DOI: 10.5748/20CONTECSI/PSE/SEC/7211

eLocator: e207211

RESILIÊNCIA E CONTINUIDADE DE NEGÓCIOS POR MEIO DE ARMAZENAMENTO DE DADOS EM NUVEM

Eduardo Ferreira Silveira
Ipt - Instituto De Pesquisas Tecnológicas

Antonio Rigo
Ipt - Instituto De Pesquisas Tecnológicas

Resiliência e Continuidade de Negócios por meio de Armazenamento de Dados em Nuvem.

Resumo

A cada dia as empresas estão mais expostas às ameaças cibernéticas e a continuidade de suas atividades é colocada à prova. Diante dos desafios de segurança, é necessário adotar estratégias e elaborar um plano eficiente baseado em boas práticas para garantir a continuidade dos negócios. Neste sentido, a computação em nuvem apresenta-se como uma ferramenta relevante e oportuna, sendo capaz de proporcionar serviços online de grande escala, como *backup* e recuperação de dados, a um custo competitivo. Ainda assim, o uso de recursos de nuvem demanda cuidados específicos para garantir a segurança das informações em relação a confidencialidade, integridade e disponibilidade dos dados. Este trabalho tem o objetivo de levantar e analisar documentos e pesquisas anteriores, por meio de uma revisão sistemática da literatura, que descrevam as características e estratégias do uso de computação em nuvem em suas atividades econômicas, para garantir a continuidade dos negócios das empresas e prover resiliência da operação da tecnologia da informação. Em especial, em relação à preservação dos dados de uma organização, este texto apresenta os desafios da criação de plano de armazenamento de dados no contexto de "*cloud computing*" encontradas na literatura recente. Os principais resultados obtidos neste artigo de revisão sistemática destacam as boas práticas no uso de "Cloud Computing", a análise revela o comprometimento da comunidade científica em explorar o potencial da computação em nuvem, apesar dos desafios. A maioria dos autores ressalta as vantagens, como a implementação do Disaster Recovery as a Service (DRaaS), fortalecendo a segurança dos dados. A pesquisa destaca a contribuição da computação em nuvem para a continuidade e competitividade dos negócios, aproveitando benefícios como flexibilidade e custos sob demanda.

Palavras-Chave: "Computação em Nuvem"; "*Backup e* Restauração"; "Continuidade de negócios".

Abstract

Every day companies are more exposed to cyber threats and the continuity of their activities is put to the test. Faced with security challenges, it is necessary to adopt strategies and develop an efficient plan based on good practices to ensure business continuity. In this sense, cloud computing presents itself as a relevant and timely tool, capable of providing large-scale online services, such as backup and data recovery, at a competitive cost. Even so, the use of cloud resources requires specific care to ensure the security of information in relation to confidentiality, integrity and availability of data. This work aims to collect and analyze previous documents and research, through a systematic literature review, that describe the characteristics and strategies of using cloud computing in their economic activities, to guarantee the continuity of companies' business and provide resilience of information technology operation. In particular, in relation to the preservation of an organization's data, this text presents the challenges of creating a data storage plan in the context of "cloud computing" found in recent literature. The main results obtained in this systematic review article highlight good practices in the use of cloud computing. The analysis reveals the scientific community's commitment to exploiting the potential of cloud computing, despite the challenges. Most of the authors highlight the advantages, such as the implementation of Disaster Recovery as a Service (DRaaS), strengthening data security. The research highlights the contribution of cloud computing to business continuity and competitiveness, taking advantage of benefits such as flexibility and on-demand costs.

Keywords: "Cloud Computing"; "Backup and Restore"; "Business Continuity".

1 INTRODUÇÃO

A computação em nuvem surgiu em resposta a uma demanda crescente de serviços online e à complexidade de infraestrutura inerente a estes serviços, por outro lado, as organizações enfrentam desafios em relação à segurança e ao armazenamento de dados que podem representar um risco à continuidade de seus negócios (ABUASLKISHIK et al., 2020). Neste contexto, muitas empresas encontram na computação em nuvem uma ferramenta para garantir segurança e resiliência de suas atividades. Segundo Peter M. Mell and Timothy Grance (2011), a computação em nuvem é um modelo que provê acesso compartilhado a uma variedade de recursos computacionais através de serviços sob demanda, a mesma definição aponta que este modelo possui cinco características essenciais (autoatendimento sob demanda, amplo acesso à rede, agrupamento de recursos, elasticidade e metrificação de serviços/recursos), três modelos de serviço ("*Software as a Service - SaaS*", "*Plataform as a Service* - PaaS" e "*Infrastructure as a Service* - IaaS") e 4 modelos de implementação (Nuvem Privada, Nuvem Pública, Nuvem Híbrida e Nuvem de Comunidade).

Inserido no contexto do "IaaS", o armazenamento de dados em “nuvem” apresenta uma série de vantagens como flexibilidade, custo-benefício, confiabilidade e escalabilidade, mas tal tecnologia também possui riscos particulares como questões envolvendo privacidade e sigilo das informações, Sauber, El-Kafrawy, Shawish, Amin e Hagag (2021) destacam que proporcionalmente ao crescimento do número de pessoas que usam o serviço de computação em nuvem, cresce também o número de vazamentos de dados impetrados por agentes maliciosos, desafiando engenheiros e pesquisadores a buscarem melhores mecanismos de segurança para proteger dados confidenciais nestes ambientes. No entanto, em face das vantagens econômicas do uso da computação em nuvem para armazenamento de dados e sua adoção por organizações de tamanhos variados (ABUASLKISHIK et al., 2020), apresentam-se abordagens diferentes para mitigar os riscos e maximizar as vantagens competitivas de sua aplicação.

Shirvani, Rahmani e Sahafi (2017) argumentam que com a adoção da computação em nuvem, as despesas de capital (CAPEX) de custo fixo são transformadas em custos variáveis como despesas operacionais (OPEX), reduzindo assim o custo total de propriedade (TCO) e refletindo em benefício econômico, além de tornar as operações mais flexíveis e ágeis. No entanto, deve-se levar em conta os impactos financeiros gerados pelos riscos de um incidente, portanto é necessário escolher provedores de serviços capazes satisfazer os requisitos de segurança.

Segundo Sauber, El-Kafrawy, Shawish, Amin e Hagag (2021), uma estratégia de armazenamento de dados baseada em nuvem inclui flexibilidade e redução de custo frente à abordagem tradicional. Ainda, o texto indica que "um sistema de armazenamento em nuvem é composto por quatro camadas, ou seja, armazenamento físico, gerenciamento de infraestrutura, interface de aplicativo e acesso". Não obstante, outra questão relevante neste tipo de abordagem deve ser a questão do volume de dados e o tempo necessário para efetivar a recuperação das informações na ocorrência de um desastre, sendo também uma análise importante a viabilidade financeira de manter os dados armazenados frente aos impactos de uma ameaça que se concretiza.

Outro desafio em relação ao armazenamento de dados em nuvem é a garantia da confidencialidade dos dados, uma vez que o comprometimento de dados online cresce a cada

ano, garantir que os dados confidenciais de uma organização não serão acessados por terceiros não autorizados tornou-se uma questão prioritária para a continuidade dos negócios das corporações. Uma maneira de atingir este objetivo é o uso de criptografia simétrica de dados e criptografia assimétrica na garantia de identidade dos operadores do armazenamento (SAUBER; EL-KAFRAWY; SHAWISH; AMIN; HAGAG, 2021).

Este trabalho tem por objetivo identificar a bibliografia no contexto de serviços de "*Cloud Computing*" que apresente técnicas e estratégias que possibilitem maior resiliência por parte da infraestrutura das empresas e viabilizem a continuidade de negócios na ocorrência de um desastre. O artigo divide-se em cinco seções. A segunda trata da fundamentação teórica com uma visão panorâmica sobre computação em nuvem, resiliência e continuidade de negócios. A terceira seção apresenta a revisão sistemática da literatura. A quarta seção apresenta, de forma objetiva, os resultados obtidos na revisão sistemática e, por fim, a quinta seção apresenta as conclusões e considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta secção são conceituados os principais tópicos referenciados nos trabalhos selecionados na Revisão Sistemática da Literatura – RSL.

2.1 *Cloud Computing*

Segundo Yoo e Kim (2018) o surgimento do "*Cloud Computing*" deve-se à quarta revolução industrial (revolução digital) que possui como característica "a fusão de tecnologias que enfraquecem as barreias entre as esferas física e digital". Ainda o autor aponta que a computação em nuvem envolve diversas tecnologias como variedade de hardware, virtualização, computação distribuída e tecnologias de automação, fornecendo serviços customizáveis sob demanda.

Torres, Callou e Andrade (2018) definem computação em nuvem como um modelo de serviço que proporciona aos clientes um conjunto de serviços e recursos como rede, hardware, armazenamento, aplicativos com capacidade de ser escalável conforme as necessidades da corporação. Em seu texto, o autor aponta para o serviço de armazenamento como um tipo de serviço IaaS (Infraestrutura como serviço) capaz de oferecer versatilidade aos usuários por meio de funcionalidades como compartilhamento de conteúdo e execução de mídias.

Hamadah e Aqel (2019) em seu texto listam os diferentes modelos de serviços que os provedores de computação em nuvem fornecem em seus portifólios, elencando os seguintes modelos:

Infraestrutura como serviço (IaaS): "Serviço que fornece infraestrutura de computação, como servidores, armazenamento sistemas, switches, roteadores, máquinas virtuais, IP endereços, redes e sistema operacional";

Plataforma como serviço (PaaS): "Serviço que fornece uma plataforma e ambiente na nuvem que permite clientes para desenvolver e construir aplicativos. Isso também fornece as ferramentas adicionais, como banco de dados sistema de gestão, "analytics" e inteligência de negócios";

Software como serviço (SaaS): "Serviço que fornece um acesso a software e suas funções remotamente e os torna disponível para os clientes através da Internet. exemplos de SaaS são Facebook, Dropbox, Salesforce, Microsoft Office 365, e Tableau";

Recuperação de desastres como serviço (DRaaS). "Serviço de computação em nuvem e serviços de *backup* usados para ajudar organizações na proteção de aplicativos e dados contra as consequências destrutivas dos desastres, quer tenha sido como um incidente cibernético ou um desastre natural. Espera-se que este serviço obtenha recuperação rápida e permita que as organizações façam *backup* e recuperem seus ativos na nuvem". (HAMADAH; AQEL, 2019)

Shirvani, Rahmani e Sahafi (2017) lembram que além dos modelos de serviços, a computação em nuvem possui 5 características essenciais que trazem diversos benefícios:

- Autoatendimento sob demanda: "Pessoas físicas e as organizações podem usar os serviços de nuvem sob demanda e se beneficiar para reduzir seus custos";
- Amplo acesso à rede: "Os clientes podem se conectar à Internet para usar serviços em nuvem de diversos modos, até mesmo através de um celular qualquer usuários pode lançar mão dos serviços da computação em nuvem";
- Pool de recursos:" A computação em nuvem fornece uma gama recursos para usuários ou aplicativos. Além disso, reduz as despesas de operação com uma economia de escala";
- Elasticidade: "Na computação em nuvem pode-se aumentar ou diminuir os recursos alocados com base na necessidade do negócio."
- Monitoramento de consumo: "Os clientes podem monitor seus serviços ajudando a tomar futuras estratégias adequadas, poupando recursos financeiros".

(SHIRVANI; RAHMANI; SAHAFI, 2017)

2.2 Recuperação de Desastres (Disaster Recovery)

Prabantoro e Aji (2021) definem recuperação de desastre como o "processo de restauração ao seu estado original, de uma função em uma organização ou comunidade que foi danificada por um desastre". Os autores alertam que recuperação de desastres e continuidade de negócios estão intimamente ligados, sendo assim, é necessário um plano de prevenção e recuperação de desastres para preservar a continuidade do negócio e manter a competitividade. Ainda, os autores conceituam desastre como um evento imprevisível que pode gerar impactos negativos para a continuidade do negócio de uma organização, sendo que os desastres podem ser de causa humana, sistêmica ou natural.

Hamadah e Aqel (2019) defendem que a recuperação de desastres baseada em computação em nuvem é um serviço que permite o *backup* e recuperação de máquinas remotas, reduzindo os custos. No mesmo texto, desastre é descrito como "um evento inesperado com graves consequências para as organizações e com potencial de gerar perdas". Os autores alertam que as organizações devem estar preparadas para a incidência de desastres e manter um planejamento para recuperação. Em seu trabalho, destacam que a recuperação de desastres possui um ciclo no qual um planejamento bem feito é fundamental. Este ciclo apresenta quatro fases: mitigação, preparação, resposta e recuperação.

Mitigação: "Envolve etapas para eliminar ou reduzir vulnerabilidade aos impactos de desastres, como ferimentos, perda de vida e propriedade. Esta fase inclui edificações fortificadas e fortalecer a infraestrutura pública para reduzir os danos e destruição por certos eventos de perigo natural. O planejamento de mitigação envolve a organização de recursos; avaliação de riscos; desenvolvendo estratégias de mitigação, implementação e revisão de planos. Na fase de mitigação, o planejamento permite que os gerentes tomem boas decisões com base na identificação de perigos sólidos e dados de avaliação de risco para reduzir os riscos de perigos futuros";

Preparação: "Refere-se às atividades e programas que fornecem informações sobre como preparar melhor uma organização e uma para um desastre. Esses programas se concentram em entender como um desastre pode impactar a comunidade e como a educação, divulgação e treinamento poderia apoiar a resposta e recuperação de um desastre. Preparar-se para um desastre é uma função de pensar sobre a pior coisa que poderia possivelmente causar danos à sua organização";

Resposta: "Esta fase refere-se à reação imediata a um evento de desastre. Inclui salvar vidas e atender às necessidades humanitárias. Durante a fase de resposta, a organização inicia o processo retomando e retornando às operações enquanto se move da emergência inicial à recuperação do desastre e início da restauração dos serviços";

Recuperação: Esta fase refere-se à restauração de todos os aspectos do impacto do desastre e se concentra no retorno a algum senso de normalidade. O principal objetivo da recuperação é restaurar as funções menos sensíveis ao tempo para a operação na organização. A fase de recuperação do desastre pode ser dividida em dois períodos de fase, que são a fase de curto prazo e a fase de longo prazo. A fase de curto prazo normalmente envolve a entrega imediata de serviços a empresa. A fase de longo prazo refere-se a como uma organização finalmente coloca a si mesma e suas operações em funcionamento pleno". (HAMADAH; AQEL, 2019)

2.3 *Disaster Recovery as a Service* – DRaaS

Segundo Prabantoro e Aji (2021) recuperação de desastres como um serviço - DRaaS é um serviço de computação em nuvem que apresenta uma forma de serviço de *backup* desenhado para ajudar às organizações a manterem a disponibilidade dos sistemas frente a incidentes destrutivos, como ataques cibernéticos ou desastres naturais. Os autores explicam que o DRaaS pode restaurar sistemas de organizações com agilidade e pode ser usado como *backup* e recuperação de ativos organizacionais na nuvem. Neste momento, provedores como Microsoft Azure, Amazon, Google Cloud Platform e Alibaba Cloud já possuem serviços e modelos de DRaaS em seus portifólios.

2.4 RTO e RPO

Torres, Callou e Andrade (2018) esclarecem que o serviço de recuperação de desastres eficaz possui duas métricas principais, o objetivo de tempo de recuperação (RTO) e o objetivo do ponto de recuperação (RPO). Os autores argumentam que o RTO se refere a quanto tempo pode demorar para um recurso voltar online após a ocorrência de um incidente grave, em contraste, o RPO refere-se ao tempo máximo aceitável no qual os recursos podem

ficar indisponíveis. Defendem que o principal objetivo do plano de DR (desaster recovery) é minimizar o RPO e RTO.

2.5 Técnicas de Redundância

Segundo Araujo, Maciel, Andrade, Callou, Alves e Cunha (2018) "em vários domínios de aplicação, diferentes técnicas são adotadas para aumentar a confiabilidade dos sistemas. Essas técnicas são tradicionalmente classificadas em quatro grupos: prevenção de falhas, remoção de falhas, previsão de falhas, e tolerância a falhas". Ainda, os autores argumentam que "redundância" diz respeito a recursos ociosos que serão acionados na ocorrência de falhas para garantir a prestação do serviço. As técnicas de redundância para tolerância a falhas incluem:

- "active-standby" e "active-active redundancy".

Em um mecanismo de redundância "active-active", ambos os elementos estão permanentemente ativos. Os usuários não percebem a ocorrência de falhas, nem a ocorrência de degradação. Em contraste, os mecanismos de "active-standby" são caracterizados pela detecção de falhas seguida por ações de recuperação que requerem maior tempo de processamento. Este tipo de estratégia utiliza dois tipos de componentes: "Active and standby". O módulo "active" geralmente fornece o serviço para todos os ambientes; se o módulo "active" falhar, o componente de "standby" assume. Módulos de "standby" são classificados como quentes (hot), mornos (warm) ou frios (cold), dependendo do nível de restauração do serviço (ARAUJO; MACIEL; ANDRADE; CALLOU; ALVES; CUNHA, 2018).

2.6 Continuidade de Negócio.

Al-Shammari e Alwan (2018) definem continuidade de negócio como "uma metodologia usada para criar e validar um plano para manter as operações de negócios contínuas antes, durante e após desastres e eventos disruptivos". Argumentam que se trata de um gerenciamento dos elementos operacionais que permite que um negócio funcione normalmente para gerar receita, possuindo uma abordagem holística de um problema e ajudando a organização continuar com suas operações. Ainda os autores defendem que o plano de continuidade de negócio deve:

• Dar resposta imediata e adequada a emergências;

• Proteger vidas e garantir a segurança;

• Reduzir o impacto nos negócios;

• Retomar os serviços críticos de negócios;

• Trabalhar com fornecedores durante o período de recuperação;

• Reduzir a confusão durante um desastre;

• Assegurar a continuidade dos serviços empresariais;

• Obter “instalação e funcionamento” rapidamente após um desastre.

(AL-SHAMMARI; ALWAN, 2018)

3 MÉTODO

No esforço de construir uma pesquisa com metodologia clara e reproduzível, apontando trabalhos anteriores sobre o tema, elegeu-se a revisão sistemática da literatura como método para identificar os processos e técnicas existentes na literatura em relação a armazenamento de dados no contexto de *"Cloud Computing"* que possibilitem maior resiliência por parte da infraestrutura das empresas e viabilizem a continuidade de negócios. A Revisão Sistemática da Literatura está dividida em três partes:

- Planejamento: Identificação do intuito da revisão sistemática, proposta de revisão da bibliografia e protocolo da pesquisa;
- Execução: Identificação da fonte da pesquisa, extração dos dados, seleção e avaliação dos artigos;
- Síntese: Seleção final dos trabalhos, síntese dos resultados e conclusão.

3.1 Planejamento

O intuito desta seção é descrever o planejamento da revisão sistemática e suas etapas para lograr a identificação de estudos que possam auxiliar na resposta à questão da pesquisa:

- Quais são os processos e boas práticas em relação ao armazenamento de dados no contexto de *"Cloud Computing"* que possibilitem maior resiliência por parte da infraestrutura das empresas e favoreçam a continuidade de negócios?

Para responder tal questão, a pesquisa será dividida e analisada sob a perspectiva dos quatro elementos inerentes à RSL:

- População;
- Intervenção;
- Controle;
- Resultado esperado.

População: Interessados no uso de *"Cloud Computing"* para prover resiliência aos negócios.

Intervenção: Boas práticas em relação ao uso de *"Cloud Computing"* em relação ao armazenamento de dados.

Controle: Os estudos que serviram de apoio à revisão sistemática tiveram origem em uma pesquisa exploratória preliminar. A pesquisa exploratória foi realizada por meio de consulta bibliográfica de artigos publicados em conferências e disponíveis em bases de dados eletrônicas e baseou a escolha das palavras chaves, base de dados e período utilizados na revisão sistemática.

O quadro 1 apresenta os artigos utilizados na pesquisa exploratória e apoiaram o trabalho de revisão sistemática.

Artigos Utilizados na Pesquisa Exploratória		
Autores	**Títulos**	**Ano**
SAUBER, Amr M.; EL-KAFRAWY, Passent M.; SHAWISH, Amr F.; AMIN, Mohamed A.; HAGAG, Ismail M..	*A New Secure Model for Data Protection over Cloud Computing.*	2021
MCBRIDE, Timothy; EKSTROM, Michael; LUSTY, Lauren; SEXTON, Julian; TOWNSEND, Anne.	*Data Integrity: recovering from ransomware and other destructive events*	2020
ABUASLKISHIK, Abedallah Zaid	*Disaster Recovery in Cloud Computing Systems: An overview*	2020
KUMAR, Rajeev; BHATIA, M P s.	*A Systematic Review of the Security in Cloud Computing: data integrity, confidentiality and availability.*	2020
SHARMA, Yoshita; GUPTA, Himanshu; KHATRI, Sunil Kumar.	*A Security Model for the Enhancement of Data Privacy in Cloud Computing.*	2019
ROSS, Ron (org.)	*Risk management framework for information systems and organizations.*	2018
BHARADWAJ, Deepak R; BHATTACHARYA, Anamika; CHAKKARAVARTHY, Manivannan.	*Cloud Threat Defense – A Threat Protection and Security Compliance Solution.*	2018
Peter M. Mell and Timothy Grance	*The NIST Definition of Cloud Computing. Technical Report.*	2011

Quadro 1 – pesquisa exploratória

Resultado: Visão geral das ferramentas e boas práticas em relação boas práticas em relação ao uso de "*Cloud Computing"* para prover resiliência e continuidade de negócios.

Base de busca

Neste artigo foi selecionada a base de pesquisa "Scopus Digital Library", e assim foi possível centralizar a pesquisa em uma única ferramenta e ao mesmo tempo consultar as principais revistas e eventos científicos.

- Scopus Digital Library – endereço eletrônico: http://www.scopus.com .

Idioma dos artigos científicos

Nesta pesquisa foram selecionados somente artigos em **inglês**, porque a grande maioria trabalhos científicos é publicada neste idioma.

Palavras-Chave

Através da pesquisa exploratória, foram estabelecidas as seguintes palavras-chave para esta pesquisa:

- *Backup and Restore* (Inglês);
- *Business Resilience* (Inglês);
- *Business Continuity* (Inglês);
- *Business competitiveness* (Inglês);
- *Cloud Computing* (Inglês).

String de busca

As palavras-chave foram usadas em combinação com os operadores lógicos “and” e “or” para compor a “*string”* de busca usada na base de dados eletrônica:

> *(TITLE-ABS-KEY ("Cloud Computing" AND "Business Continuity") OR TITLE-ABS-KEY ("Backup" AND "Restore" AND "Cloud Computing") OR TITLE-ABS-KEY ("Cloud Computing" AND "Business Resilience") OR TITLE-ABS-KEY ("Business competitiveness" AND "Cloud Computing")) AND PUBYEAR > 2017 AND PUBYEAR > 2017*

Estratégia de busca para a identificação dos trabalhos

Busca automática

A pesquisa automática foi conduzida por meio da aplicação da string de busca na base selecionada, delimitando o período de 2017 a 2022. Tal escolha justifica-se diante da rápida evolução tecnológica, tornando períodos anteriores menos apropriados para a análise.

Critérios de inclusão e exclusão dos trabalhos

Com o objetivo de estabelecer limites à seleção dos artigos conforme sua relevância para esta pesquisa, foram estabelecidos critérios de inclusão e exclusão de textos.

Critérios de inclusão:

- Estudos que abordam competitividade de negócios e uso de *Cloud Computing*;
- Estudos que abordam proteção de dados e uso de *Cloud Computing*;
- Estudos que abordam resiliência de negócios e uso de *Cloud Computing*.

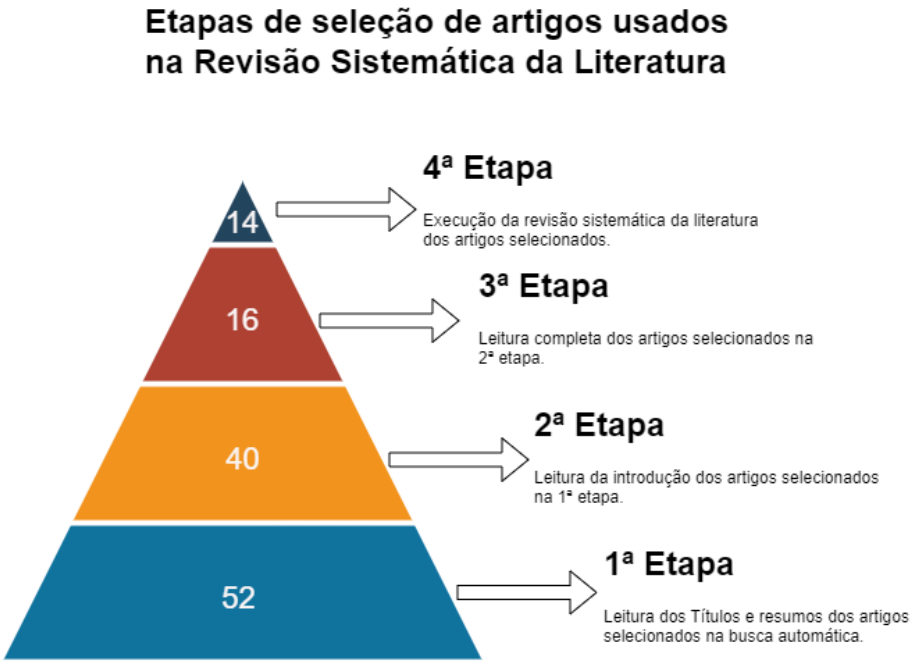
Critérios de exclusão:

- Estudos fora do contexto de *Cloud Computing*;
- Estudos que não estejam em inglês;
- Estudos não relacionados à resiliência ou continuidade de negócio;
- Estudos sem acesso livre ou gratuito;
- Estudos não relacionados à armazenamento de dados no contexto de *Cloud Computing*.

Estratégia para seleção dos trabalhos:

A estratégia de seleção ocorreu através de quatro etapas, na primeira foi realizada a leitura dos títulos e resumos dos artigos encontrados na busca automática (52) aplicando os critérios de identificação dos artigos estabelecidos. Em uma segunda etapa, foi realizada a leitura da introdução dos artigos que permaneceram após a primeira seleção (40), na terceira etapa foi feita a leitura completa dos artigos selecionados na segunda etapa (16) e por fim foi realizada a seleção dos artigos que compõe a revisão sistemática (14). A figura 1 ilustra as etapas da seleção.

Figura 1 – Etapas da RSL



Fonte: autor

4 RESULTADOS – ARTIGOS SELECIONADOS

Ao longo da pesquisa realizada foram encontrados 52 artigos com a seguinte distribuição anual, dentre os quais 15 trabalhos em 2018, 8 trabalhos em 2019, 9 trabalhos em 2020, 15 trabalhos em 2021 e 5 trabalhos em 2022.

Após a aplicação dos critérios definidos no protocolo, foram selecionados 14 trabalhos, sendo publicados 7 artigos em 2018, 4 artigos em 2019, 1 artigo em 2020 e 2 artigos em 2021.

4.1 Análise dos Artigos Selecionados

Mediante os resultados da pesquisa, esta seção tem o objetivo de realizar uma síntese geral e resumida dos estudos encontrados e selecionados segundo os critérios de

identificação e tecer considerações sobre os resultados observados nos trabalhos selecionados.

Al-Shammari e Alwan (2018) abordam a necessidade de um framework prático de Recuperação de Desastres (DR) fundamentado em multi-nuvem, visando a minimização dos custos de *backup* e a redução do risco de perda de dados. Os autores destacam pontos importantes para obtenção deste objetivo. Segundo o texto alguns serviços como Banco de Dados em Nuvem são adotados para otimizar os custos de armazenamento em ambientes de Tecnologia da Informação (TI), proporcionando benefícios como a acessibilidade aos dados por meio da internet.

Ainda são apresentadas estratégias como a utilização "Multi-Nuvens" em detrimento do uso de nuvem única. O argumento apresentado é que a transição de uma única nuvem para um ambiente multi-nuvens é crucial por diversas razões, pois os serviços em nuvem única estão suscetíveis a interrupções que impactam a disponibilidade dos serviços. Em cenários de desastre, uma única nuvem pode incorrer em perda parcial ou total de dados.

Outro aspecto importante do artigo é a abordagem sobre recuperação de desastres (DR) na Nuvem. O artigo argumenta que ao empregar a recuperação de desastres na nuvem, os recursos de múltiplos provedores de serviços em nuvem podem ser coordenados pelo provedor de serviços de DR e propõe um framework com o objetivo assegurar a disponibilidade contínua de dados, alcançando elevada confiabilidade, custos de *backup* reduzidos e recuperação ágil, garantindo a continuidade das operações empresariais antes, durante e após um incidente de desastre.

Shirvani, Rahmani e Sahafi (2017) apresentam uma estrutura matemática para apoiar a tomada de decisões no contexto de migração para a Computação em Nuvem na indústria de Tecnologia da Informação, considerando o modelo de computação em nuvem economicamente mais viável em comparação com a implantação local. No entanto, preocupações com segurança, privacidade e confiabilidade têm sido limitantes importantes na adoção generalizada deste paradigma pelas organizações. O artigo propõe um modelo de decisão focado em custo e segurança, especialmente em Acordos de Nível de Serviço (SLA) que abrangem vetores como preço, disponibilidade, integridade e confidencialidade.

Os desafios discutidos no texto incluem o risco associado a serviços críticos, a dependência de um único provedor de nuvem e variações na qualidade de serviço e segurança entre diferentes provedores. Diante de tais considerações, um ambiente multi-nuvem é proposto, integrando serviços de vários provedores. O artigo aplica então o modelo a um estudo de caso real, avaliando opções para investir em infraestrutura de TI no local ou terceirizar serviços de TI em um ambiente de *multicloud*. O texto conclui destacando a dependência da aplicabilidade do modelo em fatores como tamanho da organização, criticidade, cultura, ambiente e questões políticas.

Em seu artigo, Mendonca, Lima, Queiroz, Andrade e Kim (2019) abordam a relevância das soluções de Recuperação de Desastres (Disaster Recovery - DR) em ambientes de *Backup*-as-a-Service - BaaS para empresas contemporâneas de Tecnologia da Informação (TI). Enfatiza-se a necessidade crítica de manter uma infraestrutura de TI operacional 24 horas por dia, sete dias por semana, devido aos riscos financeiros substanciais associados a interrupções no sistema. Apesar da importância das soluções de DR, observa-se que essas soluções podem ser onerosas, especialmente para pequenas e médias empresas (PMEs).

O estudo propõe a aplicação de Modelos para avaliar um ambiente real de BaaS em relação a métricas-chave de recuperação de desastres, como Objetivo de Tempo de Recuperação (RTO), Objetivo de Ponto de Recuperação (RPO), disponibilidade e tempo de inatividade. A conclusão do texto destaca as contribuições do estudo, incluindo uma abordagem de modelo-experimento para a avaliação de soluções de Disaster Recovery e uma análise para identificação de componentes críticos.

Torres, Callou e Andrade (2018) destacam a importância dos serviços de armazenamento em nuvem, destacando sua função como Infraestrutura como Serviço (IaaS). Esses serviços oferecem sincronização de pastas, reprodução de mídia, sincronização de dispositivos e envio de e-mail. Indicam ainda que a alta disponibilidade e desempenho são cruciais para garantir a continuidade de negócios e serviços públicos ininterruptos. O estudo propõe uma abordagem hierárquica, combinando análise de disponibilidade e desempenho para serviços de armazenamento em nuvem privada. A abordagem hierárquica proposta visa auxiliar na construção de ambientes de armazenamento em nuvem eficientes e econômicos.

Araujo, Maciel, Andrade, Callou, Alves e Cunha (2018) destacam a importância da tomada de decisões eficientes na escolha de infraestruturas de computação em nuvem, ressaltando a necessidade de equilibrar confiabilidade e custo. Ainda, os autores apontam os desafios enfrentados pelas empresas ao oferecer serviços em nuvem que atendam às necessidades dos clientes, considerando parâmetros como confiabilidade, disponibilidade e custo. Não obstante, alertam que estratégias de redundância são cruciais para evitar interrupções. A discussão sobre técnicas de redundância destaca a tolerância a falhas como uma abordagem fundamental para garantir a entrega correta de serviços, mesmo na presença de falhas. As estratégias de redundância ativa-ativa (*active-active*) e ativa-espera (*active-standby*) são explicadas em detalhes, destacando suas características e aplicações específicas.

Outro aspecto importante abordado no texto refere-se à tomada de decisão, reconhecendo a importância de avaliar simultaneamente diferentes alternativas ao considerar compromissos de longo prazo e alocação de orçamento. O artigo explora a modelagem e avaliação de confiabilidade de sistemas, destacando conceitos como confiabilidade, disponibilidade e capacidade.

Em resumo, o texto oferece uma visão abrangente sobre a importância da tomada de decisões eficientes na escolha de infraestruturas de computação em nuvem, enfatizando a necessidade de equilibrar critérios como confiabilidade e custo.

Em seu artigo, Yoo e Kim (2018) abordam a transformação digital em empresas durante a 4ª revolução industrial, destacando o surgimento de tecnologias que apoiaram tal transformação. Os autores indicam fatores críticos e determinantes para a adoção da computação em nuvem, explorando relações entre confiança, capacidade técnica, capacidade gerencial e desempenho de implantação na nuvem e indicam que a “Expertise” e “disponibilidade” do fornecedor é crucial para os clientes, enquanto a visão de longo prazo é essencial para os provedores.

Ainda os autores argumentam que a confiança e relacionamento com fornecedores são fundamentais para a decisão de adoção do modelo de computação em nuvem e que a posição competitiva relativa, visão de longo prazo, comprometimento de recursos, incentivo governamental, lei e política são fatores-chave na decisão de adotar a computação em nuvem, influenciando a competitividade durante a transformação digital.

Rajasingh e Wesley (2020) esclarecem a distinção entre virtualização e computação em nuvem, destacando a frequente utilização desses termos de maneira intercambiável. Os autores ressaltam o crescente interesse das organizações na adoção da nuvem e a importância de os gerentes de projeto considerarem cuidadosamente essa transição em vez de manterem uma infraestrutura virtualizada. Ainda, o texto destaca fatores críticos, como redução de despesas de capital, custos operacionais, custo total de propriedade e disponibilidade de infraestrutura, como elementos essenciais na tomada de decisão. Ainda os autores comparam as vantagens da virtualização, focada na eficiência dos recursos de TI, com as da computação em nuvem que oferecem flexibilidade e escalabilidade.

Uma análise de custo-benefício é apresentada, comparando virtualização e nuvem em termos de custo total de propriedade (TCO) e utilização de despesas. No artigo recomenda-se a nuvem quando há um elevado número de instâncias de servidor e a necessidade de provisionamento em tempo real, visando um maior retorno sobre o investimento e a redução do custo total de propriedade. Diversos provedores de nuvem, como VMware, IBM Cloud, Amazon Web Services e Google Cloud Platform, são mencionados como opções para auxiliar os gerentes de projeto na avaliação da migração para a nuvem. A conclusão destaca que a virtualização é eficaz para consolidar funcionalidades de hardware, reduzindo custos e aumentando a eficiência. Por sua vez, a computação em nuvem automatiza amplamente tarefas operacionais, embora o software de nuvem possa ser caro e complexo, representando um desafio adicional para os gerentes de projeto.

Mendonca, Lima, Matos, Ferreira e Andrade (2018) abordam a avaliação da disponibilidade de soluções de recuperação de desastres (DR) por meio da aplicação de modelos estocásticos e experimentos de injeção de falhas. Considerando a imperatividade de operações ininterruptas nas organizações de Tecnologia da Informação (TI). Argumentam que com a crescente popularidade da computação em nuvem, as soluções de recuperação de desastres baseadas nesse modelo têm adquirido destaque.

O artigo propõe uma abordagem integrada de experimento de modelo, utilizando redes de Petri estocásticas (SPNs) e experimentos de injeção de falhas para avaliar métricas de disponibilidade, incluindo disponibilidade em estado estacionário e tempo de inatividade. Os autores argumentam que diversas soluções de DR baseadas em nuvem, como *active-active* e *active-standby*, são modeladas e analisadas para demonstrar a viabilidade da abordagem. No entanto, os autores ressaltam que as soluções de DR não são economicamente acessíveis, especialmente devido ao investimento associado e à raridade de ocorrência de desastres. Destaca-se a urgência de soluções que sejam não apenas eficientes, mas também economicamente viáveis, considerando a importância de estabelecer, testar e implementar tais medidas. Enfatiza-se que não existe uma solução "à prova de falhas" que elimine todas as vulnerabilidades, destacando a importância de uma avaliação criteriosa da solução adotada para garantir a continuidade dos negócios e evitar gastos desnecessários.

O artigo também destaca o aumento da popularidade das soluções de DR baseadas em nuvem, atribuindo isso à escalabilidade, baixo custo e alta disponibilidade oferecidos por provedores de nuvem. O serviço de recuperação de desastres em ambientes de nuvem é considerado crucial para a sobrevivência das empresas, devido à necessidade de manter os serviços de TI em operação sem interrupções.

Em seu artigo, Shahzadi, Ubakanma, Iqbal e Dagiuklas (2018) descrevem uma solução de serviço de nuvem para o gerenciamento de recuperação de desastres, visando reduzir o tempo de inatividade e os custos associados a interrupções de serviços em caso de

desastres. A abordagem da solução inclui a migração de infraestrutura como serviço (IaaS) de uma nuvem para outra sem perturbar os negócios, incorporando um mecanismo de seleção de *host on-the-fly* para implantar funções de rede virtual em hosts alternativos em caso de indisponibilidade. O objetivo é garantir alta disponibilidade de serviços durante situações de desastre, reduzindo despesas e proporcionando uma maneira eficiente de acessar dados durante a recuperação.

Ao longo do artigo, os autores destacam que para otimizar a recuperação, a solução propõe a implementação de um modelo de recuperação multi-nuvem, gerenciando recursos de vários provedores de nuvem. Também visa reduzir os tempos de espera de recuperação, utilizando matrizes como objetivo de tempo de recuperação (RTO) e ponto de recuperação objetivo (RPO). Estratégias como a orquestração centralizada de serviços e a replicação na nuvem são mencionadas como meios de aprimorar essas métricas. Além disso, o texto aborda a otimização do tráfego de serviço para manter o tempo de recuperação e as perdas de dados baixos, enquanto minimiza os custos. O uso de Apache libcloud de código aberto para otimização em tempo real, gerenciamento entre nuvens e balanceamento de carga é mencionado como parte do conceito.

Por fim, o artigo destaca a importância do *backup* como serviço, utilizando conceitos como *Hot Backup Site*, *Warm Backup Site* e *Cold Backup Site*. A orquestração *multi-cloud broker* e arquiteturas de nuvem de operadora são apontadas como desempenhando um papel crescente na oferta de *backup* como serviço, garantindo que os clientes possam recuperar não apenas sua infraestrutura e serviços em nuvem, mas também tenham acesso confiável a recursos de dados de *backup* durante desastres naturais.

Segundo Prabantoro e Aji (2021), existe uma crescente necessidade de sistemas de informação e tecnologia da informação nas organizações, destacando a importância da proteção e manutenção de dados confidenciais para garantir a sustentabilidade. Os autores apresentam o caso do Instituto de Agama Islam Negeri (IAIN) Manado, uma universidade com diversos alunos que enfrenta problemas em seu sistema de informações, como perda de dados e inatividade. Para mitigar esses problemas, a pesquisa propõe a implementação de um Plano de Recuperação de Desastres (DRP) com duas estratégias baseadas em *Disaster Recovery as a Service* (DRaaS) em um serviço de nuvem pública (Microsoft Azure) para ajudar a garantir a disponibilidade de seus sistemas.

Ao longo do texto, o artigo descreve o DRaaS como uma solução eficaz para recuperação de desastres, eliminando a necessidade de dispositivos adicionais e permitindo o acesso remoto pela internet. Segundo os autores a proposta de utilizar a computação em nuvem visa reduzir custos de TI, oferecer serviços gerenciados, aumentar a segurança dos dados e facilitar o *backup* e recuperação. Além disso, destaca-se que o DRaaS não apenas auxilia na recuperação rápida após eventos destrutivos, mas também serve como *backup* e recuperação de ativos organizacionais na nuvem que grandes provedores de serviços de computação em nuvem, como Microsoft Azure, Amazon Web Service, Google Cloud Platform e Alibaba Cloud, já oferecem serviços especializados de DRaaS garantidos em sua implementação.

Hamadah e Aqel (2019) destacam a importância das estratégias de recuperação de desastres na tecnologia da informação, com ênfase nas abordagens baseadas em nuvem. Propõe o Plano de Recuperação Preventiva de Desastres com Réplica Mínima (PRPMR) como uma solução única de réplica para garantir alta disponibilidade de dados. Detalha o ciclo de desastre em quatro fases e destaca a necessidade de segurança na computação em

nuvem, explorando o serviço de Recuperação de Desastres como Serviço (DRaaS) como uma tecnologia crucial na nuvem.

Ao longo do artigo, os autores ressaltam a importância da continuidade dos negócios ao optar por sistemas primários na nuvem e apresentam a DRaaS como essencial para proteger serviços e dados contra desastres. Concluem enfatizando que as estratégias baseadas em nuvem alcançaram eficiência superior, com disponibilidade de dados, escalabilidade, economia financeira e resposta mais rápida em comparação com o modelo convencional de recuperação de desastres.

Solis, Shashidhar e Varol (2021) abordam as diretrizes e estruturas atuais para recuperação de desastres no contexto de pequenas e médias empresas, propondo a introdução de uma nova estrutura que permite a essas empresas, mitigar riscos e retomar atividades pós-desastre, com ênfase em soluções de armazenamento em nuvem. Os autores destacam a importância de melhorar a mitigação de riscos e esforços de recuperação para pequenas e médias empresas, considerando o orçamento operacional incerto e a gestão muitas vezes familiar. Ainda sugerem melhorias, como a implementação de comandos SSH, o uso de servidores FTP como locais de armazenamento alternativos e a programação de *backup*s em horários específicos.

Por fim, propõe a redução de riscos por meio de um modelo de virtualização e a apresentação de uma abordagem única para *backup* e recuperação de imagens do sistema na nuvem, tornando essas soluções acessíveis e eficazes para pequenos negócios.

Artur ROT (2018), em seu artigo, aborda questões e desafios de segurança de dados e serviços em ambientes de computação em nuvem. O autor destaca a transferência de riscos para provedores externos, reconhecendo que, embora mais seguro, o controle sobre recursos de TI é reduzido. Ainda Identifica riscos em disponibilidade, segurança de dados e compatibilidade, destacando a segurança e privacidade como áreas críticas e aponta a importância da gestão de riscos e conformidade legal na adoção da nuvem, enfatizando a necessidade de conhecer normas e regulamentos.

Não obstante, o texto apresenta uma discussão sobre barreiras mentais e técnicas à adoção da computação em nuvem por empresas e conclui enfatizando a importância de abordar preocupações de segurança e sugere soluções tecnológicas, organizacionais e legais.

Em resumo, o artigo oferece uma análise abrangente dos desafios de segurança na adoção da computação em nuvem, ressaltando a necessidade de abordagens multifacetadas para uma transição segura, destacando a necessidade contínua de conscientização e educação sobre os benefícios e desafios da computação em nuvem.

Amron, Ibrahim, Bakar e Chuprat (2019) abordam os fatores que impactam a aceitação da computação em nuvem nas organizações, destacando flexibilidade, economia e escalabilidade como benefícios. Ainda destacam os desafios que incluem segurança de dados, custos iniciais e dependência de provedores, enfatizando o modelo do NIST que define a computação em nuvem como acesso sob demanda a recursos compartilhados.

Os autores exploram benefícios econômicos e destacam 22 fatores influenciadores na adoção da computação em nuvem, introduzindo três novos: experiência externa, experiências do usuário e continuidade de negócios. Por fim, ressaltam as preocupações específicas de organizações e a promissora, mas complexa, adoção da computação em nuvem, incentivando futuras pesquisas aprofundadas.

4.2 Extrato da Análise dos Artigos Selecionados

A presente revisão sistemática da literatura contém estudos sobre a computação em nuvem e seus desdobramentos, abordando questões como recuperação de desastres, migração, segurança e tomada de decisões. Os estudos variam em enfoques, desde a recuperação de desastres até a aceitação da computação em nuvem como paradigma para o ambiente de tecnologia da informação nas organizações.

Ao longo dos trabalhos selecionados, diferentes estratégias, como ambientes multi-nuvem, modelos de decisão, e soluções específicas para setores (BaaS em PMEs) são apresentadas. Muitas vezes são destacados os desafios que incluem segurança, custos e dependência de provedores. A necessidade de abordagens personalizadas, a importância da tomada de decisões eficientes, e a busca por soluções economicamente viáveis permeiam os estudos. Os diversos estudos abordam questões cruciais relacionadas à implementação e gestão de serviços em nuvem, especialmente no contexto de Recuperação de Desastres (DR) e Continuidade de Negócios.

Os autores Al-Shammari e Alwan (2018) propõem um framework baseado em multi-nuvem para DR, visando minimizar custos de backup e ressaltando a importância de serviços em nuvem, como Bancos de Dados, na otimização de custos de TI. Shirvani, Rahmani e Sahafi (2017) apresentam um modelo matemático para a tomada de decisões na migração para a nuvem, enfocando custos e segurança, introduzindo o conceito de ambiente multi-nuvem para superar desafios como dependência de provedores. Já Mendonca, Lima, Queiroz, Andrade e Kim (2019) destacam a relevância das soluções de DR em ambientes de Backup-as-a-Service (BaaS), propondo modelos para avaliar métricas-chave de recuperação de desastres.

Torres, Callou e Andrade (2018) salientam a importância dos serviços de armazenamento em nuvem como Infraestrutura como Serviço (IaaS), propondo uma abordagem hierárquica para análise de disponibilidade e desempenho. Araujo, Maciel, Andrade, Callou, Alves e Cunha (2018) exploram estratégias de redundância na escolha de infraestruturas de computação em nuvem, destacando a importância da tomada de decisão e modelos de avaliação de confiabilidade.

Yoo e Kim (2018) abordam a transformação digital nas empresas, enfatizando a confiança nos fornecedores e a visão de longo prazo como determinantes para a adoção da computação em nuvem. Rajasingh e Wesley (2020) esclarecem a distinção entre virtualização e nuvem, realizando uma análise de custo-benefício e recomendando a nuvem em cenários específicos. Os estudos também abordam a disponibilidade de soluções de DR baseadas em nuvem, utilizando modelos estocásticos e experimentos de injeção de falhas (Mendonca, Lima, Matos, Ferreira e Andrade, 2018), bem como soluções de nuvem para gerenciamento de recuperação de desastres, visando reduzir tempo de inatividade e custos associados (Shahzadi, Ubakanma, Iqbal e Dagiuklas, 2018).

Outras contribuições incluem propostas de Planos de Recuperação de Desastres baseados em Disaster Recovery as a Service (DRaaS) para instituições específicas, como uma universidade (Prabantoro e Aji, 2021) e estratégias de recuperação de desastres baseadas em nuvem, como o Plano de Recuperação Preventiva de Desastres com Réplica Mínima (PRPMR) (Hamadah e Aqel, 2019).

Por fim, a abordagem de segurança na adoção da computação em nuvem é destacada por ROT (2018), enfocando desafios como a transferência de riscos para provedores externos e a importância da gestão de riscos. Amron, Ibrahim, Bakar e Chuprat (2019) investigam os fatores que impactam a aceitação da computação em nuvem nas organizações, explorando benefícios econômicos e identificando 22 fatores influenciadores. Cada artigo contribui para uma compreensão mais ampla dos desafios e benefícios associados à adoção da computação em nuvem em diversas áreas.

1) ***Disaster Recovery and Business Continuity for Database Services in Multi-Cloud*; Al-Shammari e Alwan (2018)** propõem um framework de Recuperação de Desastres (DR) baseado em multi-nuvem para minimizar custos de *backup*. Destacam a importância de serviços em nuvem, como Bancos de Dados, para otimizar custos em ambientes de TI.

2) ***An iterative mathematical decision model for cloud migration: A cost and security risk approach*; Shirvani, Rahmani e Sahafi (2017)** apresentam uma estrutura matemática para a tomada de decisões na migração para a CC, focando em custos e segurança. Introduzem o conceito de ambiente multi-nuvem para superar desafios como dependência de provedores e variações na qualidade de serviço.

3) ***Evaluation of a Backup-as-a-Service Environment for Disaster Recovery*; Mendonca, Lima, Queiroz, Andrade e Kim (2019)** destacam a importância das soluções de Recuperação de Desastres (DR) em ambientes de *Backup*-as-a-Service (BaaS). Propõem modelos para avaliar métricas-chave de recuperação de desastres.

4) ***A hierarchical approach for availability and performance analysis of private cloud storage services*; Torres, Callou e Andrade (2018)** salientam a importância dos serviços de armazenamento em nuvem como Infraestrutura como Serviço (IaaS), propondo uma abordagem hierárquica para análise de disponibilidade e desempenho.

5) ***Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models*; Araujo, Maciel, Andrade, Callou, Alves e Cunha (2018)** exploram estratégias de redundância na escolha de infraestruturas de computação em nuvem, destacando a importância da tomada de decisão e modelos de avaliação de confiabilidade.

6) ***A decision-making model for adopting a cloud computing system*; Yoo e Kim (2018)** abordam a transformação digital nas empresas e os fatores críticos para a adoção da CC, enfatizando a confiança nos fornecedores e a visão de longo prazo como determinantes.

7) ***Step into the cloud or stop with virtualization - The project manager's dialectic dilema*; Rajasingh e Wesley (2020)** esclarecem a distinção entre virtualização e CC, destacando fatores críticos na tomada de decisão. Realizam uma análise de custo-benefício entre virtualização e CC, recomendando a CC em cenários específicos.

8) ***Availability Analysis of a Disaster RecoverySolution through Stochastic Models and FaultInjection Experiments*; Mendonca, Lima, Matos, Ferreira e Andrade (2018)** avaliam a disponibilidade de soluções de DR baseadas em nuvem, utilizando modelos estocásticos e experimentos de injeção de falhas. Destacam a necessidade de soluções economicamente viáveis.

9) ***Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies during Disaster Recovery***; **Shahzadi, Ubakanma, Iqbal e Dagiuklas (2018)** descrevem uma solução de nuvem para gerenciamento de recuperação de desastres, visando reduzir tempo de inatividade e custos associados. Enfatizam a importância do *backup* como serviço (BaaS).

10) ***Cloud Computing Implementation to Support a Disaster Recovery Plan: A Case Study of Institut Agama Islam Negeri Manado*; Prabantoro e Aji (2021)** propõem um Plano de Recuperação de Desastres (DRP) baseado em *Disaster Recovery as a Service* (DRaaS) para uma universidade, destacando a importância da computação em nuvem na proteção de dados.

11) ***A Proposed Virtual Private Cloud-Based Disaster Recovery Strategy*; Hamadah e Aqel (2019)** destacam estratégias de recuperação de desastres baseadas em nuvem, propondo o Plano de Recuperação Preventiva de Desastres com Réplica Mínima (PRPMR) como uma solução única de réplica.

12) ***A Novel Risk Mitigation & Cloud-Based Disaster Recovery Framework for Small to Medium Size Businesses*; Solis, Shashidhar e Varol (2021)** propõem melhorias para recuperação de desastres em pequenas e médias empresas, enfatizando soluções de armazenamento em nuvem para mitigação de riscos.

13) ***Data and Services Security Issues and Challenges in Cloud Computing Environments*;** Artur ROT (2018) aborda desafios de segurança na adoção da CC, destacando a transferência de riscos para provedores externos e a importância da gestão de riscos.

14) ***Determining Factors Influencing the Acceptance of Cloud Computing Implementation*; Amron, Ibrahim, Bakar e Chuprat (2019)** investigam os fatores que impactam a aceitação da CC nas organizações, explorando benefícios econômicos e identificando 22 fatores influenciadores, incluindo três novos: experiência externa, experiências do usuário e continuidade de negócios.

5 CONCLUSÃO

Este artigo de revisão sistemática da literatura proporcionou uma visão geral das boas práticas em relação ao uso de "*Cloud Computing*", destacando a relevância da revisão sistemática como ferramenta essencial em projetos de pesquisa.

No esforço de responder à pergunta da pesquisa (Quais são os processos e boas práticas em relação ao armazenamento de dados no contexto de *"Cloud Computing"* que possibilitem maior resiliência por parte da infraestrutura das empresas e favoreçam a continuidade de negócios?), a análise dos resultados revelou o notável empenho da comunidade científica no apontamento do uso viável da computação em nuvem, destacando os desafios inerentes desta tecnologia.

Ainda que existam cuidados no uso da computação em nuvem, a franca maioria dos autores selecionados na pesquisa destaca as vantagens do uso da computação em nuvem, como por exemplo a possibilidade da implementação do *Disaster Recovery as a Service* (DRaaS), incrementando de forma significativa a segurança dos dados das organizações. Outro aspecto relevante levantado ao longo da pesquisa é o provimento da continuidade e competitividade dos negócios através da computação em nuvem, desfrutando dos benefícios como flexibilidade e custo sob demanda para infraestrutura de TI.

Entretanto, a pesquisa levantou aspectos gerais sobre boas práticas em relação ao uso de "*Cloud Computing"* para provimento de resiliência e continuidade de negócios, ainda há um vasto campo de pesquisa na exploração e mensuração de tais apontamentos.

Como perspectiva para trabalhos futuros, sugere-se aprofundar o processo proposto e realizar estudos empíricos para mensurar sua efetividade, realizando estudo comparativo entre a utilização de nuvem híbrida e infraestrutura local, ainda há a possibilidade da realização do comparativo entre diferentes nuvens públicas mediante o estabelecimento de um plano de *Disaster Recovery as a Service*.

REFERÊNCIAS BIBLIOGRÁFICAS

ABUASLKISHIK, Abedallah Zaid et al. ***Disaster Recovery in Cloud Computing Systems: an overview***. International Journal of Advanced Computer Science and Applications. Cleckheaton, v. 11, n. 9, p. 702-710. jan. 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110984.

AL-SHAMMARI, Mohammad Matar; ALWAN, Ali Amer**.** ***Disaster Recovery and Business Continuity for Database Services in Multi-Cloud***. 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, p. 1-8, abr. 2018. IEEE. http://dx.doi.org/10.1109/cais.2018.8442005.

AMRON, Mohd Talmizie; IBRAHIM, Roslina; BAKAR, Nur Azaliah Abu; CHUPRAT, Suriayati. ***Determining Factors Influencing the Acceptance of Cloud Computing Implementation***. Procedia Computer Science, v. 161, p. 1055-1063, 2019. Elsevier BV. http://dx.doi.org/10.1016/j.procs.2019.11.216.

ARAUJO, Julian; MACIEL, Paulo; ANDRADE, Ermeson; CALLOU, Gustavo; ALVES, Vandi; CUNHA, Paulo. ***Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models***. Journal of Cloud Computing, London, Uk, v. 7, n. 1, p. 1-19, 27 mar. 2018. Springer Science and Business Media LLC. http://dx.doi.org/10.1186/s13677-018-0106-7.

Artur ROT, ***Data and Services Security Issues and Challenges in Cloud Computing Environments***, World Multi-Conference on Systemics, Cybernetics and Informatics, 2018.

BHARADWAJ, Deepak R; BHATTACHARYA, Anamika; CHAKKARAVARTHY, Manivannan. ***Cloud Threat Defense – A Threat Protection and Security Compliance Solution***. 2018 IEEE International Conference on Cloud Computing In Emerging Markets (Ccem), Bangalore, p. 1-5, nov. 2018. IEEE. http://dx.doi.org/10.1109/ccem.2018.00024.

HAMADAH, Siham; AQEL, Darah. ***A Proposed Virtual Private Cloud-Based Disaster Recovery Strategy***. 2019 IEEE Jordan International Joint Conference On Electrical Engineering And Information Technology (JEEIT), Amman, Jordan, p. 1-5, abr. 2019. IEEE. http://dx.doi.org/10.1109/jeeit.2019.8717404.

KUMAR, Rajeev; BHATIA, M P s. ***A Systematic Review of the Security in Cloud Computing: data integrity, confidentiality and availability***. 2020 IEEE International Conference On Computing, Power And Communication Technologies (Gucon), New Delhi, p. 1-4, 2 out. 2020. IEEE. http://dx.doi.org/10.1109/gucon48875.2020.9231255.

MCBRIDE, Timothy; EKSTROM, Michael; LUSTY, Lauren; SEXTON, Julian; TOWNSEND, Anne. ***Data Integrity: recovering from ransomware and other destructive events***. NIST Special Publication 1800-11, Gaithersburg, p. 1-454, 22 set. 2020. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.1800-11.

MENDONCA, Julio; LIMA, Ricardo; MATOS, Rubens; FERREIRA, Joao; ANDRADE, Ermeson. ***Availability Analysis of a Disaster Recovery Solution Through Stochastic Models and Fault Injection Experiments***. 2018 IEEE 32Nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, p. 135-142, maio 2018. IEEE. http://dx.doi.org/10.1109/aina.2018.00032.

MENDONCA, Julio; LIMA, Ricardo; QUEIROZ, Ewerton; ANDRADE, Ermeson; KIM, Dong Seong. ***Evaluation of a Backup-as-a-Service Environment for Disaster Recovery***. 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, p. 1-6, jun. 2019. IEEE. http://dx.doi.org/10.1109/iscc47284.2019.8969658.

PETER M. Mell and TIMOTHY Grance. 2011. ***SP 800-145. The NIST Definition of Cloud Computing***. Technical Report. National Institute of Science and Technology.

PRABANTORO, Rifqi; AJI, Rizal Fathoni. ***Cloud Computing Implementation to Support a Disaster Recovery Plan: a case study of Institut Agama Islam Negeri Manado***. 2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE), Bandar Lampung, Indonesia, p. 112-117, 27 out. 2021. IEEE. http://dx.doi.org/10.1109/iccteie54047.2021.9650632.

RAJASINGH, Jebaraj s J; WESLEY, J. Reeves. ***Step into the Cloud or Stop with Virtualization – The Project Manager's Dialectic Dilemma***. Procedia Computer Science, Chennai, India, v. 172, n. 0, p. 1077-1083, 2020. Elsevier BV. http://dx.doi.org/10.1016/j.procs.2020.05.157.

ROSS, Ron (org.). ***Risk management framework for information systems and organizations***. NIST Special Publication 800-37, Gaithersburg, v. 183, dez. 2018. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-37r2.

SAUBER, Amr M.; EL-KAFRAWY, Passent M.; SHAWISH, Amr F.; AMIN, Mohamed A.; HAGAG, Ismail M.. ***A New Secure Model for Data Protection over Cloud Computing***. Computational Intelligence and Neuroscience, London, v. 2021, p. 1-11, 24 nov. 2021. Hindawi Limited. http://dx.doi.org/10.1155/2021/8113253.

SHAHZADI, Sonia; UBAKANMA, George; IQBAL, Muddesar; DAGIUKLAS, Tasos. ***Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies During Disaster Recovery***. 2018 IEEE 20Th International Conference On High Performance Computing And Communications; IEEE 16Th International Conference On Smart City; IEEE 4Th International Conference On Data Science And Systems (Hpcc/Smartcity/Dss), London, UK, p. 1048-1053, jun. 2018. IEEE. http://dx.doi.org/10.1109/hpcc/smartcity/dss.2018.00174.

SHARMA, Yoshita; GUPTA, Himanshu; KHATRI, Sunil Kumar. ***A Security Model for the Enhancement of Data Privacy in Cloud Computing***. 2019 Amity International Conference On Artificial Intelligence (AICAI), Dubai, p. 1-5, fev. 2019. IEEE. http://dx.doi.org/10.1109/aicai.2019.8701398.

SHIRVANI, Mirsaeid Hosseini; RAHMANI, Amir Masoud; SAHAFI, Amir. ***An iterative mathematical decision model for cloud migration: a cost and security risk approach***. Software: Practice and Experience, v. 48, n. 3, p. 449-485, 13 set. 2017. Wiley. http://dx.doi.org/10.1002/spe.2528.

SOLIS, Roberto; SHASHIDHAR, Narasimha; VAROL, Cihan. ***A Novel Risk Mitigation & Cloud-Based Disaster Recovery Framework for Small to Medium Size Businesses***. 2021 9Th International Symposium On Digital Forensics And Security (ISDFS), Elazig, Turkey, p. 1-5, 28 jun. 2021. IEEE. http://dx.doi.org/10.1109/isdfs52919.2021.9486373.

TORRES, Elton; CALLOU, Gustavo; ANDRADE, Ermeson. ***A hierarchical approach for availability and performance analysis of private cloud storage services***. Computing, v. 100, n. 6, p. 621-644, 25 jan. 2018. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/s00607-018-0588-7.

YOO, Seok-Keun; KIM, Bo-Young**. *A Decision-Making Model for Adopting a Cloud Computing System***. Sustainability, v. 10, n. 8, p. 2952, 20 ago. 2018. MDPI AG. http://dx.doi.org/10.3390/su10082952.