UNIVERSIDADE POLITÉCNICA A POLITÉCNICA

INSTITUTO SUPERIOR DE GESTÃO, CIÊNCIAS E TECNOLOGIAS

DEPARTAMENTO DE CIÊNCIAS TECNOLÓGICAS E ENGENHARIAS

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

ANÁLISE DA SEGURANÇA CIBERNÉTICA NA COMPUTAÇÃO EM NUVEM

CASO DE ESTUDO: VODACOM MOÇAMBIQUE

Autora: Neila da Conceição Mabombo

Supervisor:

MSc. Euclides José Tchaúque

Maputo, Outubro de 2021

UNIVERSIDADE POLITÉCNICA A POLITÉCNICA

INSTITUTO SUPERIOR DE GESTÃO, CIÊNCIAS E TECNOLOGIAS

DEPARTAMENTO DE CIÊNCIAS TECNOLÓGICAS E ENGENHARIAS

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

ANÁLISE DA SEGURANÇA CIBERNÉTICA NA COMPUTAÇÃO EM NUVEM

CASO DE ESTUDO: VODACOM MOÇAMBIQUE

Autora: Neila da Conceição Mabombo

Supervisor:

MSc. Euclides José Tchaúque

Maputo, Outubro 2021

PARECER DO SUPERVISOR

Neila da Conceição Mabombo

ANÁLISE DA SEGURANÇA CIBERNÉTICA NA COMPUTAÇÃO EM NUVEM CASO DE ESTUDO: VODACOM MOÇAMBIQUE

NOME DO TUTOR: ***Euclides José Tchaúque***

_____

PARECER:

Hoje, todas as empresas, grandes ou pequenas, estão adoptando ou com tendência a adoptar a computação em nuvem para permitir sua transformação digital. O crescimento desta tecnologia criou uma demanda para trabalhos de computação em nuvem, de desenvolvedores de nuvem e funções mais especializadas, como arquitectos de soluções e engenheiros de segurança em nuvem.

A estudante Neila Mabombo, propôs realizar o trabalho com o tema: ***Análise da segurança cibernética em nuvem,*** durante o qual demonstrou muita vontade, dedicação e esforço enorme para uma área até bem pouco tempo não muito estudada no domínio das tecnologias de informação e comunicação em Moçambique. O estudo pretendia analisar os principais tipos de ataques cibernéticos na computação em nuvem e compreender as principais técnicas de prevenção com o recurso a tecnologias de informação e comunicação. Após a identificação do tema, a estudante formulou o problema, os objectivos e hipóteses que conduziram à recolha de dados numa entidade da praça.

A estudante usou como metodologia entrevistas a técnicos da Vodacom, uma entidade do ramo de telecomunicações em Moçambique. Tratando-se de uma área relativamente nova em Moçambique a opção foi usar a Vodacom como referência não só por ser a maior operadora de telefonia móvel actualmente no País, mas especialmente por ser uma multinacional com sucursais em várias partes

do mundo e possuir uma experiência no uso desta tecnologia que é parte do objecto de estudo no presente trabalho.

Por fim, esta informação permitiu produzir um documento exaustivo com análises e propostas de uma nova técnica para prevenção de ataques cibernéticos na computação em nuvem.

Deste modo, a estudante conseguiu lograr os seus objectivos, o que lhe confere absoluta certeza de que pode realizar uma investigação científica independente.

Maputo, aos 22 de Junho de 2021.

DECLARAÇÃO DE HONRA

Eu Neila da Conceição Mabombo, nascida aos 11 de fevereiro de 2000, no Hospital Central de Maputo, filha de Sérgio Alfredo Mabombo e Gertrudes Sandra Gomache Nhantumbo, discente da Universidade Politécnica A Politécnica, no curso de engenharia informática e de telecomunicações, declaro por minha honra que este trabalho é resultado da minha autoria pessoal e das orientações do meu supervisor, feita segundo os critérios em vigor da Universidade. O seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto e na bibliografia.

Maputo, 22 de junho de 2021

_____

(Neila da Conceição Mabombo)

AGRADECIMENTOS

Primeiramente agradeço a Deus pelo dom da vida, pela saúde e por tudo que tem feito por mim neste período.

Agradeço aos meus pais Sérgio Alfredo Mabombo e Gertrudes Sandra Gomache Nhantumbo por sempre estarem comigo, pela força, confiança, atenção e motivação que têm me dado durante a minha vida pessoal e académica.

Aos meus irmãos, Natércia Graciete Sandra Mabombo, Jurene Sandra Mabombo e Shelton Sérgio Mabombo, pelo apoio e suporte neste percurso.

Endereço os meus sinceros agradecimentos aos meus Professores do Curso de Licenciatura em Engenharia Informática e Telecomunicações, pela dedicação, pelas horas de apoio, e competência que demonstraram ao longo do curso, disseminando conhecimento.

Agradeço em especial ao Dr. Euclide José Tchaúque pela colaboração durante a realização deste trabalho.

Os agradecimentos estendem-se aos meus avós Paternos Catarina da Conceição Correia e Alfredo Nelson Mabombo (in memorian) e Maternos Américo Gomache Nhantumbo e Felismina Joaquim Nhantumbo que sempre estiveram presentes na minha vida estudantil procurando saber como vai e incentivando a sempre dar o melhor de mim.

As minhas colegas Marlen Beatriz Cumbane e Neidy Mário Canda pelos incentivos, pelas horas perdidas nas madrugadas a estudarmos.

À minha família e a todos aqueles que de forma directa ou indirecta contribuíram para que este trabalho se tornasse uma realidade.

A tecnologia ensinou uma lição à humanidade:

nada é impossível

(Lewis Mumford)

RESUMO

Actualmente, a tecnologia de computação em nuvem surge da necessidade de construir infraestruturas de TI menos complexas, onde os usuários da mesma não precisam de configurar, instalar, e actualizar o software, sendo um novo modelo de computação emergente que move todos os dados e as aplicações dos usuários para grandes centros de armazenamento de dados, os chamados data centers.

A presente pesquisa refere-se a um estudo da computação em nuvem com ênfase no conceito de segurança cibernética, tendo o objetivo de analisar os principais tipos de ataques cibernéticos sofridos na instituição Vodacom Moçambique e compreender quais as técnicas utilizadas para prevenir. Quanto à metodologia, a pesquisa caracteriza-se como quantitativa. A colecta de dados foi realizada por meio de questionário. Os resultados obtidos revelaram que entre os principais tipos de ataques cibernéticos, destaca-se o ataque de phishing. É essencial que as organizações conscientizem todos os seus funcionários sobre as consequências que os atacantes cibernéticos podem causar para poderem acarretar à sua política interna de Segurança Cibernética, para a redução dos índices de ataques cibernéticos.

Palavras – chaves: Computação em nuvem, Segurança cibernética, Ataques cibernéticos, Técnicas de prevenção.

.

ABSTRACT

Currently the cloud computing technology arises from the need to build less complex IT infrastructure, where users don’t need to configure, install, and update software being a new emerging computing model that moves all users data and applications to large data storage centers, the so called data centers.

This present research refers to a study of cloud computing with emphasis on the concept of cyber security, with the aim of analyzing the main types of cybers attacks suffered at Vodacom Mozambique and understanding the techniques used to prevent. As for the methodology, the research is characterized as quantitative. Data collection was carried out through questionnaires. The results obtained revealed that among the main types of cybers attacks, the phishing attack stands out. It is essential that organizations make all their employees aware of the consequences that cyber attackers can cause to comply with its internal cyber security pollical, to reduce Cyber Attack indices.

Keywords: Cloud computing, Cyber security, Cyber Attacks, Prevention techniques.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELA

LISTAS DE SIGLAS E ABREVIATURAS

APTs Application programming Interface

AWS Amazon Web Services

CIA Confidentiality, Integrity, Availability

CRM Customer Relationship Management

CSPs Cloud Service Providers

DNS Domain Name System

DoS Denial of Services

DDoS Distributed Denial of Services

EC2 Elastic Compute Cloud

HaaS Hardware as a Service

IA Inteligência Artificial

IaaS Infrastructure as a Service

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

ISO International Organization for Standardization

MITM Man-in-the-middle

NIST National Institute of Standards

PaaS Plataform as a Service

TI Tecnologia da Informação

SaaS Software as a Service

SOAP Simple Object Access Protocol

SQL Structured Query Language

XML Extensible Markup Language

XSS Cross-site Scripting

1. CAPÍTULO I – INTRODUÇÃO

A Tecnologia da Informação, TI, tem como maior objectivo o apoio nos processos de tomada de decisões na empresa, e seu foco está direccionado ao principal negócio empresarial. (REZENDE, 2002)

Segundo o trabalho de Chaves (2011), na busca de por serviços de Tecnologia da Informação (TI), com melhores relações benefício/custo, as instituições e organizações de negócios têm optado por mesclar serviços de provimento próprio com os adquiridos por terceiros. Neste último decênio, cresceram e se diversificaram de modo significativo tanto a procura quanto a oferta de serviços de TI por parte, respectivamente, de clientes em potencial e provedores dos mais diversos tipos.

O mundo está mudando cada vez mais rápido como consequência de um desenvolvimento tecnológico acelerado.

Segundo especialistas na área de tecnologia, importantes mudanças e avanços tecnológicos surgem frequentemente, e uma delas é a *Cloud Computing* ou Computação em Nuvem.

Conforme Simon (2003) não importa quanto seja feito de investimentos na área de tecnologias da segurança da informação e treinamentos de pessoal para garantir a confidencialidade de seus dados, bem como, os colaboradores seguirem as melhores recomendações para práticas de segurança e instalação de programas que, ainda assim, a organização estará vulnerável.

Esta arquitetura em nuvem refere-se como um modelo no qual a computação (processamento, armazenamento e softwares) está em algum lugar da rede e é acessada remotamente, por exemplo: uma empresa ou pessoa não precisar ter mais nenhum software instalado em sua máquina, pois o acesso a todo e qualquer recurso será via internet (nuvem), num sistema operacional a partir de qualquer computador e em qualquer lugar, pode-se ter acesso a informações, arquivos e programas num sistema único, independente de plataforma. (SCHIAVO, 2015)

Diante deste cenário surge a questão da segurança cibernética na computação em nuvem, pois é necessário prevenir as informações e arquivos dos atacantes cibernéticos para evitar o roubo ou qualquer acto mal-intencional neste meio.

1.1. Problema de investigação

Actualmente a computação em nuvem em inglês *Cloud Computing* é uma tecnologia bastante aprofundada. Essa nova tecnologia da computação é uma tendência que permite utilizar as mais variadas aplicações via Internet, em qualquer lugar e independente de plataforma, com a mesma facilidade de tê-las instaladas no próprio computador.

Hoje em dia, existem muitas vantagens da computação em nuvem, onde a principal é trazer as empresas mais agilidade para atingir os seus objectivos. Porém, a nuvem traz consigo um nível adicional de riscos, que estão directamente associados à terceirização de serviços essenciais (serviços em nuvem). Pois várias informações e dados são processados diariamente, podendo haver roubo, vazamento de dados e exclusão se não tivermos em conta o problema de segurança cibernética.

Todas empresas que migraram para a nuvem estão sujeitas a ataques cibernéticos, contudo, a maioria só toma medidas de mitigação quando sofre algum ataque, o que não é considerado certo.

O presente trabalho tem como objectivo de responder a seguinte questão: Como a instituição Vodacom pode prevenir-se de ataques cibernéticos na computacao em nuvem?

A pesquisa gira em torno dessa questão, uma vez que os atacantes cibernéticos se beneficiam das vulnerabilidades da computação em nuvem, analisamos técnicas para evitar esses ataques, garantindo uma melhor segurança na computação em nuvem.

1.2. Objectivos

1.2.1. Objectivo Geral

- Propor a Vodacom Moçambique uma técnica de prevenção dos ataques cibernéticos na computação em nuvem.

1.2.2. Objectivos Específicos

- Esclarecer os conceitos de computação em nuvem e segurança cibernética;
- Analisar os principais tipos de ataques cibernéticos na computação em nuvem ocorridos na instituição Vodacom Moçambique;
- Identificar técnicas que a instituição Vodacom Moçambique utiliza para prevenir-se dos ataques cibernéticos na computação em nuvem;
- Propor uma nova técnica à instituição Vodacom Moçambique para prevenção de ataques cibernéticos na computação em nuvem.

.

1.3.Questões de Pesquisa e Hipóteses

1.3.1. Questões de pesquisa

- Quais os conceitos da computação em nuvem e segurança cibernética?
- Quais são os principais tipos de ataques cibernéticos na computação em nuvem ocorridos na instituição Vodacom Moçambique?
- Quais são as técnicas que a instituição Vodacom Moçambique utiliza para prevenir-se dos ataques cibernéticos na computação em nuvem?
- Qual técnica a instituição Vodacom Moçambique pode adotar para prevenir-se dos ataques cibernéticos na computação em nuvem?

1.3.2. Hipóteses

Ho – *Com a nova técnica proposta a instituição Vodacom Moçambique não poderá prevenir-se dos ataques cibernéticos ocorridos na computação em nuvem.*

H1 – *Com a nova técnica proposta a instituição Vodacom Moçambique poderá prevenir-se dos ataques cibernéticos ocorridos na computação em nuvem.*

1.4. Justificativa

Hoje em dia, à medida que a computação em nuvem cresce, a prevalência de violações cibernéticas para serviços em nuvem também está crescendo significativamente. A computação em nuvem facilita às empresas o desenvolvimento mais rápido de produtos e serviços. Ele não apenas permite que aumente o poder de computação para atender às crescentes demandas de seus clientes, mas também fornece melhores insights que ajudam a criar serviços personalizados para seus clientes.

A própria natureza da computação em nuvem, terceirizar o armazenamento e a recuperação de dados de negócios muitas vezes sensíveis requer um foco profundo na segurança e na confiança. A segurança de TI é (ou deveria ser) uma prioridade máxima na maioria das organizações, uma vez que uma única violação de segurança tem o potencial de expor dados de clientes, roubar propriedade intelectual valiosa e prejudicar permanentemente a reputação de uma empresa.

Abordar a computação em nuvem na visão de segurança cibernética é colocar em questão a essência desta tecnologia. Essa segurança cibernética na nuvem se refere às ferramentas, dados e infraestrutura que protegem os produtos baseados na nuvem de agentes mal-intencionados.

A utilização de uma infraestrutura em nuvem possibilita o acesso a recursos tecnológicos de alta performance, facilmente incrementados e gerenciados de forma segura.

Diante deste contexto pretendemos fazer uma análise geral de como podemos prevenir os ataques cibernéticos na computação em nuvem evitando o vazamento ou roubos mal intencionados de informações, para garantir a integridade, confidencialidade, e autenticidade dos dados de uma forma mais segura.

1.5. Estrutura do trabalho

O presente trabalho estará dividido em seis capítulos:

Capítulo I: Introdução

Neste capítulo consta a introdução do trabalho, definição do problema de pesquisa, questão de pesquisa, hipóteses, objectivos gerais e específicos e a justificativa.

Capítulo II: Revisão Bibliográfica

O segundo capítulo apresenta a fundamentação teórica onde são básicos importantes para a compreensão do tema em estudo

Capítulo III: Metodologia de pesquisa

Neste capítulo, mostraremos os métodos e as técnicas que utilizamos para atingir o objectivo da pesquisa.

Capítulo IV: Resultados

Este capítulo destina-se ao caso de estudo proposto pela autora: a autora inicia o capítulo apresentado pelo resumo das actividades realizadas (nomeadamente: questionários, entrevista).

Capítulo V: Discussões

Este capítulo destina-se em analisar os resultados do caso de estudo proposto pela autora.

Capítulo VI: Conclusões e Recomendações

Neste capítulo a autora apresenta as conclusões e recomendações do presente trabalho. A autora divide este capítulo em duas partes: a primeira parte aborda as conclusões onde são apresentadas considerações gerais acerca do trabalho; a solução proposta em relação ao problema colocado; o nível de alcance dos objectivos definidos. Na segunda parte são apresentadas recomendações, para que se possa ter em conta trabalhos futuros, consiste na análise e avaliação dos resultados obtidos, a fim de sugerir melhorias para esse problema.

2. CAPÍTULO II – FUNDAMENTAÇÃO TEÓRICA

2.1.Computação em nuvem

2.2.Surgimento

Segundo o site https://pt.wikipedia.org/wiki/Computação_em_nuvem a ideia da computação em uma "nuvem" remonta às origens da computação utilitária, um conceito que o cientista da computação John McCarthy propôs publicamente em 1961: "Se os computadores do tipo que defendo se tornarem os computadores do futuro, então a computação pode algum dia ser organizada como serviço público, assim como o sistema telefônico é serviço público. O utilitário do computador pode se tornar a base de uma e importante indústria".

Em 1969, Leonard Kleinrock, um cientista-chefe da Rede de Agências de Projectos de Pesquisa Avançada ou Projecto ARPANET que semeou a internet, declarou: "A partir de agora, as redes de computadores ainda estão em sua infância, mas à medida que crescerem e se tornarem sofisticadas, iremos provavelmente ver a disseminação de 'utilitários de computador'...".

Foi só em 2006 que o termo "computação em nuvem" surgiu na arena comercial. Foi durante essa época em que a Amazon lançou seus serviços Elastic Compute Cloud (EC2) que permitiram que as organizações "alugassem" capacidade de computação e poder de processamento para executar seus aplicativos empresariais. O Google Apps também começou a fornecer aplicativos empresariais baseados em navegador no mesmo ano, e três anos depois, o Google App Motor se tornou outro marco histórico.(TAURION, 2009).

A computação em nuvem é a concepção de utilização dos mais diversos tipos de aplicações através da Internet, em qualquer lugar e independente de dispositivo ou plataforma, como se estes aplicativos estivessem instalados nos dispositivos dos usuários. Para que os usuários usufruam dos serviços da computação em nuvem, é necessário que tenham em seus dispositivos conectividade com a internet, acessando o tal serviço através de um navegador de Internet ou programa específico para esta tarefa.

2.3.Definição

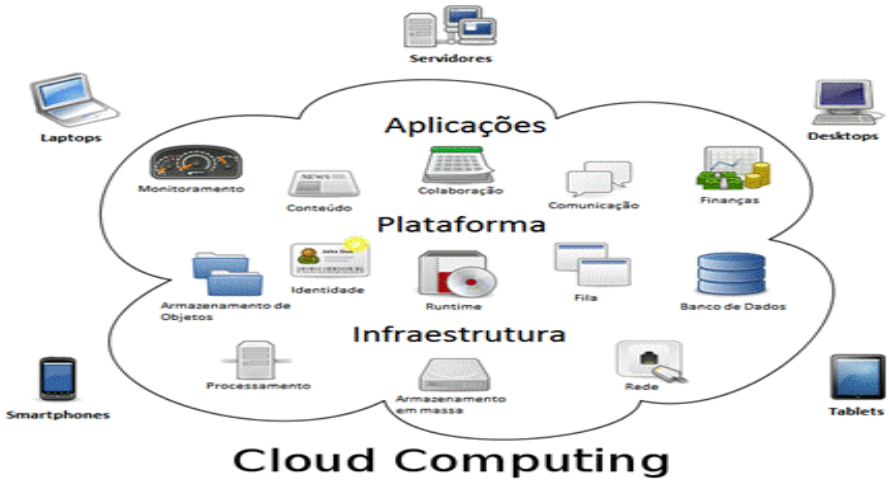

Figura 1: Esquema da Computação em Nuvem
Fonte: (pt.wikipedia.com)

Segundo TAURION (2009) o termo computação em nuvem surgiu em 2006 em uma palestra de Eric Schmidt, da Google, sobre como sua empresa gerenciava seus data centers. Hoje, a computação em nuvem, se apresenta como o cerne de um movimento de profundas transformações do mundo da tecnologia.

SOUZA (2009) propõe a seguinte definição: “A computação em nuvem é um conjunto de serviços de rede activados, proporcionando escalabilidade, qualidade de serviço, infraestrutura barata de computação sob demanda e que pode ser acessada de uma forma simples e pervasiva”.

SILVA (2010) diz que a computação na nuvem ou Cloud Computing é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independentes da plataforma, bastando para isso ter um terminal conectado à “nuvem”.

Um relatório do Gartner listando a computação em nuvem no topo de suas áreas estratégicas de tecnologia reafirmou sua proeminência sua definição formal como: “um estilo de computação no qual recursos escalonáveis e elásticos habilitados para TI são

fornecidos como serviço externo para clientes que usam tecnologias da Internet". (GARTNER, 2008).

A Forrester Research forneceu sua própria definição de computação em nuvem como: "uma capacidade de TI padronizada (serviços, softwares ou infraestrutura) fornecida por meio de tecnologias da internet em um modo de autoatendimento com pagamento conforme o uso". (THOMAS ERL, 2013).

A definição que obteve aceitação em todo o sector foi composta pelo National Institute of Standards (NIST). O NIST publicou sua definição original em 2009, seguida por uma versão revisada após uma análise mais aprofundada e sugestões da indústria que foram publicadas em setembro de 2011:

> "A computação em nuvem é um modelo para permitir o acesso onipresente, conveniente e sob demanda à rede a um pool compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberado com mínimo esforço de gerenciamento ou interação do provedor de serviços. Este modelo de nuvem é composto por cinco características essenciais, três modelos de serviços e quatro modelos de implatação". (NIST, 2009).

2.4. Elementos da computação em nuvem

Segundo Velte A., Velte T. e Elsenpeter (2012) uma solução de computação em nuvem é composta de três elementos:

- Clientes;
- Data center;
- Servidores distribuídos.

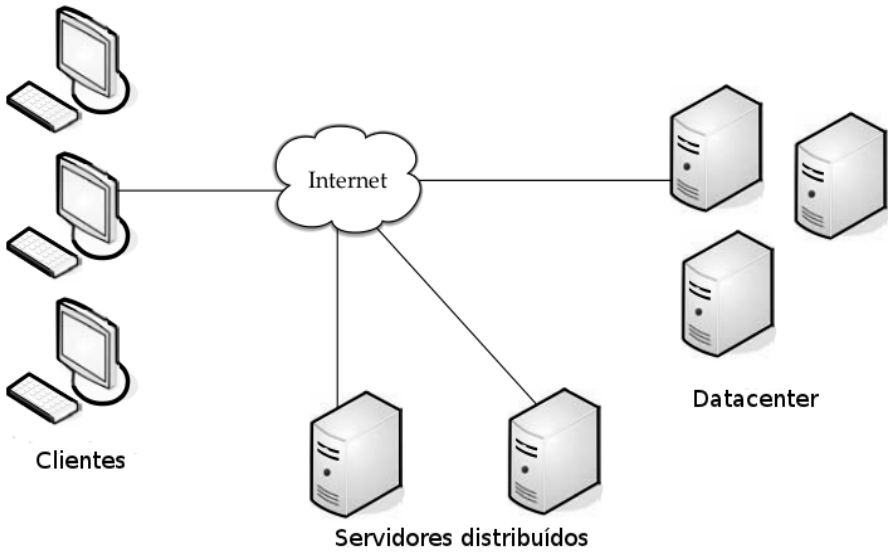

Figura 2: Elementos da computação em nuvem
Fonte: (DevMedia)

2.4.1. Clientes

Conforme Velte A., Velte T. e Elsenpeter (2012), os clientes de uma arquitetura em computação em nuvem são exactamente o que são os clientes de uma antiga rede local, conhecida como LAN. Eles são os computadores pessoais, laptops, celulares, tablets etc. Nesse sentido, os clientes são os dispositivos que os usuários finais utilizam para gerenciar sua informação na nuvem, e podem ser classificados em três categorias:

a) Dispositivos móveis: PDAs, smartphones e tablets.

b) Clientes thin: são computadores que não possuem disco rígido interno, porém permitem que o servidor faça todo o trabalho.

c) Thick: esse cliente é um computador normal, que utiliza um browser da web para conectar-se na nuvem.

2.4.2. Data centers

Para Velte A., Velte T. e Elsenpeter (2012), um data center é um conjunto de servidores onde os aplicativos são armazenados. Esses servidores geralmente estão em um andar de um edifício. Uma tendência crescente na tecnologia da informação é a virtualização de

servidores. Isto é, o software pode ser instalado permitindo que vários servidores virtuais sejam usados. Dessa maneira é possível ter vários servidores virtuais rodando em um mesmo servidor físico.

Para PINHEIRO (2004), um data center é uma modalidade de serviço de valor agregado que oferece recursos de processamento e armazenamento de dados em larga escala para que organizações de qualquer porte e mesmo profissionais liberais possam ter ao seu alcance uma estrutura de grande capacidade e flexibilidade, alta segurança, e igualmente capacitada do ponto de vista de hardware e software para processar e armazenar informações.

2.4.3. Servidores distribuídos

Conforme Velte A., Velte T. e Elsenpeter (2012) são servidores de uma mesma solução que não necessitam, necessariamente, estar alocados em um mesmo local. Normalmente os servidores estão em diferentes posições geográficas, mas para um usuário da nuvem, eles agem como se estivessem em um mesmo lugar. Isso permite ao prestador de serviços maior flexibilidade nas opções e na segurança. Por exemplo, a Amazon possui uma solução de nuvem nos servidores do mundo inteiro. Se algo acontecer em um local, causando uma falha, o serviço ainda poderá ser acessado através de outro local. Inclusive, se a nuvem precisar de mais hardware, podem ser adquiridos servidores em qualquer lugar, bastando torná-los parte da nuvem.

2.5. Modelos NIST da computaçãem nuvem

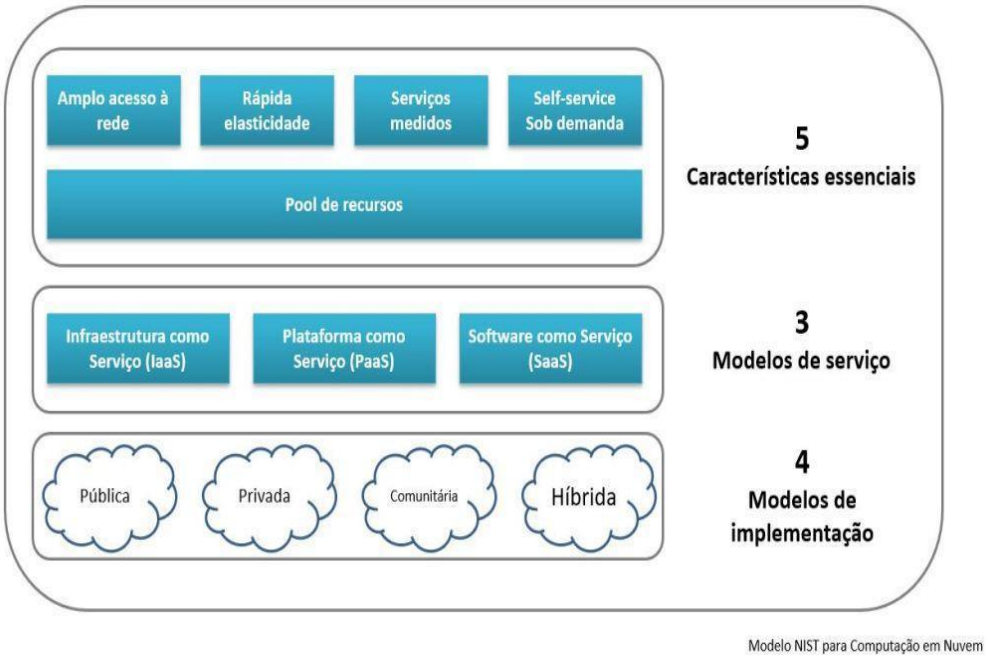

Figura 3: Modelo NIST da computação em nuvem
Fonte: (jornada para nuvem.com.br)

Segundo NIST, a computação possui cinco características, três modelos de serviços e quatro modelos de implementação:

2.5.1. Cacacterísticas da computação em nuvem

Para o NIST (National Institute of Standards and Technology) ou Instituto Nacional de Padrões e Tecnologia, existem cinco características essenciais para a computação em nuvem:

- **Autoatendimento sob demanda –** Um consumidor pode utilizar unilateralmente recursos de computação, com tempo de servidor e armazenamento de rede, conforme necessário, automaticamente, sem exigir interação humana com cada provedor de serviços. (OLIVEIRA, 2017)
- **Amplo acesso à rede –** Os recursos estão disponíveis na rede e são acedidos por meio de mecanismos padrão que promovem o uso por plataformas heterogêneas

(por exemplo, telefones celulares, tablets, notebooks e estações de trabalho). (OLIVEIRA, 2017).

- **Pool de recursos –** Os recursos de computação do provedor são agrupados para atender a vários consumidores usando um modelo da multilocação, com diferentes recursos físicos e virtuais atribuídos dinamicamente de acordo com a demanda do consumidor. (OLIVEIRA, 2017).
- **Elasticidade rápida –** Os recursos podem ser provisionados e liberados elasticamente, em alguns casos automaticamente, para escalar rapidamente para fora e para dentro de acordo demanda, para o consumidor, os recursos disponíveis para utilização muitas vezes parecem ilimitados e podem ser apropriados em qualquer quantidade e a qualquer momento. (OLIVEIRA, 2017).
- **Serviço medido –** Os sistemas em nuvem controlam e otimizam automaticamente o uso de recursos aproveitando um recurso de medição em algum nível de abstração apropriado ao tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de utilizador activas). O uso de recursos pode ser monitorado, controlado e relatado, fornecendo transparência tanto para o provedor quanto para o consumidor do serviço utilizado. (OLIVEIRA, 2017).

De acordo com Taurion (2009):

> A computação em nuvem cria uma ilusão da disponibilidade de recursos infinitos, os quais podem ser acessíveis sob demanda. Uma outra característica é que ela elimina a necessidade de adquirir e provisionar recursos antecipadamente. A elasticidade permite que as empresas usem os recursos na quantidade que forem necessários, aumentando e diminuindo a capacidade computacional de forma dinâmica. Por último, o pagamento dos serviços em nuvem é pela quantidade de recursos utilizados (pay-per-use), que significa que pagamos pelos serviços que utilizamos.

Para (ALECRIM, 2008), “independente da aplicação, com a Cloud Computing o usuário não necessita conhecer toda a estrutura que há por trás, ou seja, ele não precisa saber quantos servidores executam determinada ferramenta, quais as configurações de hardware

utilizadas, como o escalonamento é feito, onde está a localização física do datacenter, enfim".

2.5.2. Modelos de serviços da computação em nuvem

Os recursos de computação em nuvem são heterogêneos, variando de serviços de software a armazenamento de dados, para sistemas operacionais e infraestrutura de hardware. Dependendo do tipo ou granularidade do serviço, existem três modelos diferentes de entrega em nuvem: infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (Saas):

2.5.2.1. Infraestrutura como Serviço (IaaS)

Em Infraestrutura como serviço, conhecida também de Hardware como serviço (HaaS), o consumidor recebe a capacidade de provisionar processamento, armazenamento, redes, dentre outros recursos de computação, na qual ele será capaz de implementar e executar software arbitrário, que podem incluir sistemas operacionais e aplicativos. Assim como nos dois tipos anteriores, o consumidor não gerencia ou controla a infraestrutura de nuvem subjacente, mas detém o controle sobre sistemas operacionais, armazenamento, aplicativos implementados e possivelmente controle limitado de componentes específicos de rede (NIST, 2012).

Em IaaS a infraestrutura pode ser dinamicamente ajustada para cima ou para baixo, baseada nas necessidades de recurso do aplicativo. E múltiplos locatários podem utilizar o equipamento ao mesmo tempo (VELTE et. al., 2012).

Às vezes, os provedores de nuvem contratam ofertas de IaaS de outros provedores de nuvem para escalar seus próprios ambientes de nuvem. Os tipos e marcas dos recursos de TI fornecidos pelos produtos IaaS oferecidos por diferentes provedores de nuvem podem variar. Os recursos de TI disponíveis por meio de ambientes IaaS são geralmente oferecidos como novas instâncias virtuais inicializadas. Um recurso de TI central e primário em um ambiente IaaS típico é o servidor virtual. O servidor virtual é alugado especificando os requisitos de hardware do servidor, como capacidade do processador, memória e espaço de armazenamento local.

2.5.2.2. Plataforma como Serviço (PaaS)

O modelo de entrega PaaS representa um ambiente "pronto para usar" pré-definido, normalmente composto por recursos de TI implantados e configurados. Especificamente, PaaS depende (e é principalmente definido por) o uso de um ambiente pronto que estabelece um conjunto de produtos pré-embalados e ferramentas usadas para apoiar todo ciclo de vida de entrega de aplicativos personalizados.

Fornece ao consumidor a capacidade para implementar sobre a infraestrutura de nuvem aplicações criadas ou adquiridas usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. O consumidor não gerencia ou controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas detém controle sobre os aplicativos implementados e possivelmente sobre as definições de configuração para o ambiente de hospedagem dos aplicativos (NIST, 2012).

A PaaS fornece todos os recursos necessários para construir aplicativos e serviços directamente da Internet, sem precisar baixar ou instalar software. Incluindo design de aplicativos, desenvolvimento, testes, implantação e hospedagem. Outros serviços incluem a colaboração em equipe, integração de serviços web, integração de banco de dados dentre outros (VELTE et. al., 2012).

2.5.2.3. Software como Serviço (SaaS)

Nesse modelo, a capacidade fornecida ao consumidor é a utilização de aplicativos do provedor rodando em uma infraestrutura de nuvem. As aplicações são acessíveis a partir de diferentes dispositivos clientes, como um navegador web, ou uma interface de programação. O consumidor não gerencia ou controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento, ou mesmo capacidade individuais dos dispositivos, pode haver uma pequena excepção de configuração do aplicativo, específica para o usuário (NIST, 2012).

Com SaaS o software é entregue como serviço de uma forma diferente do modelo tradicional, neste a empresa adquire uma licença de uso e instala o software nos próprios

servidores. Com o modelo SaaS estas regras mudam, pois com o SaaS não são mais necessários os contratos de manutenção, visto que estas atividades ficam a cargo do provedor e não mais da empresa. O usuário passa somente a usar o software sem se preocupar com as actividades de instalação, manutenção e upgrades de aplicações. (TAURION, 2009).

Entre as ofertas de SaaS são oferecidos vários serviços de aplicações, cuja funcionalidade é baseada principalmente em aplicações simples, assim como, em aplicações complexas. O Google Maps é uma das aplicações que os usuários finais podem acessar. Dentre as aplicações mais complexas temos sistemas de Gerenciamento do Relacionamento com o Cliente CRM (Customer Relationship Management). (BAUN et. al., 2011).

2.5.3. Modelo de responsabilidade compartilhada

Esse modelo estabelece onde termina a responsabilidade do provedor (segurança da nuvem) e onde começa a responsabilidade do cliente (segurança na nuvem).

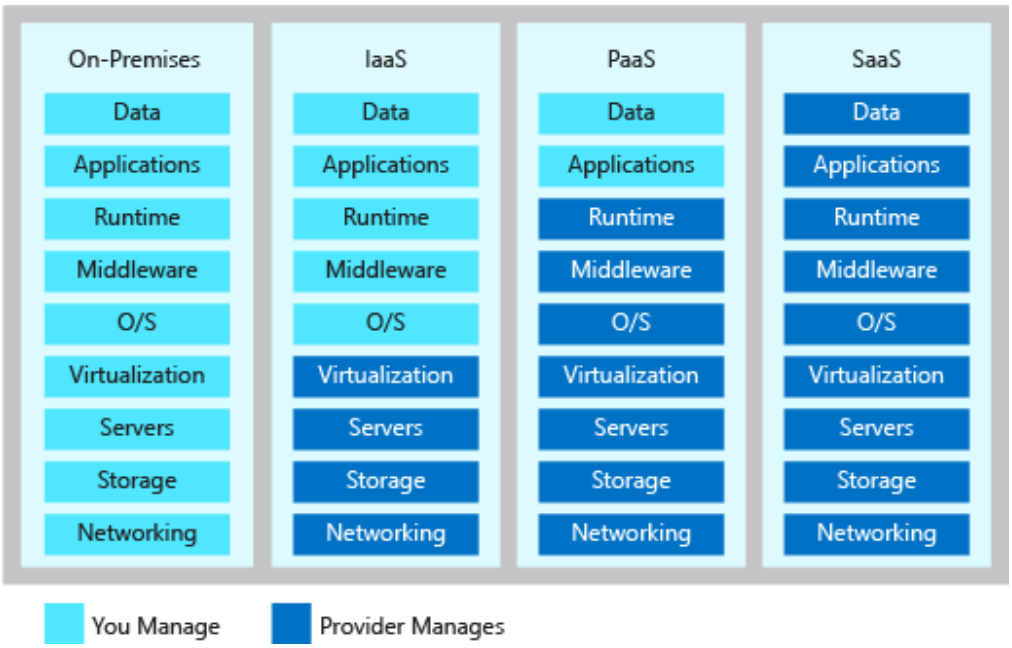

Figura 4: Modelo de responsabilidade compartilhada
Fonte: (oaca-project.org)

Essencialmente, seu provedor de nuvem é responsável por garantir que sua infraestrutura construída dentro de sua plataforma seja inerentemente segura e

confiável, pense em instalações físicas, utilitários, cabos, hardware, etc. Por outro lado, recursos de nuvem personalizáveis, como gerenciamento de aplicativos, configuração de rede e criptografia, controles de rede, gerenciamento de identidade e acesso, configurações de aplicativos e dados são de responsabilidade do usuário final. (BERNHARD, 2010).

Dito isso, essa divisão de responsabilidades pode mudar dependendo do modelo de serviço. Em um nível básico, a definição NIST de computação em nuvem define três modelos de serviço em nuvem primários:

- Infraestrutura como serviço (IaaS): No modelo IaaS, o CSP é responsável pelo data center físico, rede física e servidores/hospedagem físicos.
- Plataforma como serviço (Paas): em um modelo PaaS, o CSP assume mais responsabilidade por coisas como patching (que os clientes são historicamente terríveis e serve como principal caminho para incidentes de segurança) e manutenção de sistemas operacionais.
- Software como serviço (SaaS): no SaaS, o cliente só pode fazer alterações nas configurações de um aplicativo, com o controle de todo o resto sendo deixado para o CSP (pense no Gmail como um exemplo básico).

2.5.4. Modelo de implentação da computação em nuvem

Para MACHADO (2009), para definir o modelo de implementação a ser escolhido, é necessário que se faça uma avaliação do tipo de serviço a ser implementado, o processo de negócio, o tipo de informação e o nível em que ela deve ser gerada e sua forma de ser disponibilizada. É essencial também o controle de acesso a essas aplicações, de forma que se tenha controle a nível de usuário, delegando ou revogando acesso a determinado recurso, conforme assim definido por determinada organização.

De acordo com o Sun (2009):

> As organizações devem fazer observações perante ao modelo de computação em nuvem a ser escolhido, podendo também usarem mais de um modelo, a fim de atender a especificações diferentes e resolver diferentes problemas, como um aplicativo temporário, na qual deva ser mais adequado sua implantação no modelo público, evitando que seja necessário a compra de equipamentos para solucionar um problema temporário. Assim como um aplicativo permanente, que necessite de requisitos específicos, ou de localização de dados, deve ser melhor implantado em uma nuvem privada ou híbrida.

O *National Institute of Standards and Technology* (NIST, 2009), divide os modelos de implantação de computação em nuvem em:

2.5.4.1. Nuvem Privada (*Private Cloud*)

Uma nuvem privada é, em geral, construída sobre um data center privado. Este modelo de implementação permite que esta seja administrada pela própria organização ou por terceiros através de políticas de acesso aos serviços. Segundo o NIST (2009), as ferramentas utilizadas para prover tais características podem ser em nível de gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização.

Segundo TAURION (2009), as nuvens privadas também são chamadas de nuvens empresariais. Elas correspondem ao uso do conceito de nuvem computacional aplicado aos servidores localizados internamente no firewall da empresa, e são gerenciadas pela mesma.

Diferentemente dos outros modelos de implementação de nuvem em detrimento de sua natureza privada, esse é o que provê um menor risco. Em termos de automação de tarefas como actualizações, torna-se engessado pelo facto de estar directamente atrelado aos processos corporativos. Além disso, por exigir um gerenciamento interno, e embora traga algumas facilidades por estar no ambiente da empresa, este diminui a economia de recursos. (SCHIAVO, 2015).

2.5.4.2. Nuvem Pública (*Public Cloud*)

De acordo com o NIST (2009):

> Este modelo de implementação da infraestrutura de nuvens é disponibilizado para o público em geral ou para grupos de indústrias, sendo acessado por qualquer usuário que conheça a localização do serviço. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento, o que pode parecer ineficiente a princípio, porém se adotadas as políticas de segurança e uma estrutura organizada, a existência de outras aplicações na mesma nuvem permanece transparente para os usuários.

Em termos de economia e compartilhamento de recursos, o conceito de nuvens públicas proporciona um maior desempenho, por outro lado, uma vez que os dados podem ser armazenados em locais desconhecidos e não podem ser facilmente recuperados, o modelo possui certas limitações de customização relacionadas justamente à segurança das informações, SLAs (Service Level Agreement) e políticas de acesso (SCHIAVO, 2015).

2.5.4.3. Nuvem Comunitária (*Community Cloud*)

No modelo de implementação de nuvem comunitária ocorre o compartilhamento por diversas empresas de uma nuvem localmente ou remotamente, sendo esta suportada por uma comunidade específica que partilha de interesses semelhantes, tais como a missão, os requisitos de segurança, política e considerações sobre flexibilidade.

O NIST (2009) cita que este tipo de modelo de implementação pode existir localmente ou remotamente e pode ser administrado por alguma empresa da comunidade ou por terceiros, semelhante ao modelo de Nuvem Privada em relação à definição de políticas de acesso e a utilização de tecnologias de autenticação e autorização. Outro factor importante é o facto dos dados e informações poderem ser armazenados com os dados de outros concorrentes pertencentes à mesma comunidade. (SCHIAVO, 2015).

2.5.4.4. Nuvem Híbrida (*Hybrid Cloud*)

De acordo com SCHIAVO (2015), este modelo é composto de dois ou mais modelos de implementação de nuvem (nuvem pública ou comunidade privada) que permanecem como entidades únicas, sendo relaccionadas por uma tecnologia padronizada ou proprietária que permite a portabilidade de dados e de aplicações (por exemplo, nuvem de ruptura para balanceamento de carga entre nuvens).

Para garantir que os dados sejam atribuídos ao tipo de nuvem correto, a escolha deste modelo exige uma minuciosa classificação e rotulagem dos dados. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas, por exemplo. Como factor negativo do modelo está o alto risco, uma vez que funde diferentes formas de implementação. (SCHIAVO, 2015).

2.6. Modelo multi – inquilinos

De acordo com Taurion (2009):

> Uma das características da computação em nuvem, definida pelo NIST como pool de recursos, é que uma aplicação deve atender a múltiplos clientes, chamados de inquilinos. Inquilinos não são usuários individuais, mas empresas clientes do software. Uma arquitectura multi-inquilinos é essencial para a computação em nuvem, pois permite que múltiplas empresas clientes compartilhem recursos físicos comuns (hardware e software), mas que permanecem isoladas na camada lógica.

Todavia, há também o modelo de inquilino isolado, o qual possui recursos exclusivos. Os modelos de inquilinos são:

2.6.1. Inquilino Isolado

Nesse modelo, cada inquilino tem recursos exclusivos, não ocorrendo o compartilhamento dos mesmos com outros inquilinos. Possui conjunto de tecnologias também de forma exclusiva. É similar ao modelo tradicional de hospedagem, em que cada usuário tem seu próprio conjunto de recursos e sua própria instância da aplicação. Esse modelo não é muito

utilizado e recomendado, pois não possui características de elascticidade, visto que os recursos são únicos e exclusivos;

2.6.2. Multi-inquilino via hardware compartilhado (virtualização)

Neste modelo, cada inquilino tem tecnologias exclusivas, porém, o hardware é compartilhado entre os inquilinos via virtualização, sendo alocados de forma dinâmica através de um pool de recursos;

2.6.3. Multi-inquilino via container

Neste modelo, vários inquilinos são executados na mesma instância de um container de aplicação (um servidor de aplicações), mas cada inquilino está associado a uma instância separada do software de banco de dados;

2.6.4. Multi-inquilino totalmente compartilhado

é uma evolução do modelo anterior, agora com todo o software compartilhado. Assim, nesse modelo o banco de dados também é compartilhado, sendo necessária apenas uma instância para o mesmo.

2.7. Vantagens e desvantagens da computação em nuvem

2.7.1. Vantagens da computação em nuvem

De acordo com CHIRIGATI (2009), as principais vantagens da computação em nuvem são:

- **Custos baixos**

Como mencionamos, antes do advento da computação em nuvem, muitas empresas tiveram que executar seus próprios recursos de computação interna. Isso significava empregar membros da equipe de TI para executá-lo, bem como assumir a responsabilidade directa de garantir que informações confidenciais fossem mantidas firmemente a sete chaves.

- **Melhora a experiência do cliente**

As soluções baseadas em nuvem também podem permitir que as empresas ofereçam melhores padrões de atendimento ao cliente. A experiência do cliente é de vital importância

hoje, e os consumidores passaram a esperar que as empresas estejam muito mais atentas às suas necessidades. As empresas que conseguem fazer isso são muito mais propensas a estabelecer relacionamentos com clientes de longo prazo. (CHIRIGATI, 2009).

- **Mais flexibilidade**

No mundo moderno dos negócios, flexibilidade é uma palavra de ordem crucial. As necessidades dos clientes e clientes estão mudando o tempo todo, e as empresas precisam ser adaptáveis o suficiente para se ajustarem. A computação em nuvem pode fornecer a flexibilidade extra que pode dar às empresas uma vantagem competitiva crucial.

- **Melhor comunicação e trabalho em equipa**

Com a computação em nuvem, esse tipo de colaboração é muito mais simples. Colegas, clientes e terceiros contratados ou consultores podem trabalhar todos com os mesmos arquivos, todos acessíveis através da nuvem. Também é muito mais fácil compartilhar registros relevantes com, digamos, consultores financeiros e contadores. Isso torna uma série de processos mais suaves.

- **Continuidade confiável**

O tempo de inactividade é um dos grandes medos das empresas modernas. Todos os tipos de coisas podem colocar a infraestrutura de TI das empresas fora de acção, desde cortes de energia até desastres naturais. As empresas, portanto, precisam garantir que sejam tomadas medidas adequadas para garantir uma continuidade confiável

- **Forte segurança**

A segurança de dados tem sido um dos tópicos quentes dos últimos anos, com regulamentações mais duras introduzidas para garantir uma protecção mais robusta. Mesmo agora, muitas empresas ainda se preocupam que migrar para a nuvem possa deixar seus dados menos seguros, e mais em risco de olhares curiosos.

- **Mobilidade mais fácil**

Nesta era de trabalho de qualquer lugar, a mobilidade é primordial. Hoje, é possível ser muito mais flexível em termos de nossos arranjos de trabalho do que antes. Agora, estamos trabalhando em todos os tipos de locais diferentes: em escritórios em todo o país e no exterior, em casa, no café, na biblioteca, ou talvez fora do jardim.

- **Recuperação de desastre**

A computação em nuvem garante que a recuperação de desastres seja muito mais fácil do que poderia ser. Isso ocorre porque os dados vitais são armazenados fora do local em data centers de terceiros, facilitando assim a recuperação em caso de inactividade não programada.

- **Escalabilidade fácil**

À medida que seu negócio muda e se expande, também seus requisitos de TI. Alternactivamente, pode ser que você tenha que reduzir sua operação e, com ela, suas necessidades de armazenamento de TI. A computação em nuvem oferece uma escala fácil, permitindo que você descreva à medida que suas circunstâncias mudam.

- **Actualizações automáticas**

As empresas que execuctam sua própria infraestrutura de TI também têm que lidar com actualizações de software, para que quaisquer vulnerabilidades de segurança sejam corrigidas e que a tecnologia em que estão execuctando esteja actualizada.

2.7.2. Desvantagens da computação em nuvem

Segundo CHIRIGATI (2009), as principais desvantagens da computação em nuvem são:

- **Conectividade de internet**

Computação em nuvem precisa de conectividade com a internet como se não houvesse conexão com a internet, você não poderá acessar a nuvem. Além disso, não há outra maneira de colectar os dados da nuvem.

- **Largura de banda inferior**

A largura de banda mais baixa reduz os benefícios das nuvens de tal forma que não possa ser usada adequadamente. Uma conexão de satélite pode levar a uma interrupção de qualidade, devido à maior latência ou maior largura de banda.

- **Afecte a velocidade**

Se um cliente está usando uma internet que usa vários usuários para baixar arquivos como música, documentos e muito mais. Isso reduzirá a velocidade para usar a Nuvem.

- **Questões de segurança**

Como a computação em nuvem é muito segura, ainda assim requer a assistência e aconselhamento de uma empresa de consultoria de TI. Negligenciar isso pode levar ao facto de que o negócio se tornará vulnerável aos hackers e às ameaças.

- **Acordos**

Existem muitos fornecedores disponíveis que têm acordos que são inegociáveis. É uma das desvantagens para as empresas.

- **Falta de apoio**

As empresas de computação em nuvem às vezes não fornecem suporte adequado aos clientes. Além disso, eles querem que os clientes dependam totalmente de faqs, o que pode ser um trabalho tedioso.

- **Variação de custo**

Computação em nuvem é uma opção econômica, mas se você considerar a instalação do software pode ser caro. A instalação pode levar a algum recurso caro que pode ser não benéfico no futuro.

2.8. Principais fornecedores de computação em nuvem

Actualmente existem várias empresas que estão chegando com serviços de nuvem e têm um desempenho melhor a cada dia. Esses provedores oferecem os três modelos de serviços de nuvem: SaaS, PaaS e IaaS.

Os principais provedores de computação em nuvem são:

Provedores de nuvem	**Definição**
Amazon Web Services (AWS)	É uma plataforma de computação em nuvem que fornece serviços como poder de computação, armazenamento de banco de dados, entrega de conteúdo e muitas outras funções que ajudarão a integrar um negócio.
Sever space	Estes são servidores em nuvem com sistemas operacionais Windows e Linux. No Servidores de Nuvem Server Space, podemos escolher nossas próprias configurações personalizadas, acelerar a VM em 40 segundos, alterar a configuração a qualquer momento e pagar conforme usar.
Microsoft Azure	O Microsoft Azure é um serviço de computação em nuvem usado para criar testes, implantar e gerenciar aplicativos. Esse processo é feito em uma rede global de data center gerenciada pela Microsoft. É uma plataforma de nuvem privada e também pública.

Google Cloud Platform	A plataforma em nuvem do Google é um dos principais serviços de computação em nuvem oferecidos pelo Google e funciona na mesma infraestrutura que o Google usa para seus produtos de usuários finais.
IBM	A nuvem IBM oferece serviços como plataforma como serviço e infraestrutura como serviço. Essa organização em nuvem pode implantar e acessar seus recursos, como rede de armazenamento e poder de computação, com a ajuda da Internet. Existem várias ferramentas que ajudam o cliente a obter um profundo conhecimento do sector.
Adobe	A nuvem criativa da Adobe oferece a melhor experiência em fotografia de design de serviços de aplicativos e web. Os serviços em nuvem da adobe fornece tutoriais e modelos com os quais um iniciante pode acessar facilmente a nuvem e começar a usá-la. Ele oferece muitas facilidades para iniciantes e também para profissionais para fácil acesso à nuvem.

Tabela 1:Principais fornecedores da computação em nuvem

Fonte: Elaborada pela autora.

2.9.Segurança cibernética na computação em nuvem

Figura 5: Espaço cibernético
Fonte: (forbes.com)

2.9.1. Espaço cibernético

Segundo o site https://gestaodesegurancaprivada.com.br/ciberseguranca-seguranca-cibernetica/ a norma internacional ISO-IEC 27032 Ciberespaço ou Espaço Cibernético pode ser entendido como "um ambiente complexo resultante da interação entre pessoas, softwares e serviços existentes na Internet, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física".

Actualmente as sociedades, estão totalmente mergulhadas numa lógica de funcionamento em rede virtual, encontram-se dependentes do Espaço Cibernético.

Existem muitos indivíduos que encaram o Espaço Cibernético como uma área livre de controle, identificação ou punição. Essa aparente vulnerabilidade de espaço virtual, leva muitos a fazerem uso do mesmo para o cometimento de crimes, que vão desde a simples invasão de privacidade, à grandes.

Visando a proteção do Espaço Cibernético contra os ataques existentes surgiu a Segurança Cibernética, que virou um recorrente e importante assunto face ao momento tecnológico que vivemos.

2.9.2. Definição: Segurança cibernética

REFERÊNCIAS	**DEFINIÇÃO: Segurança Cibernética**
(Kemmerer,2003)	A segurança cibernética consiste principalmente em Métodos defensivos usados para detectar e impedir possíveis intrusos.
(Lewis, 2006)	A segurança cibernética envolve a proteção de redes de Computadores e das informações nelas contidas contra penetração E das informações nelas contidas contra penetração e danos ou interrupções maliciosas.
(Amoroso, 2006)	A segurança cibernética envolve a redução do risco de ataques maliciosos a softwares, computadores e redes. Isso inclui ferramentas usadas para detectar invasões, interromper vírus, bloquear acesso malicioso, impor autenticação, habilitar comunicações criptografadas e assim por diante.
(ITU, 2009)	A segurança cibernética é a colecção de ferramentas, políticas, conceitos de segurança, proteções de segurança, diretrizes, abordagens de gerenciamento de riscos, acções, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os activos da organização e do usuário.
(CNSS, 2010)	A segurança cibernética é a capacidade de proteger ou defender o uso do espaço cibernético contra ataques cibernéticos.
(Segurança Pública do Canadá)	A segurança cibernética é o conjunto de tecnologias, processos, práticas e medidas de resposta e mitigação destinadas a proteger redes, computadores, programas e dados de ataques, danos ou acesso não autorizado, de modo a garantir a confidencialidade,

	integridade e disponibilidade.
(Canongia & Mandarino, 2014)	A segurança cibernética é a arte de garantir a existência e a perenidade da sociedade da informação de uma nacção, garantindo e protegendo, no espaço cibernético, as suas informações, bens e infraestruturas críticas.
(Oxford University Press, 2014)	A segurança cibernética é o estado de protecção contra o uso criminoso ou não autorizado de dados electrônicos, ou as medidas tomadas para isso.
(DHS, 2014)	A segurança cibernética é a actividade ou processo, habilidade ou capacidade, ou estado pelo qual os sistemas de informação e comunicação e as informações neles contidas são protegidos e / ou defendidos contra danos, uso não autorizado ou modificação ou exploração.

Tabela 2:Definições da segurança cibernética
Fonte: elaborada pela autora

Segundo o site blog.starti.com.br/tudo-sobre-seguranca-cibernetica/ a segurança cibernética é a proteção de softwares, hardwares e dados de recursos conectados e armazenados na Internet. A partir de um indivíduo para uma grande empresa, todos se preocupam com a segurança de seus dados, softwares e informações online.

A protecção dos dados pessoais, financeiros, comerciais, continuidade operacional, integridade de dados e disponibilidade de serviços de software online caem no domínio da segurança cibernética. Regulando o acesso físico e controle de intrusão maliciosa, permitindo o acesso autorizado, criptografando as informações valiosas e salvaguardar a privacidade são os componentes da segurança cibernética.

Segurança Cibernética é basicamente o nome de práticas padrão que envolvem as pessoas, tecnologia e processos em uma organização, ou mesmo em um ambiente autônomo no qual os computadores com dados valiosos são conectados à internet.

2.9.3. Importância da segurança cibernética

Para STOPATTO (2009), a segurança cibernética é importante porque diversas organizações como: organizações governamentais, militares, corporativas, financeiras e médicas colectam, processam e armazenam imensas quantidades sem precedentes de dados em computadores e outros dispositivos. Uma parte significativa desses dados pode ser informação sensível, seja propriedade intelectual, dados financeiros, informações pessoais ou outros tipos de dados para os quais o acesso ou exposição não autorizados podem ter consequências negativas. As organizações transmitem dados confidenciais através de redes e para outros dispositivos no curso de seus negócios, e a segurança cibernética dedica-se a proteger essas informações.

2.9.4. Ameaças cibernéticas

Uma ameaça cibernética é um acto malicioso que tem como o principal objectivo danificar dados, roubar dados ou interromper a vida digital em geral.
As ameaças enfrentadas pela segurança cibernética são três: Guerra Cibernéticoa, Ataques Cibernéticos e o Terrorismo Cibernético. (GOMPERT, 2019).

2.9.4.1. Guerra cibernética (Ciberguerra)

Segundo GOMPERT (2019), a guerra cibernética é o foco dos conflitos cibernéticos, sendo equiparada às guerras históricas vivenciadas por diferentes países ao longo dos tempos, devido aos danos causados em ambos os casos.

De uma maneira geral, uma guerra cibernética se utiliza de ataques cibernéticos para atingir um alvo, mas a grande diferença está na origem e no destino desses ataques. Para ser categorizado como uma guerra cibernética, é preciso que um ataque envolve alvos, autores e ferramentas usadas que indiquem conflicto entre diferentes nações é possível investimento público nas acções, o que resultaria em ferramentas mais avançadas. (FINLAY, 2018).

2.9.4.2.Terrorismo cibernético (Ciberterrorismo)

Envolve uma acção pontual mas devastadora para as vítimas, podendo afectar diversas vítimas de maneira inesperada e ágil, algo como o que aconteceria em um acto de terrorismo tradicional. A partir do terrorismo cibernético também nasceu o terror cibernético, que é o trauma e medo constante de um possível novo ataque, uma consequência real e que faz muitas vítimas a todo instante, afectando inclusive países que não sofreram com o acto mas por estarem em conflitos internacionais estão mais susceptíveis a crer em falsas ameaças. (GOMPERT, 2019).

O terrorismo cibernético querer chamar a atenção e para isso podem preferir atacar sistemas públicos como governo, hospitais, programas de segurança pública, e qualquer outro alvo que possa fazer com que a população duvide da supremacia do próprio governo e com isso causa conflitos internos.

2.9.4.3. Ataque Cibernético

Os ataques cibernéticos, representam o que há de mais comum nos crimes digitais. É possível afirmar que toda guerra cibernética utiliza os ataques cibernéticos para acontecer, mas o mesmo não pode ser dito sobre o oposto, pois nem todo ataque tem a intenção de formalizar uma guerra. (AMOROSO, 2006).

Existem elementos em um ataque cibernético que nos ajudam a entender as diferenças: os alvos, os autores das ameaças por trás do ataque, bem como as ferramentas usadas. Dificilmente um ataque envolve apenas uma técnica.

Um ataque cibernético é obter acesso aos sistemas legítimos-servidores, computadores, rede, ou programas de software ilegalmente e estabelecendo controle sobre o legítimo sistema para a realização de actividades maliciosas, como furto de informações, armazenamento de dados, danos ao sistema e interrupção nas operações regulares das redes e sistemas. Um ataque cibernético é uma tentativa eletrônica deliberada e maliciosa de uma parte, que pode ser uma organização ou um indivíduo para violar o ambiente cibernético, roubando, excluindo ou danificando o valor das informações.

Esses objectivos podem ser alcançados quando qualquer um ou todos os sistemas sofrem violações de dados realizados por um hacker rompendo a tríade “CIA” (confidencialidade, integridade e disponibilidade), tornam um ataque cibernético bem sucedido.

2.10. Tipos de ataques cibernéticos na computação em nuvem

Actualmente a tecnologia de computação em nuvem é um paradigma da tecnologia de informação (TI) que fornece um pool compartilhado de recursos pela Internet. A nuvem possui várias vantagens e comparação com os modelos locais, ainda assim é susceptível a ataques cibernéticos.

Segundo o site https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/ o relatório da McAfee divulga que os dados armazenados em nuvem, colaboração SaaS e plataformas PaaS/IaaS são propensos a erros de configuração que podem expor dados a criminosos cibernéticos. A conclusão foi feita após a análise de bilhões de eventos em várias implantações em nuvem.

Os pesquisadores descobriram que os provedores de Nuvem apenas protegem a plataforma de nuvem, não os dados dos clientes. Assim, o ônus de proteger os dados recai completamente sobre os clientes que os utilizam, diz o relatório.

2.10.1. Principais vulnerabilidades de ataques cibernéticos na computação em nuvem

Uma vulnerabilidade e uma omissão, lacuna, fraqueza ou outra falha na postura de segurança da organização. Isso pode incluir um firewall configurado incorrectamente, um sistema operacional sem patch ou dados não criptografados. (BRYK, 2010)

As principais vulnerabilidades da computação em nuvem são:

- **Configurações incorrectas**

Os usuários são responsáveis pelas configurações, portanto, sua equipe de TI precisa priorizar o domínio das várias configurações e opções. Os recursos da nuvem são protegidos por uma série de definições de configurações que detalham quais usuários

podem acessar aplicativos e dados. Erros de configuração e omissões podem expor dados e permitir o uso indevido ou alteração desses dados.

- **Controle de acesso deficiente**

Os usuários não autorizados tiram proveito do controle de acesso deficiente para contornar métodos de autenticação ou autorização fracos ou ausentes.Por exemplo, os atacantes cibernéticos tiram vantagem de senhas fracas para advinhar credenciais.

- **Shadow IT**

Qualquer pessoa pode criar uma conta de nuvem pública, que pode ser usada para provisionar serviços e migrar cargas de trabalho e dados. Mas aqueles que não estão bem familiarizados com os padrões de segurança muitas vezes confundem as opções de segurança, deixando vulnerabilidades exploráveis na nuvem. Em muitos casos essas implementações de “TI sombra" podem nem mesmo reconhecer ou relatar explorações. Isso nega à empresa qualquer oportunidade de mitigar o problema até muito depois de o dano ter sido feito.

- **APIs inseguras**

Produtos de software não relacionados usam APIs para se comunicar e interoperar sem nenhum conhecimento do funcionamento interno do código um do outro. As APIs geralmente exigem e concedem acesso a dados corporativos confidenciais. Muitas APIs são tornadas públicas para ajudar a acelerar a adoção, permitindo que desenvolvedores externos e parceiros de negócios acessem os serviços e dados da organização.

- **Violações**

Na computação em nuvem, o provedor é responsável pela segurança da nuvem, enquanto o cliente é responsável pela segurança na nuvem.

- **Interrupções**

As infraestruturas de nuvem são vastas, mas ocorrem falhas e geralmente resultam em interrupções de nuvem amplamente divulgadas. Essas interrupções são causadas por

problemas de hardware e omissões de configuração, exactamente os mesmos problemas que afectam os data centers locais tradicionais.

2.10.2. Principais tipos de ataques cibernéticos na computação em nuvem

Segundo CUARELI (2016), que selecionou os artigos estudados de quatro bibliotecas digitais de trabalhos científicos: *IEEE Xplore, Science Direct, Google Scholar* e ACM Digital Library, chegou na conclusão que existem doze principais tipos de ataques cibernéticos na computação em nuvem. Onde esses principais tipos de ataques coincidiram com a pesquisa da BRYK(2010), que com a sua investigação verificou que também existem doze principais tipos de ataques mais frequentes no ambiente em nuvem cujo começaremos a citar:

2.10.2.1. Ataque de Injecção de Malware

Os ataques de injeção de malware são efectuados para assumir o controle das informações do usuário na nuvem, onde um invasor tenta injectar um serviço malicioso ou uma máquina virtual na nuvem. Neste tipo de ataque, os atacantes criam os seus próprios módulos de implementação de serviços (SaaS e PaaS) ou máquina virtual (IaaS) e tentam adicioná-los ao sistema da nuvem. Portanto, o invasor tem que se comportar de forma a torná-lo um serviço válido para o sistema em nuvem que é alguma nova instância de implementação de serviço entre as instâncias válidas. Se o invasor tiver sucesso neste, a nuvem redirecciona automaticamente as solicitações do usuário para a implementação do serviço malicioso, e o código do invasor começa a ser executado.

O cenário actual por trás do ataque de injeção de malware em nuvem é que um invasor transfere uma instância de serviço da vítima. Este ataque é o principal representante da exploração da superfície de ataque do serviço para a nuvem. O objectivo do ataque pode ser qualquer coisa em que o invasor esteja interessado, pode ser modificações de dados, roubo de dados ou até mesmo espionagem.

Existem duas formas mais comuns de ataques de injeção de malware na computação: ataques injecção de SQL e ataque de scripting.

- **Ataque de Injecção do SQL**

A injeção SQL, também conhecida como SQLI, é uma espécie de ataque que emprega código malicioso para manipular bancos de dados para acessar informações que não eram destinadas à exibição. Isso pode incluir vários itens, incluindo detalhes privados do cliente, listas de usuários ou dados confidenciais da empresa.

SQLI pode ter efeitos devastadores em um negócio. Um ataque SQLI bem-sucedido pode causar exclusão de tabelas inteiras, visualização não autorizada de listas de usuários e, em alguns casos, o invasor pode obter acesso administrativo a um banco de dados. Isso pode precisar considerar a perda de confiança do cliente no caso de informações pessoais como endereços, detalhes do cartão de crédito e números de telefone serem roubados.

Embora o SQLI possa ser usado para atacar qualquer banco de dados SQL, os culpados geralmente visam sites.

- **Ataque de Cross Site Scripting (XSS)**

O scripting cross-site (XSS) é uma espécie de violação de injecção onde o invasor envia scripts maliciosos para conteúdo de sites de outra forma respeitáveis. Isso acontece quando uma fonte duvidosa é autorizada a anexar seu próprio código em aplicativos da Web, e o código malicioso é empacotado com conteúdo dinâmico que é então enviado para o navegador da vítima.

O código malicioso geralmente é enviado na forma de peças do código Javascript execuctadas pelo navegador do alvo. As explorações podem incluir scripts execuctáveis maliciosos em muitas línguas, incluindo Flash, HTML, Java e Ajax. Os ataques XSS podem ser muito devastadores, no entanto, aliviar as vulnerabilidades que permitem esses ataques é relactivamente simples.Um ataque de cross site scripting bem-sucedido pode ter consequências devastadoras para a reputação de uma empresa online e seu relacionamento com seus clientes.

2.10.2.2. Ataques de Negação de Serviço (DoS)

Os ataques de negação de serviços ou em inglês Denial of Services DoS são projectados para sobrecarregar um sistema e tornar os serviços indisponíveis para os seus usuários. Esses ataques são muito perigosos para os sistemas de computação em nuvem, pois muitos usuários podem sofrer como resultado de inundar até mesmo um único servidor em nuvem.

Apesar de não causarem a perda ou roubo dos dados, os Ataques DoS são graves, pois deixa a rede indisponível quando um usuário precisa utilizá-la, ferindo uma das propriedades essenciais da SID, a qual garante que a informação estará disponível para o usuário (ISO 27002, 2005).

Em caso de carga alta de trabalho, os sistemas em nuvem começam a fornecer mais poder computacional, envolvendo mais máquinas virtuais e instâncias de serviço. Os hackers exploram activamente a vulnerabilidade dos serviços da computação em nuvem e enviam o bombardeio de solicitações e mensagens automatizadas para que esse servidor de nuvem em particular responda. O servidor de nuvem fica sobrecarregado e sufocado e para de funcionar normalmente. Em certos casos, o serviço para de funcionar devido ao servidor de nuvem sobrecarregado.

2.10.2.3. Ataques de Negação de Serviço Distribuída (DDoS)

Negação de Serviço Destruída ou em inglês Distributed Denial of Service (DDoS) é um tipo de Ataque DoS. Como o Ataque DoS, neste tipo de ataque cibernético, os servidores ficam congestionados ou sobrecarregados com o tráfego malicioso para evitar que os usuários legítimos acessem suas contas ou serviços online legítimos.

Este tipo de ataque se aproveita de duas falhas em serviços de internet, a falsificação da origem (IP Spoofing) e servidores DNS recursivos abertos, pois menos botnets são necessários para gerar grandes volumes de tráfego de ataque, devido às técnicas de reflexão e ampliação (DUNN, 2013).

No entanto, a principal diferença entre ataques DoS e DDoS é que o Ataque DoS é direcionado de uma origem específica de tráfego para o servidor vítima, enquanto no caso

de ataque DDoS, múltiplas fontes de tráfego são usadas para atacar o servidor vítima (ao mesmo tempo). No ambiente de nuvem os ataques DDoS podem ser ainda mais perigosos se os hackers usarem máquinas zumbis para atacar um grande número de sistemas.

2.10.2.4. Ataque de Canal Lateral

Estes tipos de ataques são organizados por hackers quando eles colocam uma máquina virtual maliciosa no mesmo host que a máquina virtual de destino. Durante este tipo de ataque, os hackers visam as implementações de sistemas de algoritmos criptográficos.

2.10.2.5. Ataques Man-In-The-Middle (MITM)

Este ataque MITC se baseia em serviços comuns de sincronização de documentos como o Drive, Dropbox, OneDrive, etc. Sua infraestrutura é baseada em C&C, compreendendo acesso remoto e exfiltração de dados.

O ataque MITM consiste basicamente em o atacante infiltrar na comunicação entre duas partes, interceptar os dados, manipulá-los e retransmiti-los sem que nenhuma das partes perceba (JORGE, 2011).

O ataque vulnerável não exige que nenhum programa malicioso específico ou exploração seja utilizado na fase inicial de infecção**,** portanto, dificultando a prevenção. Além de tudo isso, o uso dos protocolos de sincronização torna intensamente difícil diferenciar o tráfego malicioso e o tráfego normal. Em caso de comprometimento de contas, a descoberta e análise de evidências não é de todo simples. É assim porque existem pelo menos pequenas evidências (que estão completamente escondidas) da incidência em qualquer um dos ataques, principalmente nos pontos finais. O invasor cibernético ganha acesso na conta da vítima no ataque man in the Cloud e que também sem compor as credenciais da conta da vítima. Para um investigador forense, é difícil determinar o tipo de perfil comprometido. Além disso, a recuperação da conta após este ataque do MITC nem sempre é viável (BRYK, 2010).

2.10.2.6. Ataque de Phishing

O phishing é mais relevante quando o aplicativo em questão é exposto à Internet, típico de aplicativos em nuvem pública. Embora os aplicativos privados hospedados em nuvem geralmente tenham a segurança adicional de uma VPN, eles também são suscetíveis a um determinado ataque de phishing. Conhecendo a URL do serviço de nuvem, um invasor pode realizar ataques de phishing direccionados aos funcionários e se infiltrar no perímetro da organização.

Ataques genéricos de phishing são análogos a uma campanha de e-mail marketing para a qual bancos de dados de e-mail altamente personalizados estão disponíveis no mercado. Predominantemente utilizados para vendas e marketing, esses bancos de dados também podem ser usados indevidamente para phishing. O phishing de lança é muito mais selectivo, e envolve um bom grau de pesquisa, usando conteúdo altamente direccionado relevante para o grupo alvo específico.

Ataques de phishing podem resultar em um pouso de dados confidenciais nas mãos de um concorrente, com consequências devastadoras para o negócio. Os serviços em nuvem que usam apenas uma senha para autenticação são especialmente suscetíveis a isso. Aqui estão alguns processos e controles que você pode colocar em prática para se proteger contra ataques de phishing na nuvem.

2.10.2.7. Ataques de Embrulho

Os ataques de embrulho fazem uso do embrulho de assinatura extensible Markup Language (ou reescrita XML) para explorar uma fraqueza quando os servidores web validam solicitações assinadas. Esse tipo de ataque cibernético é realizado durante a tradução de mensagens SOAP (Simple Object Access Protocol, protocolo de acesso a objetos simples) entre um usuário legítimo e o servidor web.

O invasor cibernético incorpora um elemento falso (o invólucro) na estrutura da mensagem, move o corpo de mensagem original sob o invólucro e substitui o conteúdo da mensagem

por código malicioso. A partir daqui ele é então enviado para então para o servidor hospedado na infraestrutura de computação em nuvem. O servidor será então enganado para autorizar a mensagem que foi realmente alterada. Como resultado, o invasor cibernético é então capaz de obter acesso não autorizado a recursos protegidos. A partir daqui, as operações ilegais podem então prosseguir.

Como os usuários de nuvem normalmente solicitam serviços de provedores de serviços de computação em nuvem através de um navegador da Web, ataques de embrulho também podem causar danos aos sistemas de nuvem. A Nuvem de Computação Elástica (EC2) da Amazon foi descoberta como vulnerável a ataques de embrulho.

2.10.2.8. Ataques de Força Bruta

O Ataque da Força Bruta é um hack criptográfico. Também conhecido como Pesquisa Exaustiva, esse tipo de hack envolve tentar várias combinações para uma senha até que uma delas te deixe entrar. O hacker também pode tentar advinhar a chave derivada da senha usando uma função de derivação chave. Isso é conhecido como Exaustivo Busca de Chaves.

Ataques de força bruta podem funcionar para uma simples e curta quebra de senha, mas pode não ser uma escolha ideal para senhas complicadas e mais longas. Levará muito tempo para descobrir todas as combinações para uma senha mais longa.

2.10.2.9. Ataques Internos

Nesse tipo de ataque, alguém que abusa maliciosamente e intencionalmente de credenciais legítimas, normalmente para roubar informações para incentivos financeiros ou pessoais. Por exemplo, um indivíduo que guarda rancor contra um ex-empregador, ou um empregado oportunista que vende informações secretas a um concorrente. Os ataques internos têm uma vantagem sobre outros atacantes porque eles estão familiarizados com as políticas de segurança e procedimentos de uma organização, bem como suas vulnerabilidades.

2.10.2.10. Ameaças Persistentes Avançadas (APTs)

As ameaças persistentes avançadas (APTs) são ataques que permitem que os hackers roubem continuamente dados confidenciais armazenados na nuvem ou explorem serviços em nuvem sem que sejam notados pelos usuários legítimos. A duração desses ataques permite que os hackers se adaptem às medidas de segurança contra eles. Uma vez que o acesso não autorizado é estabelecido, os hackers podem se mover pelas redes do data center e usar o tráfego da rede para suas actividades maliciosas.

2.10.3. Principais técnicas de prevenção de ataques cibernéticos na computação em nuvem

Segundo BRYK (2010), a natureza dinâmica dos serviços em nuvem quebra o modelo de segurança tradicional usado para software no local. É óbvio que um provedor de serviços em nuvem é incapaz de garantir a segurança total na nuvem. Parte da responsabilidade também é dos usuários de nuvem. Embora a melhor maneira de proteger os dados dos usuários na nuvem seja fornecer uma abordagem de segurança em camadas, os provedores de serviços em nuvem devem implementar as melhores práticas do setor para garantir o nível máximo de segurança na nuvem do seu lado. Aqui estão sete dicas sobre como os desenvolvedores de nuvem podem garantir a segurança de suas soluções baseadas em nuvem.

As principais técnicas para prevenir os ataques cibernéticos na computação em nuvem são:

2.10.3.1. Melhorar as políticas de segurança

Ao fornecer serviços em nuvem, os fornecedores de software devem limitar o escopo de sua responsabilidade de proteger os dados e operações do usuário na nuvem em suas políticas de segurança. Informe seus clientes sobre o que você faz para garantir a segurança na nuvem, bem como quais medidas de segurança eles precisam tomar ao seu lado.

2.10.3.2. Utilização de autenticação forte

Roubar senhas é a maneira mais comum de acessar os dados e serviços dos usuários na nuvem. Assim, os desenvolvedores de nuvem devem implementar forte autenticação e

gerenciamento de identidade. Estabeleça autenticação multifatorial. Existem várias ferramentas que requerem senhas estáticas e senhas dinâmicas. Este último confirma as credenciais de um usuário fornecendo uma senha única em um telefone celular ou usando esquemas biométricos ou tokens de hardware.

2.10.3.3. Implementação da gestão de acesso

Para aumentar a segurança dos serviços, os desenvolvedores de nuvem devem permitir que os usuários de nuvem atribuam permissões baseadas em papéis a diferentes administradores para que os usuários só tenham os recursos atribuídos a eles. Além disso, a orquestração em nuvem deve permitir que usuários privilegiados estabeleçam o escopo das permissões de outros usuários de acordo com suas funções dentro da empresa.

2.10.3.4. Protecção dos dados

Os dados no ambiente de nuvem precisam ser criptografados em todas as fases de sua transferência e armazenamento:

- na fonte (do lado do usuário)
- em trânsito (durante sua transferência do usuário para o servidor em nuvem)
- em repouso (quando armazenado no banco de dados de nuvem)

Os dados precisam ser criptografados antes mesmo de ir para a nuvem. As modernas tecnologias de criptografia de dados e tokenização são uma defesa eficaz contra o sequestro de contas. Além disso, é importante provar criptografia de ponta a ponta para proteger dados em trânsito contra ataques man-in-the-middle. O uso de algoritmos de criptografia fortes que podem efectivamente desviar ataques cibernéticos.

2.10.3.5. Detecção de invasões

É o processo de monitoramento e análise de eventos que ocorrem em um sistema para

Detectar sinais de ataques ou tentativas, com intenção de comprometer a confidencialidade, integridade e disponibilidade.

2.10.3.6. Garantir APIs e acessos

Os desenvolvedores em nuvem devem ter certeza de que os clientes podem acessar o aplicativo apenas através de APIs seguras. Isso pode exigir limitar a gama de endereços IP ou fornecer acesso apenas através de redes corporativas ou VPNs. No entanto, essa abordagem pode ser difícil de implementar para aplicações públicas. Assim, você pode implementar protecção de segurança através de uma API usando scripts, modelos e receitas especiais. Você pode até ir mais longe e construir protecção de segurança em sua API.

2.10.3.7. Protecção de serviços em nuvem

Limitar o acesso a serviços em nuvem é necessário para evitar que os invasores obtenham acesso não autorizado às operações e dados de um usuário por meio de fraquezas nos serviços em nuvem. Ao projectar a arquitectura de serviços em nuvem, minimize as permissões do manipulador de eventos apenas às necessárias para executar operações específicas. Além disso, você pode restringir as decisões de segurança apenas aos serviços em nuvem que são confiáveis aos usuários para gerenciar sua segurança de dados.

2.10.3.8. Utilização da nuvem privada

Você pode ser tentado a ir com uma nuvem pública para reduzir custos, mas esses tipos de nuvens são compostas de vulnerabilidades e desafios de segurança. Nuvens privadas custam mais, mas têm menos pontos de entrada e medidas de segurança mais rigorosas. Além disso, os provedores privados de nuvem estão em melhor posição para monitorar sua conta, permitindo que eles desviem preventivamente os ataques e minimizem seu impacto.

3. CAPÍTULO III – METODOLOGIA

O presente trabalho tem como objectivo de determinar as principais técnicas para prevenir os ataques cibernéticos no ambiente de nuvem e um conjunto de técnicas que permitem prevenir os ataques cibernéticos na computação em nuvem. Para a realização do presente trabalho, foi usada uma metodologia, nomeadamente:

3.1. Tipo de Estudo e Desenho de Investigação

Nesta pesquisa fizemos um estudo exploratório.Segundo GIL (2002) estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado.

O presente trabalho basear-se-á na abordagem de pesquisa quantitativa. Essa técnica tende a salientar os aspectos dinâmicos, holísticos e individuais da experiência humana, para apreender a totalidade no contexto daqueles que vivenciam o fenômeno, (SILVEIRA e CÓRDOVA, 2009).

A pesquisa quantitativa tem como premissa de aproximar a teoria dos dados da pesquisa, utilizando para isso a análise dos fenômenos através do modo como estes são descritos ou interpretados (TEIXEIRA, 2005, p. 137).

Nesta pesquisa, o método quantitativo foi utilizado na análise dos resultados das questões do questionário, sendo então apresentado o percentual das respostas.

3.2. População e Amostra

População é um conjunto definido de elementos que possuem determinadas características, enquanto que, a amostra é um subconjunto da população, por meio do qual se estimam as características dessa população (GIL, 1999).

Para a realização do trabalho, constituiu a população, as instituições que possuem a tecnologia de computação em nuvem. Sendo que a amostra foi a instituição Vodacom Moçambique.

3.3. Técnicas e Instrumentos de Recolha de Dados

Para o desenvolvimento do presente trabalho, foram usados quatro métodos de investigação:

Questionário

Foi realizado um questionário de pesquisa, com algumas perguntas necessárias para esclarecer melhor o tema em questão, visando esclarecer:

- Os principais ataques cibernéticos sofridos;
- As principais técnicas para prevenir de Ataques Cibernéticos no seu ambiente de Computação em Nuvem;

Segundo LAKATOS (2007:197), questionário é um instrumento de colecta de dados, constituído por uma série ordenada de perguntas, que devem ser respondidas por escrito e sem a presença do entrevistador.

Para elaboração, foi utilizado o software Google Forms, da Google, que possibilita a criação de formulários de pesquisa. Todas as questões são obrigatórias, e não há perguntas de múltipla escolha.

Entrevista Telefônica

Foi realizada uma entrevista telefônica a fim de obter respostas sobre o formulário e esclarecimento da técnica proposta.

Internet

As consultas na web sites das plataformas dos provedores de nuvem, para avaliar as suas políticas de segurança e privacidade a fim de compreender como eles fornecem uma boa segurança para os seus usuários.

Revisão Bibliográfica

A revisão bibliográfica consistiu na pesquisa dos seguintes materiais: livros, monografias, artigos periódicos e actualmente com material disponibilizado na internet, websites.

Segundo (VERGARA, 2010, p. 54; GIL, 2002, p. 44; ROESCH, 1999 p. 107), a revisão bibliográfica consiste na seleção e análise de todo material já elaborado relevante ao tema da pesquisa, incluindo toda bibliografia já publicada, seja baseada na literatura, seja por outros meios impressos, orais ou audiovisuais.

3.4.Análise e Interpretação de Dados

Para a análise e interpretação dos resultados utilizou-se o software Microsoft Excel para confeccionar os gráficos apresentados nos resultados, decorrentes das análises estatísticas.

4. CAPÍTULO IV – RESULTADOS

4.1.Objecto de estudo

A pesquisa foi realizada tendo como objecto de estudo a instituição de serviços de telecomunicações Vodacom Moçambique.

a) Vantagens da computação em nuvem sobre o ponto de vista da Vodacom Moçambique

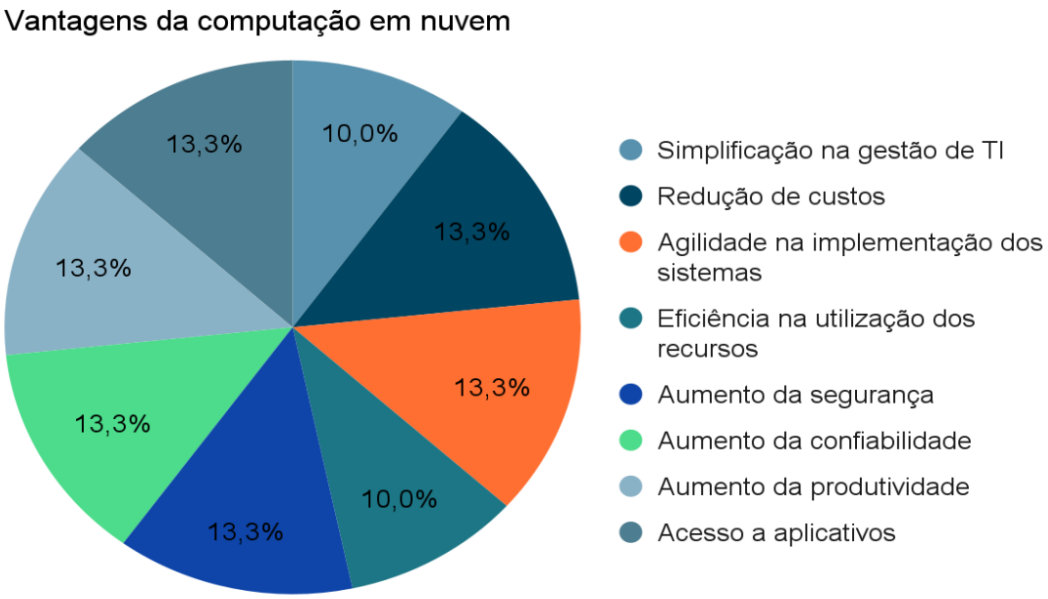

Figura 6: Gráfico das vantagens da computação em nuvem.
Fonte: elaborado pela autora.

De acordo com a figura 6, é possível verificar que numa percentagem de 100%, das principais vantagens da computação em nuvem apresentadas na tese, a instituição Vodacom Moçambique destacou com uma percentagem de 13,3%, as seguintes: redução de custos, a agilidade na implantação dos sistemas, a eficiência na utilização dos recursos, o aumento da confiabilidade e o aumento da produtividade. Onde com uma percentagem de 10% verificou-se: a simplificação na gestão de TI e o acesso a aplicativo.

b) Desvantagens da computação em nuvem

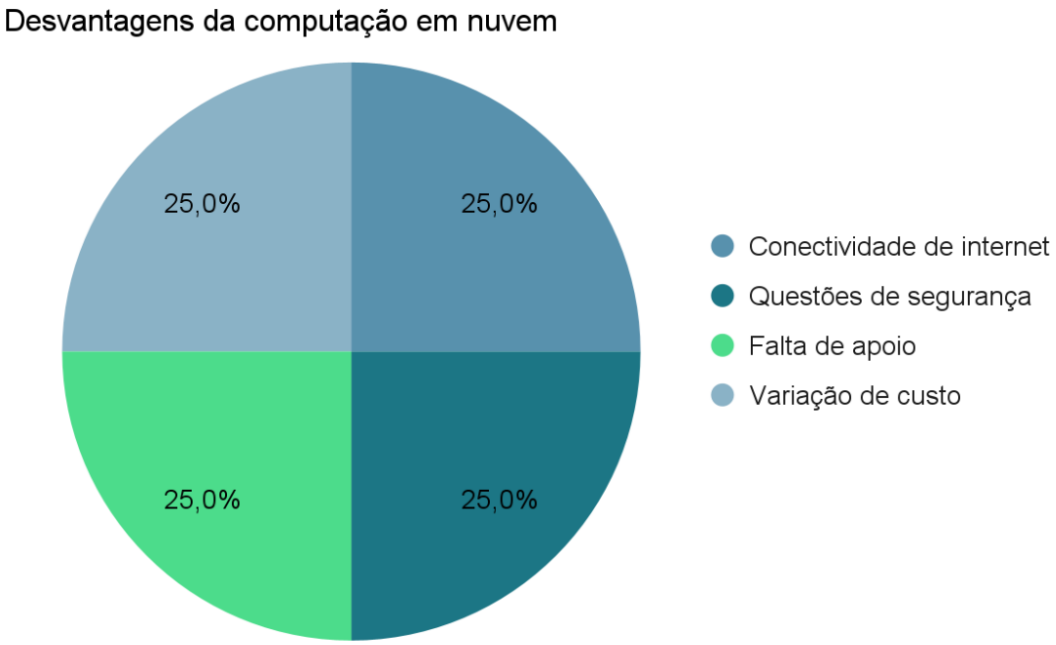

Figura 7: Gráfico das desvantagens da computação em nuvem.
Fonte: elaborado pela autora.

Por meio da figura 7, é visível que numa percentagem de 100% das principais desvantagens da computação em nuvem citados na tese, a instituição Vodacom Moçambique, verificou quatro principais desvantagens com a sua migração para a nuvem, das quais as quatros tiveram a mesma percentagem 25% de dificuldade.

c) Características da computação em nuvem

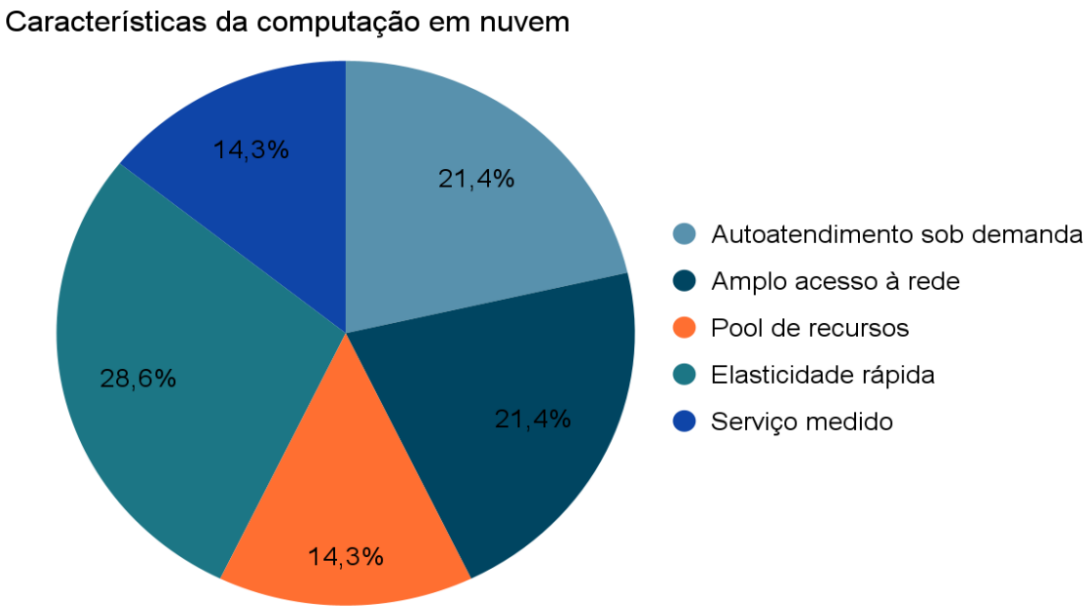

Figura 8:Gráfico das características da computação em nuvem.
Fonte: elaborado pela autora.

Conforme disposto no figura 8, é possível interpretar que das principais características da computação em nuvem, numa percentagem 100%, a instituição avalia como melhoria para seus serviços a (elasticidade rápida) que teve uma percentagem 28,6% comparativamente com as outras características, que em seguida destacaram-se com 21,4% o (autoatendimento sob demanda e o amplo acesso à rede) e por fim com 14,3% o (serviço medido), porém todas características trariam melhorias para as empresas e são consideradas muito importantes.

d) Vulnerabilidades da computação em nuvem

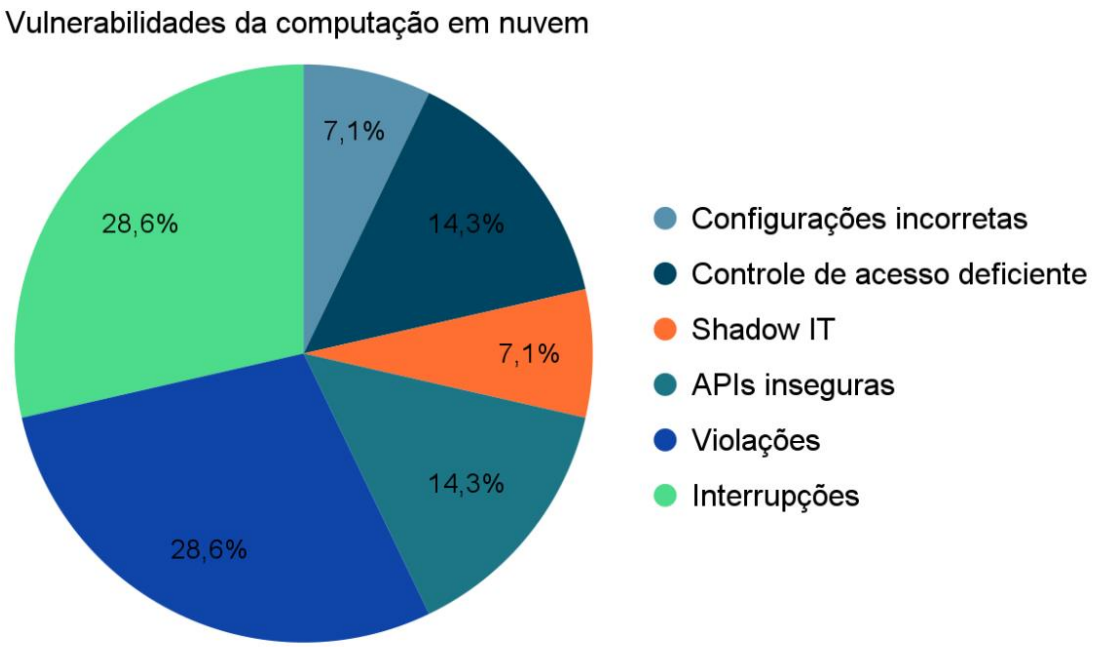

Figura 9: Gráfico das vulnerabilidades da computação em nuvem
Fonte: elaborado pela autora.

Por meio da figura 9, é ilustrado que das principais vulnerabilidades da computação em nuvem a Vodacom Moçambique numa percentagem de 100%, tem como destaque duas que tiveram uma percentagem de 28,6% de ocorrência, das quais são (as interrupções e as violações). Onde em seguida com 14.3% de ocorrência o (controle de acesso deficiente e as APIs inseguras) e por fim com uma percentagem 7,1% de ocorrência as (configurações incorretas e o shadow IT) que são vulnerabilidades que devem ser consideradas.

e) Ataques cibernéticos

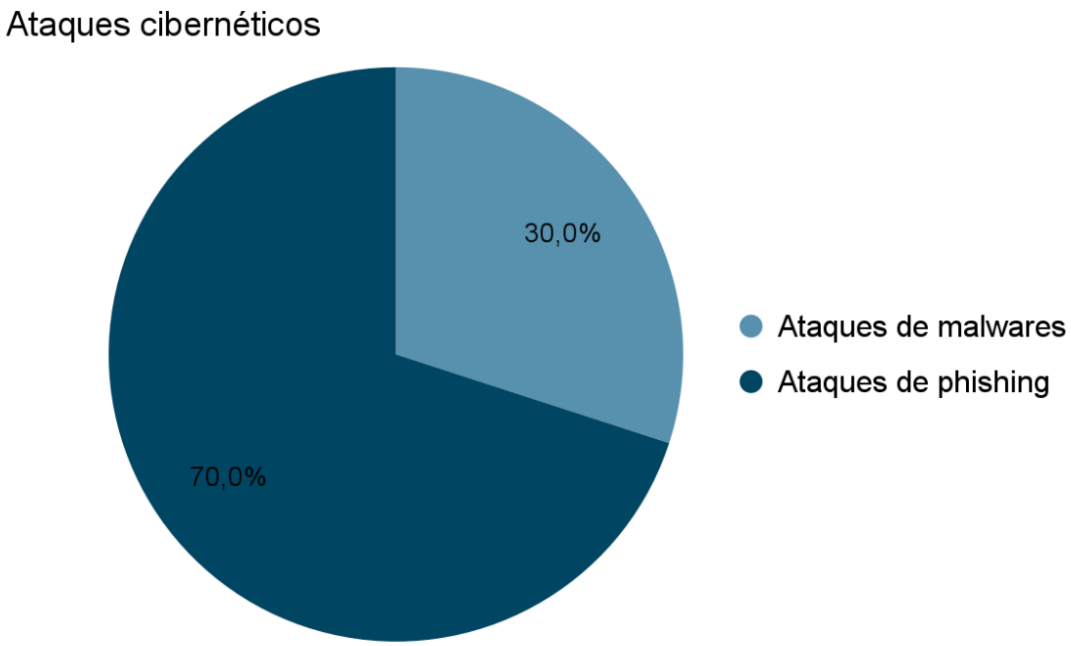

Figura 10: Gráfico dos ataques cibernéticos.
Fonte: elaborado pela autora.

Conforme disposto na figura 10, é possível interpretar que a instituição Vodacom Moçambique já sofreu ataques cibernéticos, e dos principais tipos de ataques cibernéticos abordados na tese numa percentagem 100%, a instituição já sofreu dois tipos de ataques em destaque o ataque de phishing com uma ocorrência de 70% comparativamente com o outro, de seguida com uma ocorrência de 30% os ataques de ataques malwares.

f) Segurança cibernética na computação em nuvem

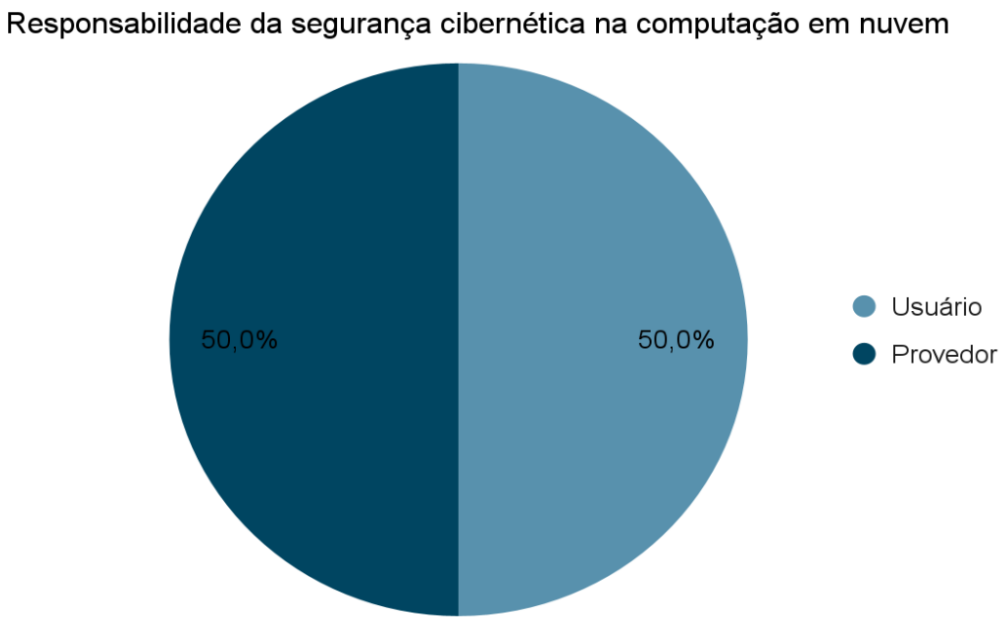

Figura 11: Gráfico da responsabilidade para garantir a segurança cibernética na computação em nuvem.
Fonte: elaborado pela autora.

Conforme a figura 11, nota-se que a instituição acredita que tanto os usuários quanto os provedores são responsáveis por garantir a segurança cibernética na computação em nuvem, numa percentagem de 100%, verificou-se que a instituição Vodacom Moçambique concorda que tanto o usuário, quanto o provedor, ambos têm a responsabilidade compartilhada com a percentagem de 50%.

g) Prevenção de ataques cibernéticos na computação em nuvem

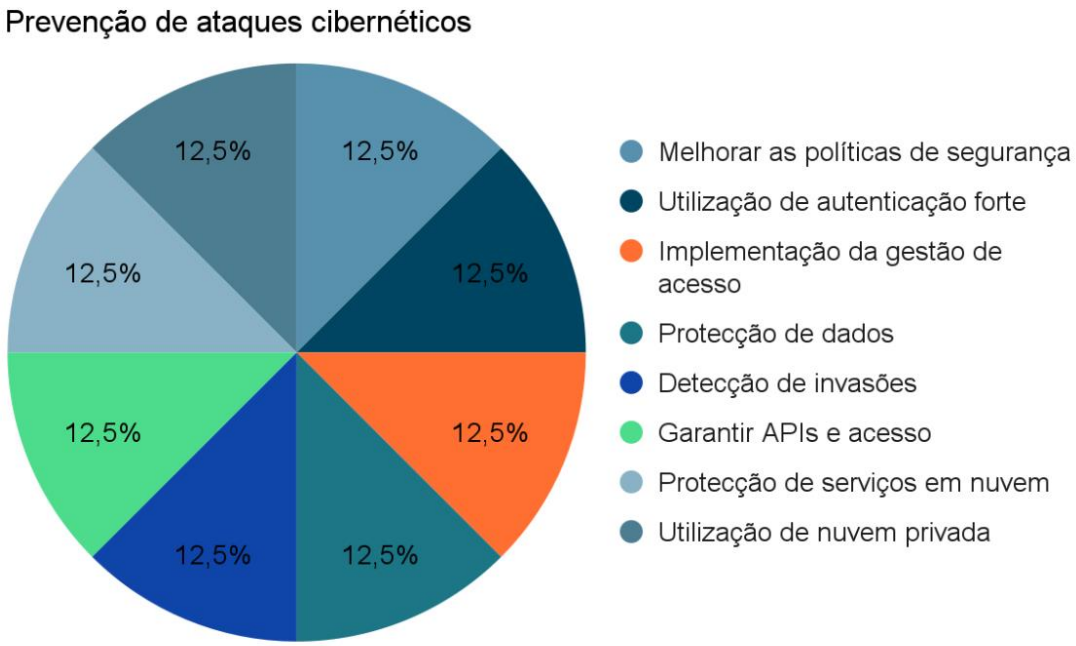

Figura 12: Gráfico das técnicas de prevenção de ataques cibernéticos.
Fonte: elaborado pela autora

De acordo com a figura 12, é notório que a instituição utiliza todas técnicas para prevenção de ataques cibernéticos, com a mesma atenção.

5. CAPÍTULO V – DISCUSSÃO

5.1.Caracterização da Vodacom Moçambique

A Vodacom Moçambique é uma empresa moçambicana que iniciou sua operação em Moçambique em dezembro de 2003 e seu principal objetivo é oferecer uma rede móvel confiável e de alta qualidade e através de novas tecnologias de comunicação trazer tudo o que é bom para Moçambique. Os acionistas da Vodacom Moçambique incluem a Vodacom International Limited (85%) e parceiros locais como EMOTEL Moçambique Telecommunications Company, SARL (5%), Intelec Holdings Limited (5%) e Whatana Investments Limited (5%). Determinada a oferecer o melhor serviço e focada em questões sociais, a Vodacom desenvolveu importantes ações de responsabilidade social em diversas áreas, principalmente na reabilitação e construção de escolas, instalação de salas de informática e distribuição de livros didáticos e material escolar em várias escolas do país. A Vodacom continua introduzindo novas formas de levar o Tudo Bom a mais pessoas no país.

5.1.1. Política da segurança cibernética na computação em nuvem adotada pela vodacom moçambique

A Vodacom Moçambique possui internamente uma Política de Segurança Cibernética no seu ambiente em nuvem, que foi criada em 2003 e aprovada pelos responsáveis administrativos.

Entretanto, a Política possui orientações a respeito de Segurança Lógica e Segurança Física, com o objetivo de conscientizar os colaboradores a adotarem melhores práticas para a proteção dos activos de informação para além de se prevenir de agentes mal-intencionados.

Em seu regulamento, também estão previstas sanções para os usuários que descumprirem as normas. É um passo muito importante para conscientizá-los sobre as responsabilidades da utilização dos recursos de TI, ou seja, que devem aplicá-los apenas para o trabalho e benefício da organização, pois as imprudências ou negligências evidenciadas resultarão em repreensões.

Contudo, a Política determina que os incidentes ocorridos no ambiente em nuvem envolvendo a segurança cibernética deve ser direcionado ao sector responsável, para que este possa divulgá-los, de modo que sirvam de alerta aos demais colaboradores.

5.2. Descrição e análise dos dados colectados

A empresa Vodacom Moçambique tem como o provedor dos seus serviços de computação em nuvem a Amazon Web Services (AWS), e possui todos modelos de serviço em nuvem: a Infraestrutura como Serviço (IaaS), o Software como Serviço (SaaS) e a Plataforma como Serviço (PaaS).

A empresa possui o modelo de implantação da nuvem privada, que de acordo com a pesquisa da Capgemini (2014), a nuvem privada também é a mais aderente entre os modelos de implantação da computação em nuvem, indo de acordo com os resultados obtidos. Esses resultados mostram a preocupação com a segurança dos dados das empresas, pois com a nuvem privada, ainda é possível obter um maior controle de segurança, se comparado com as demais implementações.

Contudo a Vodacom Moçambique acredita que a computação em nuvem é mais segura comparando com a computação normal, pois puderam verificar essa segurança ao migrarem para a nuvem.

A instituição não acredita que os dados armazenados na nuvem são vulneráveis a ataques cibernéticos, porém a mesma afirma que ao migrar para a nuvem já sofreu alguns ataques cibernéticos.

Entretanto, uma das principais formas que a instituição utiliza para prevenir os seus dados, as suas informações e os seus arquivos no seu ambiente em nuvem é implementar as boas práticas de políticas de segurança, para garantir a segurança cibernética em seu ambiente de nuvem.

Contudo, ela costuma fazer testes cibernéticos frequentemente, de seis em seis meses para poder prevenir-se de ataques cibernéticos.

Aa instituição Vodacom Moçambique verificou em destaque seis vantagens ao migrarem para a nuvem que foram: redução de custos, a agilidade na implantação dos sistemas, a

eficiência na utilização dos recursos, o aumento da confiabilidade e o aumento da produtividade. E quanto as desvantagens da computação em nuvem verificou quatro ao migrarem para a nuvem, que foram: Conectividade de internet, questões de segurança, falta de apoio e a variação de custos,

Contudo, verificou-se que das principais características da computação em nuvem, a instituição Vodacom Moçambique verificou no seu ambiente em nuvem a elasticidade rápida como melhoria para os seus serviços.

Entretanto, das principais vulnerabilidades da computação em nuvem, a instituição verificou em destaque no seu ambiente em nuvem as violações.

Porém, dos principais tipos de ataques cibernéticos na computação em nuvem, a instituição Vodacom Moçambique verificou com mais frequência no seu ambiente em nuvem os ataques de phishing. Onde a mesma afirma que tanto o provedor quanto os usuários ambos são responsáveis.

Perante a prevenção de ataques cibernéticos na computação em nuvem a instituição verificou com a mesma percentagem todas as medidas exposta na figura 12.

Diante deste cenário realizamos uma pergunta aberta que foi para podermos compreender a principal técnica para prevenir a instituição de ataques cibernéticos e garantir uma boa segurança cibernética no seu ambiente em nuvem, pudemos observar que a instituição utiliza boas práticas de implementação de segurança cibernética. O principal objectivo dessas boas práticas é de auxiliar a instituição para que a mesma possa ter ideia do que pode ser feito para prevenir problemas decorrentes do mau uso da tecnologia ou mesmo auxiliar na proteção contra os ataques cibernéticos. As principais práticas da segurança cibernética que a vodacom Moçambique utiliza são:

a) Criação de um regulamento interno da segurança da informação

Onde a Vodacom Moçambique define quais são os direitos e deveres de seus funcionários, suas responsabilidades, os limites de acesso às informações da empresa, a possibilidade de uso dessas informações dentro e fora da empresa, a confidencialidade das informações

obtidas e as penalidades caso as regras sejam desobedecidas, e ainda os mecanismos de controle e monitoramento do aparato tecnológico da empresa;

b) Estabelecer políticas de privacidade

Dirigida para o pessoal da instituição, para poder compreender qual é a expectativa de privacidade do indivíduo perante a empresa, bem como as formas de monitoramento dos acessos e comunicações do usuário, sendo funcionários ou não, quando os mesmos fazem o uso do aparato tecnológico fornecido pela empresa, e inclusive, informando sobre videovigilância, se houver, e os limites da sua utilização pela empresa, caso necessário;

c) Criar termos de uso

Para poder definir as regras de utilização da infraestrutura tecnológica da empresa, incluindo seus sistemas internos, e-mails ou até mesmo contas para armazenamento de documentos na nuvem, bem como quaisquer equipamentos eletrônicos fornecidos pela própria aos usuários (funcionários ou não), tais como tablets, celulares e computadores.

d) Classificar as informações de acordo com o grau de confidencialidade

Para poder proteger as informações e definir quem pode acessar o que nos sistemas da empresa.

e) Estabelecer a melhor maneira para armazenar as informações e arquivos

Para poderem criar, se possível, um único padrão e poderem definir regras claras sobre como usar e manter essas informações e arquivos, e até mesmo seu descarte.

f) Criar regras sobre o uso de senhas

Para poderem acessar ambientes seguros das empresas, informando sobre possível monitoramento de atividades, bem como regras sobre cancelamento de contas e proibição de acesso aos sistemas e aparato tecnológico da empresa, após extinção da relação de trabalho;

Garantir que a segurança cibernética não seja um processo único. É uma atividade contínua que deve ser mantida e seguida por cada instituição. A conscientização cibernética ajuda as pessoas a tomar decisões precisas ao confrontar uma situação adversa, o que, em última análise, fortalece a defesa cibernética da empresa. Sempre se envolve em um comportamento on-line seguro implementando práticas de segurança recomendadas.

Todavia, existe a questão de responsabilidade compartilhada onde precisa-se saber qual é a responsabilidade do provedor e qual é a responsabilidade do usuário.

5.2.1. Proposta de técnica para a instituição Vodacom Moçambique utilizar na prevenção de ataques cibernéticos no ambiente em nuvem

Perante os dados analisados percebeu-se que o ataque que ocorreu com mais frequência na instituição Vodacom Moçambique foi o ataque de phishing, cujo mesmos afirmam que foi decorrente de funcionários da instituição que violaram umas das regras da sua política de segurança cibernética, onde os mesmos passaram informações para que os hackers pudessem invadir.

Todavia, foi possível verificar que das técnicas abordadas no trabalho, a instituição Vodacom Moçambique utiliza todas para prevenir-se dos ataques cibernéticos, porém mesmo assim continuam sofrendo esses ataques.

Entretanto sugere-se a implantação de um hacker digital benéfico utilizando a inteligência artificial, uma vez que a inteligência artificial (IA) refere-se à simulação da inteligência humana em máquinas que são programadas para pensar como humanos e imitar suas acções. O termo também pode ser aplicado a qualquer máquina que exaúde características associadas a uma mente humana, como aprendizado e resolução de problemas.

Contudo, a principal característica da inteligência artificial é sua capacidade de racionalizar e tomar acções que tenham a melhor chance de alcançar um objetivo específico.

Diante deste cenário a Vodacom Moçambique poderia criar um hacker digital programado utilizando tecnologia da inteligência artificial para fazer testes de penetração à favor da instituição, onde o mesmo teria a missão de invadir os seus sistemas, e caso conseguisse, a

equipe de segurança cibernética da instituição poderá procurar formas de se defender dos demais atacantes cibernéticos. Entretanto, podem educar o hacker para limitar o acesso dos funcionários no que tange a localização dos mesmos, e também criar um log de todas tentativas que possam ser feitas pelos atacantes cibernéticos e fazer delas estratégias para ensinar o hacker digital baseado em inteligência artificial.

Essa proposta, foi feita ao departamento de segurança cibernética da instituição Vodacom Moçambique, onde a mesma foi avaliada e posteriormente respondida, cujo disseram que não poderiam afirmar se daria certo, pois seria necessário se debater melhor acerca do assunto para compreender como isso poderá ser feito e implementado para se saber se será viável ou não.

6. CAPÍTULO VI– CONCLUSÕES E RECOMENDAÇÕES

6.1. Conclusões

O objectivo desta pesquisa, foi de propor a Vodacom Moçambique uma técnica de prevenção dos ataques cibernéticos na computação em nuvem.

Pode-se afirmar que o objectivo foi atingido, por meio dos objectivos específicos estabelecidos e da metodologia aplicada.

Para tal objectivo realizou-se uma pesquisa bibliográfica de várias fontes, a elaboração deste trabalho pretende responder esse problema, desenvolvendo-se e focando-se na análise de uma determinada instituição.

Primeiramente, foram esclarecidos os conceitos básicos na investigação, que foram a computação em nuvem e a segurança cibernética, onde nosso foco esteve virado para a segurança cibernética na computação em nuvem, abordou-se os objectivos desta tecnologia, a importância, as características, as vantagens e desvantagens da mesma.

Referente às características e as vantagens da computação em nuvem, conclui-se, através das pesquisas realizadas, que elas trazem melhorias significativas, com destaque para a redução de custos, a agilidade na implantação dos sistemas, a eficiência na utilização dos recursos, o aumento da confiabilidade, aumento da produtividade e a elasticidade rápida, respectivamente, os quais obtiveram maior percentagem na pesquisa quantitativa. Através desses aspectos as empresas também demonstram interesse pelo paradigma de computação em nuvem .

Contudo referente as desvantagens da computação em nuvem destacou-se quatro principais com a mesma percentagem de ocorrência, que foram: conectividade de internet, falta de apoio, questões de segurança e variação de custos.

Desta forma, analisou-se os principais tipos de ataques cibernéticos na computação em nuvem, onde primeiramente foi necessário listar as principais vulnerabilidades nesse ambiente que abrem as portas para esses ataques, que através de pesquisas bibliográficas foi possível listar essas vulnerabilidades e efectuar-se uma comparação com a instituição

pesquisada para conseguir compreender quais vulnerabilidades essa instituição já verificou, entretanto depois analisou-se os principais ataques cibernéticos decorrentes dessas vulnerabilidades nessa instituição.

Todavia analisei as principais técnicas para mitigação desses ataques, onde também realizou-se uma pesquisa bibliográfica de diversas fontes e foram constatadas algumas técnicas, que com as mesmas realizou-se uma análise comparativa para compreender quais as mais utilizadas para prevenir-se dos atacantes cibernéticos e constatou-se a utilização de boas práticas de implementação de políticas de segurança, onde as instituições criam normas e procedimentos nas suas organizações para poderem lidar com esses desafios.

Após a realização deste trabalho, conclui-se que: a implementação da tecnologia de computação em nuvem é bastante atrativa, por várias vantagens que a mesma pode oferecer para as organizações e que são descritos ao longo do trabalho, porém apresentam também as suas desvantagens. No entanto, apresentam também os problemas em questão as vulnerabilidades da mesma, que abrem as portas para os ataques cibernéticos, contudo a segurança cibernética deve ser meticulosamente ponderada e avaliada, a utilização de nuvens privadas é um dos pormenores para garantir a segurança nesse ambiente.

De forma a reduzir a incerteza da segurança, as organizações devem munir-se de métodos e técnicas para mitigar os ataques a quem podem estar expostos.

Entretanto propôs-se a implantação de uma técnica que poderia ajudar a prevenir esses ataques, que foi a implementação de um hacker digital benéfico baseado na tecnologia da inteligência artificial, onde poderá ser programado para invadir o sistema, contudo caso conseguisse seria uma forma da instituição se beneficiar para saber as vulnerabilidades que o hacker utilizou para o fazer, onde ela poderá detectar e prevenir de uma forma eficiente os ataques cibernéticos e garantir uma boa segurança na computação em nuvem.

Com a nova técnica proposta a instituição Vodacom Moçambique poderá prevenir-se dos ataques cibernéticos ocorridos na computação em nuvem.

Quanto às limitações da pesquisa, ressalta-se que, por se tratar de um estudo de caso, os resultados obtidos aplicam-se apenas ao objeto de estudo e, portanto, não podem ser utilizados para análises e interpretações de outras organizações.

6.2. Recomendações

- Tendo em conta que uma das principais características da computação em nuvem é a elasticidade. Contudo recomenda-se soluções de Big Data, apoiadas por aprendizado de máquina e inteligência artificial, pois essas três técnicas juntas podem dar esperança para que as instituições sejam mantidas seguras em face de uma violação de segurança cibernética.

- Recomenda-se a implantação das técnicas do aprendizado de máquina, que através de uma pesquisa foi constatada as técnicas mais comuns que foram: Support Vector Machines (SVM), Árvore de Decisão, Naive Bayes, K-Nearest Neighbors (KNN) e K-Means. Pois devido as principais características da computação em nuvem que são a disponibilidade e elasticidade será mais prático a utilização dessas técnicas.

7. BIBLIOGRAFIA

[1]. ALECRIM, Emerson. O que é Cloud Computing? **InfoWester**, São Paulo, dez. 2008, Disponível em: <http://www.infowester.com/cloudcomputing.php>. Acessado em: 12 jun. 2021.

[2]. Amoroso, E. 2006.*Cyber Security.* New Jersey: Silicon Press..

[3]. BAUN, Christian, MARCEL Kunze, Jens Nimis, and Stefan Tai. **"Cloud Management." In Cloud Computing**, 39–48. Springer Berlin Heidelberg, 2011. Disponível em: <http://dx.doi.org/10.1007/978-3-642-20917-8_5> Acessado em: 23 de abril. 2021.

[4]. BRYK, Anna. **Cloud Computing Attacks**, Disponível em: <https://www.apriorit.com>. Acessado em: 10 mai. 2021.

[5]. Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. *In Crisis Management: Concepts, Methodologies, Tools and Applications*: 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

[6]. CHIRIGATI, Fernando Seabra**. Computação em Nuvem**. Rio de Janeiro, RJ. 2009. Acessado em: 23 mai.2021.

[7]. CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No.4009: https:www.ncix.gov/publications/policy/docs/CNSSI 4009.pdf

[8]. CUARELI, Nathalia Viali. **Detecção de Anomalias De Segurança em Ambientes Cloud Computing**; 2016. Trabalho de conclusão de curso apresentado na Universidade Estadual de Londrina.

[9]. Disponível em: https://pt.wikipedia.org/wiki/computacao-em-nuvem/

[10]. Disponível em: https://gestaoodesegurancaprivada.com.br/ciberseguranca-seguranca-cibernetica/

[11]. Disponível em: https://azure.microsoft.com/pt.br/overview/types-of-cloud-computing/

[12]. Disponível em: https://cryptoid.com.br/ciberseguranca-segurannca-da-informacao/

[13]. DHS. 2014. A Glossary of Common Cybersecurity Terminology.National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. Disponível em http://niccs.us-cert.gov/glossary#letter c Acessado em 1 de abr. 2021.

[14]. ERL, Thomas; PUTTINI, Ricardo; MAHMOOD, Zaigham. *Computação em nuvem*.Pearson,2013.

[15]. FINLAY, Christopher J. **Just war, cyber war, and the concept of violence**. Philosophy & Technology, v. 31, n. 3, p. 357-377, 2018.

[16]. GARTNER, july. 2008: https://b3compuvision.com/yahoo/

[17]. GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Editora Atlas, 1999.

[18]. GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

[19]. ITU. 2009. Overview of Cybersecurity. Recomendação ITU-T X.1205.Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

[20]. KEMMERER, Richard A. Cybersecurity. In: **Software Engineering, 2003. Proceedings. 25th International Conference on**. IEEE, 2003. p. 705-715

[21]. Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection Washington, DC: Center for Strategic and International Studies.https://csis.org/publication/cybersecurity-and-critical-infrastructure-protectio.

[22]. MARCONI, Marina A.; LAKATOS, Eva M**. Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados. 5. ed. - São Paulo: Atlas, 2002.

[23]. NIST (National Institute of Standards and Technology). The NIST Definition of Cloud Computing, Version 15, **National Institute of Standards and Technology, Information Technology Laboratory**. Gaithersburg, Maryland, EUA, 2009. Disponível em: <http://www.nist.org> Acesso em: 15 fev. 2021.

[24]. NIST. **The NIST Definition of Cloud Computing**. Disponível em: <http://www.nist.gov/itl/cloud/> Acessado em 13 jun. 2021.

[25]. NIST (2011). *NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292* (VOL.292). https://doi.org/500-299.

[26]. Oxford University Press. 2014.Oxford Online Dictionary. Oxford: OxfordUniversity Press. Disponível em: <http://www.oxforddictionaries.com/definition/english/Cybersecurity> Acessado em 1 abr. 2021.

[27]. Pinheiro-Junior, L., & Cunha, M. A. (2017). Cloud Computing in Government: Benefits and Risk in Cloud Contracting. In *Twenty-third Americas Conference on Information Systems-AMCIS* (pp. 1-10). Boston, USA.

[28]. TAURION, Cezar. Segurança em Cloud Computing. **WordPress**, São Paulo, mar. 2010. Disponível em: <http://computingonclouds.wordpress.com/2010/03/04/seguranca-em-cloudcomputing-3>. Acesso em: 12 março. 2021.

[29]. TAURION, Cezar. Cloud Computing: computação em nuvem. Rio de Janeiro, ed. Brasport, 2009.

[30]. TAURION, Cezar. **Cloud Computing: Computação em nuvem: Transformando o mundo da Tecnologia da informação**. Rio de Janeiro: Brasport, 2009. Disponível em:<http://books.google.com.br/books?hl=pt-BR&lr=lang_en|lang_pt&id=mvir2XA2mcC&oi=fnd&pg=PA29&dq=armazenamento+em

+nuvem&ots=C8Lr7CTVWs&sig=dxAFtbMCx
kKnjMmCHgYQObjfZCo#v=onepage&q=armazenamento%20em%20nuvem&f=false>
Acesso em: 15 de fev. 2020.

[31]. TEIXEIRA, Elizabeth. **As três metodologias**: acadêmica, da ciência e da pesquisa. Petrópolis, RJ: Vozes, 2005.

[32]. REZENDE, D. A.; ABREU, A. F. **Tecnologia da Informação aplicada a sistemas de informação empresariais.** 9 ed. São Paulo: Atlas, 2013.

[33]. SILVA, F. H. R**. Um estudo sobre os benefícios e os riscos de segurança na utilização de Cloud Computing**; 2010. 15f. Artigo científico de conclusão de curso apresentado no Centro Universitário Augusto Motta, UNISUAM-RJ.

[34]. SCHIAVO, J. M. A. **Cloud Computing: Uma questão de segurança**; 2015. Monografia apresentada ao Programa de Pós-Graduação em Gestão de Serviços de Telecomunicações da Universidade Tecnológica Federal do Paraná - Campus Curitiba.

[35]. Souza, Carlos Henrique Medeiros e Gomes, Maria Lúcia Moreira (2009). **Educação e Ciberespaço**. Brasília: Usina de Letras.

[36]. STOPATTO, S.; ***Cloud security***. São Paulo. Ed. Universidade de São Paulo. CBTU, 2009.

[37]. SUN MICROSYSTEMS, INC**. Introduction to Cloud Computing Architecture**. White Paper, 1ª edição, junho 2009a.

[38]. Sun, Y. and He, D. (2012). "Model Checking for the Defense Against Cross-site Scripting Attacks". In: Proceedings of the Computer Science & Service System (CSSS), 2012 International Conference On, IEEE.

[**39].** VELTE, Anthony T. VELTE, Toby J.; ELSENPETER, Robert. **Computação em Nuvem**: Uma Abordagem Prática. Rio de Janeiro: Alta Books, 2012.

[40]. https://www.iso.org, acessado em 12 Abr.2021, às 19:15 min.

[41]. https://aws.amazon.com, acessado em 25 Abr.2021. às 07:42 min.

[42]. https://www.ibm.com, acessado em 25 Abr.2021, às 08:27min.

8. ANEXOS

Apêndice A – Questionário usado para colecta de dados

Questionário de pesquisa

Este questioário tem como objectivo, recolher informações para realização de uma monografia, do curso de Engenharia Informática e de Telecomunicações, na Universidadade Apolitécnica, cujo tema é: Análise da Segurança Cibernética na Computação em Nuvem.

Agradeço, desde já, o seu contributo!

1. Qual é o sector da instituição?

- ◯ Bancário
- ◯ Telecomunicações
- ◯ Tecnologia de informação
- ◯ Outros

2. Qual provedor de nuvem a instituição possui?

- ◯ Amazon Web Services
- ◯ Microsoft Azure
- ◯ Google Cloud Plataform
- ◯ Alibaba Cloud
- ◯ IBM
- ◯ Outros

3. Qual modelo de serviço de nuvem a instituição possui?

- ◯ Infraestrutura como Serviço (IaaS)
- ◯ Software como Serviço (SaaS)
- ◯ Plataforma como Serviço (PaaS)
- ◯ Todos

4. Qual modelo de implementação da computação em nuvem a instituição possui?

- ◯ Nuvens públicas
- ◯ Nuvens privadas
- ◯ Nuvens comunitárias
- ◯ Nuvens híbridas

5. Acredita que a computação em nuvem é mais segura que a computação normal?

- ◯ Sim
- ◯ Não
- ◯ Talvez

6. Dentre as vantagens que a computação em nuvem proporciona, quais os ja visíveis que a instituição notou?

- ◯ Simplificação na gestão de TI
- ◯ Redução de custos
- ◯ Agilidade na implantação dos sistemas
- ◯ Eficiência na utilização dos recursos
- ◯ Aumento da segurança
- ◯ Aumento da confiabilidade
- ◯ Aumento da produtividade
- ◯ Acesso a aplicativos sofisticados utilizado sob demanda

7. Dentre as desvantagens que a computação em nuvem proporciona, quais os ja visíveis que a instituição notou?

- ◯ Conectividade de internet
- ◯ Largura de banda inferior
- ◯ Afete a velocidade
- ◯ Questões de segurança
- ◯ Acordos
- ◯ Falta de apoio
- ◯ Variação de custo

8. De acordo com as características da computação em nuvem, avalie como melhoria para a instituição.

- ◯ Segurança (Infraestrutura centralizada e rotinas de backups)
- ◯ Disponibilidade (sistemas disponíveis pelo maior tempo possível)
- ◯ Elasticidade (Gerenciamento da carga ao longo do tempo)
- ◯ Custo (Diminuição dos custos ao longo do tempo)
- ◯ Serviços medidos (Os serviços utilizados devem ser transparentes entre o fornecedor e o cliente)

9. Acredita que os dados armazenados na "Nuvem" são vulneráveis á ataques cibernéticos?

- ◯ Sim
- ◯ Não
- ◯ Talvez

10. A instituição já sofreu algum ataque cibernético?

- ◯ Sim
- ◯ Não
- ◯ Talvez

11. Dentre as vulnerabilidades que a computação em nuvem proporciona, quais os ja visíveis que a instituição notou?

- ◯ Configurações incorretas
- ◯ Controle de acesso deficiente
- ◯ Shadow IT
- ◯ APIs inseguras
- ◯ Violações
- ◯ Interrupções

12. Se a resposta for "sim", quais desses ataques cibernéticos a instituição ja sofreu?

- ◯ Ataques de negação de serviços
- ◯ Ataques de injeção de SQL
- ◯ Ataques cross-site scripting (XSS)
- ◯ Ataques de envolvimento (XML)
- ◯ Ataques de phishing
- ◯ Ataques man-in-the-middle (MITM)
- ◯ Ataques de injeção de malware
- ◯ Insideres maliciosos
- ◯ Ataques de canal lateral
- ◯ Ameaças persistentes avançadas (APTs)
- ◯ Outros

13. De quem é a responsabilidade de garantir a segurança cibernética na computação em nuvem?

- ◯ Provedor
- ◯ Do usuário
- ◯ Ambos

14. O que a instituição faz para se prevenir dos ataques cibernéticos nos serviços de nuvem?

- ◯ Educar seus funcionários
- ◯ Projectar um plano de backup de dados
- ◯ Limitar o acesso dos funcionários aos dados
- ◯ Usar autenticação forte
- ◯ Todas opções

15. A instituição possui politicas para garantir a segurança cibernética nos seus serviços de nuvem?

- ◯ Sim
- ◯ Não

16. A instituição costuma fazer testes cibernéticos para prevenir dos ataques cibernéticos?

- ◯ Sim
- ◯ Não

17. Se a resposta for "Sim", com que frequência?

- ◯ De 6 em 6 meses
- ◯ De 1 em 1 ano
- ◯ Outros

18. Quais são as técnicas que a instituição utiliza para combater ataques cibernéticos?

Texto de resposta longa

Apêndice B – Nota enviada juntamente com o questionário

Exmo Senhor (a)

Director de Recursos Humanos de Vodacom Moçambique

Maputo 25 de Março de 2021

Assunto: Pedido de realização de pesquisa para trabalho de final do curso

Neila da Conceição Mabombo, de 21 anos de idade, Solteira, Natural de Maputo, Residente na Matola, bairro de Fomento, filha de Sergio Alfredo Mabombo e de Gertrudes Sandra Gomache Nhantumbo, Portadora de Bilhete de Identidade número 110104569094M, emitido aos 05 de Fevereiro de 2020, pelo arquivo de Identificação Civil da Cidade de Maputo, Estudante finalista da Universidade Politécnica A politécnica, frequentando o curso de Engenharia Informática e de Telecomunicações, 4^0ano.

Solicita encarecidamente a V.excia se digne conceder à realização de uma pesquisa científica para a culminação da licenciatura cujo tema é **Análise da Segurança Cibernética em Computação em Nuvem**.

Manifesta deste modo a sua total disponibilidade para um posterior contacto onde prestara todas as informações que se considerarem relevantes.

Agradecendo antecipadamente a atenção que possam dispensar Melhores cumprimentos.

Neila da Conceição Mabombo

Anexo: Link do questionário de pesquisa, credencial da universidade

https://docs.google.com/forms/