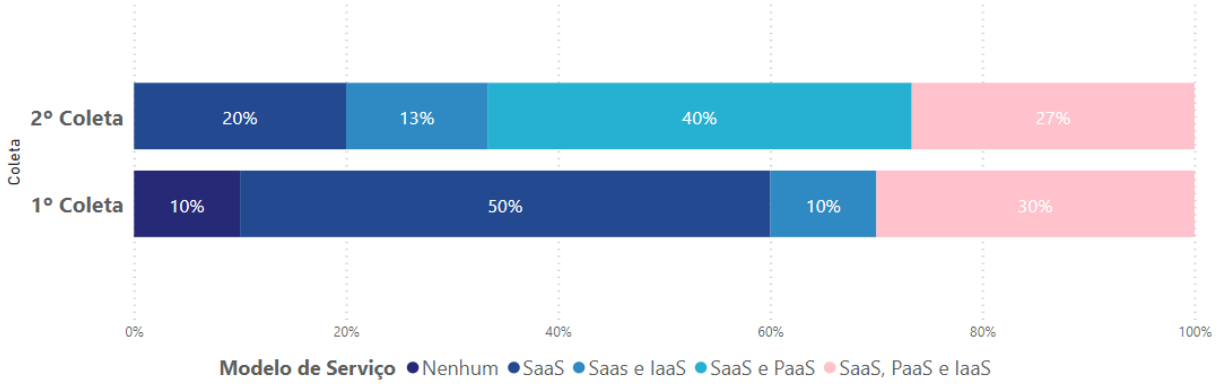

Figura 4.6: Modelos de Serviços em Computação em Nuvem.

Em complemento, verifica-se que os 60% dos órgãos públicos com adoção mais recente, inferior a média em anos, não se encontram mais executando testes e planejamento, mas implantando de forma integral a adoção dessas plataformas pelos seus usuários internos, cenário esse muito diferente da 1º coleta, onde as organizações, majoritariamente, realizavam uma abordagem de lançamento limitado a certos departamentos como forma de piloto.

Tratando-se de migração de serviços internos para computação em nuvem, a média apontada dentre os entrevistados foi de 27% de efetiva migração, algo também muito diferente da 1º coleta, onde a hospedagem de sistemas na nuvem, era predominante um dos receio quanto ao fato de suas equipes ainda não possuírem conhecimentos técnicos avançados e ainda se encontrarem testando tais serviços.

Considerando os depoimentos dos entrevistados, pode-se concluir que estes acreditam nos benefícios, na segurança e no valor agregado do uso de nuvem. Nos resultados da 1ª coleta, entre os maiores desafios à implementação estava a mudança da cultura das organizações para adotar todas as soluções em nuvem porque, a princípio, poucos possuíam conhecimentos técnicos aprofundados. Todavia, agora na 2º coleta, observa-se que o desafio da cultura das organizações foi superado pela necessidade de computação onipresente provocado pela pandemia, mas a falta de conhecimento aprofundado, de suas equipes, na tecnologia ainda é, para a maioria, um obstaculo a ser superado.

Esta categoria atingiu o objetivo de caracterizar a maturidade no uso de computação em nuvem das organizações entrevistadas, conforme a seguir:

> (i): caracterização maturidade no uso de computação em nuvem: o tempo de uso pode variar de acordo com o tamanho da organização (micro, pequeno, médio e grande).
>
> (ii):caracterização maturidade no uso de computação em nuvem: a amostra possui uma proporção maior de organizações com uso de computação em nuvem, possibilitando uma qualidade das respostas apresentadas para o estudo.

(iii): a adoção de computação em nuvem evoluiu tanto no aspecto relacionado ao modelo de serviço contratado quanto a utilização pelos usuários internos de TIC.

(iv): a topologia implantada foi identificada conforme as coletas realizadas observando uma mudança de paradigma quanto a esse aspecto.

4.4 CATEGORIA 4: GESTÃO DE RISCOS EM COMPUTAÇÃO EM NUVEM

No caso da Categoria 4, Gestão de riscos em computação em nuvem, serão apresentados os resultados da pesquisa em subcategorias com amostra dos resultados sobre o uso da computação em nuvem nos órgãos públicos, na ótica dos entrevistados e os principais pontos relatados pelos entrevistados, no que tange às recomendações para enfrentamento de riscos em nuvem, de acordo com os pontos elencados pelo NIST, ENISA e a CSA.

Após serem entrevistados quanto ao uso da nuvem, a abordagem aos entrevistados contemplou os pontos elencados na Tabela 3.5, com relação à gestão de riscos em nuvem, levando em conta os domínios citados, objeto de estudo extraído conforme apresentado no Referencial Teórico deste trabalho.

Nessa etapa da entrevista, o objetivo foi que os entrevistados elencassem os riscos a serem endereçados pelas organizações e avaliar quais são os planos delas para mitigar os riscos relacionados. Buscou-se categorizar, na ótica de cada entrevistado e com base no seu relato, a situação atual do planejamento estratégico de cada organização, observando se estão sendo executadas ações à gestão dos referidos riscos ou não, como também se existiram planos à implementação de práticas ou políticas a respeito dos citados riscos.

Essa categoria com as suas subcategorias tem por objetivo identificar e caracterizar a gestão de riscos no uso de computação em nuvem seguindo o roteiro de entrevista já estabelecido. Os dados foram tratados de acordo com os nove domínios de recomendação para gestão de riscos em computação em nuvem conforme as subcategorias a seguir.

4.4.1 Subcategoria 4.1: Legislação e Regulamentações

Esta subcategoria, Legislação e Regulamentações, tem como objetivo caracterizar a evolução dos aspectos legais e regulamentares aplicados aos serviços de computação em nuvem para as organizações entrevistadas seguindo o roteiro de entrevista mostrado na Tabela 4.8.

Tabela 4.8: Roteiro sobre o domínio Legislação e Regulamentações

Itens	Caracterização do Núcleo de Sentido
Em quais aspectos você acredita que a legislação brasileira vigente pode prejudicar ou promover o avanço tecnológico do Governo quanto ao uso de serviços em nuvem?	Aspectos legais e regulamentares aplicados aos serviços de computação em nuvem
Quais são os riscos (negativos ou positivos) implicados à sua organização pela legislação brasileira quanto ao uso de serviços em nuvem? Quais são as medidas ou controles que a sua organização tem tomado para se adequar à legislação?	Aspectos legais e regulamentares aplicados aos serviços de computação em nuvem

No que tange ao levantamento dos aspectos de adoção de computação em nuvem que a legislação brasileira proporciona ao avanço tecnológico do Governo, foram apresentados relatos de 16 participantes. A partir do processo de análise de conteúdo foi possível identificar que a legislação mais promove do que prejudica a adoção de computação em nuvem, conforme nuvem de palavras ilustrada na Figura 4.7.

Figura 4.7: Nuvem de palavras Aspectos de legislação e regulamentação em 2022.

Quanto à legislação e regulamentações, comparando-se a 1ª e 2ª Coletas, observou-se que houve uma redução de 60% para 40% das instituições que demonstraram maior relevância quando se trata da possibilidade de não estarem em conformidade com as normas que limitam o tráfego de informações sigilosas. De maneira geral, observou-se também que as responsabilidades quanto ao tráfego de informações sigilosas não estão bem definidas dentro da organização. O gerador do dado é que deve possuir a atribuição e não a área de TIC, e mesmo assim, os usuários que produzem informação possuem um maior trabalho para

categorizar, decidir e classificar o que pode ser trafegado no ambiente em nuvem, correndo-se o risco de serem armazenadas informações em lugares considerados indevidos por sua classificação.

Dos atuais 40% dos entrevistados, destacou-se, inclusive, na 1ª Coleta e 2ª Coleta, que a regulamentação atual implica consequências negativas quanto à praticidade do uso da nuvem, afirmando que as legislações impostas podem prejudicar o avanço tecnológico do governo no caso dos usuários não se adequarem a tais exigências, limitando certas formas de utilização da nuvem que podem inviabilizar o seu uso pelas organizações.

Já os atuais 60%, onde houve um aumento comparando a 1ª e 2ª coleta de 40% para 60% dos entrevistados, se posicionaram de maneira oposta ao relato do parágrafo anterior, afirmando que a legislação estabelece diretrizes mais seguras quando se trata da utilização da nuvem pelo governo, sendo benéficas, pois ajudam a evitar vazamentos de dados.

Apesar dos pontos adversos, os entrevistados concordaram que, após a divulgação da IN nº 05/2021 pelo Gabinete de Segurança Institucional [30] e pela ENTIC-JUD [31] que fomenta o uso de nuvem por todas as instituições da Administração Pública, os normativos estão evoluindo gradativamente para que o governo tenha mais abertura para se desenvolver tecnologicamente no uso de computação em nuvem. Os entrevistados atribuíram essa evolução à pandemia de COVID-19, onde muitas organizações se viram obrigadas a migrar para nuvem devido à demanda urgente de teletrabalho no período de *lockdown* aplicado pelos governos estaduais do país.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou a questão sem resposta. Nesse sentido, após a análise de conteúdo, foi possível identificar a menção dos riscos e controles elencados na Tabela 4.9.

Tabela 4.9: Riscos e controles para o domínio de Legislação e Regulamentações relatados

Riscos	**Controles**	**Total de Relatos 2019 [13]**	**Total de Relatos 2022**
Positivo: Fomento no uso de computação em nuvem	N/A	2	0
Positivo: Modernização dos instrumentos legais para adoção de computação em nuvem	N/A	0	2
Positivo: Punições nulas quando da ocorrência de vazamento de dados	N/A	0	1
Negativo: Mudança de Jurisdição dos dados	Conformidade Legal	3	0
	Utilização de multi-cloud	0	2
	Cláusulas contratuais	0	2
	Bloqueios de acesso a nuvens sem contratos	0	1
Negativo: Falta de classificação dos dados	Aplicação de *frameworks*	0	1
	Compartilhamento de responsabilidade com os gestores dos dados	2	2
Negativo: Vazamento de dados	Cláusulas contratuais	2	4
Sem resposta	-	1	0
Totais		**10**	**15**

Dados os riscos mencionados, pode-se constatar que os controles que tiveram mais relatos estão diretamente relacionados ao domínio de legislação e regulamentações no uso de computação em nuvem, uma vez que as dificuldades experimentadas com a sua adoção no período da pandemia foram muito desafiadoras para os gestores públicos.

Essa subcategoria atingiu o objetivo de caracterizar os aspectos legais e regulamentares, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos legais e regulamentares no uso de computação em nuvem.

(ii): caracterização dos riscos legais e regulamentares no uso de computação em nuvem.

(iii): caracterização de controles associados aos riscos legais e regulamentares.

(iv): identificação da evolução ao enfrentamento dos riscos legais e regulamentares: considerando as duas coletas feitas.

4.4.2 Subcategoria 4.2: Governança de TIC

Esta subcategoria, Governança de TIC, tem como objetivo caracterizar a evolução dos aspectos de Governança de TIC aplicados aos serviços de computação em nuvem para as organizações entrevistadas, seguindo o roteiro de entrevista mostrado na Tabela 4.10.

Tabela 4.10: Roteiro sobre o domínio de Governança de TIC

Itens	Caracterização do Núcleo de Sentido
A sua organização estabeleceu uma política ou norma para decidir em quais casos é apropriado o uso de serviços em nuvem? Quais são as medidas ou controles aplicados de governança de TIC sobre o uso de serviços em nuvem?	Aspectos de governança em TIC aplicados a computação em nuvem

Tratando-se das maiores tendências de governança entre os entrevistados, destacam-se as questões relativas à Portaria GSI N.º 9/2018 [46], bem como a Instrução Normativa GSI N.º 05/2021 [30], que orienta as instituições governamentais a apenas trafegarem informações classificadas como não sigilosas por meio da nuvem, o que tem sido discutido e incentivado internamente por todas as organizações entrevistadas. Porém, no período da 1ª Coleta, não existiam controles implementados nas instituições para identificar se essa orientação vinha sendo executada propriamente pelos usuários. Na 2ª Coleta, houve uma evolução quanto aos controles implementados conforme a Tabela 4.10, mas 80% dos entrevistados comentaram que os controles ainda são fracos quanto à classificação de dados, conforme achados constantes na subcategoria de Privacidade e Proteção de Dados.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.11.

Tabela 4.11: Normas, riscos e controles para o domínio de Governança de TIC relatados

Normas	Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Não possui norma interna	Perda de governança Vendor Lock-In	Análise de Riscos	5	1
		Adoção de Multi-cloud	0	1
		Não utilizar ferramentas proprietárias	0	1
		Framework "CIS Control"	0	1
		Nenhum	3	2
Não possui norma interna, mas utiliza normas de órgãos superiores	Perda de governança	Análise de Riscos	1	2
		Comitê interno definir o que vai pra nuvem	0	1
		Dados sem classificação não vai pra nuvem	0	1
		Nenhum	0	1
Possui norma interna	Perda de governança	Análise de Riscos	0	1
		Dados sem classificação não vai pra nuvem	0	2
		Uso de tecnologia de segurança (CASB)	0	1
Sem resposta	-	-	1	0
Totais			**10**	**15**

Na 1ª Coleta, todos os entrevistados informaram que os planejamentos quanto à governança de TIC específica para o uso de nuvem estavam em andamento e em fase inicial, ou seja, nenhum possuía normativo a respeito. Já na 2ª Coleta, o cenário mudou apresentando uma melhora, onde quatro organizações relataram possuir normativo interno para uso de computação em nuvem.

Ressaltou-se a preocupação quanto a necessidade de políticas que governem o uso dos recursos em nuvem de forma a controlar os gastos, para que se mantenham no orçamento planejado pela instituição no momento de sua contratação. Sem políticas efetivas, podem ocorrer situações em que o uso indevido dos recursos implique em gastos não previstos, os quais, se estiverem fora do orçamento, podem gerar um impacto no funcionamento de sistemas críticos da organização.

Com base nos dados obtidos da 1ª e 2ª Coleta, identificou-se ainda que houve uma melhora com a diminuição de 30% das instituições que ainda não iniciaram o seu planejamento para estruturar uma governança específica de nuvem e não haviam estabelecido nenhum controle ainda. Na 2ª Coleta, 54% das instituições ainda estavam iniciando processos para estruturar comitês de arquitetura e segurança, contrastando com os 70% observados na 1ª Coleta. São esses comitês de arquitetura e segurança que deverão elaborar as especificações a serem seguidas pelas entidades, incluindo as definições de quais sistemas e informações deverão ser trafegadas em nuvem, com base em análises dos riscos elencados pelo Acórdão nº 1.739/2015 do TCU[17]. 26% das instituições da 2ª Coleta já criaram os seus comitês em conjunto com a publicação de seus normativos para computação em nuvem.

Essa subcategoria atingiu o objetivo de caracterizar os aspectos de governança, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de governança de TIC no uso de computação em nuvem.

(ii): caracterização dos riscos de governança de TIC no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de governança de TIC: considerando as duas coletas feitas.

4.4.3 Subcategoria 4.3: Privacidade e Proteção de Dados

Esta subcategoria, Privacidade e Proteção de Dados, tem como objetivo caracterizar a evolução dos aspectos de privacidade e proteção de dados aplicados aos serviços de computação em nuvem para as organizações entrevistadas seguindo o roteiro de entrevista mostrado na Tabela 4.12.

Tabela 4.12: Roteiro sobre o domínio de Privacidade e Proteção de Dados

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos relacionados aos dados institucionais armazenados (sensíveis e não sensíveis) associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de privacidade e proteção de dados em computação em nuvem

Tratando-se das questões relativas à privacidade e a proteção de dados, o risco de vazamento de informações sensíveis foi o ponto de maior relevância, citado por todos os entrevistados enquanto evidenciavam as regras estabelecidas pela LGPD [14], afirmando que, por se tratarem de organizações governamentais, um vazamento de informações poderia acarretar em significativos problemas econômicos e políticos com impacto de nível nacional. Além do referido vazamento, também foram consideradas possíveis perdas de dados e o tratamento de tais dados por terceiros de maneira não autorizada.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.13.

Tabela 4.13: Riscos e controles para o domínio de Privacidade e Proteção de Dados relatados

Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Vazamento de Dados e Acesso não Autorizado	Análise de Riscos	2	2
	Classificação de dados	0	3
	Conscientização de usuário	0	1
	Dados não sensíveis em nuvem	0	2
	Uso de tecnologia de segurança	0	2
	Nenhum	6	1
Shadow IT	Bloqueios de acesso a nuvens sem contratos	0	1
Configurações erradas ou inadequadas	Capacitação de equipe técnica	1	3
Sem resposta	-	1	0
Totais		**10**	**15**

Considerando a ótica dos entrevistados desta pesquisa, na 1ª Coleta todas as instituições ainda estavam desenvolvendo processos e práticas para garantir a privacidade e proteção dos dados conforme a legislação. Entre as táticas citadas, 20% dos entrevistados afirmaram que as organizações estiveram buscando apoio jurídico-legal para a análise de risco de forma a se manter em conformidade por meio de serviços de consultoria para verificar a maturidade delas quanto à aderência aos requisitos das leis que tangem à proteção de dados. Na 2ª Coleta, as organizações partiram pra ações efetivas quanto à implementação de controles, observando-se que 93% das organizações apresentaram controles para os riscos relatados.

Em meio às demais estratégias das organizações públicas citadas pelos entrevistados estão: evitar o tráfego de informações não públicas em ambientes de nuvem; executar o tratamento de metadados, buscando evitar o vazamento de informação pessoal identificável; implementação de processos de classificação das informações, definindo permissões para serem tratadas em ambientes de nuvem; iniciativas de comitês para a análise de riscos, de forma a coordenar futuras contratações dos serviços de nuvem e bloqueio de acesso a serviços de armazenamento em nuvem que a organização não possui contrato de forma a mitigar os riscos conhecidos como *Shadow IT* que refere-se a dispositivos, software e serviços de TI fora da propriedade ou do controle da área de TIC das organizações.

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto a privacidade e proteção de dados, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de privacidade e proteção de dados no uso de computação em nuvem.

(ii): caracterização dos riscos de privacidade e proteção de dados no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de privacidade e proteção de dados: considerando as duas coletas feitas.

4.4.4 Subcategoria 4.4: Gestão de Identidade e Acessos

Esta subcategoria, Gestão de Identidade e Acessos, tem como objetivo caracterizar a evolução dos aspectos de gestão de identidade e acessos aplicados aos serviços de computação em nuvem para as organizações entrevistadas, seguindo o roteiro de entrevista mostrado na Tabela 4.14.

Tabela 4.14: Roteiro sobre o domínio de Gestão de Identidade e Acessos

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos de gestão e identidade e acessos associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de gestão de identidade e acessos em computação em nuvem

Ao serem abordados na 1ª Coleta a respeito dos riscos inerentes à gestão de identidade e acessos, os entrevistados elencaram preocupações quanto à baixa maturidade das políticas de gestão nas organizações em que atuam. Como parte das estratégias para a remediação dos riscos relacionados ao tema, todos os entrevistados afirmaram que as organizações em que atuavam estavam planejando ou estiveram em processo de implementação de soluções como: múltiplo fator de autenticação, segmentação de privilégios, acesso condicional, biometria, dupla validação de alterações nas configurações do ambiente e liberação momentânea de privilégios.

Na 2ª Coleta, os entrevistados consideram que o processo de gestão de identidade e acessos está em desenvolvimento, porém os controles relacionados estão implantados principalmente com a aquisição de soluções tecnológicas como: Solução de Gestão de Acesso (PAM) como Cofre de Senhas; habilitação de recursos de múltiplo fator de autenticação (MFA) fornecidos pelos serviços prestados na modalidade de Software como Serviço - SaaS, a exemplo dos produtos da Microsoft da família Office 365 e tecnologia de Análises Comportamentais de Entidade e Usuário (UEBA).

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que quatro deixaram essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.15

Tabela 4.15: Riscos e controles para o domínio de Gestão de Identidade e Acessos relatados

Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Comprometimento de credenciais	Análise de Riscos	3	1
	Implantação de *framework*	0	1
	Políticas de Confiança Zero (*Zero Trust*)	0	1
	Uso de tecnologias de segurança (PAM e UEBA)	0	4
	Habilitação de funcionalidades SaaS (MFA)	2	3
Sequestro de contas	Processo de Gestão de Identidade e Acessos	1	1
	Uso de tecnologia de segurança (PAM)	0	1
	Habilitação de funcionalidades SaaS (MFA)	1	1
	Conscientização de Usuários	1	1
Sem resposta	-	2	2
Totais		**10**	**15**

Na 1ª Coleta, foi apontado por 30% dos entrevistados que ainda não haviam sido implementadas soluções mais robustas de gestão de acessos nas organizações em que atuavam. Porém, observou-se que essas

organizações estavam executando um plano de controle de acessos e identidade, o qual estaria previsto para ser tratado em futuras contratações, considerando os riscos inerentes ao tema. Tal achado, na 2ª Coleta, apresentou uma diminuição, bem como uma melhora na aplicação de controles efetivos voltados para gestão de identidade e acessos, onde o uso de tecnologias de segurança como soluções de MFA, PAM e UEBA foi implantado por 60% dos entrevistados.

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto a gestão de identidade de acessos, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de gestão de identidade e acessos no uso de computação em nuvem.

(ii): caracterização dos riscos de gestão de identidade e acessos no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de gestão de identidade e acessos: considerando as duas coletas feitas.

4.4.5 Subcategoria 4.5: Isolamento de Cliente em Nuvem

Esta subcategoria, Isolamento de Cliente em Nuvem, tem como objetivo caracterizar a evolução dos aspectos de isolamento de clientes em nuvem aplicados aos serviços de computação em nuvem para as organizações entrevistadas, seguindo o roteiro de entrevista mostrado na Tabela 4.16.

Tabela 4.16: Roteiro sobre o domínio de Isolamento de Clientes em Nuvem

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos de isolamento de clientes em nuvem associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de isolamento de clientes de computação em nuvem

Quando a abordagem se tratou dos riscos relacionados ao isolamento dos ambientes hospedados em infraestrutura de nuvem pública, os entrevistados da 1ª Coleta elencaram riscos relacionados ao isolamento lógico dos ambientes virtuais e o possível acesso por outros clientes do provedor que estejam compartilhando o uso do mesmo hardware, como também ao acesso não permitido de funcionários do provedor aos ambientes das instituições.

Apesar de tais afirmações, metade dos entrevistados da 1ª Coleta afirmou não possuir preocupações quanto ao isolamento de ambientes das organizações em que atuam, acreditando que os provedores de

nuvem oferecem maior garantia de isolamento dos recursos por conta da natureza de sua estrutura compartilhada, envolvendo tecnologias e procedimentos que talvez não sejam implementados de maneira igualmente eficiente em servidores das referidas organizações.

Durante a 2ª Coleta, os entrevistados já apresentavam preocupações quanto aos riscos relacionados a esse domínio, uma vez que o incidente ocorrido em dezembro de 2021, com o aplicativo ConectaSUS do Ministério da Saúde [36], afetou os serviços de 4 dentre os 15 entrevistados.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que quatro deixaram essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.17.

Tabela 4.17: Riscos e controles para o domínio de Isolamento de Clientes em Nuvem relatados

Riscos	**Controles**	**Total de Relatos 2019 [13]**	**Total de Relatos 2022**
Acessos não autorizados	Responsabilidade do provedor	2	0
	Segmentação de ambiente	4	1
	Cláusulas Contratuais	2	1
	Monitoramento	0	1
	Supervisão do provedor	0	1
	Nenhum	1	0
Ataques laterais	Uso de tecnologia de segurança (Micro-segmentação)	0	2
	Arquitetura de Segurança com Criptografia	0	1
	Capacitação de equipe	0	1
	Contratação sem intermediário de nuvem (*broken*)	0	1
	Cláusulas Contratuais	0	1
	Nenhum	0	1
Indisponibilidade	Processo de Gestão de Continuidade	0	1
Sem resposta	Sem resposta	1	3
Totais		**10**	**15**

Quanto às estratégias para mitigar os riscos, ambos os grupos de entrevistados afirmaram que as organizações em que atuavam praticavam determinadas medidas para evitá-los, incluindo: a segmentação de acessos para funcionalidades de administração dos recursos; o isolamento de ambientes de desenvolvimento, homologação e produção; e a construção de exigências em cláusulas contratuais para garantir que esse fator de segurança seja gerenciado pelo provedor.

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto ao isolamento de clientes em nuvem, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de isolamento de clientes em nuvem no uso de computação em nuvem.

(ii): caracterização dos riscos de isolamento de clientes em nuvem no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de isolamento de clientes em nuvem: considerando as duas coletas feitas.

4.4.6 Subcategoria 4.6: Segurança das Operações e Comunicações

Essa subcategoria, Segurança das Operações e Comunicações, tem como objetivo caracterizar a evolução dos aspectos de segurança das operações e comunicações aplicados aos serviços de computação em nuvem para as organizações entrevistadas, seguindo o roteiro de entrevista mostrado na Tabela 4.18.

Tabela 4.18: Roteiro sobre o domínio de Segurança das Operações e Comunicações

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos de segurança das operações e comunicações associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de segurança das operações e comunicações em computação em nuvem

A respeito dos riscos relacionados à segurança, os participantes da pesquisa na 1ª Coleta apontaram maior relevância quanto à possibilidade de vazamento de informações decorrente de acessos por invasores. Desses, um percentual de 40% reconhecem que, além dos controles e certificações de segurança fornecidos pelo provedor, também precisa ser considerada a segurança dos sistemas gerenciados pela entidade pública para garantir que eles não tenham vulnerabilidades.

Na 2ª Coleta, os entrevistados apontaram os riscos de comprometimento da plataforma de nuvem como sendo o que tem maior importância nesse domínio, em razão do incidente que causou a indisponibilidade da Plataforma de Nuvem do contratado integrador de dois ou mais provedores de serviço de computação em nuvem [36]. Para esses entrevistados, os controles necessitam de maiores estudos quanto às medidas mitigadoras aplicáveis devido à complexidade tecnológica envolvida.

Houve uma preocupação levantada na 1ª Coleta quanto à situações em que os códigos dos sistemas elaborados pela instituição, mesmo quando hospedados em nuvem, não sejam suficientemente seguros, considerando também que o uso de software de fontes públicas (imagens de sistemas operacionais, trilhas de desenvolvimento, entre outras aplicações) pode conter *malware* e necessitam de uma maior atenção e controle.

Os entrevistados da 2ª Coleta abordaram, nos riscos envolvendo a exploração de vulnerabilidades em nuvem, a necessidade de um processo de análise de vulnerabilidade aliado ao uso de tecnologias como soluções de gestão de vulnerabilidade baseado no risco ou a contratação de serviços de SOC com equipe denominada *Blue Team*.

Os entrevistados na 1ª e 2ª Coletas afirmaram que ainda estão desenvolvendo táticas para reforçar a segurança de seus ambientes em nuvem, visto que na 1ª Coleta estavam em fase de testes ou no processo

de aquisição e, na 2ª Coleta, a fase já era de operação e produção dos serviços em nuvem, porém, com a modernização dos ataques cibernéticos, as ações táticas mitigadoras para reforçar o ambiente precisam estar em constante evolução.

No geral, os entrevistados evidenciaram que atualmente estão empreendendo ações com o objetivo de solicitar medidas de contorno aos fornecedores no momento da contratação, bem como construindo exigências específicas por meio de cláusulas contratuais e não se limitando a ações junto aos provedores, mas também adotando uma cautela maior na migração de serviços internos críticos para computação em nuvem do lado da organização.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que três deixaram essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.19.

Tabela 4.19: Riscos e controles para o domínio de Segurança das Operações e Comunicações relatados

Riscos	**Controles**	**Total de Relatos 2019 [13]**	**Total de Relatos 2022**
Configurações erradas ou inadequadas	Adoção de topologia Híbrida ou Multi-cloud	0	1
	Capacitação de equipe	0	2
Comprometimento da Plataforma de Nuvem	Uso de tecnologia de gestão de nuvem	0	1
	Uso exclusivo de nuvem para acesso interno	0	1
	Em estudo	0	3
Exploração de Vulnerabilidades em Nuvem	Análise de vulnerabilidade	0	2
	Contratação de serviço SOC e *Blue Team*	0	1
	Uso de funcionalidade de segurança em nuvem	0	1
	Cláusulas contratuais	1	0
	Contratar somente modelo de serviços SaaS	1	0
	Limitar o uso de repositórios públicos	1	0
	Nenhum	1	0
Transferir o risco para o provedor	Conscientização da alta gestão	0	1
Vazamento de dados	Nenhum	4	0
Nenhum	Nenhum	1	0
Sem resposta	-	1	2
Totais		**10**	**15**

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto à segurança das operações e comunicações, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de segurança das operações e comunicações no uso de computação em nuvem.

(ii): caracterização dos riscos de segurança das operações e comunicações no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de segurança das operações e comunicações: considerando as duas coletas feitas.

4.4.7 Subcategoria 4.7: Resposta a Incidentes

Esta subcategoria, Resposta a Incidentes, tem como objetivo caracterizar a evolução dos aspectos de resposta a incidentes aplicados aos serviços de computação em nuvem para as organizações entrevistadas seguindo o roteiro de entrevista mostrado na Tabela 4.20.

Tabela 4.20: Roteiro sobre o domínio de Resposta a Incidentes

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos a resposta a incidentes associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de resposta a incidentes de computação em nuvem

No âmbito dos temas relacionados com a resposta a incidentes, os entrevistados pontuaram riscos que causassem a ineficiência de tais processos, levando em consideração a falta de maturidade quanto à estruturação desse tipo de resposta tanto do lado da organização como do lado dos provedores de serviços em nuvem. Situações nas quais não existe um histórico ou indicadores de eficiência de casos em que incidentes foram tratados, implicam na impossibilidade de se identificar problemas crônicos.

A respeito das estratégias das organizações públicas, os entrevistados da 1ª Coleta, em todos os casos, comunicaram que não existia planos completamente estruturados quando se tratava de tecnologias em nuvem. Porém, conforme evidenciado por metade dos entrevistados, estavam sendo estabelecidas equipes dedicadas nas referidas organizações para dar tratamento de incidentes com planos de comunicação e alertas definidos.

Nos demais casos, quando do início do processo de renovação contratual, os entrevistados afirmaram que as organizações em que atuavam estiveram avaliando os riscos elencados pelo acórdão do TCU e classificados quanto à sua criticidade, buscando-se elencar tais questões no momento da renovação da contratação, de forma a fazer requisições para que os provedores de nuvem disponibilizassem recursos que auxiliassem no tratamento de incidentes.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo, foi possível identificar a menção dos riscos e controles elencados na Tabela 4.21.

Tabela 4.21: Riscos e controles para o domínio de Resposta a Incidentes relatados

Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Falta de informação técnica do provedor de nuvem	Contratação de SOC e Blue Team	1	3
	Clausulas Contratuais - Penalidades	0	2
	Integração das equipes (Provedor e Organização)	0	1
	Habilitação dos recursos adicionais de segurança	0	1
	Somente dados públicos em nuvem	0	1
	Em estudo	0	1
Plano de resposta a incidente fraco do provedor de nuvem	Plano de resposta integrado (Provedor e Organização)	2	2
	Alteração de modelo de contratação (*Service Provider*)	4	1
	Estruturação do grupo de resposta a incidente (CSIRT)	1	1
Vazamento de dados	Nenhum	1	1
Dependência total do provedor (SaaS e PaaS)	Nenhum	0	1
Sem resposta	Sem resposta	1	0
Totais		**10**	**15**

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto a resposta a incidentes, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de resposta a incidentes no uso de computação em nuvem.

(ii): caracterização dos riscos de resposta a incidentes no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de resposta a incidentes: considerando as duas coletas feitas.

4.4.8 Subcategoria 4.8: Continuidade de Negócio

Esta subcategoria, Continuidade de Negócio, tem como objetivo caracterizar a evolução dos aspectos de continuidade de negócio aplicados aos serviços de computação em nuvem para as organizações entrevistadas, seguindo o roteiro de entrevista mostrado na Tabela 4.22.

Tabela 4.22: Roteiro sobre o domínio de Continuidade de Negócio

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos de continuidade de negócio associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de continuidade de negócio em nuvem

Sobre os riscos relacionadas à continuidade dos negócios, os entrevistados evidenciaram, entre outros, a finalização do contrato com o provedor. Tal fato pode ocorrer após uma série de fatores inerentes à gestão no setor público, incluindo possíveis cortes de orçamento em períodos de renovação contratual. Em casos mais críticos, pode ser necessário optar pela portabilidade dos serviços para outro provedor, sendo, nesse caso, considerados riscos de dependência do provedor de serviços de nuvem, conhecido também como *Lock-in* ou Aprisionamento.

Dos entrevistados da 1ª Coleta, 30% apontaram que, em casos de falhas de conexão, indisponibilidade dos sistemas, degradação de desempenho, perda de dados, e limitação de orçamento contratual para prover escalabilidade da capacidade computacional são riscos relevantes com potencial para causar a interrupção de suas atividades. Na 2ª Coleta, houve um aumento do percentual de entrevistados que alegaram os mesmos riscos, chegando a 60%, o dobro.

Dentre esses entrevistados, tanto da 1ª como da 2ª Coletas, metade declarou que as organizações em que atuam já possuíam planos de contingência em execução, abrangendo: a formação de comitês de segurança e arquitetura com o objetivo de construir e executar procedimentos que assegurem a continuidade dos negócios em caso de incidentes; arquitetura de topologia contemplando o modelo de implantação Híbrido ou *Multi-cloud*; e planos de contingência já estruturados no caso da interrupção de serviços essenciais para as entidades governamentais.

A outra metade dos entrevistados declarou que as organizações em que atuam ainda não possuíam planos de contingência estruturados, majoritariamente em consequência de ainda estarem desenvolvendo a sua maturidade com a utilização de serviços em nuvem, ou por ainda estarem em processo de implantação de modelo de serviço de Infraestrutura como Serviço. Porém, esses entrevistados declararam que os órgãos públicos em que atuavam estavam efetuando: implantação de serviços não críticos; análises de riscos; classificação de sistemas críticos que necessitam de maior prioridade quanto à sua disponibilidade; e elaboração de cláusulas contratuais específicas que prevejam essas situações de maneira a contorná-las se necessário, exigindo que os provedores estejam aptos a suprir as necessidades personalizadas de cada órgão.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo foi possível identificar a menção dos riscos e controles elencados na Tabela 4.23.

Tabela 4.23: Riscos e controles para o domínio de Continuidade de Negócio relatados

Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Indisponibilidade do provedor de nuvem	Contratação de Multi-cloud	2	2
	Redundância com topologia Híbrido	0	1
	Plano de Contingência de Negócio	1	3
	Cláusula Contratual - Penalidades	0	1
	Somente dados públicos em nuvem	0	1
	Comunicação redundante (Provedor e Organização)	1	0
	Em estudo	0	1
Perda de *Backup*	Estabelecer Plano de Contingência de Negócio	0	1
	Redundância com topologia Híbrido	1	1
	Cláusula Contratual - Penalidades	1	1
	Em estudo	0	1
Alto consumo financeiro (Custos/Preço)	Gestão financeira com limitadores por consumo	1	1
Transição contratual	Nenhum	2	1
Sem resposta	Sem resposta	1	0
Totais		**10**	**15**

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto a continuidade de negócio, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de continuidade de negócio no uso de computação em nuvem.

(ii): caracterização dos riscos de continuidade de negócio no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de continuidade de negócio: considerando as duas coletas feitas.

4.4.9 Subcategoria 4.9: Auditoria e Conformidade

Esta subcategoria, Auditoria e Conformidade, tem como objetivo caracterizar a evolução dos aspectos de auditoria e conformidade aplicados aos serviços de computação em nuvem para as organizações entrevistadas seguindo o roteiro de entrevista mostrado na Tabela 4.24.

Tabela 4.24: Roteiro sobre o domínio de Auditoria e Conformidade

Itens	Caracterização do Núcleo de Sentido
Quais são as preocupações quanto aos riscos de auditoria e conformidade associados ao uso de serviços em nuvem? Existe algum planejamento ou controle para prevenir / mitigar / transferir esses riscos?	Aspectos de auditoria e conformidade em nuvem

Tratando-se dos temas relacionados à conformidade e auditoria, 50% dos entrevistados da 1ª Coleta acreditam que a utilização de soluções em nuvem é mais adequada quando se refere às práticas de conformidade, pois os provedores disponibilizam maiores recursos de rastreabilidade e verificação de conformidade e complementam que o risco é menos significante ao se utilizar a nuvem no caso de ser necessário atender a alguma demanda de e-discovery ou auditoria. Na 2ª Coleta, essa perspectiva mudou para 0%, ou seja, após a utilização dos serviços, os acessos aos registros pelos entrevistados foi um problema sério, onde a principal reclamação girou em torno da retenção dos eventos de auditoria que eram limitados a poucos dias.

Os demais 50% dos entrevistados da 1ª Coleta demonstraram receio com questões relativas à efetividade das funcionalidades ofertadas pelo provedor no caso de se avaliar a conformidade das instituições com a Lei Geral de Proteção de Dados (LGPD) ou demais regulamentações referentes ao uso de nuvem. Esse percentual subiu para 86% na 2ª Coleta, evidenciando o problema mencionado e provocando os entrevistados a adotarem medidas de controles que buscassem garantir a conformidade no processo de gestão de eventos tanto do aspecto relacionado a auditoria e conformidade como do aspecto de segurança das operações e comunicações.

Todos os respondentes concluíram que não havia um processo de verificação de conformidade com maturidade suficiente em suas instituições na maioria dos casos, pois na 1ª Coleta o ambiente ainda estava em fase de testes com um número limitado de usuários e na 2ª Coleta, durante a adoção de computação em nuvem pela necessidade provocada pela pandemia, demonstrou-se que era imprescindível a aplicação de controle para mitigar os riscos relatados.

Quanto aos riscos envolvidos e seus controles mitigatórios foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo, foi possível identificar a menção dos riscos e controles elencados na Tabela 4.25.

Tabela 4.25: Riscos e controles para o domínio de Auditoria e Conformidade relatados

Riscos	Controles	Total de Relatos 2019 [13]	Total de Relatos 2022
Problema de geração e acesso a Log de auditoria em nuvem	Gestão de eventos integrada com o provedor	0	2
	Uso de tecnologia (SIEM e UEBA)	0	3
	Recomendações baseada no *framework* CIS Control	0	1
	Análise de Risco	0	1
	Auditoria técnica periodicamente	1	1
	Contratação de SOC e *Blue Team*	0	1
	Desconhece	0	1
	Em estudo	0	2
Punição de órgãos de controle quanto ao uso de nuvem	Uso de tecnologia dos provedores	1	1
Demora na resposta de informações de auditoria	Em estudo	0	1
Pouca maturidade em auditoria	Capacitação de equipe técnica	0	1
Não conformidade legal	Elaborar normas internas	2	0
A adoção favorece o cumprimento legal (Positivo)	-	5	0
Sem resposta	Sem resposta	1	0
Totais		**10**	**15**

Esta subcategoria atingiu o objetivo de caracterizar os aspectos quanto a auditoria e conformidade, riscos e controles aplicáveis no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos aspectos de auditoria e conformidade no uso de computação em nuvem.

(ii): caracterização dos riscos de auditoria e conformidade no uso de computação em nuvem.

(iii): caracterização de controles associados.

(iv): identificação da evolução ao enfrentamento dos riscos de auditoria e conformidade: considerando as duas coletas feitas.

4.4.10 Subcategoria 4.10: Riscos no uso de Computação em Nuvem

Esta subcategoria, Riscos no uso de Computação em Nuvem, tem como objetivo caracterizar os riscos aplicados ao uso de computação em nuvem para as organizações entrevistadas seguindo o roteiro de entrevista mostrado na Tabela 4.26.

Tabela 4.26: Roteiro sobre os Riscos no uso de Computação em Nuvem

Itens	Caracterização do Núcleo de Sentido
De maneira geral, quais seriam os maiores riscos associados ao uso de nuvem entendido pela sua organização?	Riscos no uso de computação em nuvem

Comparando os resultados da pesquisa, nota-se que os entrevistados da 1ª Coleta, majoritariamente acreditavam nas vantagens dos aspectos de segurança oferecidos pelos ambientes de nuvem para as organizações em que atuavam, como a maior eficiência quando comparados aos riscos de se gerenciar uma infraestrutura local, também com relação à disponibilidade, integridade e a confidencialidade dos dados. Porém, os entrevistados da 2ª Coleta, apesar de reconhecerem a superioridade da computação em nuvem, relataram preocupações que exercem relevância nas considerações e planejamentos em torno da contratação de computação em nuvem e da migração dos dados e sistemas governamentais para esses serviços terceirizados.

Entre as maiores tendências levantadas pelos entrevistados, destacam-se as preocupações quanto às imposições que a legislação atual define acerca dos ambientes em questão, incluindo contextos em volta do tratamento de dados sensíveis e às imposições quanto à residência de dados em território nacional. Foram enfatizadas inclusive questões relativas às características intrínsecas do modelo de aquisição e contratação por instituições governamentais, considerando riscos atrelados à términos de contrato e aos cortes orçamentários que podem impedir uma escalabilidade ou renovação contratual, levando em consideração também os riscos quanto à portabilidade dos ambientes de um provedor para outro, no caso de uma mudança decorrente de tais casos.

Após avaliar os posicionamentos dos entrevistados a respeito das organizações da administração pública federal brasileira em que atuavam, é possível atestar que eles, em sua maioria, indicaram que as organizações estavam em fase de planejamento e estruturação dos seus processos voltados para mitigar os riscos levantados na presente pesquisa. As que se encontravam com pouca maturidade, sem nenhum controle aplicado no momento de avaliação, eram compostas por órgãos que utilizavam a tecnologia em nuvem por um menor volume de tempo e que, inclusive, ainda estavam testando tais soluções antes da pandemia, e, depois da pandemia, já haviam implantando os serviços de maneira integral para os seus usuários, não chegando ao ponto de efetivamente implementar estratégias robustas de gestão de riscos na ocasião das duas coleta dos dados.

Apesar da baixa maturidade dessas instituições quanto ao uso de nuvem baseada na ótica dos entrevistados, existem iniciativas em todas as organizações para elaborar planos estruturados que tratam da gestão dos riscos, abordando principalmente questões em torno da contratação desses serviços. Para tais demandas, foi informado pela maioria dos entrevistados que as organizações em que atuavam estavam instituindo comitês para executar a avaliação de riscos e os planejamentos de segurança, resposta a incidentes e demais atividades relacionadas.

Nesse sentido, eles esperavam que, com os resultados dos estudos e definições trazidas pelos comitês de análise de riscos, fossem elaboradas, pelas organizações em que atuavam, cláusulas contratuais que exigiriam dos provedores a prestação de funcionalidades quanto aos temas em pauta, como exemplo, a gestão

de acessos, isolamento de recursos críticos e portabilidade para outros provedores. Também foi apontada a tendência de se adotar modelos de aquisição de dois ou mais provedores de serviços de nuvem em que há possibilidade do órgão migrar os seus serviços entre os provedores de acordo com a sua necessidade em um eventual incidente.

Com relação aos riscos no contexto das imposições regulatórias e legislativas, os entrevistados afirmaram que os órgãos em que atuavam buscaram apoio jurídico-legal por meio de consultorias, para garantir a sua conformidade com a legislação e exigir recursos específicos dos provedores no momento das contratações e renovações. Mas, conforme relatado pelos entrevistados da 2ª Coleta, essa questão foi deixada de lado, visto que a pandemia pressionou a adoção de computação em nuvem devido à necessidade de prover serviços para o trabalho remoto provocado pelo *lockdown* decretado pelos governantes.

A partir de tais posicionamentos, embora estejam em fase avançada de sua transformação digital, na ótica dos entrevistados, as organizações que participaram desta pesquisa possuem planos promissores de se modernizar de maneira eficaz, levando em conta os aspectos relacionados aos riscos e à sua gestão eficiente.

Quanto aos riscos envolvidos e seus controles mitigatórios, foram apresentados relatos por 26 participantes das 23 organizações, sendo que um deixou essa questão sem resposta. Nesse sentido, após a análise de conteúdo, foi possível identificar a menção dos maiores riscos elencados na Figura 4.8.

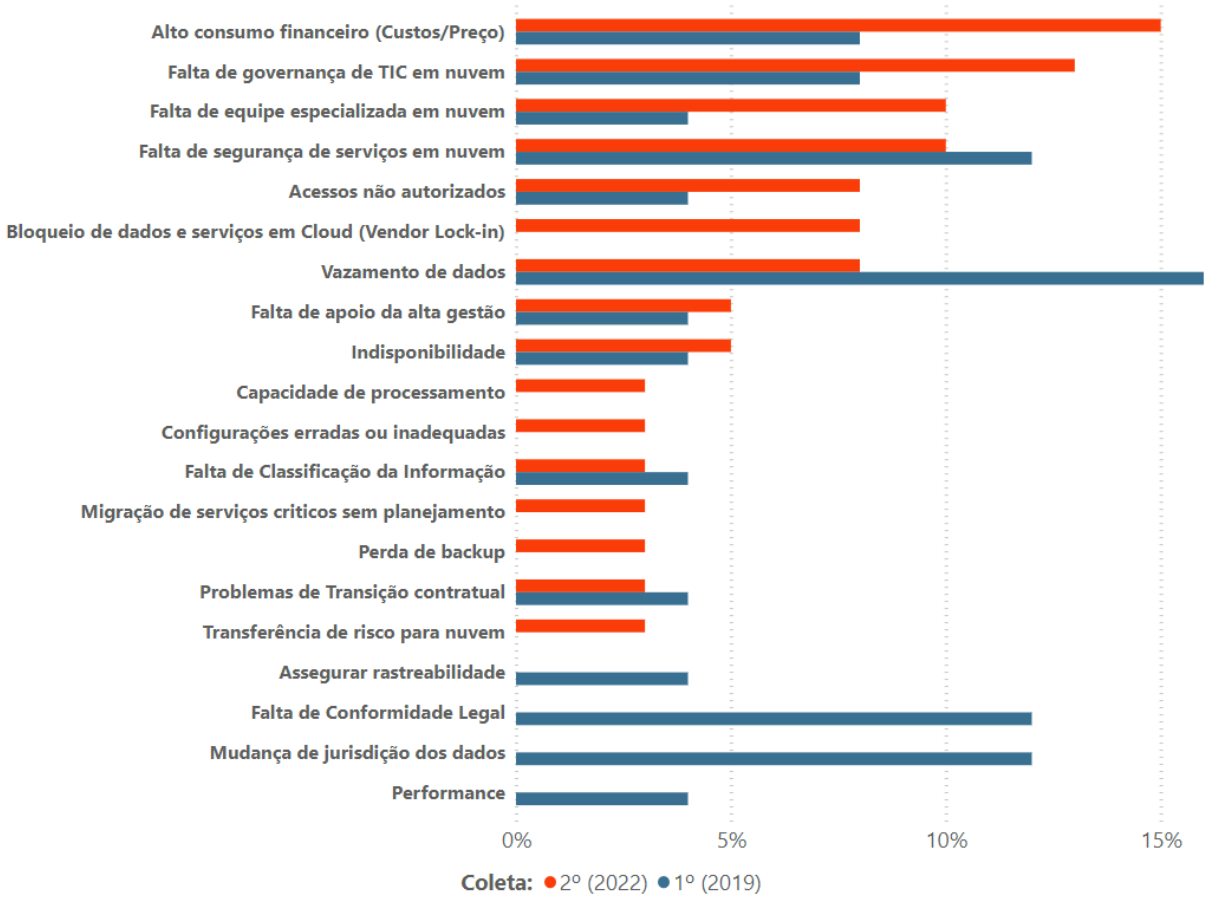

Figura 4.8: Ranking dos riscos no uso de computação em nuvem relatados.

De acordo com a Figura 4.8, houve uma migração das preocupações quanto às duas coletas em relação aos nove domínios de recomendação para gestão de riscos em nuvem constantes deste trabalho (Tab. 2.3).

Na 1ª Coleta, as organizações estavam preocupadas com o domínio de Legislação e Regulamentações, haja vista a menção dos riscos: (i) Vazamento de Dados, (ii) Falta de Conformidade Legal, (iii) Mudança de jurisdição dos dados. Na 2ª Coleta, as preocupações foram relacionadas com os domínios de Governança de TIC e Segurança das Operações e Comunicações conforme os riscos de: (i) Alto consumo financeiro (Custo/Preço), (ii) Falta de governança de TIC em nuvem, (iii) Falta de equipe especializada em nuvem, e (iv) Falta de segurança de serviços em nuvem.

Esta subcategoria atingiu o objetivo de caracterizar os riscos no uso de computação em nuvem pelas organizações entrevistadas, conforme a seguir:

(i): caracterização dos riscos no uso de computação em nuvem.

(ii): caracterização de controles associados.

(iii): identificação da evolução do enfrentamento dos riscos no uso de computação em nuvem: considerando as duas coletas feitas.

5 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Como toda pesquisa, essa também possui algumas limitações e ameaças à validação. Essa pesquisa está limitada ao universo das organizações públicas federais brasileiras para efeitos de amostra, tratando como foco único a análise da adoção de computação em nuvem do setor privado como Microsoft Azure, AWS, Oracle Cloud, Google dentre outras nuvens públicas reconhecidas mundialmente. Ou seja, não foi avaliada a utilização do serviço de computação em nuvem prestado por organizações públicas brasileiras para governo, por meio de suas infraestruturas de computação em nuvem própria, a exemplo do SERPRO com Serpro MultiCloud [80] e da Dataprev com a sua GovCloud [81].

A impossibilidade das entrevistas, entre as duas coletas, 2019 e 2022, serem realizada com os mesmos indivíduos, uma vez que a rotatividade das pessoas nas funções de gestores públicos dentro do serviço público é muito elevada, seria também uma limitação.

Outro fator que pode ser uma ameaça é quanto ao resultado das respostas dos entrevistados quanto às perguntas, uma vez que vários fatores podem influenciar no resultado da pesquisa, tais como: nível de experiência e qualificação profissional dos gestores; maturidade das organizações públicas no uso de computação em nuvem; interesse dos respondentes pelo assunto; disponibilidade (tempo para responder a entrevista); e até mesmo o meio para a realização desta, caso haja, alguma limitação tecnológica para o bom uso de sistemas síncronos de comunicação. Considerando a impossibilidade de qualquer pesquisa possuir uma amostra perfeita, neste trabalho a amostra foi gerada privilegiando a qualidade e relevância das organizações representadas por seus gestores, considerando os diferentes perfis e as diferentes organizações no mais alto nível do estado brasileiro e em todas as esferas de Poder (Executivo, Legislativo e Judiciário).

Apesar das limitações, este estudo não perde sua relevância, pois permite a compreensão de aspectos relacionados à gestão de risco pelas organizações públicas quanto ao uso de computação em nuvem considerando a amostragem estratificada baseada na proporção dos elementos de esfera de poder com o mesmo formato da população observada.

Conforme Figura 5.1, observa-se que não houve uma mudança significativa quanto à evolução das preocupações dos gestores públicos quanto à quantidade de riscos positivos envolvidos entre a 1ª Coleta [13] e 2ª Coleta em relação aos domínios de recomendação em gestão de riscos em computação em nuvem descrita nesse trabalho. Nota-se que somente dois domínios: Auditoria e Conformidade, e Legislação e Regulamentações tiveram riscos positivos apontados pelos entrevistados. Sendo que no domínio de Auditoria e Conformidade não houve menção de riscos positivos e em Legislação e Regulamentação houve uma evolução de um para dois riscos positivos.

Diante de tal evidência, foi possível inferir que a adoção de computação em nuvem sustenta-se basicamente em normativos, os quais promovem a adoção dessa tecnologia pela administração pública de maneira geral.

Obversa-se, com este estudo longitudinal, que a preocupação quanto aos riscos negativos aumentaram de forma qualitativa e quantitativa, uma vez que a Figura 5.2 demonstra que os domínios que obtiveram maior atenção foram o de Isolamento de Clientes em Nuvem (aumento de 200%) seguido pelo de Segurança

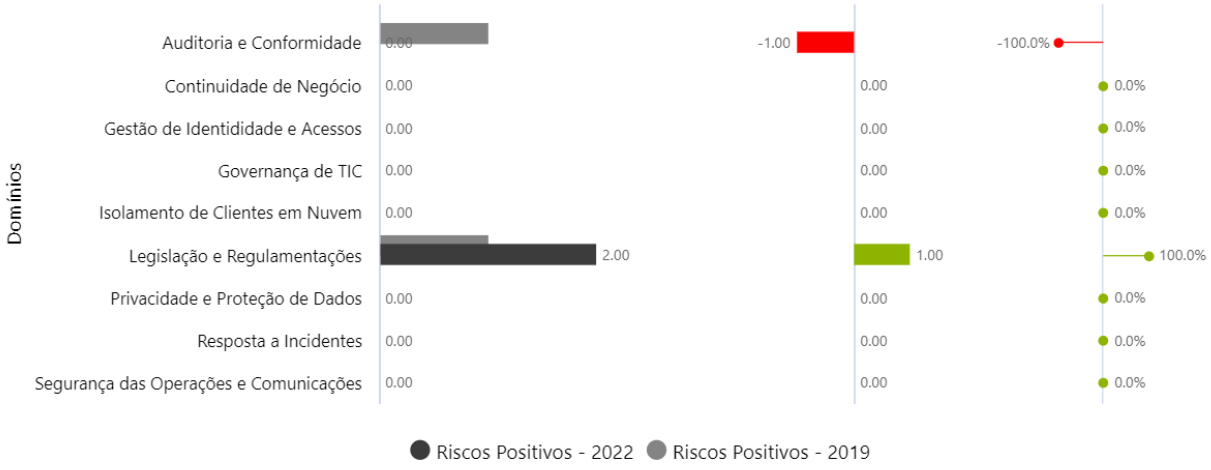

Figura 5.1: Comparação entre os Riscos Positivos dos Domínios de recomendação.

das Operações e Comunicações (aumento de 100%). Cenário esse causado pelo incidente que acometeu o Ministério da Saúde em dezembro de 2021 [36], em que os principais domínios envolvidos no incidente foram os dois aqui citados.

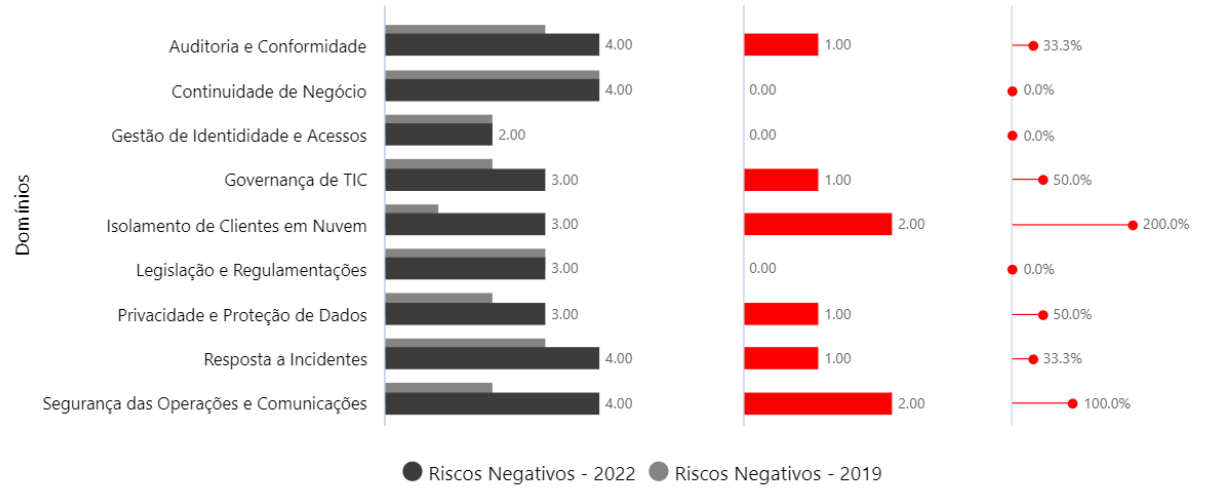

Figura 5.2: Comparação entre os Riscos Negativos dos Domínios de recomendação.

Como consequência dos riscos negativos associados, nota-se que os domínios com aumento da qualidade e quantidade de controles adotados foram 5: Governança de TIC (400%); Privacidade e Proteção de Dados (250%); Isolamento de Clientes em Nuvem (233%); Segurança das Operações e Comunicações; e Auditoria e Conformidade (166%), conforme apresentado na Figura 5.3.

Como destaque aos domínios citados e seus respectivos controles mencionados: a Governança de TIC apresenta a não utilização de ferramentas proprietárias bem como adoção de Multi-cloud; a Privacidade e Proteção de Dados, classificação dos dados e somente dados não sensíveis podem ir para nuvem; o Isolamento de Clientes em Nuvem, cláusulas contratuais e contratação sem intermediário de nuvem (Cloud Broker); e Auditoria e Conformidade com Segurança das Operações e Comunicações têm em comum a

implantação de SOC como controles mitigatórios.

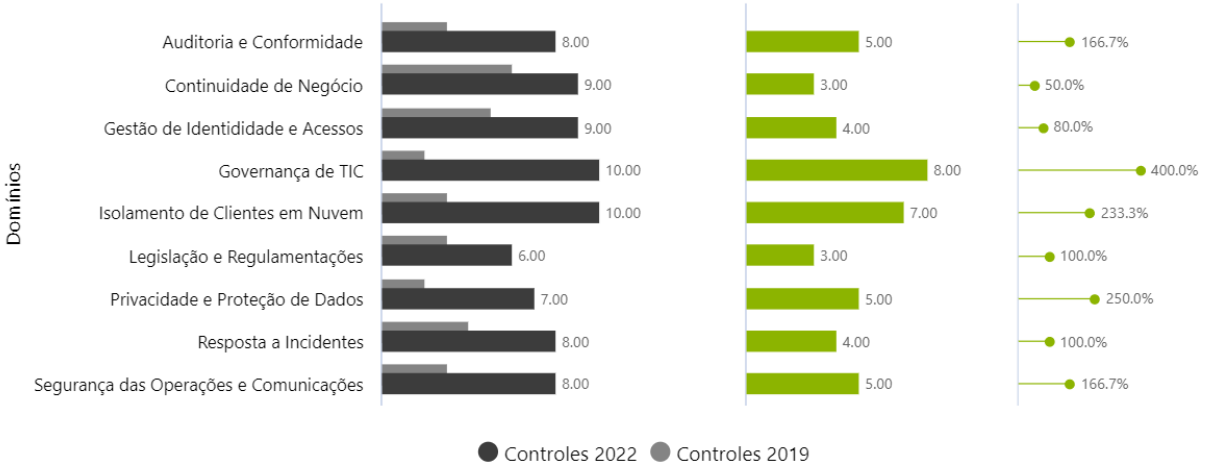

Figura 5.3: Comparação entre os Controles dos Domínios de recomendação.

6 CONCLUSÃO

Este trabalho teve como objetivo identificar e avaliar os riscos, durante a pandemia de COVID-19, e a propensão ao enfrentamento desses ao se implantar serviços em Computação em Nuvem sob a ótica dos gestores de órgãos públicos federais no Brasil. Ainda que a evolução da gestão de riscos de segurança e privacidade esteja alinhada com os *frameworks* de segurança cibernética em computação em nuvem, não está completamente adequada e implementada, haja vista a urgência na necessidade em disponibilizar serviços digitalizados em nuvem provocada pela pandemia de COVID-19, quando a população teve o seu acesso físico interrompido devido ao isolamento social, conhecido como *lockdown*, decretado pelos governos estaduais. Para chegar a esta conclusão, foram levados em consideração os relatos dos entrevistados quanto à maturidade no uso de computação em nuvem, aos domínios de recomendação para gestão de riscos e aos riscos em computação em nuvem.

Para alcançar o objetivo proposto, foram realizadas entrevistas semiestruturadas com gestores dos níveis estratégico, tático e operacional envolvidos com a gestão de tecnologia da informação de vinte e três órgãos da Administração Pública Federal das três esferas de poder que compõem a União.

O estudo explorou questões relativas a um tema atual e em ascensão no campo de administração pública e privada no âmbito de Tecnologia da Informação: a computação em nuvem e a gestão de riscos relacionados ao seu uso.

É consenso entre os entrevistados que a adoção de computação em nuvem é um caminho sem volta, considerando a otimização dos custos de investimento bem como o favorecimento do teletrabalho pelas organizações com o uso de soluções baseada em Software como Serviço (SaaS).

Com base nos resultados da pesquisa, foi possível colher impressões dos respondentes sobre a situação das organizações que participaram do estudo, trazendo questões sobre a permeabilidade da computação em nuvem na Administração Pública Federal, sobre a maturidade no uso de tais soluções e a identificação de tendências de gestão de riscos praticadas por essas organizações.

Constatou-se que a adoção de computação em nuvem pode representar uma economia de recursos públicos, porém traz desafios, principalmente quando os gestores se deparam com questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis, governança de TIC em nuvem e segurança das operações e comunicações. Em adição, para adotar a computação em nuvem, na linha de ação proposta pela Lei de Governo Digital [8], era necessário enfrentar riscos de transposição complexa, os quais acabavam por postergar a implementação dessa tecnologia pelas entidades governamentais no período pré-pandemia. Mas, no momento atual, a adoção de computação em nuvem já ocorreu e, conforme relatos dos entrevistados quanto aos riscos percebidos, bem como quanto aos incidentes [35] [37] mencionados neste trabalho, as ações de gestão de riscos precisam ainda ser fortalecidas pelas organizações.

Para verificar o atendimento às hipóteses apresentadas na subseção (1.2), são apresentadas a seguir conclusões específicas sobre cada hipótese.

Quanto à hipótese 1, observou-se que as organizações entrevistadas não implantaram processos de gestão de riscos antes da adoção de computação em nuvem, conforme relatos de ausência de normativos internos e subprocessos de classificação de dados, situação essa apresentada pelos entrevistados como ações em andamento. O risco negativo mencionado de *Shadow IT* pelos entrevistados evidencia a presente hipótese.

A comprovação da hipótese 2 ocorreu conforme os relatos de entrevistados de 4 organizações que são clientes da empresa que foi vítima do incidente do Ministério da Saúde [36], quando os contratantes sofreram com a indisponibilidade de seus serviços em nuvem hospedados com a topologia em Multi-cloud, demonstrando assim a ausência de controles adequados e implantados quanto aos riscos mencionados no domínio de Isolamento de Cliente em Nuvem.

Embora estejam, em geral, em uma operação de sua transformação digital, sob ótica dos entrevistados, as organizações em que atuavam revelavam planos de se modernizar, levando em conta os aspectos relacionados aos riscos e à sua gestão eficiente. Quanto aos riscos no contexto das imposições regulatórias e legislativas, os entrevistados da 1ª Coleta afirmaram que os órgãos em que atuavam buscaram apoio jurídico-legal por meio de consultorias, para garantir a sua conformidade com a legislação e exigir recursos específicos dos provedores no momento das contratações e renovações. Porém, na 2ª Coleta, a percepção mudou para a governança de TIC e segurança das operações e comunicações com a implantação de normativos internos e adoção de tecnologias para mitigação e até a eliminação dos riscos associados a esses domínios.

Este estudo oferece uma visão acerca do posicionamento quanto à adoção da computação em nuvem numa amostra de organizações no Governo Federal Brasileiro e coloca à disposição de interessados um rol de observações sobre a situação contemporânea no cenário de gestão de riscos a que os órgãos públicos estão sujeitos. Os resultados apresentados nesta pesquisa referem-se aos dados que foram coletados em dois determinados momentos do tempo e a partir das entrevistas dos gestores atuantes nas organizações pública.

6.1 TRABALHOS FUTUROS

Por fim, este estudo deixa uma abertura para a realização de pesquisas e trabalhos acadêmicos futuros sobre o tema, com vistas a validar os resultados posteriores de mudanças nas organizações públicas estudadas ou em futuros estudos que tratem sobre a maturidade das organizações públicas no Brasil nos diversos níveis de governo brasileiro (federal, estadual e municipal) quanto ao uso de serviços de nuvem, considerando ainda os impactos do teletrabalho e da digitalização dos serviços públicos.

Outra boa oportunidade de trabalhos futuros seria elaborar mecanismos para avaliação de riscos de produtos e serviços em nuvem ofertados no país por provedores, bem como o seu atendimento quanto aos requisitos de segurança em computação em nuvem presentes nas legislação brasileira, como a Lei de Governo Digital [8] e, principalmente, no que se refere a privacidade e proteção de dados, a LGPD [14].

REFERÊNCIAS BIBLIOGRÁFICAS

1 BRASIL. Ministério da Economia. *Portal gov.br já tem mil serviços públicos digitalizados*. 2020. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2020/10/portal-gov-br-ja-tem-mil-servicos-publicos-digitalizados-para-acesso-do-cidadao>. Acesso em: 11 fev. 2022.

2 BRASIL. Ministério da Economia. *Serviços Digitais: Transformar serviços públicos pelo digital*. 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/transformacao-digital/lista-servicos-digitais>. Acesso em: 11 fev. 2022.

3 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *COVID-19: Embracing digital government during the pandemic and beyond*. 2020. Disponível em: <https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/>. Acesso em: 11 fev. 2022.

4 BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. aprova a estratégia nacional de segurança cibernética. *Diário Oficial da União*, Poder Executivo, Brasília, DF, p. 1–38, 5 fev. 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em: 13 fev. 2022.

5 IBM. *Relatório de custo da violação de dados de 2021*. 2021. <https://www.ibm.com/br-pt/security/data-breach>. Acesso em: 13 fev. 2022.

6 JONES, S.; IRANI, Z.; SIVARAJAH, U.; LOVE, P. E. D. Risks and rewards of cloud computing in the uk public sector: A reflection on three organisational case studies. *Information Systems Frontiers*, Information Systems Frontiers, v. 21, p. 359–382, 4 2019. ISSN 1387-3326. Disponível em: <http://link.springer.com/10.1007/s10796-017-9756-0>.

7 BRASIL. Decreto nº 10.332, de 28 de abril de 2020. institui a estratégia de governo digital para o período de 2020 a 2022. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 28 abr. 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em: 13 fev. 2022.

8 BRASIL. Lei nº 14.129, de 29 de março de 2021. dispõe sobre princípios, regras e instrumentos para o governo digital e para o aumento da eficiência pública. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132>. Acesso em: 15 fev. 2022.

9 ADELMANN, F.; ELLIOTT, J. A.; ERGEN, I.; GAIDOSCH, T.; JENKINSON, N.; KHIAONARONG, T.; MOROZOVA, A.; SCHWARZ, N.; WILSON, C. *Cyber Risk and Financial Stability: It's a Small World After All*. 2020. <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622>. Acesso em: 13 fev. 2022.

10 CLOUD SECURITY ALLIANCE. *State of cloud security risk, compliance, and misconfigurations*. 2020. Disponível em: <https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-risk-compliance/>. Acesso em: 13 fev. 2022.

11 BRASIL. Ministério da Economia. *Governo economiza R$ 304 milhões com nova contratação de serviços em nuvem*. 2021. <https://www.gov.br/economia/pt-br/assuntos/noticias/2021/abril/governo-economiza-r-304-milhoes-com-nova-contratacao-de-servicos-em-nuvem>. Acesso em: 11 fev. 2022.

12 COMITÊ GESTOR DE INTERNET NO BRASIL. *TIC GOVERNO ELETRÔNICO*: Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro. São Paulo, SP: cetic.br, 2020. Disponível em: <https://www.cetic.br>. Acesso em: 10 fev. 2022.

13 ALVES, A. A.; ALVES, C. A. M.; TABOSA, F. G. F.; NUNES, R. R. Riscos da computação em nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil. In: . [s.n.], 2021. v. 11, p. 01–18. ISSN 22374558. Disponível em: <http://navus.sc.senac.br/index.php/navus/article/view/1513/pdf>.

14 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais - lgpd. *Diário Oficial da União*, Presidência da República, Brasília, DF, 2018. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132>. Acesso em: 14 fev. 2022.

15 GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. 6. ed. São Paulo: Atlas, 2008. ISBN 978-85-224-5142-5.

16 TABOSA, F. G. F.; SILVA, D. A.; SOUSA, R. T.; DEUS, F. E. G.; NUNES, R. R. Risks factors that influence a data center infrastructure through the TEMAC method. In: *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2021. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/9476286>.

17 BRASIL. Tribunal de Contas da União. *Acórdão N. 1.739/2015*. Tribunal de Contas da União, 2015. Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/destaques/>.

18 MELL, P. M.; GRANCE, T. *The NIST definition of cloud computing*. Gaithersburg, MD, 2011. v. 514, 675-685 p. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

19 CLOUD SECURITY ALLIANCE. *CSA Security Guidance v4*. [S.l.], 2017. 152 p. Disponível em: <https://cloudsecurityalliance.org/download/security->.

20 VERAS, M. *Cloud Computing - Nova Arquitetura Da TI*. [S.l.]: Brasport, 2012. 240 p. ISBN 8574524891.

21 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27017 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem*. Rio de Janiro, RJ, 2016. Disponível em: <www.abnt.org.br>.

22 TAURION, C. *Cloud Computing: computação em nuvem: transformando o mundo da tecnologia da informação*. [S.l.]: Brasport, 2009. ISBN 978-85-7552-423-8.

23 LEE, C. A.; BOHN, R. B.; LEE, C. A. *The NIST Cloud Federation Reference Architecture NIST Special Publication 500-332 The NIST Cloud Federation Reference Architecture*. [S.l.], 2020. 92 p. Disponível em: <https://doi.org/10.6028/NIST.SP.500-332>. Acesso em: 18 fev. 2022.

24 IEEE Computer Society. *IEEE 2302-2021 Standard for Intercloud Interoperability and Federation (SIIF)*. [S.l.], 2022. Acesso em: 18-02-2022.

25 COMITÊ GESTOR DE INTERNET NO BRASIL. *Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus: Painel TIC COVID-19*. 2021. Disponível em: <https://cetic.br/pt/publicacao/painel-tic-covid-19/>. Acesso em: 11 fev. 2022.

26 MANCINI, L.; CALDERON, A.; BARBOSA, A.; MARTINEZ, A. L.; PATINO, A.; AL et. *O Mercosul diante da mudança tecnológica e da transformação digital: elementos para análise*. São Paulo, SP: Núcleo de Informação e Coordenação do Ponto BR, 2021. Disponível em: <https://cetic.br/pt/publicacao/o-mercosul-diante-da-mudanca-tecnologica-e-da-transformacao-digital-elementos-para-analise/>. Acesso em: 8 fev. 2022.

27 UTA, A.; OBASEKI, H. A Performance Study of Big Data Workloads in Cloud Datacenters with Network Variability. In: *Companion of the 2018 ACM/SPEC International Conference on Performance Engineering*. New York, NY, USA: ACM, 2018. v. 2018-Janua, p. 113–118. ISBN 9781450356299. Disponível em: <https://dl.acm.org/doi/10.1145/3185768.3186299>.

28 GIULIO, C. D.; SPRABERY, R.; KAMHOUA, C.; KWIAT, K.; CAMPBELL, R. H.; BASHIR, M. N. Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? In: *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. IEEE, 2017. v. 2017-June, p. 50–57. ISBN 978-1-5386-1993-3. ISSN 21596190. Disponível em: <https://ieeexplore.ieee.org/document/8030571/>.

29 ESTADOS UNIDOS DA AMÉRICA. Office of Management and Budget. Federal cloud computing strategy. 2021. Disponível em: <https://cloud.cio.gov/strategy/>. Acesso em: 14 fev 2022.

30 BRASIL. Presidência da República. Instrução normativa nº 5, de 30 de agosto de 2021. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684>. Acesso em: 18 jun. 2022.

31 BRASIL; Conselho Nacional de Justiça. *Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário*. 2021. <https://www.cnj.jus.br/wp-content/uploads/2021/11/guia-da-entic-jud-res370-2021-10-07-rev2.pdf>. Acesso em: 18 jun. 2022.

32 INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *Risk IT Framework*. 2nd edition. ed. ISACA, 2020. 46 p. ISBN 978-1-60420-820-7. Disponível em: <www.isaca.org>. Acesso em: 14 fev. 2022.

33 BRASIL. Presidência da República. Portaria nº 93, de 26 de setembro de 2019. set. 2019. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 14 fev 2022.

34 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes*. Rio de Janiro, RJ, 2018. Disponível em: <www.abnt.org.br>.

35 BRASIL. Presidência da República. CTIR gov em números: Incidentes. 2022. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/incidentes>. Acesso em: 14 fev. 2022.

36 BRASIL. Polícia Federal. Atuação da PF no ataque hacker ao ministério da saúde. dez. 2021. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/12/atuacao-da-pf-no-ataque-hacker-ao-ministerio-da-saude>. Acesso em: 14 fev. 2022.

37 BRASIL. Presidência da República. ALERTA 08/2021 - alerta para ambientes em nuvem (cloud). dez. 2021. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-08-2021>. Acesso em: 14 fev. 2022.

38 IDENTITY THEFT RESOURCE CENTER. The 2021 data breach annual report. 2022. Disponível em: <https://notified.idtheftcenter.org/s/>. Acesso em: 13 fev. 2022.

39 GREENWALD, G.; MACASKILL, E. *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian, 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 10 fev. 2022.

40 NUGRAHA, Y.; MARTIN, A. Towards a framework for trustworthy data security level agreement in cloud procurement. *Computers & Security*, v. 106, p. 102266, 7 2021. ISSN 01674048. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167404821000900>.

41 JANSEN, W.; GRANCE, T. Guidelines on security and privacy in public cloud computing. 2011. ISSN 15227383. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>. Acesso em: 14 fev. 2022.

42 EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. Cloud computing - benefits, risks and recommendations for information security rev. b. 2012. Disponível em: <http://www.enisa.europa.eu>. Acesso em: 14 fev. 2022.

43 MODULL, R.; ARLEN, J.; GILBERT, F.; LANE, A.; MORTMAN, D.; PETERSON, G.; ROTHMAN, M. *CSA Security Guidance v4.0*: For critical areas of focus in cloud computing. [S.l.], 2017. 152 p. Disponível em: <https://cloudsecurityalliance.org/download/security-guidance-v4/>.

44 BRASIL. Conselho Monetário Nacional. Resolução no 4.658, de 26 de abril de 2018. Conselho Monetário Nacional, 2018. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu\%25C3\%25A7\%25C3\%25A3o&numero=4658>. Acesso em: 14 fev. 2022.

45 BRASIL. Banco Central do Brasil. Circular n. 3.909, de 16 de agosto de 2018. Banco Central do Brasil, 2018. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3909>. Acesso em: 14 fev. 2022.

46 BRASIL. Presidência da República. Portaria gsi nº 9 de 15 de março de 2018. Presidência da República, 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/7019183/do1-2018-03-19-portaria-n-9-de-15-de-marco-de-2018-7019179>. Acesso em: 14 fev. 2022.

47 BRASIL. Ministério da Economia. Instrução normativa n. 1, de 4 de abril de 2019. Ministério da Economia, 2019. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535>. Acesso em: 14 fev. 2022.

48 CLOUD SECURITY ALLIANCE. Enterprise architecture. 2021. Disponível em: <https://cloudsecurityalliance.org/research/working-groups/enterprise-architecture/>. Acesso em: 14 fev. 2022.

49 CLOUD SECURITY ALLIANCE. Cloud controls matrix working group. 2021. Disponível em: <https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/>. Acesso em: 14 fev. 2022.

50 NIST Cloud Computing Security Working Group. *NIST Cloud Computing Security Reference Architecture*. [S.l.], 2013. Disponível em: <https://csrc.nist.gov/publications/detail/sp/500-299/archive/2013-05-05>. Acesso em: 18 jun. 2022.

51 CLOUD SECURITY ALLIANCE. *CSA Enterprise Architecture reference guide v2*. [S.l.], 2021. Disponível em: <https://cloudsecurityalliance.org/artifacts/enterprise-architecture-reference-guide-v2/>. Acesso em: 18 jun. 2022.

52 PAPE, S.; PACI, F.; JÜRJENS, J.; MASSACCI, F. Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach. *Information (Basel)*, v. 11, n. 5, p. 261, may 2020. ISSN 2078-2489. Disponível em: <https://www.mdpi.com/2078-2489/11/5/261>.

53 ALI, O.; SHRESTHA, A.; GHASEMAGHAEI, M.; BEYDOUN, G. Assessment of complexity in cloud computing adoption: a case study of local governments in australia. *Information Systems Frontiers*, 1 2021. ISSN 1387-3326. Disponível em: <http://link.springer.com/10.1007/s10796-021-10108-w>.

54 LEE, S.; CHOI, Y.; RA, J.; KIM, J.; ASHIHARA, K. Impact of public cloud computing service in korean government organizations. *ICIC Express Letters, Part B: Applications*, ICIC International, v. 11, p. 313–318, 2020. Top risk cloud governo da Korea. Disponível em: <http://www.icicelb.org/ellb/contents/2020/3/elb-11-03-13.pdf>.

55 MUDAWI, N. A.; BELOFF, N.; WHITE, M. Issues and challenges: Cloud computing e-government in developing countries. *International Journal of Advanced Computer Science and Applications*, v. 11, p. 7–11, 2020. ISSN 21565570. Disponível em: <http://thesai.org/Publications/ViewPaper?Volume=11&Issue=4&Code=IJACSA&SerialNo=2>.

56 KUSHWAHA, N.; ROGUSKI, P.; WATSON, B. W. Up in the air: Ensuring government data sovereignty in the cloud. *2020 12th International Conference on Cyber Conflict (CyCon)*, IEEE, p. 43–61, 5 2020. ISSN 2325-5366. 12th International Conference on Cyber Conflict (CyCon) - 20/20 Vision - The Next Decade, ELECTR NETWORK, MAY 26-29, 2020. Disponível em: <https://ieeexplore.ieee.org/document/9131718/>.

57 KYRIAKOU, N.; EURIPIDES, L.; PARASKEVI, D. Factors affecting cloud storage adoption by greek municipalities. *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, ACM, p. 244–253, 9 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3428502.3428537>.

58 AL-RUITHE, M.; BENKHELIFA, E. Determining the enabling factors for implementing cloud data governance in the saudi public sector by structural equation modelling. *Future Generation Computer Systems*, Elsevier B.V., v. 107, p. 1061–1076, 6 2020. ISSN 0167739X. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167739X17321489>.

59 ALANNSARY, M. O.; HAUSAWI, Y. M. Adopting and Implementing a Government Cloud in Saudi Arabia, an Integral Part of Vision 2030. In: *Proceedings of 34th International Conference on Computers and Their Applications, CATA 2019*. [s.n.], 2019. p. 387–376. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075280835&partnerID=40&md5=d6af96be7f51497ae816be73e325a674https://easychair.org/publications/paper/Xp9c>.

60 HAMID, N. binti A.; MOHAMED, I.; DAUD, M.; SALIMIN, N.; AHMAD, N. I. Otpaf: A security requirement conceptual model of saas for malaysian government based on common criteria. *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, IEEE, v. 2019-July, p. 69–74, 7 2019. Disponível em: <https://ieeexplore.ieee.org/document/8988832/>.

61 ALZADJALI, K.; ELBANNA, A. Smart Institutional Intervention in the Adoption of Digital Infrastructure: The Case of Government Cloud Computing in Oman. *Information Systems Frontiers*, v. 22, n. 2, p. 365–380, apr 2020. ISSN 1387-3326. Disponível em: <http://link.springer.com/10.1007/s10796-019-09918-w>.

62 SINNOTT, R.; PURSULTANI, H. Migrating a National Cloud Platform for Urban Analytics: A Performance Assessment Framework. IEEE, v. 2019-Decem, p. 354–361, dec 2019. Disponível em: <https://ieeexplore.ieee.org/document/8968860/>.

63 NGHIHALWA, E.; SHAVA, F. B. An assessment of cloud computing readiness in the namibian government's information technology departments. *2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)*, IEEE, p. 92–97, 5 2018. Disponível em: <https://ieeexplore.ieee.org/document/8379074/>.

64 NGHIHALWA, E. N.; SHAVA, F. B. A Secure Cloud Adoption Framework (SCAF) for the Namibian Government Information Technology Departments. In: Yang, XS and Dey, N and Joshi, A. (Ed.). *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 2018. p. 246–253. ISBN 978-1-5386-7280-8. Disponível em: <https://ieeexplore.ieee.org/document/8611573/>.

65 AL-RUITHE, M.; BENKHELIFA, E.; HAMEED, K. Key issues for embracing the cloud computing to adopt a digital transformation: A study of saudi public sector. *Procedia Computer Science*, Elsevier B.V., v. 130, p. 1037–1043, 2018. ISSN 18770509. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S1877050918305076>.

66 PAGE, M. J.; MCKENZIE, J. E.; BOSSUYT, P. M.; BOUTRON, I.; HOFFMANN, T. C.; MULROW, C. D.; SHAMSEER, L.; TETZLAFF, J. M.; AKL, E. A.; BRENNAN, S. E.; CHOU, R.; GLANVILLE, J.; GRIMSHAW, J. M.; HRÓBJARTSSON, A.; LALU, M. M.; LI, T.; LODER, E. W.; MAYO-WILSON, E.; MCDONALD, S.; MCGUINNESS, L. A.; STEWART, L. A.; THOMAS, J.; TRICCO, A. C.; WELCH, V. A.; WHITING, P.; MOHER, D. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery*, v. 88, p. 105906, apr 2021. ISSN 17439191. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S1743919121000406>.

67 QUEZADA-GAIBOR, D.; TORRES-SOSPEDRA, J.; NURMI, J.; KOUCHERYAVY, Y.; HUERTA, J. Cloud Platforms for Context-Adaptive Positioning and Localisation in GNSS-Denied Scenarios—A Systematic Review. *Sensors*, MDPI, v. 22, n. 1, p. 110, dec 2021. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/22/1/110>.

68 BRASIL; Ministério da Educação. Portal .periodicos. CAPES. 2022. Disponível em: <https://www.periodicos.capes.gov.br/index.php/acesso-cafe.html>. Acesso em: 17 fev. 2022.

69 PETTIGREW, A. M. What is a processual analysis? *Scandinavian Journal of Management*, v. 13, n. 4, p. 337–348, dec 1997. ISSN 09565221. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0956522197000201>.

70 TANG, W.; QIANG, M.; DUFFIELD, C. F.; YOUNG, D. M.; LU, Y. Incentives in the Chinese Construction Industry. *Journal of Construction Engineering and Management*, Beijing, v. 134, n. 7, p. 457–467, jul 2008. ISSN 0733-9364. Disponível em: <http://ascelibrary.org/doi/10.1061/%28ASCE%290733-9364%282008%29134%3A7%28457%29>.

71 LONGHURST, R. *Semi-structured interviews and focus groups*. Londres: [s.n.], 2003. 103 p.

72 BURLESON, B. R.; LEVINE, B. J.; SAMTER, W. Decision-making procedure and decision quality. *Human Communication Research*, Oxford, v. 10, n. 4, p. 557–574, jun 1984. ISSN 0360-3989. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2958.1984.tb00032.x>.

73 CAMERON, D.; KNEALE, P.; SEE, L. An evaluation of a traditional and a neural net modelling approach to flood forecasting for an upland catchment. *Hydrological Processes*, Londres, v. 16, n. 5, p. 1033–1046, apr 2002. ISSN 0885-6087. Disponível em: <https://onlinelibrary.wiley.com/doi/10.1002/hyp.317>.

74 LOMBARDI, M. R.; SÁ, M. A. Á. S.; PAULA, M. A. B. *O PRAZER DA ENTREVISTA EM PESQUISAS QUALITATIVAS*. EDITORA CRV, 2021. ISBN 9786525118369. Disponível em: <https://www.editoracrv.com.br/produtos/detalhes/36649-crv>.

75 VALENTINE, G. Tell me about... Using interviews as a research methodology apud Flowerdew, R. and Martin, D.(eds.). *Methods in human geography: A guide for students doing a research project*, Pearson Harlow, Harlow, v. 2, p. 110—-127, 2005. Disponível em: <https://ucl.rl.talis.com/items/8DCA1D60-D21E-0B81-1790-4E27EC52DDCA.html>.

76 KITCHIN, R.; TATE, N.; NICHOLAS, J. T. *Conducting Research in Human Geography: Theory, Methodology and Practice*. 1. ed. Ann Arbor: Prentice Hall, 2000. 346 p. ISBN 9780582297975.

77 MILES, M. B.; HUBERMAN, A. M. *Qualitative Data Analysis: An Expanded Sourcebook*. 2. ed. Thousand Oaks, CA: SAGE Publications, 1994.

78 BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em ciências sociais. *Em tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC*, v. 2, n. 1, p. 68–80, 2005. Disponível em: <https://periodicos.ufsc.br/index.php/emtese/article/view/18027>.

79 BARDIN, L. *Análise de Conteúdo*. São Paulo: Edições 70 - Almedina Brasil, 2016. 232 p. ISBN 9788562938047.

80 SERPRO. *Serpro MultiCloud: a escolha certa de nuvem para governo*. 2022. Disponível em: <https://campanhas.serpro.gov.br/serpro-multicloud/>. Acesso em: 1 set. 2022.

81 DATAPREV, Empresa de Tecnologia e Informações da Previdência. *Soluções de Governo para Governo*. 2022. Disponível em: <https://portal3.dataprev.gov.br/solucao/solucoes-para-governo>. Acesso em: 1 set. 2022.