FACULDADE PARA O DESENVOLVIMENTO SUSTENTÁVEL DA AMAZÔNIA
CURSO TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

WILIAN DE LIMA BRITO

NUVEM COMPUTACIONAL: FUNCIONAMENTO, SEGURANÇA E REGULAMENTAÇÃO

PARAUAPEBAS
2023

WILIAN DE LIMA BRITO

NUVEM COMPUTACIONAL: FUNCIONAMENTO, SEGURANÇA E REGULAMENTAÇÃO

Trabalho de Conclusão de Curso (TCC) apresentado a Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas para a obtenção do Título de Tecnólogo.

Orientador (a): Prof.ª Sara Debora Carvalho Cerqueira.

PARAUAPEBAS
2023

BRITO. Wilian de Lima,

NUVEM COMPUTACIONAL: FUNCIONAMENTO, SEGURANÇA E REGULAMENTAÇÃO; Sara Debora Carvalho Cerqueira.

58 f. (Cinquenta e oito páginas)
Trabalho de Conclusão de Curso (Graduação) – Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA, Parauapebas – PA, 2023.

Palavras – Chave: nuvem; criptografia; multicloud; segurança;

Nota: A versão original deste trabalho de conclusão de curso encontra-se disponível no Serviço de Bilioteca e Documentação da Faculdade para o Desenvolvimento Sustentável da Amazônia – FADESA em Parauapebas – PA.

WILIAN DE LIMA BRITO

NUVEM COMPUTACIONAL: FUNCIONAMENTO, SEGURANÇA E REGULAMENTAÇÃO

Trabalho de Conclusão de Curso (TCC) apresentado a Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas para a obtenção do Título de Tecnólogo.

Aprovado em 14 de Novembro de 2023.

Banca Examinadora

Prof. Mateus da Silva Sousa
Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA

Prof. Esp. Antônio Soares da Silva
Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA

Prof.(a) Sara Debora Carvalho Cerqueira
Faculdade para o Desenvolvimento Sustentável da Amazônia – FADESA

WILIAN DE LIMA BRITO

NUVEM COMPUTACIONAL: FUNCIONAMENTO, SEGURANÇA E REGULAMENTAÇÃO

Trabalho de Conclusão de Curso (TCC) apresentado a Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas para a obtenção do Título de Tecnólogo.

Aprovado em 14 de Novembro de 2023.

Wilian de Lima Brito
Discente

Prof. Mateus da Silva Sousa
Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA

À minha esposa que é minha fonte constante de inspiração e o alicerce do nosso lar. Sua força, amor e compaixão são o que me impulsionam todos os dias. Agradeço por ser minha parceira, minha amiga e minha fonte de felicidade. Juntos, somos imparáveis.

Aos meus professores pois suas palavras e ensinamentos moldaram não apenas a minha mente, mas também o meu caráter. Agradeço pelo incansável compromisso em compartilhar conhecimento e orientação. Vocês têm um papel fundamental na minha jornada e serei eternamente grato.

Aos meus colegas que são a extensão da minha família no ambiente acadêmico. Juntos, superamos desafios, celebramos conquistas e construímos memórias que levarei para sempre. Agradeço por cada momento compartilhado e pela amizade que nos une.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão à professora Sara Debora Carvalho Cerqueira pela sua orientação excepcional ao longo deste processo de elaboração do meu Trabalho de Conclusão de Curso. Sua dedicação, paciência e conhecimento foram fundamentais para o sucesso deste projeto.

Suas sugestões valiosas não apenas aprimoraram a qualidade do meu trabalho, mas também enriqueceram minha compreensão do assunto. Sua orientação me encorajou a buscar a excelência em cada etapa.

Além disso, sua disponibilidade para esclarecer demonstram o seu compromisso incansável com a educação e o desenvolvimento dos seus alunos. Sou verdadeiramente privilegiado por ter tido a oportunidade de ser orientado por você.

“A necessidade é a mãe da inovação.”

Platão

RESUMO

A pesquisa explora a essência e a operação da computação em nuvem, destacando sua capacidade de fornecer recursos computacionais escaláveis e flexíveis por meio da virtualização e abstração de infraestrutura física. A segurança emerge como um componente crítico, abordando desafios como autenticação, criptografia e proteção contra ameaças cibernéticas, essenciais para a preservação da integridade e confidencialidade dos dados na nuvem. Além disso, o estudo examina a complexa paisagem regulatória que permeia a computação em nuvem. A conformidade com normas e regulamentações se revela como um fator determinante na gestão de dados sensíveis. Diante do cenário em constante evolução, são discutidas estratégias proativas, como a implementação de arquiteturas multicloud para mitigar a dependência de um único provedor, e a adoção de práticas de segurança avançadas, como auditorias regulares e monitoramento contínuo. Ressalta ainda a importância crítica da nuvem na atualidade e a necessidade de compreender e abordar seus desafios inerentes. Ao integrar os pilares do funcionamento, segurança e regulamentação, a pesquisa oferece uma visão abrangente e atualizada sobre a computação em nuvem, fornecendo insights valiosos para empresas e organizações em sua jornada rumo à inovação e conformidade.

Palavras-chave: nuvem; criptografia; multicloud; segurança;

ABSTRACT

The research delves into the essence and operation of cloud computing, highlighting its ability to provide scalable and flexible computational resources through virtualization and abstraction of physical infrastructure. Security emerges as a critical component, addressing challenges such as authentication, encryption, and protection against cyber threats, which are essential for preserving the integrity and confidentiality of data in the cloud. Additionally, the study examines the complex regulatory landscape that permeates cloud computing. Compliance with standards and regulations proves to be a determining factor in managing sensitive data. Given the constantly evolving landscape, proactive strategies are discussed, such as the implementation of multicloud architectures to mitigate reliance on a single provider, and the adoption of advanced security practices like regular audits and continuous monitoring. It further emphasizes the critical importance of the cloud in today's context and the need to understand and address its inherent challenges. By integrating the pillars of functionality, security, and regulation, the research offers a comprehensive and up-to-date perspective on cloud computing, providing valuable insights for companies and organizations on their journey towards innovation and compliance.

Keywords: cloud; encryption; multicloud; security.

LISTA DE ILUSTRAÇÕES

Figura 1: Modelo de um servidor aberto ……..…..…… 16
Figura 2: Modelo de Estrutura DAS (Direct Attached Storag) ……..... 17
Figura 3: Modelo de Estrutura SAN (Storage Area Network) ……...……..…… 18
Figura 4: Exemplo dos dois tipos de Hipervisor…….....…….… 19
Figura 5: Cidade de Luleå na Suécia que se encontra no Ártico.....… 36
Figura 6: Grafana, tela de monitoramento com alguns parâmetros.....… 37

SUMÁRIO

1. INTRODUÇÃO 11
2. INFRAESTRUTURA DOS SERVIÇOS DE NUVEM 13
2.1 Hardware 13
2.2 Software 18
2.2.1 Hipervisor 18
2.2.2 Sistema operacional 20
2.2.3 Orquestração de contêineres 20
2.2.4 Gestão de recursos e virtualização de armazenamento 22
2.2.5 Sistema de gerenciamento de banco de dados (dbms) 24
2.2.6 Rede virtual e SDN (software-defined networking) 26
2.2.7 Middleware e Apis 27
2.2.8 Gestão de identidade e acesso (IAM) 29
2.2.8 Monitoramento e gerenciamento de desempenho 29
2.2.10 Segurança e Conformidade 31
2.3 IAAS, PAAS E SAAS 33
2.3.1 IAAS (infraestrutura como serviço) 33
2.3.2 PAAS (plataforma como serviço): 34
2.3.3 SAAS (software como serviço): 35
2.4 Controle do ambiente: redes, energia, temperatura 35
2.4.1 Gerenciamento de redes 36
2.4.2 Gerenciamento de energia 36
2.4.3 Monitoramento de temperatura 37
2.4.4 Softwares de monitoramento 38
3. POLÍTICAS DE SEGURANÇA E REGULAMENTAÇÃO 40
3.1 Confiabilidade, Integridade e Disponibilidade 41
3.4 Regulamentação 43
4. METODOLOGIA 49
5. RESULTADOS E DISCUSSÕES 50
6. CONSIDERAÇÕES FINAIS 52
REFERÊNCIAS 54

1. INTRODUÇÃO

Com o passar dos anos a internet passou a fazer cada vez mais parte da vida das pessoas, está em constante mudança quando se trata de como é utilizada pelos usuários, seja no meio corporativo ou para o lazer, porém a principal característica que está presente em todos os contextos é a manipulação de dados na questão da necessidade de armazená-los, pois o que antes ficava apenas restrito ao armazenamento local acabou sofrendo alterações devido a importância que dados salvos foram ganhando ao longo dos anos.

Devido a isso o serviço de nuvem já tão utilizado por grandes empresas ganhou mais notoriedade entre usuários comuns, este método computacional consiste em armazenar dados na internet por meio de servidores físicos disponibilizados de forma gratuita limitada ou paga caso o usuário queira mais espaço para armazenar mais dados ou necessita de um serviço com segurança ainda mais eficiente.

Para a Opus Software (2015, p. 15):

> Pode se falar muito sobre as vantagens tecnológicas da Computação em Nuvem em relação ao modelo tradicional. Mas o principal motivo pelo qual o movimento para a Computação em Nuvem é inevitável é baseado em sólidos fundamentos da Ciência Económica, isto é, a principal vantagem dessa nova tecnologia é econômica.

Para Lima (2020, p. 131) A proteção dos dados pessoais não pode ser encarada como um entrave à economia, ao contrário, um ambiente mais seguro e ético estimulará o maior uso destas ferramentas tecnológicas. Seja devido ao tamanho dos arquivos que foram ficando cada vez maiores, unidades de armazenamento que se tornaram mais rápidas, porém mais caras e principalmente após integração de plataformas tornando possível acessar dados de qualquer lugar, usando os mais variados dispositivos.

O que é preciso ser posto em prática é uma cultura onde ela será de duas vias, onde uma via é responsável por fornecer o serviço, dando todo o suporte necessário e do outro lado os usuários terem a consciência que não são apenas clientes utilizando o serviço, mas sim igualmente responsáveis pelos seus dados, assim adotando práticas que possibilite dificultar os vazamentos de seus dados.

Com a crescente demanda com o serviço de armazenamento em nuvem e o aumento da dependência da sociedade pelo uso da tecnologia surgem os seguintes

questionamentos, até que ponto as pessoas estão cientes dos riscos e vulnerabilidades associadas ao armazenamento de dados pessoais em servidores remotos controlados por empresas privadas e como garantir a disponibilidade e integridade desses dados considerando a possibilidade de falhas técnicas ou de segurança.

A presente pesquisa tem como objetivo geral fazer levantamentos importantes relacionados aos desafios éticos, legais e de segurança que precisa ser abordado para que a sociedade possa confiar no uso desse serviço e se beneficiar das vantagens que ele oferece.

Acrescenta-se como objetivo específico verificar quais métodos os prestadores de serviço em nuvem utilizam para garantir que os dados estejam protegidos contra acessos não autorizados, uso indevido e compartilhamento indevido trazendo muitos prejuízos financeiros a quem faça uso do serviço.

Saber sobre as práticas de segurança, pois os usuários devem ser informados sobre medidas adotadas pelo provedor de serviço, tais como protocolos de criptografia, autenticação, autorização e backup e recuperação de dados. Assim como compreender como garantem a disponibilidade e confiabilidade dos dados já que os usuários devem ter a garantia de que seus dados estarão disponíveis e acessíveis quando precisarem e que o provedor de serviço tem planos de backup e recuperação em caso de falhas do sistema.

Relacionar as principais conformidades com regulamentações o provedor de serviço deve cumprir com as normas regulatórias aplicáveis, tais como a GDPR, HIPAA e PCI-DSS, LGPD, para proteger os dados dos usuários contra violações de segurança e ameaças externas.

A utilização dos serviços de nuvem traz consigo uma série de benefícios, tais como escalabilidade, acessibilidade global e redução de custos. Contudo, a segurança dos dados ainda é uma preocupação relevante para muitos usuários. Considerando que atualmente é difícil encontrar pessoas que não dependam desses serviços, uma vez que eles se tornaram praticamente indispensáveis, devido isso justifica-se a necessidade de elaborar uma análise aprofundada que proporcione um entendimento mais abrangente para aqueles que desejam utilizar essa ferramenta de forma mais inclusiva ou que foram obrigados a adotá-la.

2. INFRAESTRUTURA DOS SERVIÇOS DE NUVEM

De acordo com Oliveira (2023), a infraestrutura de nuvem é o conjunto de recursos físicos e lógicos que fornecem suporte para serviços de computação em nuvem. Esses recursos incluem hardware, software, redes e armazenamento. A terminologia que se refere aos elementos essenciais para viabilizar a computação em nuvem é “estrutura de nuvem”. Isso abrange tanto o equipamento físico quanto os recursos virtualizados, o armazenamento e as capacidades de interconexão.

Encare esse conceito como o conjunto de instrumentos indispensáveis para a construção de um ambiente em nuvem. Quando se trata de alojar serviços e programas na nuvem, a presença de uma estrutura de nuvem se torna imperativa pois seu sistema organizacional é o que rege seu perfeito funcionamento.

A composição da infraestrutura de nuvem engloba uma diversidade de elementos, todos harmonizados em uma arquitetura unificada que se alinha às operações empresariais. Uma abordagem típica envolve componentes como hardware, virtualização, armazenamento e conectividade. A expressão "infraestrutura de nuvem" retrata o sistema abrangente da computação em nuvem, considerando a integração total de todos os elementos, indo além das tecnologias isoladas em si.

2.1 Hardware

É normal que alguns usuários tenham a impressão de que as nuvens são puramente virtuais, mas elas realmente dependem de componentes físicos de hardware como parte fundamental de sua infraestrutura. Para Smith e Johnson, (2019, p. 45) A escolha do hardware adequado é essencial para atender às demandas específicas de processamento, armazenamento e comunicação em um ambiente computacional. Este insight ressalta a importância de considerar cuidadosamente as características do hardware ao projetar e implementar sistemas de computação eficazes.

Uma rede em nuvem é composta por uma ampla variedade de elementos físicos de hardware, distribuídos em várias localizações do mundo como por exemplo o Google que possuem servidores estrategicamente alocados em 12 países estando presente em quase todos os continentes, exceto África.

As escolhas destas localizações variam muito conforme a expectativa que a empresa tem com o mercado local ou na maioria das vezes está relacionado apenas com o clima, assim como explica Silva (2019), a escolha do local de um servidor cloud é uma decisão importante que pode afetar o desempenho, a segurança e os custos de uma aplicação. Sim, pois um dos fatores a serem considerados durante a estruturação de servidor é garantir a integridade das máquinas na questão de temperatura, por isso a maioria dos servidores ficam localizados em países com clima predominantemente frio durante a maior parte do ano como é o caso do Facebook que possuem apenas 1 único e gigantesco servidor que se encontra na cidade de Luleå, na Suécia localizada a apenas 110 km do círculo Polar Ártico

Esses hardwares abrangem diversos equipamentos de rede, tais como switches, roteadores, firewalls, balanceadores de carga, sistemas de armazenamento, dispositivos de backup e servidores. A tecnologia de virtualização estabelece conexões entre os servidores, criando uma separação e abstração de recursos, tornando-os disponíveis para os usuários.

Dentro de um centro de dados, as informações podem ser armazenadas em diversos discos de conteúdo em uma única estrutura de armazenamento. A gestão do armazenamento garante a execução adequada dos backups de dados, a eliminação regular dos backups antigos e a indexação dos dados para possibilitar sua recuperação no caso de uma eventual falha em um dos componentes de armazenamento.

Por meio da virtualização, o espaço de armazenamento é dissociado de sistemas de hardware, permitindo que os usuários o acessem como uma forma de armazenamento em nuvem, Por isso Soares e Almeida (2023) afirma que a virtualização de servidores cloud é uma das principais tecnologias utilizadas na computação em nuvem. Pois assim quando o armazenamento é transformado em um recurso de nuvem, torna-se viável adicionar ou remover unidades, reutilizar o hardware e reagir às mudanças sem a necessidade de configurar manualmente servidores de armazenamento individuais para cada nova empreitada.

Um servidor ou host em inglês, é um hardware que fornece diversos tipos de serviços para outros dispositivos, referidos como clientes. Servidores representam um dos elementos fundamentais de um Centro de Dados. Os elementos essenciais de um servidor incluem placa-mãe, processador, memória ram, unidades de

armazenamento, portas para conectividade, fonte de alimentação e uma placa de vídeo conforme mostra a figura 1.

Figura 1: Modelo de um servidor aberto.

Fonte: dell (2023)

Oliveira (2023) define servidores hiperconvergentes como um sistema integrado que combina recursos de computação, armazenamento e rede em um único dispositivo.Servidores que integram todos os elementos mencionados, incluindo as unidades de armazenamento e o software de virtualização, em um único dispositivo, recebem o nome de servidores hiperconvergentes que no caso é a união de hardwares como discos, processadores, redes e um sistema para gerenciar a automação tudo isso organizado por um software.

A virtualização desempenha um papel fundamental na implementação de uma infraestrutura hiperconvergente, uma vez que é responsável por abstrair e unificar todos os recursos disponíveis nos servidores, alocando dinamicamente aplicações, máquinas virtuais e containers.

Silva (2023) explica que a hiperconvergência é uma arquitetura de TI que integra recursos de computação, armazenamento e rede em um único sistema. Isso afirma uma das principais vantagens da hiperconvergência que é a redução do número de servidores no centro de dados, conhecida como "footprint reduction" em inglês. Isso contribui significativamente para a diminuição dos gastos com energia e refrigeração. Além disso, a escalabilidade é outro benefício notável.

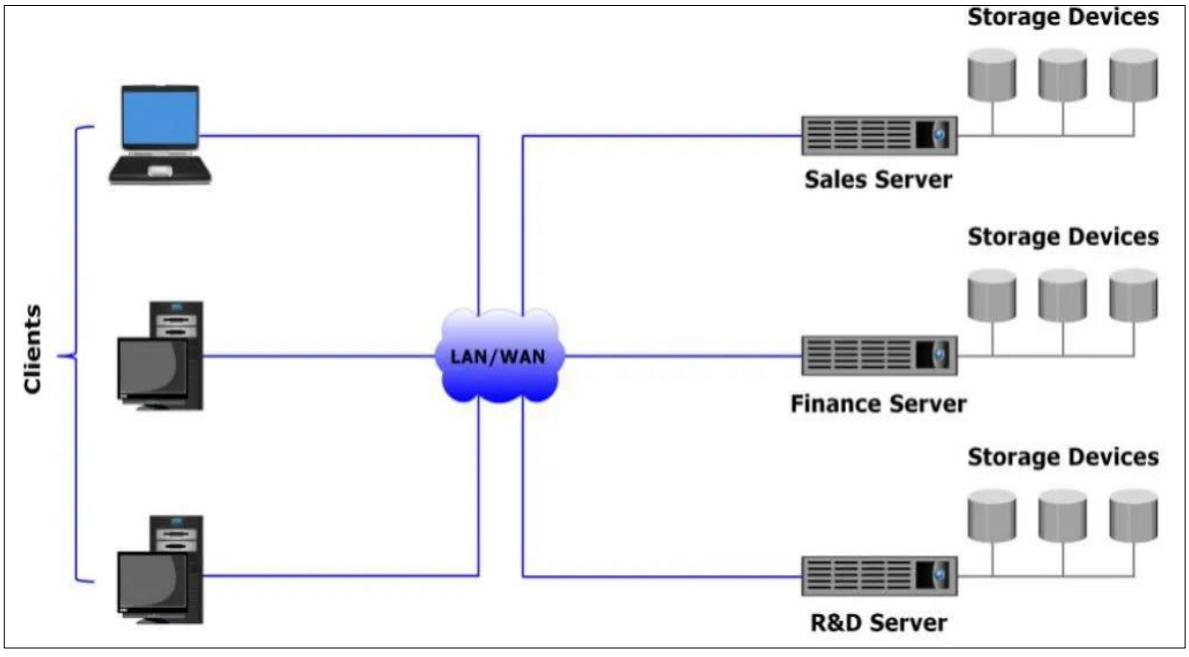
A maioria dos servidores hiperconvergentes oferecem uma flexibilidade incrível aos clientes, permitindo que comecem com um número reduzido de servidores e adicionem mais servidores (e discos) conforme suas necessidades de crescimento. O

investimento em HCI (Sigla em inglês para *hyperconverged infrastructure*) pode acomodar cargas de trabalho, aplicativos e máquinas virtuais, atendendo tanto a pequenas empresas quanto a grandes corporações. Por esse motivo, a hiperconvergência é uma tendência robusta na área de infraestrutura.

Num centro de dados convencional, cada departamento de uma organização mantém seus próprios servidores, os quais possuem discos locais diretamente dedicados a eles conforme mostra a figura 2 para fornecer armazenamento às aplicações que operam nesses servidores específicos. Esta abordagem de conectar ao servidor diretamente a cada disco dedicado apresenta desafios para as empresas, como a restrição de capacidade de armazenamento por servidor, o que limita a escalabilidade e pode ocasionar gargalos na leitura e escrita nos discos.

Soares e Almeida (2023) explica que os gargalos de um servidor cloud são pontos de estrangulamento que podem prejudicar o desempenho de uma aplicação. Para resolver esses gargalos em um servidor de nuvem é preciso identificar e abordar os pontos de estrangulamento que estão afetando o desempenho e a disponibilidade do servidor, então é preciso seguir algumas etapas para resolver problemas como este.

Figura 2: Modelo de Estrutura DAS (Direct Attached Storag)



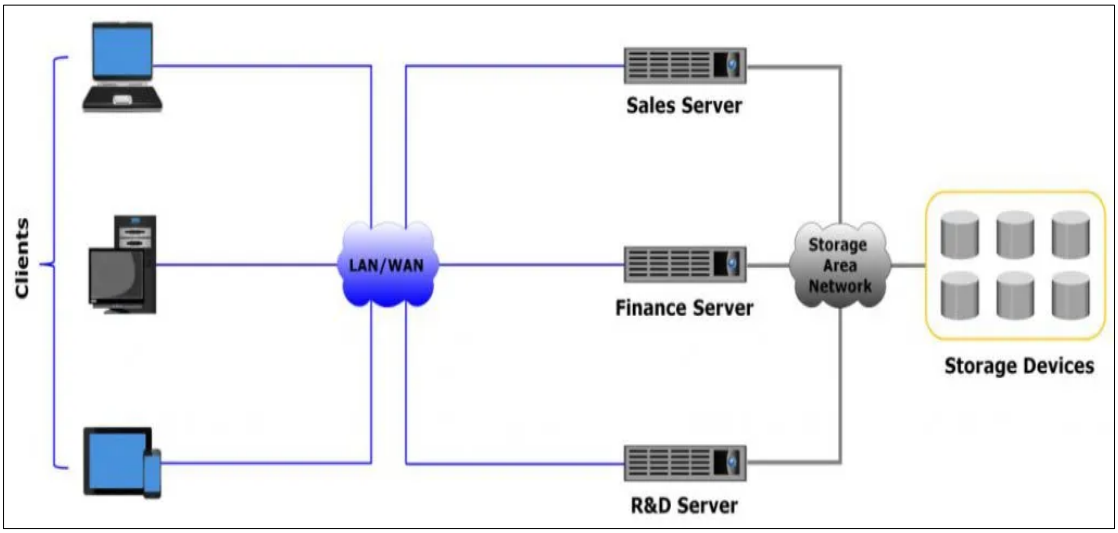
Fonte: Mycloudwiki (2020).

Outra questão problemática com essa abordagem é a ineficiência resultante do espaço não utilizado em outros servidores pois a estratégia de ter um servidor dedicado a cada setor específico acessando discos específicos para si pode proporcionar limitações a escalabilidade e entraves durante o acesso aos dados.

Após a constatação de que esse modelo de estruturação do servidor para acessos aos dados estava prejudicando foi necessário tentar novos métodos que tornasse o processo mais eficaz, o que antes era estruturado de tal forma que existia um disco para cada servidor não aproveitando a total capacidade pois alguns necessitam de menos espaço que outros, daí tendo que fazer configurações conforme a demanda. Então abordou-se uma nova estratégia onde foi adotado o que hoje é conhecido como (*storage pool)* que é um conjunto de armazenamento onde traz mais escalabilidade e eficiência aos meios de tecnologia da informação.

Silva (2023) explica que o modelo de Estrutura SAN (Storage Area Network) de um servidor cloud é uma arquitetura que utiliza uma rede dedicada para o armazenamento de dados. A SAN é uma rede de alta velocidade que conecta dispositivos de armazenamento, como servidores de armazenamento e arrays de armazenamento, a servidores de computação. Assim ao utilizar este método, todos os servidores têm acesso a vários discos, tornado o processo mais eficiente, eliminando empecilhos e mais agilidade na escalabilidade do plano como explicado na Figura 3.

Figura 3: Modelo de Estrutura SAN (Storage Area Network)



Fonte: mycloudwiki (2020)

2.2 Software

A virtualização é uma tecnologia que estabelece uma divisão entre as funções e serviços de tecnologia da informação e o hardware subjacente. No âmbito do hardware físico, é necessário implantar um software conhecido como hipervisor, que desempenha a função de abstrair os recursos do sistema, tais como memória, capacidade de processamento e espaço de armazenamento.

Como ressaltado por Brown e Green, (2021, p. 78) A escolha e a implementação cuidadosa do software são essenciais para atender às necessidades específicas de processamento, análise e gestão de dados em um ambiente tecnológico. Esta observação enfatiza a importância de considerar minuciosamente as características do software ao projetar e implementar soluções tecnológicas eficazes.

Quando esses recursos virtuais são agrupados em reservatórios centralizados, eles são reconhecidos como ambientes em nuvem. Por meio da utilização desses ambientes em nuvem, são proporcionadas vantagens como acesso via autoatendimento, capacidade de dimensionamento automático da infraestrutura e reservatórios de recursos que podem ser ajustados de forma dinâmica.

A estruturação de um serviço de nuvem é um processo complexo que requer uma compreensão dos conceitos de computação em nuvem, redes, armazenamento e segurança como explicado por Silva (2023). Pois a estruturação de um serviço de nuvem computacional envolve a implementação de uma infraestrutura tecnológica robusta e altamente escalável para armazenar, processar e disponibilizar dados e aplicações pela internet. Essa infraestrutura é suportada por uma série de softwares essenciais que desempenham papéis críticos em diferentes camadas da nuvem. As principais partes de software envolvidas nesse processo são:

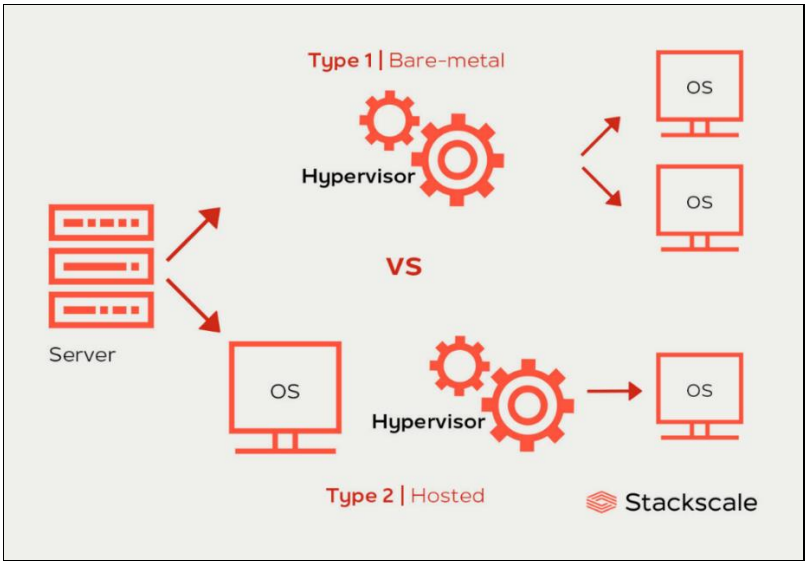
2.2.1 Hipervisor

Um hipervisor é um software ou uma camada de hardware que permite a criação e a execução de máquinas virtuais (VMs). De acordo com Aguiar (2023), um hipervisor é um software que permite que vários sistemas operacionais sejam executados no mesmo hardware. Ele proporciona uma abstração do hardware físico,

permitindo que múltiplos sistemas operacionais e ambientes de software operem de forma isolada em um único servidor físico.

Hypervisor Tipo 1 (Bare Metal) que é instalado diretamente no hardware físico do servidor assim não requer um sistema operacional host separado geralmente é mais eficiente em termos de desempenho, pois não precisa lidar com a sobrecarga de um sistema operacional adicional. Alguns exemplos são VMware vSphere/ESXi, Microsoft Hyper-V (quando instalado diretamente no hardware) e Xen. Existem dois tipos principais de hipervisores que são amplamente utilizados na configuração de servidores, seu esquema é mostrado na figura 4:

Figura 4: Exemplo dos dois tipos de Hipervisor.



Fonte: stackscale (2023).

Hypervisor Tipo 2 (Hosted) é instalado sobre um sistema operacional host. Pois requer um sistema operacional já instalado para funcionar, sendo mais comumente usados em ambientes de desenvolvimento e testes. Apesar de ser menos eficiente em termos de desempenho devido à camada adicional do sistema operacional host. Alguns exemplos mais utilizados são VMware Workstation, Oracle VirtualBox e Parallels Desktop.

Os hipervisores são amplamente utilizados em ambientes de virtualização e nuvem, permitindo a consolidação de servidores físicos, o que leva a uma melhor utilização dos recursos e uma maior eficiência operacional. Silva (2023) afirma que

um hipervisor é um software que permite que vários sistemas operacionais sejam executados em um único servidor físico. Os hipervisores são uma tecnologia fundamental para a computação em nuvem, pois permitem que os provedores de serviços em nuvem provisionem recursos de computação de forma flexível e escalável, sendo assim essenciais em ambientes de data centers modernos.

Estas ferramentas desempenham um papel fundamental na virtualização, permitindo a criação e gerenciamento de VMs. Eles possibilitam a consolidação de servidores físicos em um único servidor físico, economizando espaço, energia e custos de hardware. Além disso, os hipervisores oferecem recursos de isolamento, segurança e mobilidade, permitindo que as VMs sejam movidas facilmente entre servidores físicos, dimensionadas de acordo com as necessidades e executadas com diferentes sistemas operacionais em um único hardware físico.

2.2.2 Sistema operacional

Em cada máquina virtual, é imperativo ter um sistema operacional, que pode variar de distribuições Linux, como Ubuntu e CentOS, a sistemas Windows Server. Esses sistemas operacionais são gerenciados de forma independente dentro de suas respectivas VMs.

De acordo com Smith e Johnson (2019, p.56) O sistema operacional atua como uma interface crítica entre os usuários e o hardware, fornecendo recursos essenciais para a execução de aplicativos e garantindo a estabilidade e segurança do sistema como um todo. Essas VMs são independentes e isoladas entre si, o que significa que podem executar diferentes sistemas operacionais, versões e configurações, mesmo em um único servidor físico. Isso oferece flexibilidade, eficiência de recursos e a capacidade de consolidar várias cargas de trabalho em um único hardware.

Cada VM é tratada como uma entidade separada e pode ser reiniciada, gerenciada e configurada independentemente das outras VMs no mesmo servidor. Isso facilita a implantação e a manutenção de aplicativos e serviços distintos em um único hardware físico.

2.2.3 Orquestração de contêineres

Conforme observado por Smith (2020, p. 78) A orquestração eficaz de contêineres permite a automação de tarefas complexas, como escalabilidade dinâmica, balanceamento de carga e recuperação de falhas, facilitando a administração de ambientes distribuídos e altamente escaláveis.

Portanto, a escolha e a implementação de uma solução de orquestração adequada desempenham um papel crucial na arquitetura de sistemas modernos baseados em contêineres. A orquestração de contêineres em um servidor refere-se ao processo de gerenciar e coordenar a implantação, o escalonamento, a operação e a comunicação de contêineres em um ambiente distribuído. Isso é feito para garantir que os aplicativos em contêineres funcionem de maneira confiável, escalável e eficiente. Aqui estão alguns pontos chave sobre a orquestração de contêineres:

Os contêineres são unidades de software leves e portáteis que encapsulam uma aplicação e suas dependências. Eles fornecem isolamento entre os aplicativos e permitem que eles sejam executados de maneira consistente em diferentes ambientes.

Outra parte é o orquestrador de contêineres que é um software que automatiza e facilita a implantação, a gestão e o escalonamento de contêineres em um ambiente de produção. Os orquestradores lidam com tarefas como inicialização de contêineres, distribuição de carga, escalonamento automático, monitoramento e recuperação de falhas. Exemplos populares de orquestradores de contêineres incluem Kubernetes, Docker Swarm, Apache Mesos e Amazon ECS.

É preciso que haja um escalonamento automático, pois, orquestradores podem monitorar a carga de trabalho e adicionar ou remover contêineres conforme necessário para garantir o desempenho e a disponibilidade adequados. Tendo uma Gestão de Recursos que ajudam a alocar e gerenciar hardwares, como CPU, memória e armazenamento, entre os contêineres.

Oliveira (2023) define gerenciamento de rede de nuvem como o processo de planejamento, implementação, operação e monitoramento de redes em um ambiente de nuvem. No Gerenciamento de Rede há uma facilitação da comunicação entre os contêineres, criando redes virtuais e gerenciando o tráfego de dados e atualizações e rollbacks que permitem a atualização de aplicativos sem interrupção de serviço, além de facilitar a reversão para versões anteriores em caso de falhas. A descoberta de serviços automatiza a descoberta de serviços disponíveis para que os contêineres possam encontrar e se comunicar uns com os outros.

Com Isolamento e Segurança garantem que os contêineres operem de maneira isolada, impedindo que um contêiner afete negativamente outros. Propiciando uma melhor escalabilidade permitindo dimensionar aplicativos de maneira eficiente, adicionando ou removendo contêineres conforme a demanda. Obtendo assim uma maior confiabilidade ajudando a manter a alta disponibilidade e a resiliência dos aplicativos, gerenciando automaticamente falhas, recuperações e eficiência de recursos maximizando a utilização de recursos do servidor, permitindo que múltiplos aplicativos compartilhem a mesma infraestrutura.

A padronização e portabilidade garante que os aplicativos se comportem de maneira consistente em diferentes ambientes, Silva (2023) explica que as organizações podem usar essas técnicas para ajudar a garantir que seus aplicativos e dados possam ser movidos de um provedor de serviços em nuvem para outro. Portanto, tornando a migração e a implantação mais fáceis trazendo mais agilidade no desenvolvimento facilitando o ciclo de vida de desenvolvimento e implantação de aplicativos, permitindo a entrega contínua e a integração contínua (CI/CD).

A orquestração de contêineres é especialmente valiosa em ambientes de nuvem e em infraestruturas distribuídas, onde a escalabilidade, a confiabilidade e a eficiência são críticas para o sucesso das operações de TI pois falhas podem causar prejuízos incalculáveis a depender da finalidade que o serviço está sendo prestado, prejudicando não só o cliente, mas também o fornecedor.

2.2.4 Gestão de recursos e virtualização de armazenamento

Stallings (2023) afirma que a gestão de recursos de armazenamento é o processo de garantir que os recursos de armazenamento disponíveis sejam usados de forma eficiente e eficaz pois gestão de recursos e a virtualização de armazenamento são dois componentes essenciais em um serviço de nuvem que ajudam a melhorar a eficiência, a escalabilidade e a flexibilidade da infraestrutura de armazenamento em nuvem. Estes são alguns conceitos em detalhes:

A gestão de recursos em um serviço de nuvem necessita de otimização de recursos pois envolve a alocação eficiente de recursos de computação, rede e armazenamento para atender às necessidades dos aplicativos e dos usuários. Isso inclui a distribuição adequada de recursos para evitar subutilização ou superutilização, otimizando assim os custos.

Em um escalonamento dinâmico em um ambiente de nuvem, os recursos podem ser alocados ou liberados conforme necessário, Soares e Almeida (2023) diz, o escalonamento dinâmico pode ajudar as organizações a reduzir seus custos, melhorar o desempenho e a disponibilidade de seus aplicativos e serviços. Isso é particularmente importante para atender a picos de demanda ou para economizar recursos em momentos de menor atividade. Isto pode ser obtido através do monitoramento e gerenciamento pois provedores oferecem estas ferramentas que permitem acompanhar o desempenho dos recursos, definir alarmes e automatizar ações baseadas em políticas predefinidas.

Outro fator crucial que deve ser levado em consideração está relacionado ao isolamento e a segurança já que a gestão de recursos também envolve garantir que os recursos sejam isolados adequadamente para garantir a segurança e a privacidade dos dados dos clientes.

A virtualização de armazenamento em um serviço de nuvem conta com a abstração de armazenamento que é o processo de criar uma camada de abstração sobre os recursos de armazenamento físico, de modo que eles possam ser gerenciados de forma mais flexível e eficiente agregando recursos permitindo adicionar vários dispositivos de armazenamento físico em um único pool de armazenamento virtual, tornando mais fácil a alocação e a expansão de espaço de armazenamento conforme necessário.

O provisionamento sob demanda permite a virtualização de armazenamento provisionando volumes ou armazenamento adicional sob demanda, em vez de alocar antecipadamente espaço físico. Isso reduz o desperdício de recursos. Pois a migração de dados entre diferentes sistemas de armazenamento sem interrupção dos serviços, permite atualizações de hardware ou migrações para novos dispositivos de armazenamento.

Oliveira (2021) explica que um recurso avançado da virtualização de armazenamento é a compressão de dados. A compressão de dados reduz o tamanho dos dados armazenados, o que pode economizar espaço e melhorar o desempenho. Pois a virtualização de armazenamento oferece recursos avançados, como replicação de dados, balanceamento de carga, instantâneos e criptografia, para atender às necessidades de segurança e disponibilidade proporcionando a flexibilidade e portabilidade das escolhas dos sistemas de armazenamento subjacentes e ajuda a

criar soluções de armazenamento mais portáteis, que podem ser usadas em diferentes ambientes de nuvem ou locais.

Soares e Almeida (2023) esclarece que gestão de recursos e a virtualização de armazenamento são dois processos complementares. Em resumo, a gestão de recursos e a virtualização de armazenamento são estratégias essenciais para otimizar a utilização dos recursos de infraestrutura em um serviço de nuvem, garantindo ao mesmo tempo maior flexibilidade, escalabilidade e eficiência no armazenamento e na alocação de recursos de TI. Essas práticas desempenham um papel fundamental em permitir que os serviços em nuvem atendam às crescentes demandas dos aplicativos e usuários.

2.2.5 Sistema de gerenciamento de banco de dados (SGBD)

Segundo Ávila, Souza e Gonzalez (2019, p. 23) A criação de banco de dados é uma prática antiga e bancos de dados já existem há um bom tempo, pois a contagem em larga escala pode ser exemplificada com o censo praticado pelos antigos governos egípcios e chineses.

Um Sistema de Gerenciamento de Banco de Dados (DBMS, do inglês Database Management System) em um serviço de nuvem refere-se a um software especializado projetado para criar, acessar, gerenciar e manter bancos de dados em um ambiente de nuvem.

Os principais componentes e funções de um DBMS em um serviço de nuvem:

Gerenciamento de Dados:

a) Criação de Bancos de Dados: Permite a criação de bancos de dados para armazenar informações de forma estruturada.
b) Definição de Esquema: Facilita a definição de como os dados serão organizados e armazenados dentro do banco de dados.
c) Controle de Acesso: Gerencia quem tem permissão para acessar, modificar ou excluir dados no banco de dados, garantindo a segurança das informações.

Recuperação de Dados:

a) Backup e Recuperação: Fornece ferramentas para criar backups regulares dos dados e restaurá-los em caso de falhas ou perda de informações.
b) Recuperação de Falhas: Ajuda a lidar com falhas no sistema, garantindo que os dados não sejam perdidos permanentemente.

Consulta e Manipulação de Dados:

a) Linguagem de Consulta (SQL): Oferece uma linguagem padronizada (SQL) para consultar e manipular dados no banco de dados.
b) Consultas Complexas: Suporta consultas complexas que envolvem junções de tabelas, filtragem de dados e cálculos.

Desempenho e Otimização:

a) Índices: Permite a criação de índices para acelerar as consultas e melhorar o desempenho das operações de leitura.
b) Otimização de Consultas: O DBMS otimiza automaticamente as consultas para garantir a execução mais eficiente possível.
c) Afinidade de Dados: Pode sugerir ou implementar estratégias para melhorar o desempenho com base nos padrões de acesso aos dados.

Integridade de Dados:

a) Restrições de Integridade: Permite definir regras e restrições para garantir a integridade dos dados, evitando inserções ou atualizações inválidas.
b) Transações ACID: Garante a consistência dos dados, mesmo em cenários de múltiplas operações concorrentes.

Escalabilidade e Disponibilidade:

a) Replicação de Dados: Suporta a replicação de dados em diferentes nós para aumentar a disponibilidade e a tolerância a falhas.

b) Particionamento de Tabelas: Permite dividir grandes tabelas em partições para distribuir a carga e melhorar o desempenho.

Gerenciamento de Concorrência:

a) Controle de Concorrência: Gerencia o acesso concorrente a dados, garantindo que as operações ocorram de forma segura e consistente.

Monitoramento e Relatórios:

a) Ferramentas de Monitoramento: Oferece recursos para monitorar a saúde do banco de dados, incluindo estatísticas de desempenho e uso de recursos.
b) Geração de Relatórios: Pode gerar relatórios sobre o uso do banco de dados, comportamento de consultas e outros indicadores relevantes.

A integração de um SGBD em um serviço de nuvem permite que os dados sejam armazenados de forma escalável, altamente disponível e segura. Já que como é explicado por Araújo e Oliveira (2022) A integração de um SGBD em um serviço de nuvem é uma tendência crescente, à medida que mais organizações migram para a nuvem. Além disso, muitos serviços de nuvem oferecem opções gerenciadas de DBMS, onde o provedor lida com tarefas como manutenção, backup e escalabilidade automática, permitindo que os desenvolvedores se concentrem na aplicação em si. Exemplos populares de DBMS em nuvem incluem Amazon RDS, Google Cloud SQL, Microsoft Azure SQL Database, entre outros.

2.2.6 Rede virtual e SDN (software-defined networking)

Essa estrutura, conforme descreve Guedes (2010), permite que a rede seja controlada de forma extensível através de aplicações expressas em software. Ao novo paradigma se deu o nome de redes definidas por software. Uma rede virtual em um serviço de nuvem é uma representação lógica de uma rede física, sendo criada usando software para conectar sistemas, serviços e aplicativos hospedados na

nuvem. Essa abordagem permite isolar o tráfego de diferentes aplicativos, escalar facilmente a rede conforme necessário e configurar topologias de rede de forma flexível.

Por outro lado, o SDN (Software-Defined Networking) é uma abordagem de gerenciamento de redes que desacopla o controle do tráfego do hardware de rede. Em vez de depender de configurações estáticas, o SDN centraliza o controle em um controlador de rede programável. Isso proporciona uma maior flexibilidade, permitindo que os administradores programem o comportamento da rede por meio de software. O SDN também otimiza o encaminhamento de tráfego e prioriza dados, melhorando a eficiência geral da rede.

Ao integrar redes virtuais com SDN em um serviço de nuvem, os usuários podem ter uma rede altamente flexível e programável, permitindo uma gestão centralizada e eficiente das operações em nuvem. Isso é crucial para a execução eficaz de aplicativos e serviços na nuvem, especialmente em ambientes de nuvem pública, onde a agilidade e a eficiência na alocação de recursos são vitais.

2.2.7 Middleware e Apis

Fowler (2023) define middleware como um software que fica entre duas ou mais aplicações para fornecer serviços ou funcionalidade. Middleware e APIs são elementos essenciais em um serviço de nuvem que desempenham papéis fundamentais na facilitação da comunicação, na integração de sistemas e no desenvolvimento de aplicativos. Para entender seu funcionamento é preciso ter conhecimento do que cada componente do software é capaz de desempenhar.

Middleware é um conjunto de software intermediário que atua como uma camada de abstração e comunicação entre diferentes componentes de software ou sistemas distribuídos. No contexto de serviços de nuvem, o middleware é frequentemente usado para integração de sistemas permitindo que aplicativos e sistemas diferentes se comuniquem e compartilhem dados de maneira eficiente, independentemente das diferenças em suas tecnologias subjacentes facilitando a gestão de transações, pois ajuda a garantir que as operações sejam concluídas de maneira consistente, mesmo em cenários de múltiplas operações concorrentes.

Na parte da segurança fornece recursos como autenticação e autorização, para proteger o acesso a recursos e dados. Fornece ainda escalabilidade pois escalona

aplicativos distribuídos, gerencia recursos e balanceando a carga de trabalho. Assim como é característica crítica a interoperabilidade que facilita a interação entre diferentes sistemas, permitindo que eles compreendam e usem serviços uns dos outros.

Cohn (2023, p. 3) Uma API é uma interface de programação de aplicações que fornece um conjunto de funções para serem usadas por outros programas. As APIs são uma parte essencial da arquitetura de software moderno, pois permitem que os sistemas se comuniquem entre si de forma eficiente e eficaz. Portanto as APIs são conjuntos de regras e protocolos que permitem que diferentes softwares se comuniquem e interajam. Elas definem como os componentes de software devem interagir uns com os outros, quais operações estão disponíveis e como os dados devem ser estruturados.

Proporcionando integração de serviços permitindo que aplicativos acessem e utilizem estes serviços disponíveis na nuvem, como armazenamento, bancos de dados, autenticação e muito mais. Ajuda no desenvolvimento de aplicativos pois fornecem funcionalidades pré construídas que os desenvolvedores podem incorporar em seus aplicativos que na maioria dos casos obedecem a uma padronização estabelecida para a interação com serviços e recursos na nuvem, tornando a integração mais consistente e eficiente.

Possuem automatização permitindo que tarefas sejam automatizadas como provisionamento de recursos, gerenciamento de infraestrutura e implantação de aplicativos. Araújo e Oliveira (2022) afirmam que a automatização de servidores é uma tendência crescente, à medida que as organizações buscam maneiras de reduzir custos, melhorar a eficiência e aumentar a segurança. Assim como possuem o serviço de abstração que ocultam os detalhes de implementação subjacentes, tornando mais fácil para os desenvolvedores usar os recursos da nuvem sem precisar entender completamente a infraestrutura subjacente.

Em resumo, o middleware e as APIs desempenham papéis complementares na criação de serviços de nuvem eficazes. O middleware atua como uma camada intermediária que gerencia a comunicação e a integração entre sistemas, enquanto as APIs fornecem interfaces bem definidas e padronizadas para acessar e usar serviços na nuvem. Esses elementos são fundamentais para a flexibilidade, a interoperabilidade e a automação que os serviços de nuvem oferecem aos desenvolvedores e usuários finais.

2.2.8 Gestão de identidade e acesso (IAM)

IAM é o conjunto de práticas e tecnologias essenciais para controlar e gerenciar o acesso a recursos em ambientes de tecnologia da informação. Seu papel fundamental é assegurar a segurança da informação e prevenir acessos não autorizados. A IAM engloba elementos como identificação de usuários e entidades, autenticação por meio de diferentes métodos, definição de políticas de acesso e controle de permissões. Além disso, envolve o gerenciamento de grupos e funções, automação de provisionamento e desativação de contas, monitoramento de atividades, e administração de certificados digitais para autenticação segura.

Para Wiley (2023) IAM é um processo que ajuda a garantir que as pessoas certas tenham acesso aos recursos certos. Pois a autenticação valida a identidade de usuários e entidades através de processos como senhas, autenticação de dois fatores ou biometria. Enquanto isso, a autorização determina quais recursos podem ser acessados após a autenticação bem-sucedida, controlando o acesso a arquivos, aplicativos e bancos de dados, também facilita o agrupamento de usuários em categorias assim, a desativação de contas assegura que o acesso seja concedido e retirado de forma rápida e precisa em casos de mudanças na situação do usuário.

A auditoria e monitoramento, com trilhas de auditoria e análise de logs, são cruciais para identificar atividades suspeitas ou não conformes com as políticas de segurança. Oliveira (2023) explica que a auditoria fornece uma visão geral do estado dos servidores, enquanto o monitoramento permite identificar problemas e tomar medidas corretivas rapidamente, utilizando a gestão de certificados digitais, que por sua vez, é essencial para garantir autenticação segura, gerenciando o ciclo de vida desses certificados. Por fim, a autenticação única (SSO) permite aos usuários acessar vários sistemas ou aplicativos com um único conjunto de credenciais, simplificando a experiência de acesso.

Em ambientes de TI com um número de usuários e sistemas elevado, a gestão de identidade e acesso se torna ainda mais vital. Sua implementação eficaz minimiza os riscos de violações de segurança, assegurando que apenas pessoas e entidades autorizadas tenham acesso a recursos sensíveis.

2.2.8 Monitoramento e gerenciamento de desempenho

Gupta (2023) estabelece que o monitoramento e gerenciamento de desempenho de servidores é o processo de coletar, analisar e agir sobre dados de desempenho. O objetivo é garantir que os servidores cloud estejam funcionando de forma eficiente e eficaz, pois o tempo de resposta de aplicativos e serviços é crucial para garantir uma boa experiência para os usuários assim como o tráfego de rede que acompanhar a quantidade de dados que está sendo transmitida para otimizar a largura de banda e identificar possíveis gargalos. Já que a disponibilidade é essencial para rastrear o tempo de disponibilidade.

O monitoramento e gerenciamento de desempenho de servidores em nuvem são práticas críticas para garantir que os recursos de TI estejam operando de maneira eficiente, confiável e segura. Isso é especialmente importante em ambientes de nuvem, onde a escalabilidade e a disponibilidade são fundamentais. Os principais aspectos dessas práticas são o monitoramento de desempenho que utilizam métricas de desempenho envolvendo a coleta contínua de métricas como CPU, memória, armazenamento, largura de banda de rede, entre outros. Essas métricas ajudam a avaliar a utilização e a saúde dos recursos.

Na parte de alertas e notificações algumas configurações estabelecem limites para métricas de desempenho e configuram alertas que disparam quando esses limites forem atingidos ou excedidos através de notificações em tempo real e imediatas sobre eventos críticos ajuda a agir rapidamente para corrigir problemas antes que afetem os usuários.

Na gestão de capacidade existe a projeção de demanda com base no histórico de uso e tendências, é importante prever as necessidades futuras de capacidade para evitar escassez de recursos para que haja um escalonamento automático configurando políticas que permitam a adição automática de recursos em momentos de pico de demanda.

Numa otimização de recursos é preciso de uma análise de utilização para identificar e corrigir recursos subutilizados ou mal dimensionados, reduzindo custos desnecessários, como discorre Soares e Almeida (2023), a otimização de recursos de um servidor cloud pode ser um processo desafiador, mas pode gerar uma série de benefícios para as organizações. Ao otimizar seus servidores cloud, as organizações podem melhorar o desempenho, reduzir custos e melhorar a segurança assim, consolidando os servidores quando viável, fazendo a junção de aplicativos e serviços em menos servidores para otimizar a utilização de recursos.

A gestão de atualizações e patches mantem uma manutenção regular para garantir que o sistema operacional e os aplicativos sejam mantidos atualizados corrigindo vulnerabilidades e melhorando o desempenho através de programação de manutenção agendada. Estas atualizações são executadas em horários de menor atividade para minimizar impactos nos usuários.

Na questão da segurança e conformidade há monitoramentos de segurança que rastreiam atividades suspeitas ou potenciais ameaças à segurança do servidor. Araújo e Oliveira (2022) elucida que a segurança e a conformidade de servidores estão interligadas. As organizações precisam implementar medidas de segurança para proteger seus servidores e, ao mesmo tempo, garantir que essas medidas estejam em conformidade com as regulamentações aplicáveis.

Pois tudo deve estar em conformidade com as políticas que garantem que o servidor esteja de acordo com os padrões de segurança e regulamentações relevantes. Isto se aplica ainda à backup e recuperação onde também existem políticas de backup para proteger dados contra perdas acidentais ou ataques cibernéticos através de testes de recuperação feitos regularmente para testar a recuperação de dados garantindo que os backups estejam funcionando corretamente.

O monitoramento e gerenciamento de desempenho de servidores em nuvem são práticas contínuas e vitais para manter a operação eficaz de aplicativos e serviços. Utilizando ferramentas e práticas adequadas, as organizações podem garantir a disponibilidade, a escalabilidade e a segurança de seus recursos em nuvem.

2.2.10 Segurança e Conformidade

Silva (2023) diz que a segurança e a conformidade são dois dos principais desafios enfrentados pelas organizações que adotam a nuvem. A segurança protege os dados e aplicações da organização, e a conformidade atende às regulamentações aplicáveis. Já que a segurança e conformidade em um serviço de nuvem são pilares fundamentais para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas hospedados na nuvem. Esses aspectos tornam-se especialmente críticos em um ambiente virtualizado e distribuído, onde a proteção contra ameaças cibernéticas e o cumprimento de regulamentações são de extrema importância.

A criptografia de dados desempenha um papel crucial nesse contexto, assegurando que a informação seja protegida tanto durante o tráfego (em trânsito)

quanto quando está armazenada em servidores ou dispositivos (em repouso). Isso previne acessos não autorizados e protege contra interceptações indevidas.

Além disso, a autenticação e controle de acesso são implementados para verificar a identidade dos usuários e conceder permissões adequadas. A utilização de métodos de autenticação robustos, como senhas fortes e autenticação de dois fatores, bem como o controle preciso de quem tem acesso a quais recursos, contribuem para a segurança do ambiente.

Como é explicado por Silva (2023) a IAM é uma parte essencial da segurança na nuvem pois ao implementar medidas de IAM adequadas, as organizações podem reduzir o risco de acesso não autorizado aos seus dados e aplicações. Além disso, a auditoria de acesso registra e monitora as atividades dos usuários, fornecendo uma trilha de auditoria crucial para detectar e investigar potenciais violações de segurança.

O monitoramento contínuo da segurança, aliado à implementação de firewalls e controles de rede, contribui para proteger contra ameaças cibernéticas. A gestão de vulnerabilidades e aplicação de patches de segurança são práticas essenciais para corrigir possíveis brechas de segurança e manter o ambiente protegido.

Políticas de backup e testes de recuperação são vitais para garantir a disponibilidade e integridade dos dados em caso de incidentes ou falhas. Além disso, a conformidade com regulamentações legais é um requisito crucial para garantir a legitimidade das operações e proteger a privacidade dos dados.

Moraes e Oliveira (2021) alerta que a avaliação de riscos deve considerar uma variedade de fatores, incluindo a vulnerabilidade dos servidores, a probabilidade de uma ameaça ocorrer e o impacto potencial de uma violação. Por fim, a educação em segurança e avaliação de riscos são práticas que promovem uma cultura de segurança cibernética dentro da organização. Ao capacitar os usuários e identificar possíveis vulnerabilidades, a empresa fortalece suas defesas contra ameaças cibernéticas.

Em resumo, a segurança e conformidade em um serviço de nuvem são elementos essenciais para proteger os dados e sistemas, além de garantir que as operações estejam em conformidade com as regulamentações aplicáveis. A colaboração entre o provedor de serviços e o usuário é crucial para estabelecer e manter um ambiente de nuvem seguro e confiável.

2.3 IAAS, PAAS E SAAS

Silva, (2023) estabelece que a computação em nuvem é um modelo de computação que fornece acesso sob demanda a recursos computacionais, como servidores, armazenamento, rede e aplicativos, por meio da Internet. São elas IaaS (Infraestrutura como Serviço) oferece recursos de infraestrutura virtualizada, como servidores e armazenamento, permitindo aos usuários gerenciar e controlar sua própria plataforma e aplicativos.

PaaS (Plataforma como Serviço) proporciona um ambiente completo de desenvolvimento e execução de aplicativos, sem a necessidade de gerenciar a infraestrutura subjacente. Já o SaaS (Software como Serviço) fornece aplicativos hospedados na nuvem prontos para uso, acessíveis através de um navegador web, com o provedor responsável pela manutenção e atualizações. Cada modelo atende a diferentes necessidades, proporcionando flexibilidade e agilidade em ambientes de computação em nuvem.

2.3.1 IAAS (infraestrutura como serviço)

Para Oliveira (2023) o IaaS é uma opção ideal para organizações que precisam de flexibilidade e escalabilidade para suas necessidades de TI. (IaaS, ou Infraestrutura como Serviço, é um modelo de computação em nuvem que fornece recursos de TI virtualizados pela internet. Em vez de comprar e gerenciar servidores físicos, armazenamento e redes, os usuários alugam recursos virtuais de um provedor de serviços em nuvem.

As principais características são recursos virtualizados pois oferece uma ampla gama de recursos de TI virtualizados, como máquinas virtuais, armazenamento, redes e balanceadores de carga. Assim como elasticidade pois os recursos podem ser escalados para cima ou para baixo conforme a necessidade do usuário. Isso permite que as organizações paguem apenas pelos recursos que utilizam.

Self-service, sendo que os usuários têm a capacidade de provisionar e gerenciar seus próprios recursos de forma autônoma, sem a necessidade de intervenção manual do provedor de serviços através do acesso pela internet pois todos os recursos são acessados através da internet, o que proporciona flexibilidade e acesso remoto.

Existem o desenvolvimento e testes de aplicativos com as equipes de desenvolvimento que utilizam IaaS para criar e testar aplicativos em ambientes controlados e escaláveis numa hospedagem de sites e aplicações web assim reafirma Oliveira (2023) o IaaS é uma opção popular para organizações que precisam de um alto nível de controle sobre sua infraestrutura de TI. Pois as empresas podem hospedar seus sites e aplicativos em servidores virtuais na nuvem. Assim como fazer backup e recuperação de desastres através do modelo IaaS que fornece uma infraestrutura escalável e segura para armazenar backups e implementar estratégias de recuperação de desastres.

2.3.2 PAAS (plataforma como serviço):

Neste modelo de serviço Oliveira (2023) Estabelece que esta é uma opção ideal para organizações que precisam de uma plataforma de desenvolvimento de aplicativos flexível e escalável. Pois o modelo PaaS, ou Plataforma como Serviço, é um modelo de computação em nuvem que fornece um ambiente completo de desenvolvimento e implantação de aplicativos. Ele inclui tudo o que é necessário para construir, testar, hospedar e escalar aplicações.

As principais características desse ambiente de desenvolvimento é como o modo oferece ferramentas e ambientes de desenvolvimento que permitem aos desenvolvedores criar aplicativos de forma rápida e eficiente automatizando tarefas, em resumo Moraes e Oliveira explica que o PaaS é uma opção popular para organizações que precisam desenvolver e implantar aplicações rapidamente e com baixo custo. Utilizando gerenciamento de servidores, configuração de redes, atualizações de sistema operacional, permitindo que os desenvolvedores se concentrem no desenvolvimento de aplicativos.

Um dos fatores mais importantes, a escalabilidade pois assim como IaaS, PaaS oferece escalabilidade, mas aqui a ênfase está na escalabilidade da aplicação em vez da infraestrutura pois facilita a colaboração entre membros da equipe de desenvolvimento, permitindo o compartilhamento de código, gerenciamento de versões e integração contínua para desenvolvimento e hospedagem de aplicações web onde é ideal para construir, testar e hospedar aplicações web e móveis.

No desenvolvimento de software empresarial as empresas utilizam PaaS para criar e gerenciar aplicativos internos utilizando da integração e automação de

processos de negócio pois o modelo PaaS pode ser usado para integrar diferentes sistemas e automatizar os processos.

2.3.3 SAAS (software como serviço):

SaaS, ou Software como Serviço, é um modelo de distribuição de software onde o aplicativo é hospedado e gerenciado por um provedor de serviços na nuvem e disponibilizado para os usuários pela internet. Oliveira (2023) esclarece que esse modelo é uma opção ideal para organizações que precisam de acesso a softwares de última geração sem a necessidade de investimentos iniciais. algumas das principais características desde tipo de serviço são acesso pela internet pois os usuários acessam o software através de um navegador web, sem a necessidade de instalação local. Recebem atualizações automáticas oriundas do provedor de serviços que é responsável por manter e atualizar o software, garantindo acesso à versão mais recente.

Possuem modelo de assinatura que é oferecido sob um modelo de pagamento baseado em planos, Oliveira (2022) simplifica que esse modelo é uma opção para organizações de todos os tamanhos, pois oferece uma maneira simples e econômica de acessar o software. Pois os usuários pagam uma taxa regular (mensal ou anual).

Facilitando a escalabilidade e personalização limitada dos aplicativos SaaS oferecendo um nível de personalização limitado em comparação com soluções locais. Disponibiliza ferramentas de colaboração como e-mails, suítes de escritório, e soluções de videoconferência. Proporciona boa gestão de relacionamento com o cliente. Oferta sistemas de gerenciamento de conteúdo como plataformas de gerenciamento de conteúdo web como WordPress e Shopify.

Em resumo, IaaS fornece a infraestrutura básica de TI, PaaS oferece um ambiente de desenvolvimento e hospedagem de aplicativos, e SaaS entrega aplicativos prontos para uso através da nuvem. Cada modelo atende a necessidades diferentes, e muitas vezes são usados em conjunto para criar soluções de TI mais abrangentes.

2.4 Controle do ambiente: redes, energia, temperatura

Soares e Almeida (2023) estabelecem que o controle do ambiente de um servidor de nuvem é essencial para garantir a segurança e a disponibilidade dos recursos. Os controles de ambiente podem ser implementados por meio de ferramentas e processos. O controle do ambiente em um servidor garante que o equipamento funcione de maneira confiável e eficaz. Isso envolve o gerenciamento de diversos aspectos, incluindo redes, energia, temperatura e monitoramento. Algumas ferramentas foram criadas ou adaptadas para facilitar este tipo de monitoramento Sua funcionalidade é ampliável por meio de um sistema de extensões.

2.4.1 Gerenciamento de redes

O gerenciamento de redes é uma atividade essencial para garantir a disponibilidade, desempenho e segurança de uma rede de computadores como cita Araújo e Oliveira (2022). Pois os servidores precisam estar conectados a uma rede para que possam ser acessados remotamente e para que os dados possam ser transmitidos. Isso geralmente é feito por meio de cabos Ethernet ou, em algumas configurações, conexões sem fio.

Utilizando-se de equipamentos de rede, como switches e roteadores, ajudam a gerenciar o tráfego de dados dentro e fora do servidor. Eles garantem que os pacotes de dados sejam direcionados corretamente para seu destino, tudo sempre baseado na perfeita disponibilidade dos dados com os padrões foram estabelecidos.

Um dos fatores mais importantes em servidores é a proteção contra ataques de hackers, por isso devem ser protegidos por firewalls para evitar acessos não autorizados. Os firewalls filtram o tráfego de rede com base em regras de segurança para proteger o servidor contra ameaças. Este serviço está em constante atualização, pois a cada novas técnicas de invasão são desenvolvidas por hackers.

2.4.2 Gerenciamento de energia

Para evitar interrupções de energia, os servidores são frequentemente conectados a UPSs. Esses dispositivos fornecem energia de backup temporária para que o servidor possa ser desligado adequadamente em caso de queda de energia prolongada. Oliveira (2023) explica que o gerenciamento de energia de servidores é uma atividade essencial para reduzir os custos operacionais e o impacto ambiental.

Os servidores podem consumir uma grande quantidade de energia, portanto, é importante tomar medidas para otimizar seu consumo.

Alguns servidores têm recursos de gerenciamento de energia que permitem controlar o consumo de energia, como colocar partes do servidor em modo de suspensão quando não estão em uso. Há ainda por parte das maiores empresas que possuem servidores baseados em uma consciência ecológica, onde não emitem carbono, pois utilizam energia eólica e solar como por exemplo alguns servidores do Google.

2.4.3 Monitoramento de temperatura

Os servidores geram calor, e é importante manter a temperatura dentro de uma faixa aceitável para garantir seu funcionamento confiável. Como explicado por Oliveira (2023) a temperatura é um dos fatores mais importantes para o funcionamento e a longevidade dos servidores. Os servidores precisam ser mantidos em uma temperatura adequada para evitar o superaquecimento, que pode causar danos ao hardware e perda de dados.

Isso é feito por meio de sistemas de resfriamento, como ventiladores e sistemas de refrigeração líquida a exemplo do Google e Facebook que utilizam do clima e água do mar para resfriar seus servidores. Alguns servidores se beneficiam do clima gélido onde está localizado, outros são beneficiados com resfriamento eólico, pois são estrategicamente alocados em região que possuem fortes ventos em boa parte do ano, a exemplo disso o Google possui servidores com estas características.

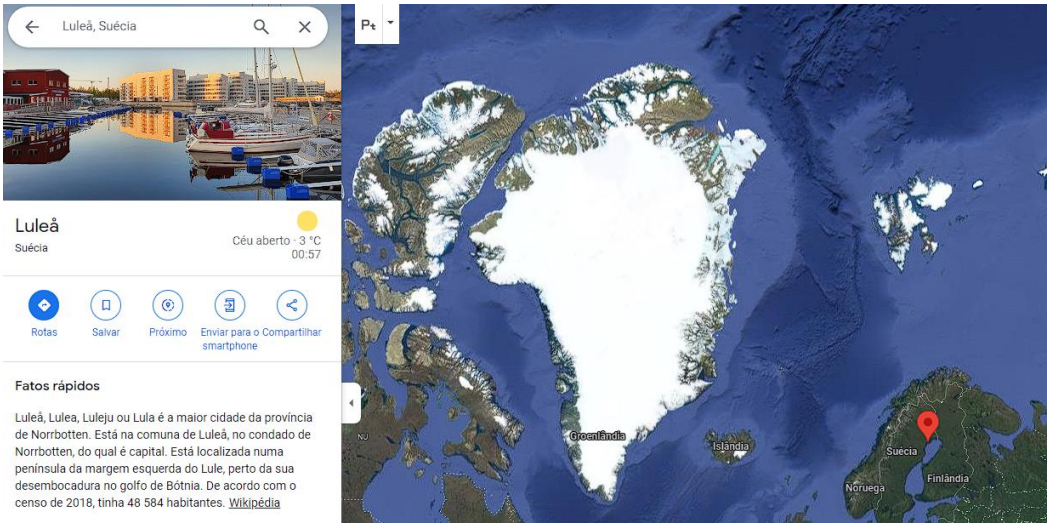
Além do método tradicional de instalação de sensores de temperatura nos servidores, existem diversas abordagens para monitorar a temperatura desses sistemas, como discutido por Araújo e Oliveira (2022). Uma alternativa comum envolve a utilização de termopares e termo resistores para obter medições precisas. Além disso, a termografia infravermelha é uma técnica avançada que permite visualizar variações de temperatura em diferentes partes dos servidores.

Estes dados podem ser integrados em softwares de monitoramento dedicados, proporcionando uma visão abrangente e em tempo real do estado térmico dos equipamentos. Isso contribui para um controle mais efetivo e proativo das condições de operação dos servidores.

Além disso, é importante destacar que a eficiência do sistema de monitoramento é crucial para garantir o funcionamento adequado dos servidores. Portanto, são empregados sensores estrategicamente posicionados dentro e ao redor dos equipamentos, que monitoram continuamente a temperatura. Caso seja detectada uma condição crítica, o sistema de monitoramento, como mencionado anteriormente, é capaz de gerar alertas instantâneos. Estes alertas podem, por sua vez, acionar automaticamente medidas adicionais de resfriamento, assegurando assim a integridade e a performance dos servidores.

Muitos fatores são levados em consideração quando o assunto é resfriamento de servidores pois até mesmo a geolocalização do local onde servidor será instalado muitas vezes é levada em consideração não só baseado do ponto de vista econômico, mas sim na criticidade que é levada em consideração, pois resfriar milhares de servidores trabalhando initerruptamente não é tarefa fácil, exatamente por isso Mark Zuckerberg escolheu uma cidade Sueca chamada Luleå que se encontra localizada no Ártico conforme mostra figura 5, por lá a temperatura varia de -14 °C a 20 °C.

Figura 5: Cidade de Luleå na Suécia que se encontra no Ártico.



Fonte: google (2023).

2.4.4 Softwares de monitoramento

Soares e Almeida (2023) cita que os softwares de monitoramento podem ajudar as organizações a identificar problemas potenciais antes que eles causem interrupções ou perda de dados, estas ferramentas de software são usadas para monitorar o desempenho do servidor, a utilização da CPU, a memória, o

armazenamento e outros parâmetros a exemplo do Grafana mostrado na figura 6 que é uma plataforma web de análise e visualização de código aberto, compatível com múltiplas plataformas oferecendo recursos como tabelas, gráficos e alertas na web ao ser integrado a fontes de dados compatíveis.

Figura 6: Grafana, tela com monitoramento com alguns parâmetros.

Fonte: unirede (2017).

Eles também podem rastrear o tráfego de rede e a integridade dos serviços em execução. Quando ocorrem falhas relacionadas ao alto uso de CPU, baixo espaço em disco ou falhas de hardware, podem gerar alertas e notificações para que a equipe de TI possa tomar medidas corretivas.

Essa capacidade de gestão remota representa uma faceta fundamental nos servidores contemporâneos, uma vez que proporciona aos administradores a habilidade de acessar e controlar os sistemas, mesmo quando estão geograficamente distantes. Essa funcionalidade desempenha um papel crucial na resolução de problemas e na realização de manutenções preventivas e corretivas de forma eficiente e conveniente.

Moraes e Oliveira (2021) explica que a gestão remota de servidores é uma necessidade para muitas organizações, pois oferece uma série de benefícios que podem ajudar a melhorar a eficiência, a disponibilidade e a segurança dos servidores. Além disso, ao eliminar a necessidade de presença física, a gestão remota reduz significativamente o tempo de resposta em situações críticas, permitindo uma intervenção rápida e assertiva em casos de falhas ou emergências. Essa capacidade

é, sem dúvida, um dos pilares que sustentam a eficácia e a confiabilidade dos servidores modernos.

O Grafana é uma plataforma poderosa de observabilidade que oferece diversas funcionalidades importantes como visualização de dados, Dashboard Personalizados, alertas, exploração de dados, suportes a diversas fontes de dados, é multiplataforma pois pode ser instalado em diferentes sistemas operacionais e ambientes, incluindo Linux, Windows e Docker, possuem extensa compatibilidade com plug-ins e integração com ferramentas de devOps, suportes a equipes de trabalhos possibilitando a colaboração em tempo real entre membros de uma equipe, facilitando a análise e tomada de decisões conjuntas.

Essas são apenas algumas das principais funcionalidades do Grafana. Silva (2023) explica que além de ser uma plataforma de análise de dados e monitoramento de código aberto, ele permite que os usuários visualizem dados de várias fontes, não apenas serviços de nuvem. Sua versatilidade e capacidade de integração o tornam uma ferramenta essencial para equipes que necessitam monitorar e analisar dados em tempo real onde a eficiência terá o resultado que se espera garantido a disponibilidade aos clientes.

Em resumo, o controle do ambiente em um servidor é essencial para garantir seu funcionamento contínuo e confiável. Isso envolve gerenciar a conectividade de rede, garantir uma alimentação elétrica estável, manter a temperatura sob controle e monitorar constantemente o desempenho e a saúde do servidor. Essas práticas garantem que o servidor seja um recurso confiável para as operações de uma organização.

3. POLÍTICAS DE SEGURANÇA E REGULAMENTAÇÃO

Seja qual for a inovação no mercado sempre haverá resistência por parte de muitos usuários, isso é um pouco mais elevado quando o assunto é tecnologia, muitas vezes por falta de habilidades específicas, outras por resistência cultural onde muitos ainda insistem que se algo está dando certo, não deve haver mudança, mesmo que seja para evoluir, porém o que mais causa desconfiança é o medo de ter dados expostos na rede web, medo maior ainda quando se trata do meio corporativo. Disto isto Silva (2023) afirma que a segurança é um aspecto fundamental da computação

em nuvem. As organizações que usam serviços de nuvem devem implementar políticas e procedimentos de segurança para proteger seus dados e sistemas

As políticas de segurança em um serviço de nuvem são essenciais para garantir que os dados e os recursos hospedados na nuvem estejam protegidos contra ameaças e acessos não autorizados. Três dos principais aspectos dessas políticas são confiabilidade, integridade e disponibilidade.

3.1 Confiabilidade, Integridade e Disponibilidade

A confiabilidade refere-se à capacidade do serviço de nuvem de manter a consistência e a precisão dos dados e dos recursos hospedados. É crucial para garantir que as informações armazenadas na nuvem sejam precisas e confiáveis para os usuários e os sistemas que as utilizam. Silva (2023) estabelece que A confiabilidade, integridade e disponibilidade de servidores em nuvem são fatores essenciais para garantir a continuidade dos negócios. A natureza distribuída da nuvem, que envolve múltiplos provedores de serviços, torna esses fatores mais desafiadores.

Algumas características de segurança são a redundância pois utiliza de sistemas redundantes para evitar falhas únicas de pontos de falha únicos. Isso pode incluir a replicação de dados em servidores geograficamente distintos. Assim como backups regulares quem mantem cópias de segurança dos dados, permitindo a restauração em caso de perda ou corrupção.

Possuir monitoramento contínuo com a implementação de sistemas de monitoramento para detectar falhas ou anomalias rapidamente, permitindo a intervenção imediata pois uma plataforma de nuvem pode usar arquiteturas de alta disponibilidade, como clusters de servidores e balanceamento de carga, para garantir que os serviços estejam sempre disponíveis mesmo em caso de falhas de hardware ou software.

A integridade se refere à proteção dos dados contra modificações não autorizadas ou não intencionais. Neste ponto Soeres e Almeida (2023) define que A integridade de dados é um dos principais desafios da computação em nuvem. A natureza distribuída da nuvem, que envolve múltiplos provedores de serviços, torna a integridade mais complexa. Os clientes precisam implementar medidas para garantir

a integridade de seus dados na nuvem. É fundamental para assegurar que as informações armazenadas permaneçam precisas e íntegras ao longo do tempo.

Para isso são necessárias que algumas medidas de segurança sejam devidamente postas em prática como controle de acesso utilizando de políticas de controle de acesso rigorosas para garantir que apenas usuários autorizados possam modificar os dados.

Contam com assinaturas digitais utilizando técnicas criptográficas, como assinaturas digitais, para verificar a autenticidade dos dados e garantir que não foram alterados assim como o uso de Checksums e hashes, algoritmos de hash para verificar a integridade dos dados. Se um arquivo for modificado, o hash será alterado, indicando a violação da integridade. Um exemplo de implementação do sistema é o uso de criptografia de dados em trânsito e em repouso para garantir que os dados não sejam interceptados ou alterados durante a transmissão ou armazenamento.

A disponibilidade refere-se à garantia de que os serviços e os recursos da nuvem estão sempre acessíveis quando necessário. É crucial para manter a continuidade dos negócios e a satisfação dos usuários, Silva (2023) explica que a disponibilidade de dados é um fator importante a ser considerado na adoção de serviços de nuvem. Ao adotar medidas para proteger a disponibilidade de seus dados, as organizações podem reduzir o risco de interrupção de negócios.

Assim como as outras duas políticas de segurança citadas anteriormente muitas medidas de segurança são de suma importação neste parâmetro também como planejamento de capacidade e dimensionamento adequado dos recursos para atender à demanda, evitando sobrecargas e garantindo uma resposta rápida.

Outro fator levado em consideração é a distribuição geográfica pois ter data centers em diferentes localizações geográficas reduz o impacto de eventos adversos locais (como desastres naturais) na disponibilidade dos serviços, tudo isso através de monitoramento em tempo real que utiliza de ferramentas de monitoramento para detectar falhas e iniciar procedimentos de recuperação automaticamente pois respeita o nível de serviço contratado onde foram definidos padrões de disponibilidade.

Vale ressaltar que a segurança na nuvem é uma responsabilidade compartilhada entre o provedor de serviços de nuvem e o cliente. Como explica Soares e Almeida (2023), A responsabilidade compartilhada é um conceito complexo que pode ser difícil de implementar na prática. No entanto, é fundamental para garantir a segurança e a conformidade dos ambientes de nuvem. O provedor é responsável

pela segurança da infraestrutura, enquanto o cliente é responsável pela segurança dos dados e sistemas que coloca na nuvem. Portanto, é essencial que ambas as partes trabalhem em conjunto para garantir a segurança abrangente dos serviços em nuvem.

3.4 Regulamentação

É muito corriqueiro notícias sobre vazamentos de dados pessoais ou de empresas, até mesmo empresas que utilização serviço de nuvem próprio, ou seja, definiram um setor da empresa para se responsabilizar apenas por essa parte, como foi caso do facebook, empresa multibilionária do ramo das redes sociais que sofreu um ataque e teve dados da milhões de pessoa vazados na web, nesse contexto a problemática é entre usuário e rede social, muitos nem sabem que tiveram seus dados vazados e por isso punições nem foram aplicadas.

Hoje tal parâmetro tem se alterado, Soares e Almeida (2023) explica que as regulamentações podem afetar significativamente a forma como as organizações usam serviços de nuvem. As organizações precisam estar cientes das regulamentações que se aplicam aos seus dados e sistemas para garantir que estejam em conformidade

Assim quando acontece com uma empresa especializada em serviços de nuvem, que é contratada para armazenar dados e arquivos, onde a relação de empresa cliente é firmada via contrato, onde são listados deveres da empresa e do cliente com punições previstas em leis é preciso está muito atento e a par destas leis que regulamentam o serviço.

Tratando-se de dados pessoais é imprescindível que fique bem claro como anda a regulamentação deste serviço no Brasil e no mundo, Moraes Oliveira (2021) explica que a regulamentação do serviço de nuvem pode ajudar a promover a confiança e a aceitação da nuvem por parte das organizações. As organizações precisam ter certeza de que seus dados estão seguros e protegidos quando armazenados na nuvem.

Entender quais leis já foram criadas, que sofreram alterações, quantas existem, casos de punições, tudo o que puder deixar o usuário mais tranquilo e também atrair mais empresas para esse ramo, pois além de ser uma ferramenta muito prática o que mais atraem usuários e empresas é a questão de sair muito mais barato do que montar

uma estrutura física local para fazer esse serviço, a começar dos custos com equipamentos, montagem, configuração, pessoas especialistas para cuidar dos sistemas, tem ainda o custo com manutenção, gastos com energia, tudo isso faz aumentar a procura.

Hoje no Brasil a principal lei que rege este e outros seguimentos é a LGPD – Lei Geral de Proteção de Dados, criada em 14 de agosto de 2018, pelo presidente Michel Temer (LGPD), sancionada sob o número 13.709/2018, disponível a partir de fevereiro de 2020, baseada em regras morais como a transparência, a justificação de custos e a sinceridade. Esta surgiu como um complemento a Lei 12.296/2014, popularmente denominado “Marco Civil da Internet”. C. E. Souza (2014) cita que O Marco Civil da Internet, de 2014, também se aplica aos serviços de nuvem. O Marco Civil estabelece regras para a liberdade de expressão, a privacidade e a segurança na internet.

Quanto a Lei Geral de Proteção de Dados A LGPD explica:

> Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Art. 5º - inciso X, a lei estabelece o tratamento de dados como qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Ainda é necessário esclarecer que anda em paralelo com o Código de Defesa do Consumidor, Lei de Acesso à Informação e a Lei do Cadastro Positivo e a Resolução BACEN 4.658/2018.

Em resumo a LGPD veio para unificar todas as regulamentações já existentes e estabelecer novos parâmetros a serem seguidos, pois ela se aplica no cuidado com informações, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que os tratamentos sejam realizados em território nacional. Abrange também todas as empresas estabelecidas em território nacional, bem como as organizações com sede no exterior que ofereçam produtos e serviços para pessoas localizadas no Brasil ou tenham operações no país.

No Brasil a Cyrela tornou-se a primeira empresa brasileira a receber uma condenação por violação de dados conforme a LGPD. O incidente ocorreu em

novembro de 2018 e teve seu desfecho judicial em 2020, culminando na determinação de uma indenização de R$10 mil para o cliente cujas informações foram compartilhadas com parceiros da empresa sem o seu consentimento.

A situação teve origem quando um cliente finalizou a compra de um apartamento junto à Cyrela em 2018. Posteriormente, passou a receber contatos de instituições financeiras e empresas de decoração oferecendo serviços para sua nova propriedade. O cliente decidiu mover uma ação contra a empresa e obteve sucesso com base na LGPD e nos direitos assegurados pelo Código de Defesa do Consumidor.

A juíza Tonia Yuka Koroku, da 13ª Vara Cível de São Paulo, considerou que a Cyrela transgrediu princípios que envolvem a honra e a privacidade do cliente, bem como violou sua esfera íntima ao expor seus dados e detalhes da compra do imóvel. Além da indenização, a empresa foi sentenciada a não mais divulgar os dados pessoais ou financeiros de clientes, sob pena de multa de R$ 300,00 a cada contrato indevidamente utilizado.

O caso mencionado anteriormente marca o pioneirismo no registro de incidentes sob a LGPD no Brasil. No entanto, desde então, diversos outros casos têm sido tratados com base nessa legislação, envolvendo gigantes da tecnologia como Google, Facebook e outras empresas renomadas. Algumas dessas situações já resultaram em penalidades aplicadas, enquanto outras ainda estão em fase de tramitação nos tribunais. Esse cenário destaca a relevância e o impacto abrangente da LGPD no âmbito jurídico e na proteção dos direitos dos cidadãos em relação aos seus dados pessoais.

Além de todas essas regulamentações brasileiras, é importante ressaltar a existência de diversas regulamentações internacionais, Soares e Almeida (2023) explica que as organizações também podem trabalhar com consultores jurídicos ou especialistas em conformidade para ajudá-las a entender e cumprir as regulamentações internacionais que, mesmo diante das mudanças no cenário nacional, continuam sendo amplamente utilizadas como referência e modelo.

Durante muito tempo, essas normas internacionais desempenharam um papel fundamental na tentativa de padronizar os serviços de proteção de dados, dada a ausência de regulamentações nacionais específicas. Algumas das regulamentações internacionais mais conhecidas e respeitadas incluem:

- GDPR - Regulamentação Geral de Proteção de Dados dos Estados Unidos;
- CCPA - Lei de Segurança Cibernética da China;
- Lei de Privacidade do Consumidor da Califórnia (CCPA).

Ao pesquisar mais a fundo é possível entender o porquê de muitas pessoas e empresas ainda optarem por armazenar seus dados localmente em computadores pessoais ou servidores locais, muitos não possuem conhecimento da área e isso acaba sendo o principal motivo, gerando medo de mudar, outros até pensam em aderir a este tipo de serviço, mas a forma como a informação é repassada ainda não é clara o suficiente para atrair as grandes massas, falta um empenho por parte do fornecedores em praticar o bom e velho porta a porta.

Neste ponto Soares e Almeida (2023) sugere que os provedores de serviços em nuvem podem aumentar a transparência de seus serviços de várias maneiras. Eles podem fornecer documentação clara e concisa sobre seus serviços, políticas e práticas de segurança. Eles também podem fornecer relatórios periódicos sobre a segurança e a disponibilidade de seus serviços. Além disso, eles podem oferecer acesso aos clientes aos seus dados e sistemas na nuvem.

A principal vantagem que muitos não têm conhecimento é o que as corporações mais buscam economia pois armazenar dados em computadores locais não é seguro, já que uma perda de dados, seja por invasão ou falha mecânica, pode resultar em prejuízos consideráveis. Além disso, a estruturação de um servidor pessoal não é uma empreitada barata.

Diversos são os custos que se associam à gestão operacional tradicional de infraestrutura, abarcando desde os gastos inerentes à manutenção, expansão do quadro de funcionários, atualizações de sistema, e manutenções regulares até as despesas diretas com energia, entre uma série de outros elementos.

Em síntese, a relação de despesas a considerar revela-se extensa e multifacetada. Diante desse cenário, a opção estratégica pela adoção da computação em nuvem não apenas se traduz em uma alternativa intrinsecamente mais segura, mas também, crucialmente, configura-se como uma escolha economicamente mais viável para as corporações.

Essa migração para a nuvem não só alivia significativamente a pressão financeira decorrente dos custos operacionais tradicionais como afirmam Araújo e Oliveira (2022) onde estimam que as organizações podem economizar até 70% em

custos operacionais ao migrar para a nuvem representando um paradigma econômico mais eficiente, permitindo que as empresas otimizem seus recursos financeiros de maneira mais ágil e adaptável às dinâmicas exigências do mercado contemporâneo.

O que realmente falta é colocar esses números à mesa, mesmo que o foco em segurança seja deixado um pouco de lado, pois no fim das contas o que acaba importando mais é o bolso. Acredito que tudo isso atrelado a forma como a empresa trata os dados, que tecnologias são usadas, quadro de pessoal qualificado, procedência da estrutura computacional, contratos com empresas importantes do mesmo ou de outros seguimentos, forma como foi tratado possíveis ataques hackers, processos na justiça.

A transparência é essencial nesta discussão, abrangendo clareza desde os aspectos jurídicos até os financeiros. Proporcionar ao cliente tranquilidade ao confiar em nós é crucial. Manter essa transparência é a base na qual construímos confiança e segurança, solidificando nossa parceria e compromisso mútuo.

Soares e Almeida (2023) ressalta que a computação em nuvem está se tornando cada vez mais popular no Brasil. De acordo com uma pesquisa da IDC, o mercado brasileiro de serviços de nuvem deve atingir US$ 11,6 bilhões em 2023, representando um crescimento de 25% em relação a 2022.

À medida que os serviços de nuvem prosseguem em sua trajetória ascendente, conquistando uma popularidade cada vez mais robusta e consolidando-se como uma parte incontestável da infraestrutura tecnológica contemporânea, a temática da segurança na computação em nuvem mantém-se como um tópico de extrema relevância e complexidade.

Apesar de os primeiros serviços dessa natureza terem sido introduzidos no cenário tecnológico no início dos anos 2000, sua adoção inicial foi marcada por uma gradualidade notável, principalmente devido às legítimas e prementes preocupações relacionadas à segurança que permeavam o ambiente tecnológico daquela época.

Araújo e Oliveira (2022) explica que o uso da nuvem é impulsionado por uma variedade de fatores, incluindo a necessidade de organizações de reduzir custos, aumentar a eficiência e melhorar a flexibilidade, mesmo nesse contexto inicial de cautela e hesitação contribuiu para a formação de uma base crítica de discussões e desenvolvimentos na esfera da segurança da informação, delineando, assim, o atual panorama no qual a segurança na computação em nuvem é considerada uma prioridade inalienável para empresas e usuários. No entanto, a crise financeira de

2008 representou um ponto de inflexão crucial que impulsionou de maneira notável a adesão aos serviços de nuvem.

Nesse contexto, as empresas estavam ávidas por encontrar maneiras de reduzir custos e aumentar a eficiência operacional, tornando a computação em nuvem uma solução altamente atraente. No entanto, essa mudança paradigmática também demandou um foco aprimorado na segurança desses serviços, uma vez que a confiança na proteção e integridade dos dados tornou-se mais crucial do que nunca.

A crescente migração de dados sensíveis para serviços de nuvem gerou uma preocupação substancial em relação à segurança da computação em nuvem. Soares e Almeida (2023) explica que a migração desses dados é uma decisão importante que deve ser tomada com cautela pois as organizações precisam considerar os riscos e benefícios envolvidos antes de tomar uma decisão.

Esse cenário impulsionou um significativo avanço no desenvolvimento de padrões e diretrizes de segurança específicos para esse ambiente. Em um marco importante, em 2009, o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos publicou o pioneiro documento de orientação sobre segurança da nuvem, intitulado "Considerações de Segurança para Sistemas em Nuvem".

Nos anos seguintes, a crescente demanda por soluções de segurança na nuvem impulsionou significativamente as atividades de pesquisa e desenvolvimento nessa área. Um exemplo notável foi a introdução, em 2011, do "Guia de Segurança para a Nuvem Computacional" pela Agência Nacional de Segurança dos Estados Unidos. Esse guia se destacou ao oferecer orientações abrangentes e atualizadas sobre as melhores práticas de segurança na computação em nuvem.

Em um significativo avanço em direção à padronização internacional no campo da segurança da informação, é digno de nota que a Organização Internacional de Normalização (ISO) apresentou, no ano de 2014, o padrão ISO/IEC 27018:2014. Este padrão, meticulosamente elaborado, estabelece os requisitos e diretrizes para assegurar a proteção dos dados pessoais em serviços de nuvem.

Silva (2023) explica que a padronização internacional é um processo de desenvolvimento de padrões por um grupo de partes interessadas, geralmente representando diferentes setores ou organizações. Os padrões internacionais são desenvolvidos por consenso e são projetados para serem usados globalmente. Tais marcos representam um firme compromisso a nível global para fomentar a segurança.

4. METODOLOGIA

Conforme os objetivos delineados na primeira seção, este trabalho é classificado como uma pesquisa explicativa, a qual se destaca por sua finalidade de identificar e analisar as causas e razões fundamentais relacionadas ao tema de nuvem computacional (Gil, 2007). Essa abordagem se propõe a aprofundar o entendimento dos fatores determinantes ou contribuintes para a ocorrência dos fenômenos, proporcionando uma visão mais abrangente e esclarecedora do campo de estudo em questão.

Além disso, é crucial ressaltar que esta pesquisa se insere na categoria de pesquisa aplicada, pois visa adquirir conhecimento com o propósito direto de aplicá-lo em um contexto específico. Gil (2010, p. 27). Dessa forma, o objetivo não se restringe apenas à compreensão dos elementos fundamentais da computação em nuvem, mas também busca ativamente contribuir para a aplicação prática desse conhecimento em cenários reais e tangíveis. Ao fazer isso, a pesquisa assume um papel ativo na solução de desafios e na melhoria da eficiência e eficácia de sistemas e processos relacionados à nuvem computacional.

No que tange ao procedimento metodológico, a pesquisa adotou uma abordagem de revisão teórica por meio de uma pesquisa bibliográfica. Essa etapa se revelou essencial para aprofundar o entendimento sobre o tema de nuvem computacional e avaliar seu desenvolvimento ao longo do tempo, conforme preconizado por Marconi e Lakatos (2010, p. 166). Ao colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre o assunto, a pesquisa bibliográfica proporcionou uma base sólida e abrangente para a condução deste estudo.

Adicionalmente, vale destacar que a pesquisa bibliográfica desempenhou um papel fundamental na construção sólida e substancial das ideias apresentadas, fortalecendo a base deste estudo. Através de uma meticulosa busca por artigos, livros e recursos audiovisuais, foi possível explorar de forma abrangente uma ampla gama de tópicos relacionados ao funcionamento, segurança e regulamentação dos serviços de computação em nuvem. Esse minucioso levantamento enriqueceu consideravelmente o espectro de informações disponíveis para este trabalho, assegurando a integridade e a confiabilidade dos dados utilizados.

5. RESULTADOS E DISCUSSÕES

A computação em nuvem emergiu como uma mudança radical da infraestrutura tecnológica moderna, revolucionando a maneira como empresas e indivíduos acessam e gerenciam dados e aplicativos. Neste contexto, a nuvem se revela como um ecossistema complexo, composto por servidores, redes e serviços que oferecem escalabilidade e flexibilidade sem precedentes.

Para Silva, (2023):

> A computação em nuvem é um modelo de provisionamento de recursos computacionais, como servidores, armazenamento, rede e aplicativos, de forma automatizada e sob demanda, por meio da Internet. Esse modelo oferece uma série de benefícios para as organizações, como escalabilidade, flexibilidade, redução de custos e agilidade.

A virtualização e a abstração de recursos físicos possibilitam a alocação dinâmica de capacidade computacional, proporcionando uma agilidade que transforma as operações empresariais. Ao aprofundar a análise do funcionamento da computação em nuvem, torna-se evidente que sua capacidade de adaptação e resposta às demandas do usuário desempenha um papel crucial em seu sucesso.

No entanto, a segurança na computação em nuvem emerge como um tema crítico e frequentemente preponderante. Soares e Almeida (2023) afirmam que as organizações que não adotarem a computação em nuvem ficarão para trás em termos de competitividade e eficiência. As organizações que desejam aproveitar os benefícios da computação em nuvem precisam entender os fundamentos da computação em nuvem e como aplicá-la de forma eficaz em seus negócios

A natureza distribuída da nuvem, apesar de seus benefícios, apresenta desafios significativos de segurança. A necessidade de robusta autenticação, criptografia em trânsito e em repouso, além da proteção contra ameaças, é imperativa para assegurar a integridade e confidencialidade dos dados. Essas medidas são essenciais para estabelecer confiança e viabilidade nos serviços de nuvem como solução segura para a gestão de dados sensíveis.

Além disso, a clareza nas responsabilidades de segurança entre provedores e usuários de serviços de nuvem é essencial para evitar lacunas na proteção, Pois Oliveira (2023) explica que a definição das responsabilidades de segurança entre Provedor e o usuário da nuvem é importante para garantir que ambas as partes estejam comprometidas com a segurança dos dados. Uma abordagem proativa para

a segurança na nuvem é, portanto, uma necessidade incontornável, visto que os riscos cibernéticos evoluem em paralelo com o avanço da tecnologia.

Isso acarreta necessidade que desenvolvedores trabalhem mais rápidos e sejam mais eficientes em comparação aos que tentam burlar a segurança e obter vantagem indevida a margem da lei de dados dos clientes, identificar e conter tais práticas em tempo hábil é um diferencial nos serviços prestados.

Para Soares e Almeida, (2023):

> A segurança é um dos principais desafios da computação em nuvem. A natureza distribuída da nuvem, que envolve múltiplos provedores de serviços, torna a segurança mais complexa. As organizações que adotam a nuvem precisam implementar medidas de segurança para proteger seus dados e aplicações.

A conformidade com regulamentações é crucial na computação em nuvem, que abrange setores diversos, como saúde e finanças. O escopo das leis aplicáveis, exemplificado pelo Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, impacta diretamente o armazenamento e processamento de dados na nuvem. Entender e aplicar essas regulamentações é essencial para garantir a conformidade e evitar implicações legais e financeiras.

Em um cenário de constante evolução tecnológica, é imperativo enfrentar os desafios emergentes e buscar soluções inovadoras na computação em nuvem. Silva (2023) explica que essa constante evolução pode ser um desafio para as organizações que usam serviços de nuvem. As organizações precisam estar cientes das últimas tendências e tecnologias em nuvem para garantir que estejam usando os serviços certos para atender às suas necessidades.

A arquitetura multicloud surge como uma estratégia valiosa para mitigar a dependência de um único provedor de nuvem, oferecendo redundância e resiliência em face de possíveis falhas. Além disso, a implementação de práticas de segurança robustas, como auditorias regulares e monitoramento contínuo, representa uma abordagem proativa para garantir a integridade dos dados armazenados na nuvem. À medida que a nuvem continua a moldar o panorama tecnológico, a adaptação a essas novas práticas e a busca por soluções inovadoras são essenciais para manter a segurança e a conformidade na das operações empresariais.

6. CONSIDERAÇÕES FINAIS

Este Trabalho de Conclusão de Curso apresentou uma análise minuciosa e abrangente de um tema que desempenha um papel cada vez mais crucial e central no cenário da tecnologia da informação. A pesquisa mergulhou profundamente nas intrincadas complexidades da computação em nuvem, investigando meticulosamente não apenas o seu funcionamento intricado, mas também os desafios de segurança que a permeiam e o contexto regulatório que exerce influência sobre sua aplicação.

Ao longo da investigação, tornou-se manifestamente claro que a computação em nuvem se destaca como uma tecnologia incrivelmente versátil, capaz de proporcionar escalabilidade, flexibilidade e eficiência operacional a empresas e organizações de todas as dimensões e áreas de atuação.

Não obstante, ressaltou-se com veemência a importância de uma abordagem cautelosa e meticulosa no que tange à segurança, visto que a preservação dos dados e a proteção da privacidade dos usuários emerge como uma inquietação permanente e premente. Ademais, a adesão irrestrita e diligente às regulamentações, a exemplo do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e outras legislações locais pertinentes, emerge como um pilar fundamental e inalienável, garantindo que a utilização da computação em nuvem ocorra de modo ético e responsável.

Em última análise, extrai-se a conclusão inescapável de que a computação em nuvem se configura como uma ferramenta exponencialmente poderosa, entretanto, sua exploração requer um entendimento profundo de seu funcionamento e, de forma igualmente importante, uma postura proativa voltada para a garantia da segurança dos dados e a observância das regulamentações pertinentes e aplicáveis.

À medida que a tecnologia prossegue em sua trajetória evolutiva, impera a necessidade premente de que empresas e profissionais do setor se mantenham atualizados e em consonância com as melhores práticas de segurança e as regulamentações em constante transformação. Dessa forma, este Trabalho de Conclusão de Curso se erige como um guia informativo e crítico, proporcionando orientação valiosa em meio a esse cenário em perene mutação e evolução.

A pesquisa sobre nuvem computacional desempenha um papel fundamental na transformação e avanço da sociedade contemporânea, influenciando diversas áreas da vida cotidiana e impulsionando inovações tecnológicas. Ao proporcionar

acesso remoto a recursos computacionais, armazenamento de dados e serviços via internet, a nuvem elimina barreiras geográficas e facilita a colaboração global.

Essa abordagem flexível e escalável tem impactos significativos em setores como educação, saúde, negócios e pesquisa científica. Na educação, por exemplo, a nuvem viabiliza a implementação eficiente de ambientes virtuais de aprendizado, enquanto na área da saúde, facilita o compartilhamento seguro de informações médicas e agiliza diagnósticos. No ambiente empresarial, a nuvem permite a escalabilidade rápida de infraestrutura de TI, promovendo a inovação e a eficiência operacional.

Além disso, a pesquisa contínua sobre nuvem computacional é crucial para aprimorar a segurança, confiabilidade e eficácia dessas tecnologias, garantindo que seus benefícios sejam maximizados e seus desafios mitigados, contribuindo assim para uma sociedade mais conectada e avançada.

A pesquisa em nuvem é crucial na academia, impulsionando avanços em computação, ciência da informação e tecnologia. Acadêmicos exploram aspectos teóricos e práticos, desenvolvendo abordagens que aprimoram eficiência, segurança e escalabilidade. A nuvem facilita experimentos em larga escala e coleta de dados, impulsionando inteligência artificial, aprendizado de máquina e análise de dados. A colaboração entre pesquisadores é facilitada pela nuvem, promovendo progresso rápido, inovações e formação de profissionais para desafios na era digital.

A pesquisa em nuvem desempenha um papel essencial para os profissionais, proporcionando valiosos insights e impulsionando o desenvolvimento contínuo de habilidades. Ao acompanhar as mais recentes descobertas, esses profissionais mantêm-se atualizados com as tecnologias emergentes no cenário digital. A pesquisa contribui para aprimorar práticas de segurança e eficiência operacional, permitindo a implementação de estratégias mais eficazes.

O aprofundamento do conhecimento sobre os detalhes intricados da nuvem não apenas capacita os profissionais, mas também os habilita a conceber e implementar soluções altamente inovadoras, que conseguem enfrentar e satisfazer as demandas em constante evolução com uma eficácia notável. Essa pesquisa contínua e a assimilação de novas percepções na nuvem são cruciais para o desenvolvimento profissional, fomentando um ambiente de trabalho que se destaca pela sua dinamicidade e competitividade, onde profissionais estão constantemente à frente, moldando o futuro da tecnologia e da inovação.

REFERÊNCIAS

Aguiar, F. **Hyper-V**: Guia Completo. São Paulo. 2023. Editora Novatec.

Araújo, P. R. M. e Oliveira, P. S. S. M. Gerenciamento de Redes de Computadores. Porto Alegre. 2021. Editora Sagra Luzzatto.

BROWN, c.; GREEN, D. **Software**: Princípios e Prática. 3 ed. Campina Grande-PB. 2021. Editora Universitária da UFPB.

Cohn, M. Design de API para Desenvolvedores. São Paulo. 2023. Editora Novatec.

Dell. (2023). Dell. Disponível em: http://www.lojati.com.br/Dell/Servidores/SVRR620/Servidor_em_Rack_Dell_PowerEdge_R620.aspx. Acesso em: 15 de Setembro de 2023.

DOE, J. **Virtualização**: Fundamentos e Aplicações. 2 ed. Rio de Janeiro. 2020. Editora Elsevier.

FERREIRA, J. E. **Computação em Nuvem:** Transformando o seu Negócio. 1 ed. São Paulo. 2013. Editora Novatec.

Google. (2023). Dell. Disponível em: https://www.google.com/maps/place/Lule%C3%A5,+Su%C3%A9cia/@65.5867107,22.0999815. Acesso em: 02 de Outubro de 2023.

Grafana. (2017). Grafana. Disponível em: https://www.unirede.net/zabbix-grafana/grafana01/. Acesso em 05 de Outubro de 2023.

Fowler, M. **Arquitetura de Software**: Princípios, Padrões e Práticas. São Paulo. 2023. Editora Novatec.

SOFTWARE, Opus. **Computação em Nuvem:** O que você realmente precisa saber. 1 ed. São Paulo, 2015. Editora Opus Software.

SMITH, J. **Orquestração de Contêineres**: Práticas Recomendadas. 2 ed. Rio de Janeiro. 2020. Editora Alta Book.

SMITH, J. **Introdução aos Sistemas Operacionais.** 3 ed. Campina Grande-PB. 2019. Editora da Universidade Federal de Campina Grande (UFCG).

Stackscale. (2023). Stackscale. Disponível em: https://www.stackscale.com/blog/hypervisors/. Acesso em: 26 de Setembro de 2023.

Gil, A. C. Métodos e técnicas de pesquisa social. São Paulo. 1999. Editora Atlas.

Guedes, D. O. **Redes Definidas por Software**: uma abordagem sistêmica para o desenvolvimento de pesquisas em Redes de Computadores. Ouro Preto. 2012. Editora da Universidade Federal de Ouro Preto (UFOP).

Gupta, A. **Monitoramento de Desempenho em Computação em Nuvem**: Princípios e Práticas. São Paulo. 2023. Editora Novatec.

Lakatos, EM; Marconi, MA. Fundamentos de metodologia científica. São Paulo. 2010. Editora Atlas.

MOLINARI, L. **Cloud Computing**: A inteligência na nuvem e seu novo valor em TI. 1 ed. São José dos Campos. 2017. Editora Inova Business.

Mycloudwiki. (2020). Mycloudwiki. Disponível em: www.mycloudwiki.com/san/server-storage-architectures/. Acesso em: 20 de Setembro de 2023.

Oliveira, L. F. L. **Arquitetura de Nuvem**: Conceitos, Princípios e Práticas. São Paulo. 2023. Editora Novatec.

Oliveira, L. F. L. **Servidores Hiperconvergentes:** Uma Abordagem Prática. São Paulo. 2023. Editora Novatec.

Oliveira, L. F. L. Redes em Ambiente de Nuvem. São Paulo. 2023. Editora Novatec. Acesso em: 2023. Editora Novatec.

Silva, A. S. Segurança e Compliance em Cloud Computing. São Paulo. 2023. Editora Novatec.

Silva, A. S. **Computação em Nuvem**: IaaS, PaaS e SaaS. São Paulo. 2023. Editora Novatec.

Soares, G. e Paulo, A, R. **Computação em Nuvem**: Uma abordagem prática. Rio de Janeiro. 2023. Editora Campus Elsevier.

Souza, C. E. Governança de TI na Nuvem. Brasília. 2021. Editora Inova Business.

Stallings, W. **Redes de Armazenamento:** Um Guia Prático. São Paulo. 2023. Editora Novatec.

VELT, A. T. **Computação em Nuvem:** Uma Abordagem Prática. 1 ed. Rio de Janeiro. 2012. Editora Campus Elsevier.

VERAS, M. **Computação em Nuvem:** Nova Arquitetura de TI. 1 ed. Rio de Janeiro. 2015. Editora Campus Elsevier.

Wiley, J. IAM para Leigos. São Paulo.2023. Editora Novatec.

Página de assinaturas

Wilian Brito
030.278.631-77
Signatário

Sara Cerqueira
017.799.872-50
Signatário

Mateus Sousa
034.782.562-16
Signatário

Antonio Silva
032.290.192-88
Signatário

HISTÓRICO

30 dez 2023 14:59:56 — **Wilian de Lima Brito** criou este documento. (E-mail: wil.brito88@gmail.com, CPF: 030.278.631-77)

30 dez 2023 14:59:56 — **Wilian de Lima Brito** *(E-mail: wil.brito88@gmail.com, CPF: 030.278.631-77)* visualizou este documento por meio do IP 170.231.134.53 localizado em Parauapebas - Para - Brazil

30 dez 2023 15:00:13 — **Wilian de Lima Brito** *(E-mail: wil.brito88@gmail.com, CPF: 030.278.631-77)* assinou este documento por meio do IP 170.231.134.53 localizado em Parauapebas - Para - Brazil

02 jan 2024 14:16:15 — **Antonio Soares da Silva** *(E-mail: ads.antoniosoares@gmail.com, CPF: 032.290.192-88)* visualizou este documento por meio do IP 200.9.67.114 localizado em Parauapebas - Para - Brazil

02 jan 2024 14:16:31 — **Antonio Soares da Silva** *(E-mail: ads.antoniosoares@gmail.com, CPF: 032.290.192-88)* assinou este documento por meio do IP 200.9.67.114 localizado em Parauapebas - Para - Brazil

31 dez 2023 10:28:41 — **Sara Debora Carvalho Cerqueira** *(E-mail: dsaracarvalho@gmail.com, CPF: 017.799.872-50)* visualizou este documento por meio do IP 186.232.206.18 localizado em Parauapebas - Para - Brazil

31 dez 2023 10:28:47 — **Sara Debora Carvalho Cerqueira** *(E-mail: dsaracarvalho@gmail.com, CPF: 017.799.872-50)* assinou este documento por meio do IP 186.232.206.18 localizado em Parauapebas - Para - Brazil

02 jan 2024 10:00:13 — **Mateus da Silva Sousa** *(E-mail: mateus85sousa@outlook.com, CPF: 034.782.562-16)* visualizou este documento por meio do IP 179.63.173.15 localizado em Vitorino Freire - Maranhao - Brazil

02 jan 2024 10:00:18 **Mateus da Silva Sousa** *(E-mail: mateus85sousa@outlook.com, CPF: 034.782.562-16)* assinou este documento por meio do IP 179.63.173.15 localizado em Vitorino Freire - Maranhao - Brazil