Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL MATHEUS BERNARDO DA SILVA

***CLOUD COMPUTING*: SEGURANÇA PARA AMBIENTES VIRTUALIZADOS COMPARTILHADOS.**

Assis/SP
2022

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL MATHEUS BERNARDO DA SILVA

CLOUD COMPUTING: SEGURANÇA PARA AMBIENTES VIRTUALIZADOS COMPARTILHADOS

Projeto de pesquisa apresentado ao curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Gabriel Matheus Bernardo da Silva
Orientador(a): Prof. Me. Fábio Eder Cardoso

Assis/SP
2022

CLOUD COMPUTING: SEGURANÇA PARA AMBIENTES VIRTUALIZADOS COMPARTILHADOS

GABRIEL MATHEUS BERNARDO DA SILVA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Prof. Me. Fábio Eder Cardoso

Examinador: _____
Prof. Dr. Luiz Carlos Begosso

FICHA CATALOGRÁFICA

S586c Silva, Gabriel Matheus Bernardo da.

Cloud Computing: Segurança para Ambientes Virtualizados Compartilhados / Gabriel Matheus Bernardo da Silva – Assis, SP: FEMA, 2022.

38 f.

Trabalho de Conclusão de Curso (Graduação) – Fundação Educacional do Município de Assis – FEMA, curso de Ciência da Computação, Assis, 2022.

Orientador: Prof. M.ª Fábio Eder Cardoso.

1. Cloud. 2. Plataforma. 3. Ambiente. 4. Segurança. I. Título.

CDD 004.6

Biblioteca da FEMA

Assis/SP
2022

DEDICATÓRIA

Dedico este trabalho à minha família, amigos e todas as pessoas que acreditaram em mim, nos meus objetivos e na busca de conquistas, sempre me apoiando com forças para que pudesse buscar suas realizações.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me proporcionado saúde, forças, motivação e persistência na busca por meus sonhos.

Ao meu orientador Prof. Me. Fábio Eder Cardoso pela orientação neste trabalho e por todos os ensinamentos no âmbito acadêmico, e por ter acreditado e apoiado meu trabalho, para buscar a realização do mesmo.

Aos meus familiares e amigos pelo apoio desde antes de iniciar o curso, e a todos que vieram depois de seu início, por sempre me apoiarem no que busquei conquistar e nos sonhos que realizei e nos que ainda pretendo realizar.

RESUMO

A utilização de ambientes com infraestrutura e/ou softwares hospedados em nuvem tem crescido cada vez mais, e com isso, as empresas que possuem esse tipo de serviço para oferecer estão cada dia mais aprimorando seus serviços proporcionando melhor aproveitamento ao usuário. A principal grande vantagem desse tipo de serviço é a economia gerada ao usuário, pois este só paga pelo serviço e por quanto deste serviço utilizar, além de se ter uma maior segurança proporcionada pelo desenvolvedor da plataforma e facilidade de uso.
A plataforma utilizada durante esse projeto é o *Google Cloud Platform*. Neste projeto foram desenvolvidos testes de segurança em máquinas com diferentes sistemas operacionais e com formas de acesso diferentes. A plataforma do Google também proporciona diversas medidas de segurança, apresentadas abaixo. Também foi possível obter maior conhecimento do ambiente podendo explorar novos conceitos e recursos.

Palavras-chave: *Cloud*, plataforma, ambiente, segurança.

ABSTRACT

The use of environments with infrastructure and/or software hosted in the cloud has grown more and more, and with that, companies that have this type of service to offer are increasingly improving their services providing better use to the user. The main advantage of this type of service is the savings generated by the user, as he only pays for the service and for how much of this service he uses, in addition to having greater security provided by the platform developer and ease of use.
The platform used during this project is Google Cloud Platform. In this project, security tests were developed on machines with different operating systems and with different forms of access. The Google platform also provides several security measures, presented below. It was also possible to obtain greater knowledge of the environment, being able to explore new concepts and resources.

Keywords: Cloud, platform, environment, security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

DDoS	Distributed Denial of Service (Negação de serviço distribuída)
LGPD	Lei Geral de Proteção de Dados Pessoais
SaaS	Software como Serviço
PaaS	Plataforma como Serviço
IaaS	Infraestrutura como Serviço
GCP	*Google Cloud Platform*
IDC	*International Data Corporation* (Corporação internacional de Dados)
vTPM	*Virtual Trusted Platform Module* (Módulo de plataforma confiável virtual)
VM	*Virtual Machine* (Máquina Virtual)
SO	Sistema Operacional

SUMÁRIO

1. INTRODUÇÃO

No dia a dia, pode não se perceber, mas possivelmente usuários utilizam ao menos alguma ferramenta que faz armazenamento em nuvem, como por exemplo Google Drive e i*Cloud* (para dispositivos que fazem backup de fotos e arquivos dos dispositivos), onde a cada dia que passa o uso de ferramentas como essas estão ganhando maior espaço no ambiente tecnológico, e assim, o desenvolvimento e infraestrutura em nuvem é maior (ENDEL A, 2020).

A computação em nuvem teve seu início com o surgimento de protótipos entre os anos 1950 e 1960, onde haviam diversas estações de máquinas interligadas a um mainframe, ou seja, uma máquina com grande poder computacional de processamento, capaz de movimentar grandes quantidades de dados. Através da constante evolução surgiu a ideia de se fazer a troca de informação entre duas ou mais máquinas que não estivessem no mesmo espaço físico (ENDEL B, 2021).

A partir dos anos de 1990, os valores para se ter um ambiente deste passou a ser mais barato, assim, diversas empresas começaram a aderir essa ideia e investir em redes virtualizadas. Sendo assim, nesse período o uso da internet começou a ser mais comum e a ideia da computação em nuvem expandiu mais. Aliás, esse nome surgiu da relação entre uma nuvem e serviços prestados a distância, remotos; e, por conta disso, houve o surgimento da *Cloud Computing* (ENDEL B, 2021).

Os modelos de serviços presentes na computação em nuvem são principalmente:

Software como Serviço (Saas), onde por meio deste serviço não se é necessário instalar o software na máquina do cliente, ou seja, a execução é feita pelo serviço de internet no servidor da aplicação; Infraestrutura como Serviço (IaaS), este serviço trata da parte estrutural computacional da aplicação, ou seja, trata de áreas como provisionamento e balanceamento de serviços, onde geralmente se utiliza em ambientes virtualizados; e por último Plataforma como Serviço (PaaS), onde apresenta a entrega de uma plataforma (ambiente) da aplicação para uso do cliente, onde se realiza a implementação do mesmo e geralmente esta fica presa ao fornecedor (CASTRO; SOUSA, 2010, p.1).

Quando se trata dos modelos de implantação de ambientes em nuvem existem 04 tipos, sendo estes: Nuvem Privada, onde permite que a administração deste ambiente seja da

própria empresa ou de terceiros; Nuvem Pública, se disponibiliza para público geral ou grupos de indústrias; Nuvem Comunitária, esta é compartilhada para vários grupos que possuem interesses de uso semelhantes; e por último, Nuvem Híbrida, caracterizada pela composição de mais de uma nuvem (as anteriores citadas) possuindo requistos de segurança e políticas com flexibilidade maior (CASTRO; SOUSA, 2010, p.1).

Alguns benefícios que podem ser obtidos com a Computação em Nuvem são:

Economia, pois os serviços utilizados em nuvem são sob demanda, ou seja, o contratante irá pagar apenas pelo que usar, assim, não haverá desperdício de espaço ou de recursos que possam estar parados; há uma menor necessidade de funcionários para trabalhar em ambientes como este, gerando menor gasto para uma empresa; há também a facilidade de implementação e uso do ambiente e das soluções nele utilizadas; além de outras vantagens como novas funcionalidades, compartilhamento de informações e grande tendência de futuro (ARRUDA, 2016).

Deve-se investir e analisar a segurança de um ambiente em nuvem, pois, principalmente devido ao fato de realizar o arquivamento e acesso aos dados por meio de diversos dispositivos e locais na internet, há grandes e diferentes rotinas que podem ser afetadas por ataques hackers ou até mesmo por alguns usuários mal-intencionados querendo prejudicar o ambiente; e diante disso, é preciso realizar um bom planejamento utilizando novas e/ou eficazes tecnologias de segurança para manter a segurança da rede blindada a ataques (ENDEL C, 2016).

De acordo com dados do IDC, até 2022 cerca de 90% das organizações possuirão algum tipo de nuvem em suas aplicações de negócio. Atualmente, o investimento em *Cloud* Computing tem feito com que assuntos como as chamadas Nuvens Inteligentes tomassem grande destaque no cenário atual, além de ser possível realizar transformações digitais cada vez mais fortes e seguras. A nuvem tem expandido seu só nas diversas áreas do mundo, principalmente em jogos e aplicativos de acervos, como a Netflix, onde no ano de 2020 teve grande crescimento e nos anos seguintes promete se desenvolver ainda mais (ENDEL E, 2020).

1.1. OBJETIVOS

Este trabalho tem como objetivo principal a criação de um ambiente focado no uso de *Cloud Computing* e, neste, realizar testes de segurança verificando formas de como este modelo se comporta em determinados testes de vulnerabilidade e como o provedor do ambiente *Cloud* trabalha com o uso de protocolos e demais ferramentas.

Outro objetivo é verificar possíveis falhas de segurança e formas de tentar melhorá-las para o desenvolvimento de novas aplicações com segurança avançada trabalhando com novos tipos de protocolos que surgem a cada dia no mercado.

1.2. JUSTIFICATIVAS

O trabalho apresentado se justifica pelo fato de que, atualmente, o tema segurança da informação tem grande ênfase, pois é necessário para qualquer aplicação ou comunicação entre dispositivos que faça a manipulação de dados; estes, por sua vez, são necessários para análises e criação de estatísticas e soluções com melhores benefícios e usos tecnológicos com inovações.

Devido ao fato de que *Cloud* Computing ser algo considerado recente de uso e a segurança estar sempre tendo que ser melhorada e atualizada, o presente trabalho pode apresentar como vantagem a aplicação de alguns métodos que pessoas do ramo ou até mesmo de outros possam fazer para minimizar os riscos de ataques cibernéticos para acesso a dados.

O tema apresenta grande relevância econômica, pois o investimento aplicado na computação em nuvem é apresentado cada ano maior, onde a projeção para 2025 é de que cerca de 34% dos usos tecnológicos sejam baseados em nuvem, sejam estas públicas, privadas ou híbridas (ENDEL D, 2021).

1.3. MOTIVAÇÃO

A principal motivação para o estudo do tema apresentado é o crescimento do uso de serviços de computação em nuvem, conforme ilustrado na Figura 1.

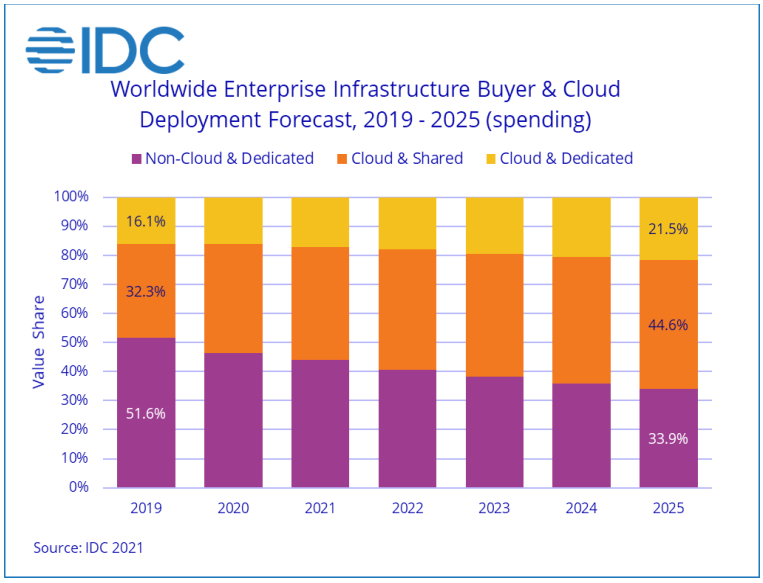

Figura 1: Previsão de Crescimento de Infraestrutura em Nuvem até 2025

(In: ENDEL D, 2019).

Com este grande crescimento, diversas ramificações dentro da área de *Cloud* computing estão surgindo tendo como ênfase melhorar seu desempenho e abranger novas áreas da tecnologia, onde, com isso, pode estar envolvido a segurança, que é o foco deste trabalho.

Desta forma, espera-se, com o estudo, contribuir com o tema de forma a de acordo com a construção de um ambiente virtualizado compartilhado, testar ataques de vulnerabilidade de segurança e permitir maior conhecimento sobre o assunto, assim, pretende-se finalizar o estudo com soluções implantadas que possam desenvolver melhor o uso da segurança nestes ambientes.

1.4. CONTRIBUIÇÃO

Conforme apresentado anteriormente, o conceito de Segurança em *Cloud* Computing tem evoluído bastante nos últimos anos, e com isso, novas soluções são implementadas.

O presente trabalho pretende contribuir com o tema baseando na virtualização do ambiente e na realização de testes, simulando ataques, assim, podendo analisar comportamentos com os protocolos diante de ataques.

Este trabalho também pretende identificar com clareza alguns pontos principais que ajudam a melhorar a segurança partindo do próprio usuário para que mesmo leigos do assunto possam identificar possíveis falhas que estejam cometendo para corrigirem e melhorar seu ambiente do dia a dia.

1.5. METODOLOGIA

A metodologia empregada no trabalho consiste inicialmente na revisão bibliográfica sobre o tema visando informações do cenário atual e das últimas atualizações e inovações presentes no mercado. Os conceitos apresentados nessa etapa servirão para a representação de *Cloud Computing*, além de se destacar a importância de um ambiente seguro e eficaz nos dias atuais, que se tem grande manuseio diário de informações.

Nas próximas etapas, aprofundou-se os conhecimentos em ferramentas para uso focado no tema, principalmente no uso de ferramentas *open-source*, buscando informações e dicas para criação de ambiente compartilhado que busque deixar claro uma alta preparação de escalabilidade, sem deixar de lado a segurança eficiente, tratando com endereços de rede na comunicação com máquinas externas ao ambiente.

Finalmente, foi desenvolvido um ambiente com máquinas virtualizadas fazendo uso de aplicações hospedadas na nuvem, inicialmente, o uso de VM Virtual Box no desenvolvimento do ambiente e do ambiente Google *Cloud*, já apresentado seu uso em diversas ferramentas da própria Google, como as aplicações Google Buscador e Youtube.

1.6. ESTRUTURA DO TRABALHO

O trabalho apresentado foi estruturado em 05 (cinco) capítulos, sendo estes: Capítulo 1 apresenta a Introdução; Capítulo 2 contém informações sobre segurança; Capítulo 3 abrange conteúdos *Cloud*; Capítulo 4 é composto pelo desenvolvimento do trabalho, apresentando etapas e ferramentas utilizadas; e Capítulo 5 inclui a Conclusão e Trabalhos Futuros.

1.7. CRONOGRAMA

A execução deste projeto é desenvolvido com base no cronograma de atividades apresentado na Tabela 1.

Atividade	2021/2022										
	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set
Levantamento da bibliografia											
Identificação de Tecnologias Envolvidas											
Desenvolvimento do Projeto visando o Exame de Qualificação											
Envio do TCC para Qualificação											
Apresentação Banca de Qualificação											
Desenvolvimento do Projeto visando a Conclusão e a Defesa Final											
Envio TCC para Banca de Defesa											
Apresentação Banca de Defesa											
Entrega do TCC											

Tabela 1: Cronograma de Atividades

2. SEGURANÇA DE REDES

A Segurança de Redes se faz necessária através de atividades que protegem integridade, uso e acesso dos dados, fazendo isso por meio da combinação de diversas camadas de defesa, mantendo controle e políticas de acesso aos recursos da rede. A segurança pode ser mantida de algumas formas como: uso de Firewalls, antivírus e antimalware, controle de acesso dos usuários, sistemas de prevenção contra invasões e contra perda de dados, uso de VPNs, além de diversas outras ações (ENDEL F, 2022).

2.1. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação atua na defesa de dados e a proteção de informações sigilosas para que somente pessoas autorizadas e que necessitem possam ter acesso a eles. A segurança da informação é necessária no mercado, pois esta garante que informações de uma empresa não sejam liberadas, e assim, outras empresas do ramo possam usufruir disso. Geralmente, nas empresas, o setor de tecnologia é responsável por realizar a instalação e manutenção nas máquinas para que estas, só possuam softwares e arquivos seguros e necessários para o dia a dia de trabalho, onde, caso precise de algo diferente, será necessário contato com o setor responsável de tecnologia. Assim, se evita que sejam instalados programas maliciosos que possam corromper arquivos e/ou roubá-los (VELASCO, 2019).

2.2. CRIMES CIBERNÉTICOS

Os crimes cibernéticos são atividades que fazem uso de algum aparelho conectado em rede e com acesso a internet para atacar outros aparelhos na mesma condição. As pessoas que praticam essa atividade, geralmente são chamadas de hackers e na maioria das vezes, o objetivo principal é a busca por dinheiro. Alguns ataques são realizados individualmente, outros são um grupo de pessoas, organizados ou não. Motivos diferentes da busca por dinheiro, basicamente são buscas pessoais ou políticas, dificilmente tentando danificar algum aparelho (ENDEL G, 2022).

A maioria dos ataques fazem uso de vírus e outros malwares, onde estes infectam o computador da pessoa e prejudica serviços do sistema. Alguns hackers atacam aparelhos, e quando possuem o controle do mesmo, usam este para atacar outros, assim, não deixando rastros da origem do primeiro ataque (ENDEL G, 2022).

O Brasil possui, desde 2012, legislação para este tipo de crime, um exemplo é a Lei Carolina Dieckmann, de Nº 12.737/2012, que está no Código Penal, onde recebeu o nome da atriz devido a mesma ter sido vítima desse tipo de crime. Outros exemplos são as leis Nº 12.735/2012 e Nº 12.965/2014, onde tratam-se das condutas por meio dos sistemas eletrônicos e regulamenta direitos e deveres dos internautas, respectivamente. Os crimes mais conhecidos são:

- **Ataques DDoS (Distributed Denial of Service)**: O criminoso, através de uma máquina, ataca várias, assim “derrubando” redes e máquinas conectadas realizando ataques em massa (FIA, 2021);
- **Phishing**: Significa “pescar”, é a ideia de tentar “fisgar” usuários através de e-mails, sites e links para roubar dados, onde, em grande parte das vezes, se passam por pessoas conhecidas dos usuários (FIA, 2021);
- **Kits de Exploits**: São coleções de explorações que muitas vezes vem junto com softwares, e estes se aproveitam de falhas no sistema, além de ser “invisível”, assim, o usuário nem percebe a presença dos mesmos (FIA, 2021);
- **Ransomware**: É um vírus que bloqueia o computador da vítima, acessa os dados e os torna inacessíveis, na maioria das vezes, em busca de dinheiro (FIA, 2021);
- **Bullying Virtual**: Se trata de um bullying igual na vida real, porem de forma online, onde o criminoso ofende e ameaça a vítima mexendo com seu psicológico (FIA, 2021).

Algumas atitudes podem ser tomadas para evitar isso, como: usar senhas fortes, manter o antivírus atualizado além de buscar ver a confiabilidade e segurança de qualquer site ou programa antes de inserir dados pessoais (FIA, 2021).

2.3. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

A LGPD, que é a Lei Nº 13.709/2018, foi criada com o intuito de proteger o direito de liberdade e privacidade de cada indivíduo. Ela trata sobre dados digitais, que em meio físico ou digital são tratados por dois agentes, sendo o Controlador e o Operador. O tratamento de dados abrange qualquer operação que seja executada com uso de dados pessoais, e antes do seu início, o agente deve ter certeza que a operação está sendo feita de forma explícita e com isso informado ao titular dos dados (ENDEL H, 2022).

A LGPD traz algumas ferramentas que identificam e mantém as obrigações diante dos dados, assim, criam-se meios processuais que mobilizam a Administração Pública, tendo a estrutura dos direitos dos titulares dos dados (ENDEL H, 2022).

A Figura 2, ilustra de forma resumida sobre a Lei.

Figura 2: LGPD Geral

(In: ENDEL I, 2022).

2.4. PENTEST

Também conhecido como teste de intrusão, os pentest são testes realizados nas redes de computadores e nos sistemas operacionais, podendo abranger mais coisas como websites e redes sem fio. A função deste é encontrar e apresentar as falhas (vulnerabilidades) presentes nesses locais. Há algumas vulnerabilidades que nem mesmo em um pentest é possível encontrar, onde este busca sempre as mais comuns encontradas e retorna ao cliente (MORENO, 2019).

2.4.1. ESTRATÉGIAS

O Pentest geralmente é dividido em 05 fases, sendo:

- Planejamento: Se identifica o que será testado, o modo dos testes e o que se busca alcançar, e é feito o termo de confidencialidade, trazendo mais segurança ao contratante;
- Reconhecimento: É feito um assessment(scan) completo do ambiente, onde se identifica o que compõe o ambiente, como seguranças, servidores, entre outros;
- Teste de Intrusão: Através do scan, é feita uma classificação de criticidade e se é explorado cada item pontuado neste de forma isolada, podendo ser de forma “exploit” ou “brute force”;
- Análise de código e de aplicações: São analisadas as aplicações que realizam manipulações de dados e informações vitais, buscando possíveis falhas de segurança;
- Documentação e reporte: Depois de ter realizado os testes, classificado as falhas e buscar evidências das origens destas falhas, se gera um relatório reportando tudo que foi encontrado, apontando os erros e possíveis melhorias (ENDEL J, 2021).

2.4.2. MODELOS DE PENTEST

SILVA (2020), destaca que os principais tipos de pentest são:

- White Box: Quem realizará o pentest recebe antes algumas poucas informações da empresa sobre a sua forma de segurança, e este tipo é o padrão.

- Black Box: Conhecido como Teste Cego. Neste tipo o contratante não repassa nenhuma informação com antecedência.
- Double-Blind: Conhecido como Teste Duplo-Cego. Neste tipo basicamente ninguém da equipe contratante sabe sobre o teste que é realizado, onde assim a segurança que está implementada será a única responsável por conter o ataque.

2.4.3. BENEFÍCIOS

ENDEL K (2022), destaca que os principais benefícios e vantagens do pentest são:

- Identificar vulnerabilidades conhecidas;
- Identificar configurações incorretas;
- Testar passivamente os controles de segurança;
- Identificar a falta de controles de segurança;
- Identificar e priorizar riscos;
- Impedir que hackers se infiltrem em seus sistemas;
- Amadurecer seu ambiente;
- Evitar vazamento de dados importantes;
- Cumprir as Normas e Regulamentações da Indústria.

3. CLOUD

ENDEL L (2022) observa que *Cloud* é uma rede global de servidores, onde, cada um deles tem funções distintas. Esses servidores, basicamente, são remotos e espalhados ao redor do globo em diversas localizações, e se conectam entre si através da rede por um único sistema. Eles armazenam e gerenciam dados, assim, podendo acessar os mesmos de forma online (ENDEL L, 2022).

3.1. COMPUTAÇÃO EM NUVEM

Essa definição se resume basicamente em realizar o uso de componentes como armazenamento, memória e processamentos de máquinas(computadores e/ou servidores) que são interligadores em rede para execução de máquinas virtuais e/ou execução de aplicações, assim, se tendo economia de forma geral, principalmente de hardware, porém se estendendo a licenças e gastos de energia (ZANUTTO, 2022).

A Figura 03 apresenta um diagrama da Computação em Nuvem.

Figura 3*:* Diagrama Computação em Nuvem

(In: BARDI, ZORZI. 2017, p. 132)

3.2. SERVIÇOS

A Figura 4 ilustra os serviços utilizados em nuvem. Nela são ilustrados os tipos de serviços e quais competências são pertencentes a cada serviço, além de mostrar características específicas.

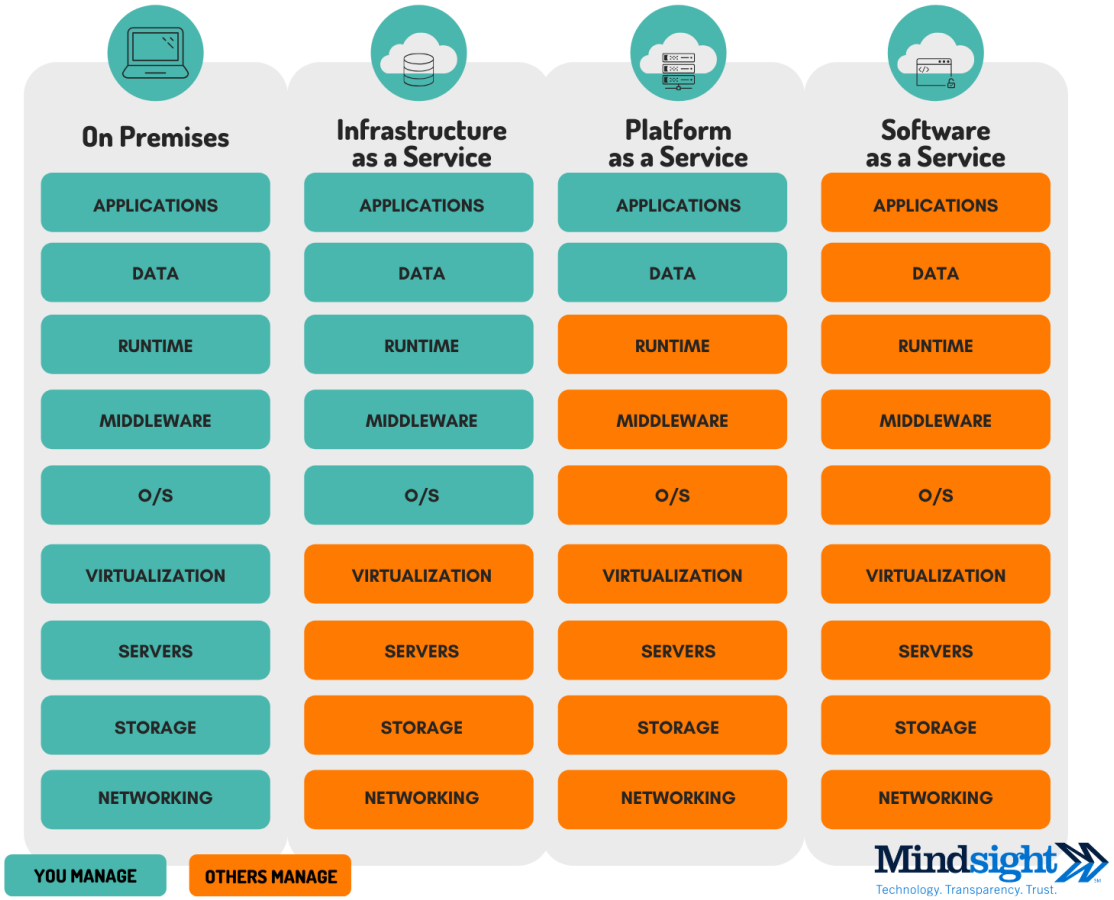

Figura 4: Serviços *Cloud*

(In: LUIZ, 2020)

3.2.1. SaaS

Nesse serviço, o software é hospedado em ambiente *Cloud* e acessado por ferramentas como navegador web, desktop ou API dedicada a isso. Esse modelo traz vantagens como: atualizações automáticas, que atualiza a aplicação assim que o provedor libera; e

proteção contra perca de dados, devido aos mesmos estarem em ambiente *Cloud*, assim evitando falhas de dispositivos. O serviço SaaS é utilizado na maioria dos softwares comerciais que usam serviços *Cloud* (VENNAM, 2020).

3.2.2. PaaS

Esse serviço contempla que o provedor *Cloud* hospede toda a solução de software, infraestrutura e ferramentas de desenvolvimento, onde o desenvolvedor apenas escolhe onde acionar cada tarefa. O serviço PaaS é bastante utilizado com contêineres, assim, facilitando a aplicação devido ao uso apenas necessário de recursos. (VENNAM, 2020).

3.2.3. IaaS

O serviço IaaS fornece recursos que são fundamentais em uma aplicação, como servidores e armazenamento, isso faz com que o usuário final diminua os recursos que serão necessários devido aos maiores gastos serem justamente com esse tipo de recurso, isso geram assim, uma economia de capital e de espaço físico, devido a possibilidade de uso de alguns recursos apenas em picos. Esse modelo é o mais utilizado de todos, porém os outros dois citados acima vem crescendo seu uso (VENNAM, 2020).

3.3. MODELOS

A Figura 05 representa os modelos de nuvem explicados a seguir. Através dela é possível visualizar se existe relação de um modelo com os demais, onde, todas tem relação com a Nuvem híbrida. Todos os modelos são descritos detalhadamente abaixo.

Figura 5: Modelos de Nuvem

(In: BARDI, ZORZI, 2017, p. 134)

3.3.1. NUVEM PÚBLICA

Nesse modelo diversos clientes fazem uso de uma mesma infraestrutura de nuvem, porém cada um destes possui um espaço determinado e individual, assim, torna o modo de utilização seguro, onde o provedor é quem administra a infraestrutura de uso. Exemplos desse tipo de nuvem são: Azure, AWS, *Google Cloud Platform* (BATAGELLO, 2022).

3.3.2. NUVEM PRIVADA

É uma infraestrutura no qual um cliente faz uso único daquela, ou seja, diferentemente da nuvem Pública, a privada torna exclusiva uma infraestrutura para cada cliente, além de permitir o uso de sistemas legados e ter controle total dos recursos internos; porém, para isso, é necessário maior investimento. Exemplos de nuvem privada são: OpenStack, Vmware (BATAGELLO, 2022).

3.3.3. NUVEM HÍBRIDA

Esta tem em sua composição o uso de duas ou mais nuvens públicas ou privadas, no qual essas são conectadas entre si para realizar portabilidade de dados e aplicações. Seu uso é maior quando se é necessário fazer uso dos dois modelos acima citados, sejam devido a recursos, investimentos ou maior flexibilidade (BATAGELLO, 2022).

3.3.4. NUVEM COMUNITÁRIA

O modelo de nuvem comunitária tem como objetivo o uso por uma comunidade que possui interesses em comum, como: segurança, negócios, políticas, entre outros. O modelo comunitário proporciona que a administração possa ser feita por membros participantes do próprio cliente ou por terceiros (BATAGELLO, 2022).

Como exemplo, pode-se criar uma nuvem comunitária entre as universidades paulistas, Unicamp, Unesp e USP, podendo estas realizar o compartilhamento de recursos e serviços em comum (ENDEL Q, 2022).

3.4. GOOGLE CLOUD PLATFORM

A plataforma Google *Cloud* consiste em um grupo de aplicações e soluções de posse da empresa Google LLC, só qual se executa blocos de serviços em nuvem. Nele se pode contratar e pagar apenas os serviços e as quantidades que utilizar, oferece uma guarda segura dos dados e traz alta disponibilidade, além do mesmo poder abrangir os três serviços: SaaS, PaaS e IaaS (MULTIEDRO, 2019).

3.4.1. PRODUTOS

Os principais produtos do GCP são:

Compute Engine: Máquinas virtuais nos data centers;

Cloud Storage: Armazenamento dos objetos;

SDK do *Cloud*: Linha de comando e bibliotecas;

Cloud SQL: Bancos de dados MySQL, PostgreSQL e SQL Server;

Google Kubernetes Engine: Ambiente gerenciado que executa apps em contêineres;

BigQuery: Data warehouse;

Cloud CDN: Conteúdo veicular Web e vídeo;

Dataflow: Análise de streaming para processamento;

Operações: monitoramentos, registros e desempenho dos aplicativos;

Cloud Run: Ambiente totalmente gerenciado que faz a execução em contêineres;

Anthos: Moderniza aplicativos atuais e cria novos;

Cloud Functions: Plataforma orientada por eventos para serviços em nuvem (ENDEL M, 2022).

3.4.2. PREÇOS

O GCP permite que ao criar sua conta no ambiente, se tenha 03 meses e US$ 300 em créditos para utilizar no ambiente. Na plataforma, o cliente só paga pelo que utilizar e consegue fazer uso de até 20 produtos (ENDEL N, 2022).

Eles pedem os dados do cartão de crédito ou outra forma de pagamento do cliente, porém não realizam cobrança por serviço não usada e não fazem cobranças automáticas após o fim dos 03 meses de uso iniciais.

3.4.3. INFRAESTRUTURA

A infraestrutura oferecida pelo Google *Cloud* contempla Data Centers seguros e eficientes, onde o Google tem disponibilidade em + de 200 países, possui 29 regiões de *Cloud*, 88 zonas e 146 locais de borda da rede (ENDEL O, 2022).

Além disso, possui uma presença global de confiança devido a conexões via cabos submarinos, e regiões redundantes de nuvem. E por fim, apresenta rede rápida e confiável com baixa latência e alto provisionamento, devido ao tráfego de rede utilizado em grande parte do tempo ser particular do Google, por conta de outros apps como Gmail e Youtube (ENDEL P, 2022).

4. DESENVOLVIMENTO DO TRABALHO

4.1. ESTUDO E INSTANCIAÇÃO DE VM

Inicialmente, foi realizado um aprofundamento diante das ferramentas utilizadas, sendo a principal delas o GCP *(Google Cloud Platform)*; foi conduzida a execução de alguns usos iniciais na plataforma, colocando com o status ativo (em execução) VMs instanciadas, como apresentado na Figura 6.

Status	Nome ↑	Zona
✓	debian	us-central1-a
○	instance-1	southamerica-east1-b
○	instance-2	us-central1-a
○	instance-3	us-central1-a
○	instance-4	us-central1-a
○	instance-migrate-test	southamerica-east1-c
✓	ubuntu	us-central1-c

Figura 6: Máquinas Virtuais Exemplos

(Fonte: Próprio Autor)

Durante a criação da VM, alguns recursos de segurança são disponíveis, apresentados resumidamente na Tabela 2.

Criação da VM	
Classificação	**Serviços Disponíveis**
Confidencialidade	Serviços de VM confidencial, mantendo a memória da VM criptografada
Acesso a API	Acesso padrão, acesso completo para todas as APIs e Definição de acesso para cada API
Firewall	Permissão tráfego HTTP e Permissão de tráfego HTTPS
Rede	Nomes de Hosts e Interfaces de Rede, encaminhamento de IP, Configurações de desempenho e interface
Segurança	Proteção da VM: inicialização segura, vTPM, monitoramento de integridade; Acesso a VM: Permissões do IAM, bloqueio e adição de chaves SSH
Administração	Políticas de: descrição, aplicativos, disponibilidade e revogação de criptografia de chave; proteção contra exclusão; metadados

Tabela 2: Segurança Criação VM

4.2. TESTES DE PORTAS

O teste de vulnerabilidade foi realizado via terminal e a ferramenta utilizada foi o *Network Mapper* (NMAP), e foi identificado, na pesquisa do endereço IP externo, as portas liberadas e não liberadas e quais serviços estavam configurados nelas, obtendo os resultados apresentados na Tabela 3.

Nmap		
Portas	**Aberta?**	**Serviço**
22	Sim	SSH
80	Não	HTTP
443	Não	HTTPS
3389	Não	MS-WBT-SERVER

Tabela 3: Nmap Resultado

Fonte: Próprio Autor

4.3. ACESSO REMOTO

Durante as tentativas de realizar acesso remoto, pelo GCP há algumas opções de acesso, onde por padrão tem a descrição “Abrir na janela do navegador”, e assim, são transferidas chaves do protocolo *Secure Shell* (SSH) para a máquina virtual (VM) e realizado o acesso.

Já para realizar o acesso por meio de outra máquina (padrão Linux pelo terminal e padrão Windows pelo Putty), é preciso realizar algumas modificações, apresentados na Tabela 4.

Acesso Remoto	
Ação	**Necessário**
Com chave pública	Nas configurações do Google colocar a chave gerada durante a tentativa de login
Acesso direto com senha	Autorizar no arquivo sshd_config autenticação com usuário e com senha

Tabela 4: Acesso Remoto VM

Para essa configuração citada no arquivo sshd_config, são necessários os comandos e passos indicados na Figura 7.

```
$ sudo nano /etc/ssh/sshd_config

/*Texto abaixo inserido do arquivo, após #ListenAddress ::*/
PermitRootLogin yes
PasswordAuthentication yes

/*Pressionar as teclas*/
Ctrl + O
Enter
Ctrl + X

$ sudo service sshd restart
```

Figura 7: Comandos Permissão SSH

(Fonte: Próprio Autor)

4.4. CUSTOS

O custo médio no ambiente GCP para uso de 02 máquinas, sendo uma com SO Ubuntu Linux e a outra com SO Debian Linux, com o tipo de ambas as máquinas sendo e2-medium (configuração média padrão, com 01 núcleo compartilhado de CPU e 4 GB de memória RAM) e tamanho de disco de 20 GB, foi de US$ 25.

5. CONCLUSÃO E TRABALHOS FUTUROS

A respeito do trabalho realizado, foi mostrado acima sobre o desenvolvimento, que consistiu na verificação de opções que a plataforma GCP oferece no quesito segurança aos seus usuários; também foi verificado sobre acesso remoto em máquinas e algumas informações sobre endereços (IP). Com isso, os objetivos apresentados foram alcançados e trabalhos futuros que serão indicados abaixo ganharam mais embasamento e consistência.

Diante do que foi apresentado nos capítulos acima, pode-se concluir que o GCP permite a realização de testes de segurança de forma livre, com a limitação de que não afete aplicações de outros usuários. Caso sejam encontradas vulnerabilidades no ambiente, o Google possui um programa de benefício para o usuário reportar, e é realizada uma remuneração ao usuário, sendo o valor de acordo com a classificação de complexidade.

Durante a realização dos testes e com a obtenção dos resultados apresentados acima, é possível dizer que o ambiente *Cloud* do Google proporciona grande segurança aos seus usuários, onde, caso o ambiente hospede uma aplicação e esta possuir bastante enfase em ser segura, as chances do usuário ter problemas com ataques e vulnerabilidades é bem pequena.

Como sugestão de trabalhos futuros, sugere-se a criação de uma máquina servidor, hospedando banco de dados de uma aplicação web, e outra máquina servidor hospedando a aplicação. A ideia é fazer a comunicação entre elas em rede, estabelecendo através de uma rede interna para ambas, onde o filtro de pacotes seja feita por uma máquina Firewall e realizar testes de segurança nesse ambiente estruturado.

REFERÊNCIAS

ARRUDA, Darlan. **Benefícios e Desafios encontrados na adoção de *Cloud* Computing**. Revistas Facol. Disponível em <http://facol.com/si/downloads/Revista_SI_2011/Artigo04.pdf>. Acesso em 18 out 2021.

BARDI, Marcelo A G; ZORZI, Lucas. **Reaproveitamento De Dispositivos Computacionais Utilizando Computação Em Nuvem Com Vistas À Sustentabilidade Na Área De Tecnologia Da Informação**. Universidade São Francisco, 2017. p. 132-134.

BATAGELLO, Patrícia. **Conheça os 4 modelos de implantação de nuvem**. InMetrics. Disponível em <https://inmetrics.com.br/blog/conheca-os-4-modelos-de-implantacao-de-nuvem/>. Acesso em 11 mar 2022.

CASTRO, Rita de C.C. de; SOUSA, Verônica L. P. de. **Segurança em *Cloud* Computing: Governança e Gerenciamento de Riscos de Segurança**. 2010. 7p.

ENDEL A. **Quem inventou a computação em nuvem?**. SKY.ONE. Disponível em <https://skyone.solutions/hub/nuvem/conheca-a-computacao-em-nuvem/>. Acesso em 18 out 2021.

ENDEL B. **O que é computação em nuvem?**. SERCOMPE. Disponível em <https://www.sercompe.com.br/o-que-e-computacao-em-nuvem/>. Acesso em 17 out 2021.

ENDEL C. **7 princípios de segurança em uma rede em nuvem para considerar**. SAPHIR. Disponível em <https://blog.saphir.com.br/7-principios-de-seguranca-em-uma-rede-em-nuvem-para-considerar/>. Acesso em 17 out 2021.

ENDEL D. **IDC: primeiro trimestre confirma forte crescimento da infraestrutura de *Cloud***. IPNEWS. Disponível em <https://ipnews.com.br/idc-primeiro-trimestre-confirma-forte-crescimento-da-infraestrutura-de-*Cloud*/>. Acesso em 05 nov 2021.

ENDEL E. **O que esperar para *Cloud* Computing em 2021**. We Colab. Disponível em <https://wecolab.com.br/blog/o-que-esperar-para-*Cloud*-computing-em-2021/>. Acesso em 08 nov 2021.

ENDEL F. **O que é segurança de rede?**. Cisco. Disponível em <https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html>. Acesso em 03 mar 2022.

ENDEL G. **Dicas de como se proteger contra crimes cibernéticos**. Kaspersky. Disponível em <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acesso em 03 mar 2022.

ENDEL H. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Gov.BR. Disponível em <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em 08 mar 2022.

ENDEL I. **O que muda com a LGPD**. Serpro. Disponível em <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em 08 mar 2022.

ENDEL J. Pentest ou Testes de Invasão: **O que é e quais são as etapas?**. Softwall. Disponível em <https://www.softwall.com.br/blog/pentest-testes-de-invasao-o-que-e-quais-etapas/>. Acesso em 08 mar 2022.

ENDEL K. **PENTEST: Como evitar ser vítima de sequestro de dados**. InfoMach. Disponível em <https://www.infomach.com.br/pentest-como-evitar-ser-vitima-de-sequestro-de-dados/>. Acesso em 11 mar 2022.

ENDEL L. **O que é nuvem?**. Azure. Disponível em <https://azure.microsoft.com/pt-br/overview/what-is-the-*Cloud*/>. Acesso em 11 mar 2022.

ENDEL M. **Produtos do Google *Cloud***. Google *Cloud*. Disponível em <https://*Cloud*.google.com/products?hl=pt-br>. Acesso em 15 mar 2022.

ENDEL N. **Preços do Google *Cloud***. Google *Cloud*. Disponível em <https://*Cloud*.google.com/pricing?hl=pt-br>. Acesso em 15 mar 2022.

ENDEL O. **Google *Cloud***. Google *Cloud*. Disponível em <https://*Cloud*.google.com/?hl=pt-br>. Acesso em 15 mar 2022.

ENDEL P. **Infraestrutura do Google *Cloud***. Google *Cloud*. Disponível em <https://*Cloud*.google.com/infrastructure?hl=pt-br>. Acesso em 15 mar 2022.

ENDEL Q. **Nuvem Computacional Unicamp**. Centro de Computação Unicamp. Disponível em <https://www.ccuec.unicamp.br/ccuec/sobre/projetos-iniciativas-e-parcerias/nuvem-computacional-unicamp>. Acesso em 21 mar 2022.

FIA. **Crimes cibernéticos: o que são, tipos, como detectar e se proteger**. FIA. Disponível em <https://fia.com.br/blog/crimes-ciberneticos/>. Acesso em 03 mar 2022.

LUIZ, Wagner. **IaaS, PaaS e SaaS: o que é e quais são as diferenças?**. Disponível em <https://minutonerd.com.br/iaas-paas-e-saas-o-que-significa-cada-uma-e-quais-as-diferencas/>. Acesso em 11 mar 2022.

MORENO, Daniel. **Introdução ao PENTEST**. 2. ed. São Paulo: Novatec Editora Ltda, 2019.

MULTIEDRO. ***Google Cloud Platform*: o que é e quais as suas vantagens?**. Multiedro. Disponível em <https://blog.multiedro.com.br/google-*Cloud*-platform-o-que-e-e-quais-as-suas-vantagens/>. Acesso em 15 mar 2022.

SILVA, Eduardo. **Pentest: o que é?**. Geekhunter. Disponível em <https://blog.geekhunter.com.br/o-que-e-pentest/#Principais_tipos_de_pentest>. Acesso em 11 mar 2022.

VELASCO, Ariane. **O que é Segurança da Informação?**. CanalTech. Disponível em <https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/>. Acesso em 03 mar 2022.

VENNAM, Sai. **O que é *Cloud*?**. IBM. Disponível em <https://www.ibm.com/br-pt/*Cloud*/learn/*Cloud*-computing#toc-servios-de-fZUgeFMw>. Acesso em 11 mar 2022.

ZANUTTO, Bruno G. **Segurança em *Cloud* Computing**. Universidade Federal de São Carlos. Sorocaba, São Paulo. p. 1.