CENTRO UNIVERSITÁRIO UNIDADE DE ENSINO SUPERIOR DOM BOSCO
CURSO SISTEMAS DE INFORMAÇÃO

VITÓRIA REGO MELO

Computing cloud**:** vulnerabilidade de nuvens computacionais com ênfase na infraestrutura da Google

São Luís
2022

VITÓRIA REGO MELO

***Computing cloud*:** vulnerabilidade de nuvens computacionais com ênfase na infraestrutura da Google

Monografia apresentada ao Curso de Sistemas de Informação do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Dr. Giovanni Lucca França da Silva

São Luís

2022

Dados Internacionais de Catalogação na Publicação (CIP)

Centro Universitário – UNDB / Biblioteca

Melo, Vitória Rego

Computing cloud: vulnerabilidade de nuvens computacionais com ênfase na infraestrutura da Google / Vitória Rego Melo. São Luís, 2022.

73 f.

Orientador: Prof. Dr. Giovanni Lucca França da Silva.

Monografia (Graduação em Sistemas de Informação) - Curso de Sistemas de Informação - Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB, 2022.

1. Segurança da informação. 2. Nuvem computacional. 3. Google. I. Título.

CDU 004.056

VITÓRIA REGO MELO

***COMPUTING CLOUD*: vulnerabilidade de nuvens computacionais com ênfase na infraestrutura da Google**

Monografia apresentada ao Curso de Sistemas de Informação do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovada em:_____/ ____/_____.

BANCA EXAMINADORA:

_____

Prof. Dr. Giovanni Lucca França da Silva (Orientador)

Doutor em Engenharia Elétrica

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

_____

Prof. Esp. Igor Luciano Cavalcanti Lima

Especialista em Análise de Dados com BI e Big Data

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

_____

Prof. Esp. Francisco de Assis Silva Moura Junior

Especialista em Ciência de Dados

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

Dedico a minha mãe e meu pai.

AGRADECIMENTOS

Agradeço a Deus por ter conseguido chegar pelo menos até aqui e sem a certeza que passarei, mas segurarei na mão dEle, aos meus amigos de classe onde sempre nos incentivaram e mesmo com toda a dificuldade nos ajudaram a permanecer, a Mafisa Christiane, amiga, irmã, com certeza sem ela a caminhada todos esses anos seria um pouco mais difícil, ao nosso coordenador Rodrigo, que com toda paciência e leveza tentou nos ajudar da melhor forma possível, e aos meus pais, que sem dúvida são um espelho de força na minha vida.

RESUMO

Este trabalho versa sobre a segurança da informação armazenada em nuvem, enfatizando a infraestrutura da Google. A partir de uma revisão de literatura, com bases em livros, trabalhos acadêmicos e científicos, além de sites especializados, foi construído o texto dissertativo abordando o conceito e a evolução de computação em nuvem, foi apresentada a classificação de serviços na *Cloud Computing*, destacando as características da *Software-as-a-Service (SaaS), Platforms-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), Function-as-a-Service (FaaS)* e Communications-as-a-Service (CaaS). As vantagens e desvantagens das nuvens privada, pública e híbrida foram discutidas e os princípios da segurança de informação na nuvem foram apresentados. A infraestrutura da nuvem Google foi analisada, sendo descritas suas características e possíveis vulnerabilidades. Conclui-se quanto aos benefícios estratégicos, serviços em nuvem oferecem aos usuários uma vantagem competitiva, fornecendo a tecnologia mais inovadora disponível no mercado. Os provedores de serviços em nuvem operam a infraestrutura subjacente, permitindo que os contratantes se concentrem DevOps e em outras prioridades.

Palavras-chave: Nuvem computacional. Segurança da informação. Google.

ABSTRACT

This work deals with the security of information stored in the cloud, emphasizing Google's infrastructure. From a literature review, based on books, academic and scientific works, in addition to specialized websites, the dissertation text was built addressing the concept and evolution of cloud computing, the classification of services in Cloud Computing was presented, highlighting the characteristics of Software-as-a-Service (SaaS), Platforms-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), Function-as-a-Service (FaaS) and Communications-as-a-Service (CaaS). The advantages and disadvantages of private, public and hybrid clouds were discussed and the principles of information security in the cloud were presented. The Google cloud infrastructure was analyzed, describing its characteristics and possible vulnerabilities. It is concluded that in terms of strategic benefits, cloud services offer users a competitive advantage, providing the most innovative technology available on the market. Cloud service providers operate the underlying infrastructure, allowing contractors to focus on DevOps and other priorities.

Keywords: Computing cloud. Information security. Google.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABAC	*Attribute-Based Access Control*
AES	*Advanced Encryption Standard*
ANS	Acordo de Nível de Serviço
APIs	*Application Programming Interfaces*
APTs	*Advanced Persistent Threat*
ARPAnet	*Advanced Research Projects Agency Network*
AWS	*Amazon Web Services*
CaaS	*Communications as a Service*
CBC	*Cipher Block Chaining*
CPUs	*Central Process Unit*
CRM	*Customer Relationship Management*
DAC	*Discretionary Access Control*
DDoS	*Distributed Denial of Services*
DES	*Data Encryption Standart*
DevOps	Desenvolvimento e Operações
DSL	*Digital Subscriber Line*
ECC	*Elliptic Curve Cryptography*
FaaS	*Function-as-a-Service*
HMAC	*Hash-based message authentication code*
HTTP	*Hypertext Transfer Protocol*
IDEA	*International Data Encryption Algorithm (IDEA)*
IDEs	*Integrated Development Environment*
IoT	*Internet* das Coisas
IP	*Internet Protocol*
IVR	*Interactive Voice Response*
LANs	*Local Area Network*
LTE	*Long Term Evolution*
MAC	*Mandatory Access Control*
MAC	*Message Authentication Code*
MD	*Message Digest Algorithm*
NFV	*Network Functions Virtualization*
NT	*New Technology*

PaaS	*Platforms-as-a-Service*
PC	Computador Pessoal
PGP	*Pretty Good Privacy*
RAID	*Redundant Array of Independent Disks*
RBAC	*Role Based Access Control*
RC	*Ron's Code*
REST	*REpresentational State Transfer*
RIPEMD	RACE *Integrity Primitives Evaluation Message Digest*
SaaS	*Software-as-a-Service*
SDS	*Safety Datasheets*
SGSI	Sistema de Gestão da Segurança da Informação
SHA	*Secure Hash Algorithm*
SLA	*Service Level Agreement*
SOAP	*Simple Object Access Protocol*
SSL	*Secure Sockets Layer*
TI	Tecnologia da Informação
TLS	*Transport Layer Security*
UPS	*Uninterruptible Power Supply*
USB	*Universal Serial Bus*
WAN	*Wide Area Network*
XOR	*Exclusive OR*

SUMÁRIO

1 INTRODUÇÃO

A computação em nuvem, ou Tecnologia da Informação (TI) em nuvem inclui dados, espaço de armazenamento, aplicativos e capacidade de computação de um *data center* virtual, que também é chamado de nuvem (*cloud*). O termo nuvem é utilizado tendo em vista que um *data center* virtual é composto por computadores interconectados (*grid*), de modo que o recurso não é fornecido por nenhum computador específico. O recurso está em algum lugar nesta nuvem de muitos computadores. Um aplicativo nãoé mais atribuído permanentemente a um servidor e os recursos são dinâmicos, além de poderem ser acessados conforme a necessidade (SINGH, 2022).

A maioria das ofertas e serviços oferecidos sob o termo "computação em nuvem" não são necessariamente novos, tendo em vista que suas soluções tornam virtuais os serviços e estruturas necessárias para armazenamento de dados, mas cadavez mais atende corporaçãos e indivíduos, ou seja, usuários ligados à área de desenvolvimento e operações (DevOps) (BLEFARI et al., 2021).

Se o usuário utiliza, por exemplo, o armazenamento em nuvem para fazer *backup* de seus dados, não precisa mais se preocupar com discos rígidos quebrados, *pendrives Universal Serial Bus* (USB) perdidos e arquivos corrompidos, pois seus dados devem permanecer acessíveis e seguros na nuvem.

A variedade de dispositivos disponíveis no mercado é grande, como notebooks, *media players, tablets* e *smartphones*, por exemplo, e os usuários, que geralmente têm mais de um dispositivo, desejam que seus arquivos estejam disponíveis em todos eles simultaneamente e facilmente acessíveis, seja para entretenimento ou trabalho (SINGH, 2022).

Nesse contexto, os serviços de armazenamento na nuvem se popularizaram, tanto para contratação por pessoas quanto por empesas de todos os portes, destacando empresas contradas como Amazon Web Services (AWS), Azure (Microsoft), Alibaba Cloud, IBM Cloud e Google Cloud. A crescente demanda de mercado faz comque muitos provedores ofertem armazenamento e alguns serviços básicos na nuvem

de forma gratuita, geralmente com pouca capacidade de armazenamento e funções essenciais, mas que podem ser expandidos de forma flexível (BLEFARI et al., 2021).

O usuário pode então acessar seus dados armazenados na nuvem de qualquer dispositivo, a qualquer hora e em qualquer lugar através da *Internet*. Os dados permanecem privados, mas o usuário decide quem tem acesso à sua nuvem e se deseja compartilhar determinados dados com outras pessoas. Todas ações que podem ser realizadas com apenas alguns cliques.

Nos últimos dez anos, as possibilidades de uso da computação em nuvem se estenderam não apenas ao armazenamento *online* puro, mas também para o desenvolvimento, acompanhamento e mapeamento de processos inteiros, o que oferece aos usuários uma gama ampla de possibilidades de usos, por isso, a maioria das formas estabelecidas de trabalhar estão migrando parcial ou completamente para a nuvem (ANDRIETTA; GEUS, 2021).

Ao mesmo tempo, o compartilhamento de recursos em conexões cabeadas está sendo cada vez mais substituído por um método no qual a infraestrutura, os serviços, as plataformas e os aplicativos sob demanda sejam fornecidos em redes, possibilitando que o usuário armazene dados em um local cuja função e estrutura exatas também são irrelevantes: a nuvem (CHAVES; CASTRO; NASCIMENTO, 2021).

O processo de funcionamento da nuvem é baseado em dados que são distribuídos para armazenamento em diferentes servidores e podem ser acessados *online* a livre demanda, contanto que o usuário tenha acesso à *Internet*. O futuro da TI está na nuvem, as vantagens do uso dessa tecnologia são muitas, mas há algumas razões que falam contra isso, em particular, a segurança e proteção de dados é uma questão importante (MOLINARI, 2017).

As principais vulnerabilidades de segurança, como os vazamentos e divulgação de dados não autorizados pelos usuários, controles de acesso fracos, ataques e interrupções na disponibilidade afetam os sistemas tradicionais de TI, assim como os em nuvem. Como em qualquer ambiente computacional, a segurança na nuvem consiste em fornecer proteção proativa eficaz para que o usuário possa: ter certeza de que seus dados e sistemas estão protegidos, monitorar o *status* de segurança, saber imediatamente quando algo incomum acontece, monitorar e responder aos eventos inesperados (VELTE, 2012).

Os dados se tornaram um produto altamente valioso. Os criminosos cibernéticos, conhecidos como *hackers*, tentam ter acesso e roubar esses dados para fazer uso indevido ou vendê-los. Além dos usuários afetados diretamente, empresas envolvidas, como bancos, também podem ser prejudicadas (MOLINARI, 2017).

Ao mesmo tempo, os provedores de serviços de nuvem estão sujeitos às penalidades sensíveis e consequências legais inclusas nos contratos e na legislação, além de outras consequências negativas, como a perda de clientes, danos à imagem e quebra de confiança associados aos vazamentos de dados e ataque de *hackers* (SANTOS, 2015).

A segurança na nuvem geralmente segue o que é conhecido como modelo de responsabilidade compartilhada. Um provedor de serviços em nuvem, a empresa ou entidade que fornece infraestrutura como serviço, deve monitorar e mitigar as ameaças de segurança à infraestrutura em nuvem. Por outro lado, os usuários finais, que são os indivíduos e corporações contratantes, também precisam proteger os dados e outros ativos armazenados na nuvem contra roubo, divulgação ou outros comprometimentos (SINGH, 2022).

A tecnologia em nuvem é uma tendência, e é por isso que cada vez mais provedores de serviços estão oferecendo essa solução. A nuvem é particularmente popular onde alta flexibilidade e escalabilidade são necessárias, por isso não está apenas trazendo grandes mudanças à TI, mas também ao modelo de negócios dos provedores. Em particular, as empresas do setor de TI que anteriormente ofereciam *softwares*, *hardwares* e serviços precisam se adaptar às novas demandas e ofertas de nuvem, justificando o interesse em trabalhar a temática da segurança na nuvem.

Esta pesquisa busca então compreender de que forma as infraestruturas de nuvem, com ênfase no provedor Google, que oferece uma plataforma de armazenamento em nuvem gratuita, trabalha para reduzir as vulnerabilidades de sua nuvem computacional?

Quanto aos meios, a pesquisa é bibliográfica. Sendo assim, foi realizado um levantamento bibliográfico sobre a temática em livros, mas também em periódicos, inclusive os *online*, e bases de dados como *Scientific Electronic Library Online* (SciELO) e Google acadêmico, em busca de artigos científicos e outras pesquisas acadêmicas como monografias e teses.

1.1 Objetivos

O objetivo principal deste trabalho é discutir a vulnerabilidade de nuvens computacionais, enfatizando a infraestrutura da Google.

Em apoio ao objetivo principal, foram delimitados como objetivos secundários:

- Conhecer os conceitos e características do *computing cloud*;
- Descrever os fatores que geram insegurança na nuvem;
- Identificar os sistema de proteção proativo disponíveis para *computing cloud*.

2 REFERENCIAL TEÓRICO

2.1 Computação em nuvem ou *cloud computing*

O termo nuvem vem do inglês, *cloud*, que foi usado por engenheiros de informação para projetar configurações estruturais de redes com a finalidade de identificar sistemas que faziam parte de sua própria rede, mas operavam externamente. A estrutura e a função desses sistemas externos eram irrelevantes para a própria rede da empresa (LIMA, 2014).

A nuvem refere-se aos recursos hospedados externamente, mas que são disponibilizados aos usuários via *software*. A computação em nuvem descreve o uso de infraestruturas e serviços de Tecnologia da Informação (TI) que estão disponíveis na *Internet* e disponibilizados como um serviço, mas também capacidade de computação (infraestrutura) ou *software* de aplicação (BARBOSA et al., 2021).

As infraestruturas de computação em nuvem e todos os dados processados são dinâmicos, escalonáveis e portáteis. Como não estão armazenados em um computador, *laptop* ou *tablet* específicos, a localização do usuário não importa, de modo que este pode acessar os serviços de qualquer lugar com a ajuda de programas ou um navegador *World Wide Web*, ou simplesmente Web (TOKUMARU, 2019).

Dessa forma, *cloud computing* descreve a terceirização de armazenamento de dados, sistemas e aplicativos para uma nuvem, que com a ajuda dos recursos de TI adequados, torna o uso disponível a qualquer hora e em qualquer lugar, além de também oferecer flexibilidade adicional por meio do uso de interfaces, protocolos ou navegador da web (MENDONÇA; SOUSA NETO, 2019).

Existem tantas definições de computação em nuvem quanto soluções. O termo "serviços em nuvem" combina os diversos serviços que são fornecidos às empresas e aos clientes sob demanda via *Internet*. Esses serviços fornecem acesso fácil e acessível aos aplicativos e aos recursos contratados sem exigir que os usuários tenham um infraestrutura física/tecnologia ou *hardware* dedicados (LIMA, 2014).

Pode-se, dessa forma, sintetizar que a computação em nuvem fornece um suporte de TI virtual e escalável, que pode incluir memória, infraestrutura de acesso, DevOps ou serviços complexos que podem ser solicitados por meio de interfaces definidas, não importando em qual *hardware* rodam, já que a execução de cargas de trabalho ocorre de forma virtual, ou seja, em um ambiente de TI do qual os recursos

são extraídos, agrupados e distribuídos em uma rede (CHAVES; CASTRO; NASCIMENTO, 2021).

O princípio básico de nuvem pode ser explicado da seguinte forma: um provedor de serviços disponibiliza seus servidores na forma de um *data center* virtual. Para isso, muitos servidores são interconectados para que os dados não fiquem mais armazenados em apenas um servidor. O usuário tem acesso *online* aos dados armazenados na nuvem a qualquer momento (BARBOSA et al., 2021).

Não há arquitetura ou infraestrutura de nuvem perfeita. Todas as nuvens requerem um sistema operacional, como por exemplo, Linux®, mas a própria infraestrutura de nuvem pode conter *bare metal*, virtualização ou *software*s em locais diferentes que abstraem, agrupam e compartilham recursos escaláveis. Portanto, as nuvens são melhor definidas por sua função e não pelo que são feitas (CHAVES; CASTRO; NASCIMENTO, 2021).

Muitas pequenas e médias empresas não têm capacidade de implantar ou operar sua própria infraestrutura de TI e mantê-la atualizada. Ao usar a *cloud computing*, podem obter como vantagens: tempo de implantação rápido, armazenamento central de dados, modelos de faturamento baseados em consumo, além de serviços em escala, flexíveis e adaptáveis às suas necessidades reais (TOKUMARU, 2019).

Os usuários podem escolher quanto controle desejam com as opções "como serviço", que incluem *softwares* como *Software*-as-a-*Service* (SaaS), *Platforms-as-a-Service* (PaaS) e *Infrastructure-as-a-Service* (IaaS). Podem ainda escolher entre uma variedade de ferramentas e recursos predefinidos para criar uma solução que atenda às suas necessidades específicas, ao mesmo tempo em que podem terceirizar os riscos de segurança, manutenção, atualização, *know-how* e tecnologia para o provedor de serviços (JENSEN; MIERS, 2021).

2.1.1 Evolução do conceito de Nuvem

O conceito de nuvem não é tão novo, as primeiras ideias nesse sentido floresceram na década de 1950, quando Dr. Herbert RJ Grosch criou os primeiros modelos conceituais que descrevem as conexões da nuvem de dados atual: a combinação de alta velocidade e baixos custos, bem como o armazenamento e

distribuição de dados em muitas unidades de computação (bancos de dados), que resultaram posteriormente a arquitetura cliente-servidor (ANDRIETTA; GEUS, 2021).

Dr. John McCarthy continuou essa linha de pesquisa e afirmou que os *data centers* seriam muito mais do que bancos de dados, já na década de 1960, assumiu que se tornariam serviços públicos e sociais, apontando para um fenômeno que se tornaria particularmente importante, a nuvem como meio de cooperação, além da teoria de que a tecnologia também se reverteria em um componente social. Mas naquela época ainda faltavam os requisitos técnicos para efetivação da computação em nuvem (VELTE, 2012).

O percurso entre a concepção da ideia e a concretização da nuvem foi trilhado com a evolução do *hardware,* porque sem a capacidade computacional e sem a largura de banda necessários para as conexões, colaboração, armazenamento ou sincronização de dados era impensável atender aos requisitos técnicos para funcionalidade da computação em nuvem (MENDONÇA; SOUSA NETO, 2019).

Por outro lado, outras duas invenções também contribuíram nesse processo evolutivo: o *microchip* e o cabo de fibra óptica. Com os primeiros *microchips* produzidos em massa pela Intel, a capacidade da computação tornou-se significativamente maior e de menor custo, o que abriu o caminho para alguns dos gigantes de serviços em nuvem atuais, como Microsoft e Apple, começarem a investir nessa tecnologia na década de 1970 (VELTE, 2012).

Outro aprimoramento veio com primeiro Computador Pessoal (PC), produzido no início dos anos 1980. Para as empresas em geral, significou a disponibilidade dos primeiros computadores para utilização em estações de trabalho, que eram configurados para trabalharem em redes locais e acessarem o *data center* da própria organização. A arquitetura de servidor-cliente clássica foi implementada inicialmente apenas dentro da cada organização. Mais tarde, com a tecnologia de fibra óptica, foi ampliada entre organizações e continentes inteiros, se tornando uma grande rede (ANDRIETTA; GEUS, 2021).

Paralelamente aos desenvolvimentos técnicos, foi realizado um trabalho na *Advanced Research Projects Agency Network* (ARPANet) do Departamento de Defesa dos Estados Unidos da América, o precursor da *Internet*. Primeiramente, a ARPAnet pretendia apenas conectar algumas universidades americanas umas às outras. Os efeitos sobre o futuro da TI e até mesmo da humanidade eram

simplesmente impensáveis na época, embora os desenvolvedores tivessem lançado as bases para a computação em nuvem (VELTE, 2012).

Os programadores da ARPANet desenvolveram e testaram protocolos, códigos e topologias. Ao fazê-los, inventaram o *e-mail* como meio de comunicação na rede de dados. Em 1991 nasceu a *Internet*, acessível a todos e baseada no protocolo *Hypertext Transfer Protocol* (VIEIRA, 2017).

Um protocolo http desempenha um papel importante ainda hoje, sendo o início de quase todos os endereços da *Internet,* vindo simplificar a troca de dados entre diferentes computadores. Portanto, o próximo passo não se limitou apenas à troca dados, mas também migrou para oferta de serviços, como aplicativos de *software* ou o primeiro armazenamento *online* (JENSEN; MIERS, 2021).

Dessa forma, no final da década de 1990, a tecnologia da nuvem estava finalmente pronta, o *Software-as-a-Service* (SaaS) era realidade. Com o SaaS, uma empresa de TI tem a possibilidade de disponibilizar um *software* que o usuário pode utilizar por meio de um navegador da Web, sem instalá-lo em seu próprio computador. O usuário, portanto, não precisa se preocupar com licenças ou atualizações do *software*. Mas, de repente, segurança, privacidade e proteção de dados pessoais, assim como a criptografia de ponta a ponta se tornaram o foco (SANTOS, 2015).

Para os usuários comuns, quando a plataforma da rede social *Facebook* foi lançada em 2004, seus membros tiveram a oportunidade de salvar e publicar fotos, vídeos e diversos tipos de arquivos de forma *online*, podendo usufruir de um armazenamento gratuito, bastando a criação de uma conta na plataforma.

No entanto, o termo computação em nuvem foi cunhado principalmente por algumas empresas de *Internet* de rápido crescimento, como Amazon, Google e Yahoo. Devido ao célere aumento do número de usuários, essas empresas se depararam com o problema de ter que manter os sistemas em constante crescimento para que fornecessem o desempenho esperado pelos usuários, especialmente nos horários de pico de carga (BAUER, 2021).

Um pré-requisito obrigatório para o uso e disseminação de serviços de computação em nuvem é uma conexão de banda larga, que se tornou tão rápida que não faz mais diferença se os dados são armazenados localmente em um PC ou em servidores remotos em uma nuvem. Como resultado, a crescente relevância da computação em nuvem para usuários privados, sejam indivíduos ou empresas, está ligada ao fornecimento de conexões *Digital Subscriber Line* (DSL) e *Long Term*

Evolution (LTE) que são tão rápidas quanto confiáveis, além do baixo custo dos serviços (BARBOSA et al., 2021).

A primeira fase da computação em nuvem foi principalmente sobre redução de custos, uma vez que o *software* central pode ser usado por várias empresas ao mesmo tempo através do navegador, mantendo o acesso e uso seguros já que se tornou possível essa interação compartilhada sem que os dados de um empresa fossem acessados por outra sem autorização. Além disso, houve significativamente maior flexibilidade e faturamento de acordo com o uso (CHEE; FRANKLIN JÚNIOR, 2013).

A computação em nuvem atual se estabeleceu como uma plataforma para inovação, produtividade e valor comercial, fazendo o gerenciamento de *Central Process Unit* (CPUs), memória, discos rígidos e outros dispositivos virtuais. O *hardware* é controlado por uma plataforma de nível superior e garante que todos os recursos de *hardware* possam ser melhor dimensionados. À grosso modo, a plataforma de gerenciamento consiste em um agendador, armazenador, serviço de imagem e uma interface a partir da qual tudo é operado (MOLINARI, 2017).

Dependendo da carga no computador, o agendador decide em qual computador uma máquina virtual é iniciada. O serviço de imagem é responsável por atribuir as imagens às máquinas virtuais, se encarregando de armazenar e entregar as imagens. O componente de armazenamento é usado de forma distribuída e redundante para todos os tipos de dados, que são armazenados em contêineres e objetos virtuais. Containers são um tipo de diretório que contém objetos, que podem ser arquivos individuais ou imagens de disco de máquinas virtuais (VERAS, 2015).

Paralelamente às larguras de banda cada vez mais rápidas e aos melhores equipamentos técnicos, o conceito de nuvem também se mantém em evolução. Mais e mais empresas de TI estão oferecendo espaço de armazenamento em seus servidores e serviços *online*, de forma gratuita ou tarifada (MOURA, 2019).

Com a computação em nuvem, o local onde o armazenamento, a capacidade de computação e os aplicativos são fornecidos mudou de um único servidor físico para vários servidores virtuais organizados em grandes *farms*. A TI também se tornou uma mercadoria, como água ou eletricidade. Então, as novas demandas de mercado requerem uma infraestrutura que esteja realmente disponível com a *Internet* e conexões de banda larga (FERNANDES, 2021).

Existem quatro modelos principais de computação em nuvem: nuvens privadas, nuvens públicas, nuvens híbridas e multi-nuvens. E existem três tipos principais de serviços em nuvem: IaaS (*Infrastructure-as-a-Service*), PaaS (*Platforms-as-a-Service*) e SaaS (*Software-as-a-Service*).

Definir um modelo ou serviço de nuvem a ser contratado é uma escolha do usuário. Mas é importante enfatizar que não há duas nuvens iguais, mesmo que sejam do mesmo tipo, nem dois serviços de nuvem adequados às necessidades do usuário. Portanto, é importante entender as semelhanças e características de cada tipo e modelo, para que seja possível avaliar melhor como as limitações e vantagens de cada tipo podem ser adequados para cada usuário.

2.1.1.1 Classificação de serviços na Cloud Computing

Os três tipos principais de soluções como serviço, IaaS, PaaS e SaaS, permitem o fluxo de dados do usuário de clientes pela *Internet* para os sistemas do provedor de serviços em nuvem e vice-versa, no entanto, diferem na forma como são implantados, sendo discutidos nos subtópicos seguintes.

2.1.1.1.1 Software-as-a-Service (SaaS)

O *Software-as-a-Service* (SaaS) é um tipo de serviço que oferece aos seus usuários um aplicativo ou *software* que o provedor em nuvem gerencia. Normalmente, aplicativos da Web ou aplicativos móveis que os usuários podem acessar por meiode um navegador da Web e mantêm a conexão com os aplicativos por meio de um painel ou de uma *Application Programming Interface* (API) (ANTUNES, 2016).

O SaaS também elimina a necessidade de instalar um aplicativo localmente no dispositivo de cada usuário e permite métodos de acesso amplo à grupos de *software*. Os usuários acessam o aplicativo em nuvem com toda a infraestrutura e plataformas de TI subjacentes, sendo ideal para grandes e pequenas empresas ou indivíduos que não desejam gerenciar a infraestrutura, as plataformas e o *software* por conta própria, ou cujas necessidades exigem personalização mínima, favorecendo as assinaturas de *software* (HINTZBERGEN, 2018).

Com o SaaS, os usuários podem reduzir seus custos iniciais eliminando as compras contínuas de *software* ou investimentos em infraestrutura de TI local robusta.

Exemplos de ofertas de SaaS incluem serviços ao cliente, como Google Docs e Microsoft Office 365, bem como serviços corporativos que fornecem *softwares* de recursos humanos, sistemas de gerenciamento de conteúdo, ferramentas de Gestão de Relacionamento com Clientes (*Customer Relationship Management* – CRM) e de Ambientes de Desenvolvimento Integrado (*Integrated Development Environment* – IDEs) (FERREIRA, 2015).

Normalmente, um provedor de serviços de nuvem, como Amazon Web Services (AWS), Azure (Microsoft) ou IBM Cloud, gerencia o ambiente de nuvem no qual o *software* está hospedado. Os aplicativos SaaS aproveitam as arquiteturas multilocatários para usar recursos de *pool*. Atualizações de *softwares*, correções de *bugs* e outros trabalhos gerais de manutenção dos aplicativos são realizados pelo provedor de SaaS (JENSEN; MIERS, 2021).

Os usuários interagem com o *software* por meio de um navegador da Web em seu computador ou dispositivo móvel. O usuário também pode usar APIs, como *REpresentational State Transfer* (REST) ou *Simple Object Access Protocol* (SOAP), para conectar o *software* a outras funções (MORETTI, 2022).

O SaaS torna mais fácil para os provedores apresentarem novos recursos para os clientes, pois a maioria dos aplicativos desse tipo são produtos *plug-and-play* prontos para uso, onde o provedor de SaaS gerencia tudo por trás do aplicativo, incluindo: componentes de *hardware*, como redes, armazenamento e servidores no *data center*, plataformas como virtualização, sistema operacional e *middleware*, além de requisitos de *software*, como tempos de execução, dados e o próprio aplicativo (SINGH, 2022).

O acesso aos aplicativos SaaS depende muito de modelos de assinatura para distribuição de licenças de *software*. Ao contrário de uma licença perpétua, com esse modelo de entrega, cada conta é associada a uma assinatura que concede acesso por um período específico de tempo, geralmente mensal ou anual. Esse período de assinatura concede acesso à documentação do produto e suporte contínuo regido por um *Service Level Agreement* (SLA) ou Acordo de Nível de Serviço (ANS). No entanto, alguns provedores de SaaS cobram taxas de suporte adicionais quando são feitas alterações de código personalizado no nível do código-fonte (VARELLA, 2019a).

2.1.1.1.2 Platforms-as-a-Service (PaaS)

No tipo de serviço *Platforms-as-a-Service* (PaaS) a plataforma de *hardware* e *software* de aplicação é fornecida e gerenciada por um provedor de serviços de nuvem externo. O usuário gerencia os aplicativos em execução na plataforma e os dados nos quais o aplicativo se baseia (WOLLINGER, 2020).

É destinado principalmente a desenvolvedores e programadores, pois essa solução oferece aos usuários uma plataforma de nuvem compartilhada para desenvolver e gerenciar seus próprios aplicativos, que é um componente importante de desenvolvimento e operações (DevOps) sem precisar construir e gerenciar a infraestrutura física normalmente necessária para o processo (OLIVEIRA; SPOHN, 2020).

Um provedor de PaaS hospeda o *hardware* e o *software* em sua própria infraestrutura e disponibiliza essa plataforma ao usuário como uma solução integrada, pilha de soluções ou serviço por meio de uma conexão com a *Internet* (FONTES, 2020).

Por exemplo, se o usuário tem uma ideia para um novo aplicativo e escreveu seu código, mas quer desenvolvê-lo evitando, contudo, o investimento adicional de instalar *hardware* em seu próprio espaço físico, manter servidores, atualizar *software* de infraestrutura e configurar uma plataforma personalizada para criar seu aplicativo, pode recorrer a um provedor de PaaS para se hospedar na plataforma e no ambiente, obtendo todo o suporte necessário para que o código funcione.

Para usuários DevOps que têm ideias para um aplicativo e também podem programá-lo, mas não têm e nem querem investir em infraestrutura para executá-lo e mantê-lo, o PaaS é uma opção vantajosa, pois podem sincronizar seu código com um modelo de PaaS e executar seu aplicativo no *hardware* e *software* do fornecedor, mantendo-o para si (MEDEIROS; CAMPOS; ARTSIA, 2020).

Este tipo de solução abre caminho para mais DevOps, reduzindo o esforço necessário para configurar e codificar a infraestrutura, já que os modelos de PaaS são facilmente escaláveis e migráveis porque residem na nuvem. As plataformas de nuvem do tipo PaaS incluem serviços fornecidos por provedores como Alibaba Cloud, Microsoft Azure, Google Cloud, AWS e IBM Cloud (BARBIERI, 2019).

2.1.1.1.3 Infrastructure-as-a-Service (IaaS)

A proposta do modelo *Infrastructure-as-a-Service* (IaaS) significa que um provedor de serviços em nuvem fornece a infraestrutura, por exemplo, os servidores físicos, a rede, a virtualização e o armazenamento de dados, que são gerenciados pelo usuário por meio de uma conexão com a *Internet*. O usuário tem acesso através de uma API ou *dashboard* e essencialmente aluga a infraestrutura (FERNANDES, 2021).

O usuário gerencia componentes como o sistema operacional, aplicativos e *middleware*, enquanto o provedor fornece a infraestrutura e é responsável por quaisquer falhas, reparos e problemas de *hardware,* sendo o modelo de implantação típico de provedores de armazenamento em nuvem (MIRANDA, 2020).

Esse tipo de solução de serviço permite aos usuários aproveitar ao máximo os recursos de computação gerenciando aplicativos, dados, sistema operacional, *middleware* e *runtimes*. O provedor de IaaS é responsável por fornecer virtualização, armazenamento, rede e servidores. Como resultado, o usuário não precisa de um *data center* local e não precisa cuidar da atualização física e manutenção desses componentes (ROSÁRIO, 2020).

Na maioria dos casos, o usuário de IaaS tem controle total sobre a infraestrutura por meio de uma API ou painel. Este é o mais flexível de todos os três tipos principais de soluções como serviço, permitindo fácil dimensionamento e atualização, além de adicionar recursos, como armazenamento em nuvem, conforme necessário, eliminando a necessidade do usuário prever necessidades futuras e possivelmente pagar por elas antecipadamente.

2.1.1.1.4 Function as a Service (FaaS)

Function as a Service (FaaS) é um conceito de computação sem servidor de um provedor de nuvem. O provedor fornece funções individuais que são usadas pelos usuários conforme necessário. No ambiente *serverless*, o provedor cuida da operação de todos os recursos necessários para fornecer e garantir a disponibilidade dos serviços e funções (VIEIRA, 2017).

As funções utilizadas são cobradas de acordo com o uso, a capacidade de computação necessária ou os requisitos de memória. O usuário só incorre em custos

para operações reais em que o código é realmente processado. Dependendo de sua carga de trabalho, os servidores subjacentes também processam outros pedidos (SINGH, 2022).

Os serviços FaaS funcionam em um princípio de solicitação-resposta. Uma função é acionada ou chamada por um evento, gatilho ou solicitação. A função é executada, atende ao resultado esperado e é finalizada. Se não há processo em andamento, a função é sem estado, então quaisquer estados e dados que surgirem devem ser salvos pelo aplicativo de chamada. Do ponto de vista do provedor, as funções sem estado são muito escaláveis. As cargas variáveis podem ser distribuídas com relativa facilidade para vários sistemas, além dos serviços serem muito galgáveis(NEPOMUCENO; SADOK, 2020).

Em teoria, um aplicativo usando um serviço FaaS pode ser criado sem uma linha de código. Só é necessária uma interface de usuário se o provedor de serviços FaaS não fornecer uma. Dessa forma, aplicativos completamente “sem servidor” podem ser construídos (LINS, 2020).

É importante entender que o FaaS não fornece dados para recuperação, mas os dados são passados pelo usuário da função e depois processados. Obviamente, seria concebível que a função enriquecesse os dados de entrada do usuário com seus próprios dados. Mas isso não corresponde ao cenário clássico de FaaS, que funcionalmente, oferece um serviço que é mais do que apenas uma consulta de banco de dados (HINTZBERGEN, 2018).

Do ponto de vista do usuário, os serviços FaaS são muito adequados para desenvolver, operar ou gerenciar aplicativos para os quais não se deseja ou não pode operar a própria infraestrutura. Por exemplo, porque o usuário não tem o *know-how,* os custos são altos ou não há mão de obra suficiente. Então, esses serviços oferecem como benefícios: potencial redução de custos, faturamento baseado no uso e foco nas competências essenciais (ROSÁRIO, 2020).

Em se tratando das desvantagens, do ponto de vista do usuário, ao decidir usar um ambiente sem servidor, uma avaliação de custo-benefício deve ser incluída. Pode não ser possível usá-lo por motivos de segurança e proteção de dados ou devido a dependências excessivas no modelo de negócios; destacando como desvantagens: alta velocidade de implementação possível; não é adequado para todos os casos de uso (desempenho, disponibilidade); limitações no monitoramento e depuração; bloqueio do fornecedor devido a interfaces específicas do fabricante; capacidade

limitada de migrar para a nuvem; e, interoperabilidade limitada. Do ponto de vista do provedor, são desvantagens: forte fidelidade do cliente relacionada ao sistema e carregar apenas parcialmente previsível (MEDEIROS; CAMPOS; ARTSIA, 2020).

Diante das informações apresentadas, foi desenvolvido o Quadro 1, que apresenta uma sucinta comparação entre os modelos de serviço em nuvem.

Quadro 1 – Quadro comparativo com a visão geral dos modelos de serviço em nuvem

Tipo de serviço	Descrição	Grupo alvo
SaaS	O aplicativo é instalado no servidor do provedor, pré-configurado e geralmente é operado por meio de um navegador. Os dados que são criados e editados também são armazenados lá. São principalmente serviços para tornar o *hardware* mais interessante. Os serviços de nuvem do consumidor, como Google Docs, Apple iCloud, Strato HiDrive ou Windows Live Services, são típicos de *Software* como Serviço.	Usuários em empresas
FaaS	O provedor fornece funções individuais que são empregadas pelos usuários conforme necessário. No ambiente *serverless*, o provedor cuida da operação de todos os recursos necessários para fornecer e garantir a disponibilidade dos serviços e funções.	Usuários e desenvolvedores
PaaS	Em princípio, este é um sistema operacional, uma estrutura técnica ou um ambiente de desenvolvimento no qual aplicativos simples podem ser desenvolvidos e operados.	Desenvolvedores
IaaS	Oferece acesso a recursos de computador virtualizados, como ambientes de servidor, poder de computação ou espaço em disco rígido, que podem ser expandidos conforme necessário. O usuário paga pelo que usa ou consome. IaaS é o modelo de serviço em nuvem no qual todos os outros modelos de serviço em nuvem são construídos. IaaS é o modelo de fazer dinheiro em escala.	Departamentos de TI Provedores de serviços de TI Serviços em nuvem

Fonte: Adaptado de Singh (2022)

2.1.1.1.5 Communications as a Service (CaaS)

O *Communication-as-a-Service* (Caas) é o fornecimento de serviço baseado em rede de aplicativos de telefonia e comunicação. Normalmente, o aplicativo de comunicação reside na nuvem. Pode ser um simples aplicativo de telefone ou um sistema telefônico virtual completo. Via de regra, os serviços CaaS vão além da pura telefonia, incluindo processos de comunicação auxiliados por computador que são terceirizados para a nuvem (ARUNDEL; DOMINGUS, 2019).

Esses serviços de comunicação estão abertos a diferentes dispositivos finais, por exemplo, *smartphones, tablets*, estações de trabalho na *web* e em escritórios ou Protocolo de *Internet (Internet Protocol – IP)* de telefones. Os

funcionários podem ser alcançados em qualquer lugar, pois os serviços de voz, dados e vídeo são integrados em uma interface acessível independentemente do local em que estejam (MENDONÇA; SOUSA NETO, 2019).

Comparado aos sistemas telefônicos convencionais, o CaaS oferece muito mais funções que se complementam perfeitamente em conexão com outros serviços em nuvem, como: IP, comunicações unificadas, mensagens instantâneas, resposta de voz interativa (*Interactive Voice Response* – IVR), Central de Atendimento, audioconferência / videoconferência, gravação de chamadas, integração móvel e compartilhamento de área de trabalho (LINS, 2020).

Mas não apenas os processos de comunicação auxiliados por computador são adequados para esse tipo de serviço de nuvem. Até mesmo aplicativos telefônicos simples podem ser fornecidos por um sistema telefônico virtual. Isso significa que as funções do sistema telefônico estão disponíveis como *software* que funciona como um sistema telefônico virtual em um servidor na nuvem (MIRANDA, 2020).

Comparado aos sistemas telefônicos convencionais, o CaaS oferece muito mais funções que se complementam perfeitamente em conexão com outros serviços em nuvem. Um exemplo disso é a integração de funções de telefonia nos aplicativos de *groupware*, bem como comunicações unificadas e funções de *contact center*. Para muitas empresas, o uso de CaaS também significa uma mudança para comunicação corporativa baseada em IP e telefone celular (CHAVES; CASTRO; NASCIMENTO, 2021).

2.2 Modelos de implantação para computação em nuvem

Existem quatro modelos principais de computação em nuvem e em cada um destes os recursos de computação escaláveis são abstraídos, agrupados e compartilhados em uma rede. Todos os modelos de nuvem também permitem a execução de cargas de trabalho no respectivo sistema.

Além disso, cada modelo consiste em uma combinação especial de tecnologias, incluindo quase sempre em um sistema operacional, uma plataforma de gerenciamento e APIs. O *software* de virtualização e automação pode ser adicionado a qualquer uma dessas nuvens para fornecer funcionalidade adicional ou maior eficiência.

2.2.1 Nuvem Privada (*Private Cloud*)

Nuvens privadas podem ser amplamente definidas como ambientes de nuvem dedicados a apenas um usuário final ou grupo de usuários e normalmente executadas por trás do *firewall* desse usuário ou grupo. (TOKUMARU, 2019).

Nuvens privadas são geralmente consideradas mais seguras porque as cargas de trabalho normalmente são executadas atrás do *firewall* do usuário. Em última análise, no entanto, isso depende do respectivo nível de segurança. Nuvens privadas são ambientes de nuvem somente para usuários finais, normalmente executados dentro de seu *firewall*. Embora as nuvens privadas costumavam ser usadas em ambientes locais, estão sendo desenvolvidas atualmente por organizações em *data center*s alugados fora do local de propriedade dos provedores (SINGH, 2022).

Software e *hardware* estão cada vez mais disponíveis com funcionalidades de nuvem privada. Na maioria das vezes, trata-se de sincronizar dados em diferentes dispositivos ou disponibilizá-los. A nuvem é o armazenamento central de dados. Os dispositivos ou clientes mapeiam o banco de dados localmente e permitem o acesso a ele. Muitos aplicativos e serviços podem ser usados de forma mais conveniente graças às ofertas de nuvem privada, como: Google Drive, Azure, iCloud (Apple) e AWS (VARELLA, 2019a).

No setor coorporativo, os processos de negócios são geralmente mais complexos, razão pela qual as ofertas de nuvem privada geralmente só podem ser usadas de forma limitada. No máximo para sincronizar contatos, compromissos e alguns documentos. Mas mesmo nesse modelo surge a questão de saber se essa nuvem privada também é bastante inadequada por motivos de proteção de dados.

Todas as nuvens se tornam nuvens privadas quando a infraestrutura de TI subjacente é atribuída a um único cliente com acesso completamente isolado. Embora sejam baseadas em várias tecnologias diferentes, usam a virtualização para combinar recursos derivados de *hardware* físico em *pools* comuns. Dessa forma, não é preciso criar ambientes sempre virtualizando recursos de vários sistemas físicos. Com a ajuda de um *script* de processo de TI, todos esses recursos podem ser recuperados de uma única fonte, como um supermercado de dados (MORETTI, 2022).

Uma camada adicional para *software* de gerenciamento oferece controle administrativo sobre toda a infraestrutura, plataformas, aplicativos e dados usados na nuvem. Os administradores de nuvem são, portanto, efetivamente apoiados no monitoramento e otimização do uso, gerenciamento de pontos de integração e armazenamento, assim como na restauração de dados (FERNANDES, 2021).

Com a camada final de automação que substitui parcial ou totalmente as operações manuais por instruções e processos repetíveis, o componente de autoatendimento está completo e muitas tecnologias diferentes podem compor uma nuvem privada. Mas, o usuário é sempre responsável por todos os custos, ou seja, custos de pessoal, bem como de gestão e manutenção da infraestrutura subjacente (NEPOMUCENO; SADOK, 2020).

No entanto, esse tipo de nuvem também pode ser fornecida por provedores como nuvens privadas gerenciadas, onde os clientes criam e usam uma nuvem privada que é fornecida, configurada e gerenciada por terceiros. Esse tipo de nuvem apresenta uma opção para corporações com equipes de TI insuficientes ou pouco qualificadas, podendo oferecer aos seus usuários melhores serviços e infraestrutura sem precisar gerenciar as complexidades do dia-a-dia de sua solução. A infraestrutura de TI *bare metal* usada por provedores de nuvem também pode ser abstraída e vendida como IaaS ou desenvolvida e distribuída como PaaS (VIEIRA, 2017).

Com a evolução do mercado e das tecnologias, as nuvens privadas não precisam mais ser baseadas em infraestruturas de TI locais. As organizações estão desenvolvendo essas nuvens em *data centers* alugados e fora das instalações de um fornecedor, tornando irrelevantes argumentos como localização e propriedade, o que também resultou em uma variedade de subtipos de nuvem privada, incluindo (OLIVEIRA; SPOHN, 2020):

a) Nuvens privadas gerenciadas: os clientes criam e usam uma nuvem privada que é fornecida, configurada e gerenciada por terceiros, sendo uma opção para organizações com equipes de TI insuficientes ou pouco qualificadas para obter melhores serviços e infraestrutura para seus usuários;
b) Nuvens dedicadas: ou a nuvem na nuvem, que pode ser integrada à uma nuvem pública ou privada, usando por exemplo a plataforma *open source* empresarial de orquestração de containers, ficando hospedado nas nuvens AWS e Google *Cloud*. Então o usuário poderia, por

exemplo, ter um departamento de contabilidade em sua própria nuvem dedicada na nuvem privada de sua corporação.

Nuvens privadas são a solução ideal para gerentes de TI que desejam disponibilizar recursos da corporação sob demanda, mas não podem (ou não desejam) usar uma nuvem pública. Os motivos para isso podem ser diretrizes de segurança, orçamentos, requisitos de conformidade ou regulamentos, como, por exemplo, nos setores de saúde e financeiro. As corporações desses setores usam protocolos de criptografia e *firewalls* para proteger seus sistemas de TI. Ao contrário das nuvens públicas, no entanto, as nuvens privadas têm uma camada de segurança adicional na forma de acesso restrito (WOLLINGER, 2020).

Se o usuário deseja ou não investir em uma infraestrutura de nuvem privada também depende das cargas de trabalho que precisam ser suportadas. Por exemplo, os produtos de virtualização prontos para corporações sempre foram adequados para cargas de trabalho com estado. No entanto, para cargas de trabalho sem estado e fracamente acopladas normalmente encontradas em desenvolvimento, pesquisa e telecomunicações, especificamente *Network Functions Virtualization* (NFV) ou seja, virtualização de funções de rede, as nuvens privadas são mais adequadas (JENSEN; MIERS, 2021).

Em nuvens privadas, as instâncias com capacidade subutilizada são reduzidas. As organizações podem configurar e reconfigurar seus recursos automaticamente e à vontade, pois os recursos não são limitados por suas instalações físicas. Esse tipo de nuvem oferece benefícios adicionais, incluindo: maior capacidade de infraestrutura para necessidades de computação e armazenamento em larga escala; serviços sob demanda com interfaces de autoatendimento e gerenciamento baseado em políticas; alocação eficiente de recursos com base nas necessidades do usuário; e, maior transparência de recursos na infraestrutura (NEPOMUCENO; SADOK, 2020).

Com o *Big Data* e a *Internet* das Coisas (IoT), a importância do armazenamento em nuvens privadas aumentou significativamente para as corporações, principalmente em áreas onde o valor de um *byte* só pode ser avaliado muito tempo depois de sua criação (TOKUMARU, 2019).

Nuvens privadas usam o que é conhecido como armazenamento definido por *software* ou *Safety Datasheets* (SDS) para arquivar e classificar dados. Uma das soluções SDS mais populares para nuvens privadas, especialmente em conexão com

OpenStack®, é o Ceph, adequado para nuvens porque combina efetivamente armazenamento de objetos, blocos e arquivos em um *pool* de recursos (BLEFARI et al., 2021).

2.2.2 Nuvem Pública (*Public Cloud*)

Uma nuvem pública é um conjunto de recursos virtuais construídos e gerenciados de *hardware* de terceiros que é automaticamente provisionado ou alocado a vários clientes por meio de uma interface de autoatendimento, fornecendo uma maneira eficiente de dimensionar cargas de trabalho com flutuações inesperadas na demanda (LINS, 2020).

Normalmente não são implementadas como uma solução de infraestrutura autônoma, mas sim como parte de uma mistura heterogênea de ambientes que oferecem mais segurança e desempenho, custos mais baixos e maior disponibilidade de infraestrutura, serviços e aplicativos, sendo configuradas da mesma forma que as nuvens privadas. São ambientes de nuvem normalmente construídos a partir de infraestrutura de TI que não é de propriedade do usuário final. Os maiores provedores de nuvem pública incluem Alibaba Cloud, AWS, Google Cloud, IBM Cloud e Azure (ROSÁRIO, 2020).

Para que a nuvem funcione, essas tecnologias não apenas precisam ser integradas entre si, mas também com qualquer outra usada nos sistemas de TI do cliente, sendo justamente essa capacidade que faz a nuvem pública se destacar, embora essa interação dependa talvez da tecnologia mais subestimada: o sistema operacional (OLIVEIRA; SPOHN, 2020).

O *software* de virtualização, gerenciamento e automação usado para criar nuvens fica no topo do sistema operacional. E a consistência, confiabilidade e flexibilidade do sistema operacional influenciam diretamente na estabilidade das conexões entre recursos físicos, *pools* de dados virtuais, *software* de gerenciamento, scripts de automação e clientes (SINGH, 2022).

Com um sistema operacional de código aberto projetado para corporações, garante que sua infraestrutura de nuvem pública ofereça uma base confiável e possa ser dimensionada com flexibilidade. É também por isso que 9 das 10 principais nuvens públicas são executadas em Linux (MORETTI, 2022).

As nuvens públicas tradicionais costumavam ser executadas quase exclusivamente "fora do local", mas os provedores de nuvem começaram à entregar esses serviços no local nos *data center*s de seus clientes. Por causa disso, argumentos como localização e propriedade da nuvem perderam o significado.

Todas as nuvens se tornam nuvens públicas quando os ambientes são particionados e espalhados por vários locatários. Além disso, as estruturas de taxas não são mais necessariamente uma marca registrada das nuvens públicas, uma vez que alguns provedores permitem que seus locatários usem suas nuvens gratuitamente. A infraestrutura de TI *bare metal* usada esse tipo de provedor também pode ser abstraída e vendida como IaaS ou desenvolvida como uma plataforma de nuvem e vendida como PaaS (VARELLA, 2019b).

Nuvens públicas estão expostas a uma variedade de ameaças de segurança devido à sua multilocação e aos vários pontos de acesso. Com esse modelo de nuvem, as responsabilidades de segurança geralmente são divididas: por exemplo, o provedor cuida da segurança da infraestrutura e o cliente cuida da segurança das cargas de trabalho (BARBIERI, 2019).

2.2.3 Nuvem Híbrida (*Hybrid Cloud*)

As corporações estão se afastando de distribuições de nuvem puramente públicas ou privadas para ambientes híbridos que integram infraestruturas *bare metal* e virtualização de ambos os modelos. Dessa forma, podem equilibrar as desvantagens de um ambiente com as vantagens do outro (ROSÁRIO, 2020).

Uma nuvem híbrida é um ambiente de TI aparentemente único criado a partir de vários ambientes conectados por meio de redes locais ou *Local Area Network* (LANs), redes de longa distância ou *Wide Area Network* (WANs), redes privadas virtuais ou *Virtual Private Network* (VPNs) e/ou APIs (VIEIRA, 2017).

As características de uma nuvem híbrida podem ser complexas e seus requisitos variam, podendo exigir, entre outras coisas: pelo menos uma nuvem privada e uma pública, além de um ambiente virtual ou *bare metal* conectado a uma ou mais nuvens públicas ou privadas (FERNANDES, 2021).

Esses diferentes requisitos são uma evolução da fase anterior da computação em nuvem, onde nuvens públicas e privadas podiam ser distinguidas com relativa facilidade por localização e propriedade. No entanto, os modelos de nuvem

modernos são muito mais complexos, porque a localização e a propriedade são critérios bastante abstratos (ARUNDEL; DOMINGUS, 2019).

No entanto, os sistemas de TI tornam-se automaticamente nuvens híbridas quando os aplicativos podem ser movidos livremente entre vários ambientes separados, mas interconectados. Alguns desses ambientes precisam ser construídos em recursos consolidados que podem ser dimensionados conforme necessário, mas todos devem ser gerenciados como um ambiente separado usando uma plataforma integrada de gerenciamento e orquestração (WOLLINGER, 2020).

Os recursos são abstraídos e agregados em *data lakes* usando virtualização, contêineres ou armazenamento definido por *software*. Em seguida, com o *software* de gerenciamento, esses recursos são distribuídos para ambientes que executam aplicativos, que são provisionados usando serviços de autenticação conforme necessário (MORETTI, 2022).

Nuvens separadas tornam-se nuvens híbridas quando esses ambientes são conectados da maneira mais transparente possível. Essa interconectividade é a condição para que a nuvem híbrida funcione e para formar a base da computação de borda. Essa interconectividade também garante migração de carga de trabalho, gerenciamento unificado e orquestração de processos. A funcionalidade da sua nuvem híbrida se mantém e diminui com a qualidade dessas conexões (HINTZBERGEN, 2018).

2.2.4 Multicloud

A chamada multicloud é uma abordagem que usa mais de um serviço de nuvem de mais de um provedor de nuvem pública ou privada. Todas as nuvens híbridas são multiclouds, mas nem todas as multiclouds são nuvens híbridas. Multi-clouds se tornam nuvens híbridas quando várias nuvens são conectadas por meio de alguma forma de integração ou orquestração (MIRANDA, 2020).

Multiclouds consistem em mais de uma implantação de nuvem do mesmo tipo (pública ou privada) de diferentes provedores. Uma nuvem híbrida é definida como várias nuvens de diferentes tipos (públicas ou privadas) com algum grau de integração ou orquestração entre as duas (TOKUMARU, 2019).

Uma multinuvem pode, portanto, consistir em duas nuvens públicas ou duas nuvens privadas. Uma nuvem híbrida pode ser composta por nuvens públicas e

privadas - com uma infraestrutura que simplifica a portabilidade das cargas de trabalho, através de APIs, *middleware* ou containers (CHAVES; CASTRO; NASCIMENTO, 2021).

Essas abordagens de nuvem são mutuamente exclusivas, o que significa que o usuário não pode usá-las simultaneamente porque as nuvens estão conectadas (nuvem híbrida) ou não (nuvem múltipla). Na verdade, a variante com vários ambientes de nuvem (públicos e privados) está se tornando cada vez mais popular porque permite que as corporações melhorem a segurança e o desempenho em um portfólio ainda maior de ambientes (HINTZBERGEN, 2018).

A segurança de nuvem híbrida é uma combinação dos melhores recursos de todos os modelos de nuvem. Assim, usuários e administradores podem mitigar os riscos de dados movendo cargas de trabalho e dados entre ambientes de acordo com as políticas de conformidade, auditoria e negócios ou requisitos de segurança.

2.3 Gerenciamento da segurança da informação na nuvem

O gerenciamento e os controles de segurança em nuvem devem ser adaptáveis às variáveis ambientais, às cargas de trabalho e ao volume de dados movimentados, considerando ainda o armazenamento e a transmissão destes, seja como parte inerente de cargas de trabalho, por exemplo, criptografia, ou dinamicamente por meio de um sistema de gerenciamento de nuvem e APIs, protegendo os ambientes de nuvem contra corrupção do sistema e perda de dados (MOURA, 2019).

2.3.1 Riscos e ameaças de usar a computação em nuvem

A terceirização de dados está sempre associada a riscos. Em particular, considerando à computação em nuvem, a segurança sofre ameaças por vários pontos. Portanto, a infraestrutura e os serviços de um provedor devem ser protegidos contra ameaças externas e internas, em um contexto em que a proteção contra perda de dados ou vazamento de informações tem a mais alta prioridade (BLEFARI et al., 2021).

Além disso, a disponibilidade permanente da *Internet* e de todas as conexões de rede deve ser garantida para que os clientes possam acessar dados e

aplicativos a qualquer momento. Ao mesmo tempo, é importante prevenir todos os tipos de ataques, como ataques *Distributed Denial of Services* (DDoS) ou *Ransomware*, que já paralisaram servidores populares da web como Amazon, Yahoo e eBay (FERNANDES, 2021).

Os cibercriminosos estão constantemente desenvolvendo novos métodos de ataque e estão se tornando cada vez mais sofisticados, pois em sua maioria utilizam tecnologia de ponta. A segurança de TI é, portanto, uma corrida constante contra ameaças crescentes (OLIVEIRA; SPOHN, 2020).

Ameaças sofisticadas são qualquer coisa que afete a computação e com ela a nuvem. *Malwares* cada vez mais sofisticados e outros ataques, como ameaças persistentes avançadas ou Advanced Persistent Threat (APTs), são projetados para contornar as defesas de rede por meio de pontos fracos na pilha de dados. As violações de dados podem resultar em divulgação não autorizada e corrupção de dados. Não existe uma solução padrão para essas ameaças. Tudo o que é possível fazer é implementar as práticas atualizadas de segurança na nuvem, que continuam a evoluir com novas ameaças (WOLLINGER, 2020).

As APTs se referem aos ataques cibernéticos direcionados que são adaptados às vítimas ou grupos de vítimas selecionados e que funcionam com métodos avançados. Os invasores obtêm acesso persistente a uma rede e o estendem a outros sistemas. Os cibercriminosos geralmente utilizam *malwares* para fazer isso (VARELLA, 2019b).

O termo *malware* inclui todos os tipos de programas de computador que executam ações indesejadas ou prejudiciais em um sistema, como vírus, *worms* e cavalos de Troia. O Ransomware é um *malware* que criptografa um sistema e desbloqueia o acesso aos dados se a vítima pagar um resgate. Essa forma de *malware* é particularmente popular, de modo que às vezes também são chamados de Trojans de criptografia, já que a chantagem se baseia no fato de que os dados são codificados inextricavelmente para o usuário (JENSEN; MIERS, 2021).

Os perpetradores chantageiam suas vítimas deixando claro que a tela ou os dados só serão liberados novamente após o pagamento de um resgate. O que emerge desses títulos alternativos é como o ransomware funciona: ele se infiltra no sistema e o usuário fica horrorizado ao descobrir que seu computador está bloqueado. Algumas variantes de ransomware têm um período de incubação. Isso significa que o

efeito nocivo só ocorre quando o usuário não consegue mais lembrar quando e onde ele pode ter pego um Trojan de chantagem (SINGH, 2022).

Um programa malicioso também pode ser detectado por um verificador de vírus e se tornar um resultado positivo da verificação. Como muitos Trojans de chantagem se excluem automaticamente após executar sua função maliciosa, é um verdadeiro desafio para o *software* de segurança detectar o *malware*.

A primeira coisa que o proprietário do computador percebe sobre o *ransomware* é uma janela de mensagem com uma solicitação de pagamento que não pode mais ser fechada. Exemplos bem conhecidos são os trojans de criptografia WannaCry e Petya (WOLLINGER, 2020).

As maneiras pelas quais os *ransomwares* se espalham dificilmente diferem das de outros *malwares*: geralmente entram no computador por meio de um site manipulado, ao qual leva um *link* de um *e-mails* de *spam, phishing* e *exploits drive-by* ou uma mensagem por meio de uma rede social, que exploram vulnerabilidades em navegadores, *plugins* de navegadores ou sistemas operacionais. Às vezes, os criminosos também enviam e-mails contendo o que parece ser um lembrete ou uma nota de entrega. Na realidade, porém, o arquivo anexado não contém nenhuma informação importante, mas sim o código malicioso (FONTES, 2020).

Outros tipos de ataques comuns a segurança na nuvem são os *spams* e *phishings*. O *spam* é um *e-mail* não solicitado e é um meio popular de disseminação de *malware*. E-mails de *phishing* são um tipo especial de *spam*, que se destinam a persuadir um usuário a realizar uma ação específica - por exemplo, revelar dados de *login* ou instalar *malware* (MIRANDA, 2020).

Os cibercriminosos também podem vincular outros sistemas de computador a *botnets*. Do ponto de vista puramente técnico, uma botnet é uma rede de computação distribuída, ou seja, uma combinação de computadores que funcionam de forma independente um do outro. Estes podem comunicar uns com os outros, mas por outro lado realizam as suas tarefas completamente separadas uns dos outros (SINGH, 2022).

Os operadores de uma botnet contrabandeiam programas maliciosos, os chamados bots (abreviação da palavra inglesa "robot") para os computadores de outras pessoas. A partir de então, esses bots agem discretamente em segundo plano sem que os donos do PC percebam nada. O computador é usado para fins do botmaster, que o usuário não percebe e certamente não suportaria. Como os

computadores são controlados remotamente e, portanto, agem como se não tivessem vontade, partes da botnet também são conhecidas como PCs zumbis (NEPOMUCENO; SADOK, 2020).

Entre outras coisas, os PCs zumbis são usados como centro de distribuição de spam. Por exemplo, e-mails de *phishing* são enviados para o mundo digital sem serem percebidos pelos proprietários de PCs. Outros *botnets* servem como espaço de armazenamento para atividades criminosas ou ajudam criminosos a obter dados confidenciais de usuários, ou esses dados são usados pelos próprios criminosos ou as informações são monetizadas na *Darknet* (SINGH, 2022).

Além disso, uma *botnet* permite que os criminosos se conectem a um terceiro computador por meio do PC zumbi e, assim, ocultem seu endereço original. Outro tipo de uso é o PC zumbi como *host* intermediário que infecta outros computadores e, assim, estimula uma reação em cadeia (TEIXEIRA FILHO, 2019).

Os bots operam pela *Internet*, o que significa que só funcionam quando o computador está ligado e conectado à *Internet*. Quanto mais bots pertencem a uma rede, maior o número de computadores ativos simultaneamente. Uma área popular de aplicação para botnets é, por exemplo, ataques DDoS (HINTZBERGEN, 2018).

Os ataques DDoS são projetados para derrubar um serviço ou servidor. Mais comumente, isso é feito por criminosos cibernéticos que enviam toneladas de solicitações ao servidor por meio de um *botnet*, fazendo que fique sobrecarregado e pare de funcionar (LINS, 2020).

Os cibercriminosos também costumam explorar vulnerabilidades em *software* ou *hardware* para seus ataques. Portanto, é crucial para a segurança de TI identificar e eliminar esses pontos fracos. Uma medida importante é, por exemplo, sempre instalar as atualizações e *patches* mais recentes para fechar as brechas de segurança (MENDONÇA; SOUSA NETO, 2019).

A proteção contra ameaças externas começa internamente, por exemplo, por meio de uma administração de nuvem confiável e sem falhas, familiarizada com a alta complexidade de seus serviços que, assim, evita falhas de serviço e perda de dados. A TI de uma corporação que utiliza serviços em nuvem também deve estar ciente de que pequenas falhas internas podem ter um grande impacto nos processos baseados em nuvem, tanto em termos de dados quanto de segurança operacional (BLEFARI et al., 2021).

Os dados podem ser perdidos por roubo, exclusão, substituição incorreta ou outra alteração inadequada. Se não houverem sistemas de backup apropriados para os dados originais, isso representa um enorme risco legal e pode potencialmente ameaçar a existência de uma corporação (NEPOMUCENO; SADOK, 2020).

Por exemplo, quando há conhecimento técnico especial, outros segredos comerciais, como listas de clientes, bases de cálculo ou contabilidade estão envolvidos. Portanto, sistemas de segurança apropriados devem ser implementados para evitar a perda de dados; que só devem ser terceirizados com relutância para a nuvem.

Falhas no sistema e na rede, bem como a indisponibilidade de recursos e serviços contratados, podem resultar em perda de dados ou acesso de pessoas não autorizadas, e a confidencialidade, segurança e integridade dos dados não podem mais ser garantidas. Além disso, essas falhas podem ter um grande impacto nas operações comerciais de uma corporação ou autoridade e, além de perdas financeiras, também podem resultar em sérios danos à reputação (FERNANDES, 2021).

No caso de terceirização, o prestador de serviços não pode divulgar como são regulamentadas as autorizações de acesso (físico e virtual) de seus funcionários e como são monitoradas nesse sentido. As declarações de confidencialidade também muitas vezes não são visíveis para o usuário. No campo da computação em nuvem, ainda mais atenção deve ser dada a esse problema quando se trata de uma nuvem pública (OLIVEIRA; SPOHN, 2020).

2.3.2 Segurança da informação na nuvem

Segredos comerciais, *know-how* técnico ou informações sobre clientes e preços são a base de muitas empresas. A proteção dessas informações é uma tarefa importante, sendo a principal preocupação a proteção contra perda e uso indevido de dados. Por essas razões, a proteção de informações confidenciais é de grande importância para proteger as corporações de danos econômicos, sendo o objeto da segurança da informação (BARBIERI, 2019).

Informações e dados são bens valiosos no mundo globalizado. O acesso a estes deve, portanto, ser restrito e controlado dentro da empresa. Somente usuários ou programas autorizados podem acessar as informações, por isso foram

definidas metas gerais de proteçãoque formam a base de todas as estratégias desegurança de TI (MEDEIROS; CAMPOS; ARTSIA, 2020).

A segurança da informação visa proteger o acesso ou modificação não autorizados de dados, ao mesmo tempo em que torna possível garantir que apenas usuários autorizados tenham acesso a esses. Esse conjunto de práticas de proteção são aplicadas tanto durante o armazenamento quanto durante a transmissão de um local físico para um virtual, ou vice-versa (VARELLA, 2019a).

De modo geral, a segurança da informação é baseada na proteção básica de TI, a partir de procedimentos criados para identificar e implementar medidas de proteção. Então, o termo segurança da informação define todas as medidas adotadas em sistemas técnicos e não técnicos que garantem os objetivos de proteção, ou seja, a confidencialidade, a disponibilidade e a integridade (JENSEN; MIERS, 2021).

A própria informação pode estar em diferentes formas e armazenada em diferentes sistemas. A informação não se limita aos dados digitais, mesmo que os sistemas de armazenamento ou registro nem sempre precisem ser componentes de TI. Podem ser sistemas técnicos e não técnicos. O objetivo é proteger contra perigos e ameaças e prevenir danos econômicos (REIS, 2018).

Na era digital, a segurança da informação muitas vezes se concentra em dados digitais, computadores, redes e suportes de dados, embora no verdadeiro sentido do termo abranja diversas áreas de segurança da informação no ambiente de TI como segurança de rede, segurança de computadores ou proteção de dados. Na aplicação prática, a segurança da informação é baseada no gerenciamento de segurança de TI, considerando os padrões ISO/IEC 27000, que é uma referência de práticas com uma série completa de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação (SGSI) e ISO 27001, que traz os requisitos para que exista um SGSI (MORETTI, 2022).

Segurança de TI, segurança cibernética ou segurança na *Internet*, todos esses termos vão na mesma direção, mas existem diferenças sutis. A segurança de TI é comumente definida como a proteção de sistemas de TI contra danos e ameaças, se estendendo desde o arquivo individual até computadores, redes, serviços em nuvem e *data center*s inteiros (FERREIRA, 2015).

A segurança cibernética estende a segurança de TI a todo o espaço cibernético. Como a maioria dos sistemas está conectada à *Internet*, a segurança de TI e a segurança cibernética são frequentemente equiparadas, já que incluem todas

as medidas técnicas e organizacionais para proteger os sistemas contra ataques cibernéticos e outras ameaças. Incluem, por exemplo, controles de acesso, criptografia, gerenciamento de direitos, *firewalls*, proxies, antivírus, gerenciamento de vulnerabilidades e muito mais. O termo segurança na *Internet* refere-se especificamente à proteção contra ameaças da *Internet* (VARELLA, 2019b).

A segurança de TI e a segurança da informação são frequentemente usadas como sinônimos. Estritamente falando, no entanto, a segurança de TI é apenas um aspecto da segurança da informação. Enquanto a segurança de TI está relacionada à proteção de sistemas técnicos, a segurança da informação geralmente trata da proteção de informações, que também podem existir em sistemas não técnicos, por exemplo, em papel (MIRANDA, 2020).

2.3.2.1 Princípios da segurança de informação em nuvem

Na sociedade contemporânea, a informação constitui uma base essencial para os negócios e ações pessoais. Sem informação, nenhuma decisão objetivamente equilibrada pode ser tomada. A vantagem do conhecimento em *know-how* técnico, processos de fabricação ou informações dos clientes torna a informação um fator competitivo decisivo. Como resultado, a informação é um ativo comercial valioso que deve ser protegido para evitar danos econômicos (JENSEN; MIERS, 2021).

Devido à alta importância da informação como valor agregado em uma corporação, a segurança da informação deve ser entendida como uma tarefa de gerenciamento necessária para evitar a perda e o uso indevido de dados, sendo os três principais objetivos da segurança da informação: a confidencialidade, a integridade e a disponibilidade da informação (MIRANDA, 2020).

Confidencialidade significa que todos os dados só podem ser visualizados e gerenciados por usuários autorizados, ou seja, é a proteção contra a divulgação não autorizada de informações. Dados confidenciais só podem ser acessados, lidos ou alterados por usuários autorizados, tanto durante o armazenamento quanto durante a transmissão de dados (OLIVEIRA; SPOHN, 2020).

Exemplos de informações confidenciais são dados de clientes, patentes ou dados de pesquisa. Na prática, para garantir a confidencialidade das informações, deve-se definir claramente quem está autorizado a acessar esses dados e de que forma.

A confidencialidade é o primeiro elemento associado à segurança da informação. Os dados são considerados confidenciais se apenas pessoas autorizadas puderem acessar os dados. Para garantir a confidencialidade, o provedor de nuvem deve ser capaz de identificar quem está tentando acessar os dados e bloquear tentativas de quem não possui a devida autorização. A confidencialidade pode ser garantida ou apoiada por uma série de práticas. O uso de autenticação de 2 fatores, criptografia e senhas são técnicas comuns em corporações e no tratamento privado de dados confidenciais (REIS, 2018).

A integridade destina-se a evitar que os dados sejam alterados e/ou manipulados despercebidos, ou seja, significa assegurar a exatidão (intacta) dos dados e o correto funcionamento dos sistemas. Quando aplicado aos dados, o termo integridade expressa que os dados estão completos e inalterados (VARELLA, 2019a).

A perda de integridade das informações pode, portanto, significar que foram alteradas sem permissão, informações sobre o autor foram falsificadas ou o horário de criação foi manipulado. A perda de integridade das informações pode ocorrer por meio de modificação, exclusão ou inserção não autorizada de dados (TEIXEIRA FILHO, 2019).

Para garantir a integridade dos dados, devem ser estabelecidas medidas através das quais as alterações nos dados possam ser detectadas ou medidas que impeçam totalmente as alterações dos dados (BARBOSA et al., 2021).

O princípio da integridade significa manter os dados em seu estado correto e completo e evitar que sejam alterados acidental ou intencionalmente. Ao fazê-lo, são utilizadas muitas das técnicas que também são utilizadas para cumprir o princípio da confidencialidade, porque estas também protegem a integridade dos dados. Por exemplo, um terceiro não autorizado não pode alterar dados aos quais não tem acesso (FONTES, 2020).

Existem também outras técnicas que permitem uma defesa profunda da integridade dos dados. Por exemplo, as somas de verificação podem ajudar a verificar a integridade dos dados. *Software* de controle de versão e *backups* frequentes são meios de restaurar os dados para um estado original em caso de emergência (MORETTI, 2022).

O princípio da integridade dos dados inclui também o conceito de não repúdio, que se aplica particularmente em contextos jurídicos. Isso significa que um

controlador de dados deve ser capaz de demonstrar que a integridade dos dados foi mantida (SINGH, 2022).

A integridade está vinculada a três objetivos que contribuem para a segurança dos dados: impedir que as informações sejam alteradas por usuários não autorizados; a prevenção de modificação não autorizada ou não intencional de informações por usuários autorizados; manter a consistência interna e externa.

A consistência interna garante que os dados sejam internamente consistentes. A consistência externa garante que os dados armazenados no banco de dados correspondam à realidade (MARTINS, 2021).

Vários métodos de criptografia podem alcançar essa integridade garantindo que uma informação não tenha sido alterada durante transferência. Essa alteração pode resultar em dados ilegíveis ou mesmo corrompidas. Se uma mensagem for adulterada, o sistema de criptografia deve indicar que a mensagem foi comprometida ou alterada (COUTINHO; NEVES; LOPES, 2021).

A disponibilidade é a prevenção de falhas do sistema para que os dados estejam sempre acessíveis. A disponibilidade de serviços, funções de um sistema de TI, aplicativos de TI ou redes de TI ou também de informações existe se sempre puderem ser usadas pelos usuários como pretendido. As falhas do sistema devem ser evitadas e o acesso aos dados deve ser garantido dentro de um prazo acordado (TOKUMARU, 2019).

A disponibilidade de dados é a contrapartida da confidencialidade. Se, por um lado, deve-se garantir que os dados não possam ser visualizados por usuários não autorizados, eles também devem estar disponíveis para usuários com a devida autorização. Na prática, garantir a disponibilidade dos dados significa que os recursos da rede e do computador correspondem ao volume esperado de acesso aos dados e as políticas de *backup* são implementadas para fins de recuperação de dados (VARELLA, 2019a).

Em um mundo ideal, os dados devem ser sempre confidenciais, em boas condições e disponíveis. Na prática, é claro, muitas vezes é preciso decidir quais princípios de segurança da informação priorizar, e isso requer uma avaliação dos dados. Por exemplo, se o usuário estiver armazenando informações médicas confidenciais, se concentrará na confidencialidade, enquanto uma instituição financeira pode enfatizar a integridade dos dados para garantir que a conta bancária de ninguém seja creditada ou debitada por engano (TEIXEIRA FILHO, 2019).

Para garantir a alta disponibilidade, são tomadas medidas para sustentar que os serviços e sistemas de informação possam continuar a ser usados durante uma falha. O objetivo da alta disponibilidade geralmente é atingir uma disponibilidade de 99,999% para serviços importantes. As estratégias de alta disponibilidade incluem redundância e *failover* (REIS, 2018).

A redundância é alcançada por sistemas que são duplicados ou fazem *failover* para outros sistemas em caso de falha. Um *failover* é a recuperação de um sistema ou a troca para outro sistema quando o sistema primário falha. No caso de um servidor, se ocorrer um erro, um servidor redundante assume a operação. Com essa estratégia, as operações podem continuar sem interrupção até que o servidor primário seja restaurado. No caso de uma rede, se houver uma falha de rede no caminho primário, o tráfego será redirecionado para outro caminho de rede (ROSÁRIO, 2020).

Implementar sistemas de *failover* pode ter um alto custo. Em uma grande rede corporativa ou ambiente de comércio eletrônico, um *failover* pode exigir que todo o tráfego de rede seja redirecionado para outro *site* até que o site principal esteja operacional novamente. Ao sincronizar os dados entre os sites primário e secundário, garante que todas as informações estejam atualizadas (JENSEN; MIERS, 2021).

Muitos sistemas operacionais, como Linux, Windows Server e Novell Open Enterprise Server, oferecem suporte a recursos de *failover* por meio de *cluster*. Com o *clustering*, vários sistemas são interconectados para auxiliar no balanceamento de carga e conectados em rede para que, se um sistema falhar, os outros assumam o controle. Isso pode degradar o desempenho de todo o *cluster* de servidores, mas a rede ou o serviço permanecem operacionais (VARELLA, 2019b).

O melhor exemplo dos benefícios do *clustering* é o Google, que aproveita essa mesma tecnologia. O *clustering* não apenas permite redundância, mas também oferece a possibilidade de dimensionamento à medida que os requisitos aumentam. A maioria dos provedores de rede mantém amplas capacidades internas de *failover* para poder oferecer alta disponibilidade a seus clientes. Se empresas e funcionários não puderem acessar as informações ou serviços de que precisam, a confiança no provedor diminui (ROSÁRIO, 2020).

No entanto, altos níveis de confiabilidade e confiança têm um custo mais alto, os sistemas de *failover* podem se tornar proibitivamente caros. Portanto, o usuário deve considerar cuidadosamente seus requisitos para determinar se seus

sistemas devem oferecer suporte a *failover*. Por exemplo, se usuário precisar de alta disponibilidade em seu ambiente, considere agrupar seus servidores. Se um dos servidores do cluster falhar, os outros servidores da rede podem assumir sua carga (MIRANDA, 2020).

Tolerância as falhas é a capacidade de um sistema continuar operando no caso de falha de um componente. Os sistemas tolerantes as falhas podem continuar operando mesmo se um componente crítico, como um disco rígido, falhar. Para isso, os sistemas são equipados com recursos em excesso (componentes e subsistemas redundantes) para reduzir o risco de tempo de inatividade (TEIXEIRA FILHO, 2019).

Por exemplo, um servidor pode ser tolerante as falhas por ter uma segunda fonte de alimentação, uma segunda CPU e outros componentes importantes. A maioria dos fabricantes (por exemplo, HP e IBM) oferece servidores tolerantes a falhas, que geralmente possuem vários processadores e podem, assim, realizar *failover* automático em caso de falha (ZAMBIASI; RABELO, 2020).

A matriz redundante de discos independentes, *Redundant Array of Independent Disks* (RAID), é uma tecnologia que atinge a tolerância a falhas usando vários discos rígidos. Existem diferentes níveis de RAID: RAID 0 (*striping*), RAID 1 (espelhamento), RAID 3 ou 4 (*striping* com paridade dedicada), RAID 5 (*striping* com paridade distribuída), RAID 6 (*striping* com paridade dupla), RAID 1 + 0 (ou 10) e RAID 0+1. (SINGH, 2022).

2.3.2.2 Criptografia

Todos os dias, o mundo digital apresenta riscos e perigos para os dados. São inúmeros os pontos de ataque para cibercriminosos. Mas existem tecnologias, em particular processos de criptografia, que protegem os dados de acesso não autorizado ou alterações indesejadas (OLIVEIRA, 2020).

Em seu caminho pela *Internet*, dados como informações de pagamento, e-mails ou dados pessoais são enviados de servidor para servidor e armazenados temporariamente. Se não forem criptografados, podem ser interceptados e falsificados por criminosos, e nem o remetente nem o destinatário estarão cientes disso. Portanto, os dados confidenciais devem ser criptografados (REIS, 2018).

Com a ajuda da criptografia, os dados podem ser transformados em um formato que não pode mais ser lido por pessoas não autorizadas. Além disso, as chaves digitais são usadas em métodos de criptografia simétricos ou assimétricos. Desta forma, o texto simples pode ser convertido em texto cifrado (criptografia), o qual pode então ser lido novamente com a chave apropriada (descriptografia) (MIRANDA, 2020).

A criptografia protege as informações contra divulgação acidental, bem como contra tentativas de ataques internos e externos. A força de um sistema de criptografia depende da eficácia com que pode impedir a descriptografia não autorizada. Um sistema de criptografia forte é difícil de quebrar. A força também é expressa como um fator de trabalho, que quantifica quanto tempo e esforços seriam necessários para derrotar as salvaguardas de segurança de um sistema (OLIVEIRA; SPOHN, 2020).

Um sistema é considerado fraco se permitir chaves fracas, tiver falhas de programação ou for facilmente descriptografado. Muitos dos sistemas disponíveis são mais do que adequados para fins comerciais e privados, mas não são adequados para proteger informações confidenciais no setor militar ou governamental, por exemplo. Algoritmos simétricos e assimétricos são usados para criptografia (VARELLA, 2019a).

2.3.2.2.1 Algoritmo HASH

A integridade também pode ser verificada usando um algoritmo de hash. Essencialmente, esse tipo de algoritimo gera um hash para a mensagem e o anexa ao final da mensagem. O destinatário calcula o valor de hash da mensagem recebida e o compara com o hash recebido. Os valores de hash só correspondem se nenhuma alteração foi feita na mensagem durante a transmissão (MIRANDA, 2020).

Em muitos casos, o hash é suficiente para verificar a integridade. No entanto, se a mensagem for interceptada e alterada intencionalmente por terceiros, o hash será ineficaz se a mensagem não for criptografada. Por exemplo, a pessoa que

intercepta a mensagem pode ver que um hash de 160 bits foi anexado à mensagem e concluir que o hash foi gerado usando SHA-1. A mensagem pode então ser manipulada à vontade. Então, tudo o que resta é excluir o hash SHA-1 original e calcular um novo hash da mensagem alterada (SANTOS, 2018).

Os algoritmos de hash usados para armazenar dados são muito diferentes dos hashes criptográficos. Em criptografia, uma função hash deve atender a três critérios: deve ser irreversível; o valor de hash não pode ser calculado de volta na cadeia de caracteres original; uma saída de comprimento fixo é produzida a partir de entradas de diferentes comprimentos. Independentemente de o valor do hash ser calculado para dois ou dois milhões de caracteres, o comprimento do hash é sempre o mesmo; o algoritmo deve levar a nenhuma ou apenas algumas colisões. O mesmo valor de hash não deve ser gerado para entradas diferentes (OLIVEIRA, 2020).

O Algoritmo de Hash Seguro, *Secure Hash Algorithm* (SHA), foi originalmente desenvolvido sob o nome de Keccak por Guido Bertoni, Joan Daemen, Michaël Peeters e Gilles Van Assche. SHA-1 é uma função de hash não reversível que produz um valor de hash de 160 bits que pode ser usado com um protocolo de criptografia. Problemas relacionados ao SHA-1 foram identificados em 2016, razão pela qual o uso do SHA-2 é recomendado. SHA-2 pode gerar valores de hash com 224, 256, 334 e 512 bits. Não há problemas conhecidos com SHA-2, e é por isso que esse algoritmo de hash ainda é o mais usado e recomendado. O SHA-3 foi lançado em 2012 e, apesar de seus muitos usos, não é amplamente utilizado, o que não se deve a problemas com o SHA-3, mas sim porque o SHA-2 funciona muito bem (OLIVEIRA; SPOHN, 2020).

O *Message Digest Algorithm* (MD) também é uma função de hash não reversível que cria um valor de hash para garantir a integridade dos dados. Existem diferentes versões do MD; as versões mais usadas são MD5, MD4 e MD2. MD5 é a versão mais recente do algoritmo e produz um hash de 128 bits. É mais complexo e seguro que as versões anteriores, mas não oferece proteção suficiente contra colisões e, portanto, não é mais recomendado hoje. Como alternativa, recomenda-se SHA 2 ou 3 (TOKUMARU, 2019).

O *RACE Integrity Primitives Evaluation Message Digest* (RIPEMD) foi originalmente baseado no MD4. Como o algoritmo não foi considerado suficientemente seguro, o sucessor RIPEMD-160 agora usa 160 bits. Existem também

versões com 256 e 320 bits, RIPEMD-256 e RIPEMD-320, respectivamente (ZAMBIASI; RABELO, 2020).

O GOST é uma cifra simétrica desenvolvida na antiga União Soviética, que após várias modificações agora pode ser usada como uma função hash. GOST processa uma mensagem de comprimento variável em uma saída de 256 bits de comprimento fixo (SANTOS, 2018).

Antes do lançamento do Windows NT, o sistema operacional da Microsoft usava o protocolo LANMAN para autenticação. LANMAN usou LM hash e duas chaves DES como um protocolo de autenticação puro. No Windows NT, ele foi substituído pelo NT (*New Technology*) LAN Manager (NTLM) (FONTES, 2020).

Com o lançamento do Windows NT, a Microsoft substituiu o protocolo LANMAN pelo NTLM (NT LAN Manager), que usa os algoritmos de hash MD4 e MD5. Existem diferentes versões deste protocolo (NTLMv1 e NTLMv2), que ainda é amplamente utilizado, embora a Microsoft prefira o protocolo de autenticação Kerberos. Embora o LANMAN e o NTLM funcionem com hash, eles são usados principalmente para autenticação (FERNANDES, 2021).

Um método comum de verificar a integridade é anexar um código de autenticação de mensagem, *Message Authentication Code* (MAC), à mensagem. Um MAC é calculado usando uma cifra simétrica no modo de encadeamento de blocos de cifras, *Cipher Block Chaining* (CBC), gerando apenas o último bloco. A saída CBC é usada essencialmente como a saída de um algoritmo de hash. No entanto, ao contrário de um algoritmo de hash, a cifra requer uma chave simétrica que é trocada entre as duas partes antes da transmissão (COUTINHO; NEVES; LOPES, 2021).

O Código de Autenticação de Mensagem Baseado em Hash*, Hash-based message authentication code* (HMAC), usa um algoritmo de hash em combinação com uma chave simétrica. Por exemplo, duas partes podem concordar em usar um hash MD5. Depois que o hash é calculado, um Exclusive OR (XOR) é aplicado ao hash da mensagem, o valor assim gerado é o HMAC (MORETTI, 2022).

2.3.2.2.2 Algoritmos simétrico

Fala-se de criptografia simétrica quando a codificação e a decodificação são realizadas com a mesma chave. Esta chave deve, portanto, ser secreta e só pode estar disponível para o remetente e o destinatário. Com algoritmos simétricos, o

remetente e o destinatário de uma mensagem criptografada devem usar a mesma chave e algoritmos de processamento (FERNANDES, 2021).

Os algoritmos simétricos geram uma chave simétrica, também conhecida como chave secreta ou chave privada, que deve ser protegida. Se essa chave for perdida ou roubada, a segurança do sistema estará em risco. Alguns padrões são usados para algoritmos simétricos (MORETTI, 2022).

O padrão de criptografia de dados *Data Encryption Standart* (DES) está em uso desde meados da década de 1970. Por muito tempo, o DES foi o padrão primário no governo e na indústria, mas não é mais considerado suficientemente seguro, o que se deve ao comprimento da chave de 64 bits, dos quais 8 bits são usados para correção de erros e os 56 bits restantes para a chave real. O padrão principal atual é o *Advanced Encryption Standard* (AES) (OLIVEIRA, 2020).

O Triple DES (3DES) é um avanço tecnológico do DES. O padrão ainda é usado, mesmo que o AES seja usado principalmente em autoridades públicas. O 3DES é muito mais difícil de descriptografar do que muitos outros sistemas e, portanto, é mais seguro do que o DES. O comprimento da chave foi aumentado para 168 bits, sendo usadas três chaves DES de 56 bits (WOLLINGER, 2020).

O AES substituiu o DES como padrão nas autoridades dos EUA. A criptografia é realizada usando o algoritmo Rijndael, em homenagem a seus desenvolvedores Joan Daemen e Vincent Rijmen. AES suporta comprimentos de chave de 128, 192 e 256 bits, o comprimento padrão é de 128 bits (MIRANDA, 2020).

Cifra de Ron ou Código de Ron, *Ron's Code* (RC), é uma família de cifras desenvolvida pela empresa RSA e nomeada em homenagem ao seu inventor Ron Rivest. As cifras RC4, RC5 e RC6 são usadas atualmente. O RC5 usa um comprimento de chave de até 2.048 bits e, portanto, é considerado um sistema forte. O RC4 é comumente usado para criptografia WiFi e WEP/WPA (JENSEN; MIERS, 2021).

A cifra de fluxo funciona com comprimentos de chave entre 40 e 2.048 bits e é usada nos protocolos de Segurança da Camada de Transporte, *Transport Layer Security* (TLS) e Protocolo de Camada de Sockets Segura, *Secure Sockets Layer* (SSL). Também é amplamente utilizado por utilitários para baixar arquivos torrent. Muitos provedores restringem o *download* desses arquivos, mas ofuscando o cabeçalho e o fluxo usando RC4, é mais difícil para eles detectarem que seus arquivos *torrent* estão sendo baixados (TEIXEIRA FILHO, 2019).

O Blowfish é um sistema de criptografia desenvolvido por uma equipe liderada por Bruce Schneier que criptografa blocos de dados de 64 bits muito rapidamente. É uma cifra de bloco simétrica com um comprimento de chave variável, entre 32 e 448 bits. O sucessor Twofish tem uma estrutura semelhante e funciona com blocos de 128 bits. Uma de suas características especiais é uma programação chave muito complexa (VARELLA, 2019a).

O *International Data Encryption Algorithm* (IDEA) foi desenvolvido por um consórcio suíço e usa uma chave de 128 bits. Em termos de velocidade e funcionalidade, este padrão é comparável ao DES, mas oferece mais segurança. O IDEA é usado no programa de criptografia PGP (*Pretty Good Privacy*), que é usado por muitos usuários para tráfego de e-mail (ZAMBIASI; RABELO, 2020).

Já os *one-time pads* são o único método de criptografia completamente seguro. Dois fatores são decisivos para essa segurança. Por um lado, é usada uma chave que é tão longa quanto a própria mensagem, portanto, a chave não contém nenhum padrão que um invasor possa usar para descriptografia. Por outro lado, os *one-time pads* são usados apenas uma vez e depois descartados. Portanto, mesmo que uma cifra de teclado de uso único pudesse ser quebrada, essa chave não seria usada novamente, portanto, saber a chave seria inúti (COUTINHO; NEVES; LOPES, 2021).

2.3.2.2.3 Algoritmo assimétrico

Algoritmos assimétricos usam duas chaves: uma chave pública e uma chave privada. O remetente criptografa uma mensagem com a chave pública e o destinatário a descriptografa com sua chave privada. A chave pública pode ser conhecida de forma geral ou apenas pelas duas partes. A chave privada, por outro lado, permanece privada e é conhecida apenas pelo proprietário (destinatário da mensagem) (BAUER, 2021).

Se alguém quiser enviar uma mensagem criptografada, o remetente pode criptografá-la com sua chave pública antes de enviá-la. Usuário pode então usar sua chave privada para descriptografar a mensagem. Se um terceiro obtiver conhecimento das duas chaves, a confidencialidade da mensagem não poderá mais ser garantida pelo sistema de criptografia. A verdadeira vantagem desses sistemas é que uma mensagem não pode ser descriptografada com a chave pública (FONTES, 2020).

A criptografia de um *e-mail*, por exemplo, funciona da seguinte forma: o remetente criptografa sua mensagem com a chave pública do destinatário, o destinatário pode então usar sua chave privada para descriptografar a mensagem. Só precisa ser garantido que a chave pública possa ser atribuída exclusivamente a um usuário. No entanto, isso pode ser regulado por certificação digital ou certificados de usuário (BARBOSA et al., 2021).

Na prática, os métodos assimétricos são muitas vezes complexos. Portanto, uma combinação de ambos os métodos é frequentemente usada. Por exemplo, pode ser gerada uma chave aleatória que criptografa simetricamente uma mensagem. Essa chave, por sua vez, é codificada usando um método assimétrico, como resultado, o procedimento mais complexo deve ser usado apenas para a última chave e não para toda a mensagem. Alguns padrões são usados para algoritmos assimétricos (SINGH, 2022).

O algoritmo Rivest-Shamir-Adleman (RSA) recebeu o nome de seus inventores Ron Rivest, Adi Shamir e Leonard Adleman. É um método de criptografia desenvolvido na década de 1970 que usa grandes números para gerar um par de chaves. É amplamente utilizado e tornou-se o padrão de fato. O RSA pode ser usado para criptografia e assinaturas digitais, sendo usado em vários ambientes, incluindo o protocolo SSL, e também pode ser usado para troca de chaves (BARBOSA et al., 2021).

O algoritmo Diffie-Hellman, desenvolvido por Whitfield Diffie e Martin Hellman, é creditado com a adoção do conceito de um par de chaves pública/privada. É usado principalmente para gerar uma chave secreta compartilhada em uma rede pública. O processo não é usado para criptografar ou descriptografar mensagens, mas apenas para gerar uma chave simétrica entre duas partes (COUTINHO; NEVES; LOPES, 2021).

A criptografia de curva elíptica, *Elliptic Curve Cryptography* (EEC), fornece funcionalidade semelhante ao RSA, mas atinge o mesmo nível de segurança com comprimentos de chave mais curtos. Os sistemas de criptografia ECC são baseados no conceito de que pontos em uma curva são combinados com um ponto no infinito e que problemas de logaritmo discreto são muito difíceis de resolver (JENSEN; MIERS, 2021).

4 RESULTADOS E DISCUSSÃO

A nuvem do Google é composta por um conjunto de plataformas, serviços e ferramentas direcionados para indivíduos, empreendedores e funcionários, professores e alunos, além de desenvolvedores e administradores de sistemas. Google Cloud é o nome de um grupo de produtos como (GOOGLE, 2022a):

a) Gmail e Drive: uma caixa de correio pessoal, unidade de nuvem, um conjunto de aplicativos para criar e editar documentos de texto, planilhas e apresentações;
b) Google One: uma unidade de nuvem com maior capacidade;
c) G Suite for Education: uma caixa de correio de domínio e um pacote de aplicativos em nuvem para o setor educacional;
d) Google Workspace: uma plataforma para empresas que apoia a produtividade e a cooperação; e,
e) Google Cloud Platform: um conjunto de serviços para desenvolvedores, possibilitando a construção da própria infraestrutura em nuvem.

Todos esses serviços são criados, desenvolvidos e disponibilizados pelo Google. Alguns estão disponíveis gratuitamente, outros por assinatura, outros são cobrados com base no nível de uso. O Gmail e Drive são soluções de nuvem gratuitas do Google para uso privado e incluem: e- mail no domínio @gmail.com, espaço de armazenamento em nuvem - 15 GB para arquivos e mensagens, acesso a aplicativos do Google, incluindo Google Agenda, notas do Keep, Documentos, Planilhas, Apresentações, Formulários além de uma plataforma para convocar e realizar videoconferências do Google Meet (GOOGLE, 2022b).

Ao criar uma conta Google, o usuário ganha um espaço livre em disco de 15 GB para arquivos e e-mails. Na nuvem, pode armazenar qualquer arquivo - documentos de texto ou planilhas criadas no Drive, arquivos do Office, documentos PDF, fotos, vídeos, gravações de som. A conexão da caixa com uma conta do Google, possibilita enviar convenientemente arquivos grandes. Tudo o que o usuário precisa fazer é enviar o arquivo para o Drive e compartilhá-lo no painel ou enviar um link para o documento (FORTINET, 2022).

O Google One é uma proposta para usuários que precisam de mais espaço em disco do que os 15 GB gratuitos. O acesso a aplicativos em nuvem (por exemplo, Documentos, Planilhas, Slides) é preservado, o espaço em disco para arquivos é

aumentado. No caso deste serviço, o Google dá a possibilidade de compartilhar o pacote com familiares, assim a unidade pode ser compartilhada por até cinco pessoas. Os usuários também podem usar a ajuda de especialistas do Google. O preço do Google One, comparado a outras unidades de nuvem ou plataformas de hospedagem de arquivos disponíveis, é favorável (ITFORUM, 2021).

O Google Workspace for Education é uma solução de nuvem do Google dedicada a alunos e professores. Inclui um conjunto de aplicações para a realização de aulas remotas, comunicação com alunos e outros colaboradores e gestão de processos educativos. Esse serviço inclui: e-mail para cada aluno e funcionário da organização no domínio da escola ou universidade, disco de nuvem ilimitado, aplicativos para criação e edição conjunta de notas, arquivos de texto, planilhas, apresentações ou formulários de pesquisa, calendário compartilhado, a possibilidade de realizar aulas remotas na forma de videoconferências pelo Google Meet (GOOGLE, 2022a).

O Google Classroom é uma plataforma de apoio à realização de aulas, atribuição e verificação de trabalhos, bem como distribuição de materiais, com painel de administrador que permite gerenciar centralmente documentos, dispositivos conectados e garantir maior segurança de arquivos no disco e caixas de correio no domínio sendo gratuito para escolas e faculdades (CISOADVISOR, 2020).

O Google Workspace é uma plataforma em nuvem com serviços de apoio à produtividade e comunicação na empresa. É uma solução dedicada aos negócios para corporações globais, médias e pequenas empresas, *startups*, mas também empreendedores individuais que desejam simplificar as atividades cotidianas ou gerenciar arquivos e documentos. Os serviços de nuvem disponíveis no Google Workspace, incluem (GOOGLE, 2022b):

a) Gmail: caixa de correio da empresa com domínio personalizado;
b) Calendário: um calendário online que inclui todos os membros da equipe (e, se necessário, pessoas de fora da organização);
c) Google Drive: uma unidade na nuvem para arquivos com qualquer extensão;
d) Google Docs: editor de documentos de texto online;
e) Planilhas Google: planilhas;
f) Google Slides: um aplicativo que permite criar, editar e realizar apresentações multimídia;

g) Google Forms: uma ferramenta para criar pesquisas e realizar análises de resultados;
h) Google Keep: um aplicativo para salvar notas;
i) Google Sites: editor de sites;
j) Google Chat: um mensageiro que funciona com outros aplicativos do Google; e,
k) Google Meet: uma ferramenta para videoconferência ou brainstorming remoto.

O Google Workspace está disponível em vários pacotes. Cada pacote inclui os mesmos aplicativos, mas os limites são diferentes, por exemplo, a capacidade de um disco na nuvem, o número máximo de participantes em uma videoconferência ou a capacidade de gravar reuniões. Empresas com até 300 funcionários podem usar os pacotes Business e o plano Enterprise é dedicado a empresas maiores (CISOADVISOR, 2020).

A grande vantagem do Google Workspace é a capacidade ser dimensionado facilmente. À medida que a empresa cresce, basta comprar contas adicionais no mesmo pacote e caso as necessidades de toda a organização aumentem, o usuário pode facilmente atualizar para um pacote superior (MARTINS, 2021).

A Criptografia no Dropbox, Google Drive e OneDrive usam uma configuração semelhante ao criptografar dados na nuvem. Todos os dados criptografados em repouso (armazenados nos servidores) com AES de 256 bits para OneDrive e Dropbox ou AES de 128 bits para Google Workplace. Isso corresponde ao estado da arte, pois atualmente é a maneira mais segura de criptografar dados. Além disso, o OneDrive usa criptografia completa de disco usando a Criptografia de Unidade de Disco BitLocker (ITFORUM, 2021).

Durante a transferência de dados, Dropbox, Google Drive e OneDrive usam criptografia SSL/TLS, que também é atualmente a melhor solução de última geração. Outro mecanismo de proteção que o Google introduziu é o *Perfect Forward Secrecy* (PFS). Essa tecnologia garante que as chaves SSL privadas não possam ser usadas para sessões anteriores. Especificamente: se um invasor obtiver uma chave SSL, essa não poderá ser usada para descriptografar o tráfego de dados anterior (MENDONÇA, 2019).

Contudo, é crucial que os dados não sejam protegidos apenas durante a transmissão do dispositivo final para a nuvem. Com a ajuda da criptografia de ponta a ponta, os dados são protegidos continuamente durante o transporte e no armazenamento. Isso garante que pessoas sem autorização de acesso não tenham chance de acessar os dados. Como apenas alguns provedores de nuvem oferecem criptografia de ponta a ponta, os usuários devem procurar uma solução de criptografia adicional adequada. Dessa forma, seus dados permanecem constantemente criptografados e protegidos contra o envio do dispositivo local para a nuvem (LIMA, 2020).

O OneDrive oferece um recurso que permite fazer backup de suas chaves no Azure Key Vault da Microsoft. Com a chave do cliente, o usuário fornece e controla as chaves de criptografia raiz para seus dados em repouso do Microsoft 365 no nível do aplicativo. Portanto, usuário está no controle das chaves da sua organização (MORETTI, 2022).

O Google também usa sua própria *Key Management Service* (KMS) para gerenciamento de chaves. Usando as chaves de criptografia gerenciadas pelo cliente (CMEK) para controlar a criptografia de dados nos produtos do Google Cloud e se beneficiar de recursos de segurança adicionais, como o Google Cloud IAM e registros de auditoria (OLIVEIRA, 2020).

O Dropbox gerencia as chaves de criptografia de maneira descentralizada. A infraestrutura de gerenciamento de chaves foi projetada com medidas de segurança operacionais, técnicas e processuais com acesso direto muito limitado às chaves. As chaves são geradas, trocadas e armazenadas de forma descentralizada em locais distribuídos (QUEIROZ, 2020).

As soluções de gerenciamento de chaves descritas são tecnicamente maduras e protegem suas chaves contra ataques externos. Mas um problema central permanece com todas: os provedores de nuvem têm acesso às chaves e, portanto, também aos dados criptografados (REIS, 2018).

Por exemplo, o Azure também é um produto da Microsoft. Em teoria, a Microsoft pode acessar as chaves gerenciadas lá. Isso é relevante, por exemplo, quando as informações precisam ser divulgadas às autoridades. O Google usa seu próprio sistema de gerenciamento de chaves e, portanto, pode acessar as chaves. E o Dropbox também pode recuperar as chaves armazenadas de forma descentralizada (SILVA, 2019).

Não é segredo que os provedores de nuvem podem acessar os dados armazenados na nuvem devido à sua configuração técnica. Então, quando as autoridades exigem a liberação de dados, Microsoft, Google, Dropbox têm que cumprir. Mesmo que os dados sejam criptografados, o provedor pode acessá-los porque eles próprios criptografaram os dados e, portanto, podem descriptografá-los novamente (TEIXEIRA FILHO, 2019).

O provedor tem as chaves, então também tem o poder. Devido a leis específicas, como a Cloud Act (Clarifying Lawful Overseas Use of Data Act, ou Lei para Esclarecer o Uso Legal de Dados no Exterior), os provedores também devem liberar os dados do usuário contra sua vontade. Em outras palavras: terceiros não autorizados podem acessar os dados, mesmo que sejam apenas funcionários ou autoridades da Microsoft, Dropbox ou Google (SILVA, 2020).

A separação de criptografia e armazenamento é ideal. Um profissional de gerenciamento e sincronização de servidores cuida do armazenamento e da disponibilidade dos dados (segurança de dados). Um profissional de criptografia independente cuida da criptografia de conhecimento zero (proteção de dados), oferecendo o melhor dos dois mundos e controle total (COUTINHO; NEVES; LOPES, 2021).

Com a criptografia de conhecimento zero, as chaves de criptografia permanecem em no dispositivo do usuário ou, se a transmissão for necessária, as chaves são criptografadas antes de serem enviadas ao provedor de criptografia. Portanto, o provedor não pode usá-los para obter os dados do usuário, mesmo que houvesse solicitações das autoridades, o provedor não poderia entregar seus dados ou chaves (OLIVEIRA, 2020).

O Google lançou seus primeiros serviços em nuvem em 2008, simplificando, as corporações podem usar a mesma infraestrutura de *software* e *hardware* que o Google usa para seus próprios produtos, como YouTube ou Gmail. Enquanto isso, o Google Cloud Platform abrange todas as principais funções para cargas de trabalho corporativas. O trabalho continua na expansão das funções da corporação, o Google Cloud Platform está um pouco à frente quando se trata de contêineres de aplicativos, gerenciamento de *Big Data,* Inteligência Artificial e *Machine Learning,* ou plataforma de aprendizado de máquina (MELO, 2020).

Por exemplo, o Google é o único provedor de nuvem pública a oferecer uma plataforma de aprendizado de máquina de código aberto e independente de

plataforma. A presença regional também está aumentando, e o Google está expandindo suas capacidades de *data center* internacionalmente descentralizadas. Com os especialistas certificados pelo Google, que oferece suporte no planejamento, configuração e migração de cargas de trabalho no Google Cloud Platform (OLIVEIRA, 2020).

Ininterruptamente e durante todo o ano, os aplicativos dos usuários são gerenciados e monitorados, incluindo as funcionalidades especiais de cada aplicação na implementação e gestão do ambiente cloud para garantir a otimização de performance, testes de carga, *go-live stand-by* e ajustes individuais (QUEIROZ, 2020).

A criptografia é um método para garantir a confidencialidade. Outro método é o controle de acesso. Existem vários mecanismos de controle de acesso que ajudam a garantir a confidencialidade. Cada um deles tem pontos fortes e fracos (CISOADVISOR, 2020).

O primeiro é o controle de acesso obrigatório, *Mandatory Access Control* (MAC). Em um ambiente MAC, todas as opções de acesso são predeterminadas. Os usuários só podem trocar informações se o administrador lhes conceder os direitos necessários. Consequentemente, as alterações a esses direitos também devem ser feitas pelos administradores. Esse processo impõe um modelo de segurança rigoroso, que também é considerado o modelo de segurança cibernética mais seguro (COUTINHO; NEVES; LOPES, 2021).

O Controle de acesso discricionário, *Discretionary Access Control* (DAC), é um modelo em que os usuários podem compartilhar informações dinamicamente entre si. O método permite um ambiente mais flexível, mas aumenta o risco de divulgação não autorizada de informações. Também é mais difícil para os administradores configurarem o ambiente para que apenas usuários autorizados possam acessar os dados (SOUSA *et al*., 2020).

O controle de acesso baseado na função, *Role-Based Access Control* (RBAC) controla o acesso com base na função ou responsabilidades de um usuário. Cada funcionário tem uma ou mais funções que lhes dão acesso a informações específicas. Se uma pessoa passar de uma função para outra, ela perderá os direitos de acesso associados à função anterior. Os modelos RBAC oferecem mais flexibilidade do que o modelo MAC, mas menos flexibilidade do que o modelo DAC. Sua vantagem é que a cessão de direitos não se baseia nas necessidades individuais do usuário, mas em sua função na corporação (PALOALTONETWORKS, 2022).

No controle de acesso baseado em regras o acesso é concedido de acordo com as configurações de políticas de segurança pré-configuradas. O acesso geralmente é negado a todos os usuários, exceto para usuários em uma lista de permissões de acesso. O acesso é negado apenas aos usuários que aparecem em uma lista de negação de acesso (MARTINS, 2021).

As entradas na lista podem consistir em nomes de usuário, endereços IP, nomes de host ou até mesmo domínios. Modelos baseados em regras são frequentemente usados em conjunto com modelos baseados em funções para obter uma combinação ideal de segurança e flexibilidade (GOOGLE, 2022b).

O controle de Acesso Baseado em Atributos, *Attribute-Based Access Control* (ABAC), é um método de controle de acesso lógico que examina atributos associados ao assunto, objeto, operação solicitada e, em alguns casos, condições ambientais, para conceder direitos a operações específicas. Eles são comparados com as políticas de segurança, regras ou relacionamentos que definem as operações permitidas para atributos específicos (GOOGLE, 2022a).

Os cartões inteligentes são normalmente usados para fins de controle de acesso e segurança. Geralmente, há uma pequena memória de trabalho no cartão, na qual as permissões e informações de acesso podem ser armazenadas. Originalmente, um *token* de segurança consistia em um dispositivo de *hardware* (como cartões inteligentes ou chaveiros) necessário para acesso. Agora também existem *tokens* baseados em *software* que geralmente contêm um certificado digital para autenticar o usuário (SOUSA et al., 2020).

O Google Cloud oferece um kit de ferramentas poderoso e flexível que permite uma transição tranquila para a nuvem. Em 2017, o Google Cloud e a Palo Alto Networks fizeram uma parceria porque acreditavam que a migração para a nuvem pode ajudar as organizações a simplificar a segurança e que a segurança aprimorada impulsiona a adoção da nuvem. Essa parceria está se expandindo para ajudar mais organizações a assumir o controle de sua própria segurança na nuvem (MELO, 2020).

Como parte da parceria, a Palo Alto Networks executa sua estrutura de aplicativos no Google Cloud para aproveitar o armazenamento em nuvem seguro e durável e as ferramentas de análise e inteligência artificial altamente escaláveis do Google Cloud Platform (PALOALTONETWORKS, 2022).

Serviços como o BigQuery ajudam os clientes do Application Framework a acelerar o tempo de percepção ao detectar e responder a ameaças de segurança. A

Palo Alto Networks também opera seu GlobalProtect Cloud Service no Google Cloud Platform. A rede e a infraestrutura globais confiáveis, de alto desempenho e seguras do Google Cloud oferecem muitas vantagens para um serviço de proteção de funcionários em filiais e dispositivos móveis (ITFORUM, 2021).

A Palo Alto Networks RedLock ajuda as organizações a gerenciar riscos de segurança e alcançar e manter a conformidade. Ao monitorar o uso da API do Google Cloud Platform, o RedLock oferece visibilidade em tempo real dos recursos, incluindo cargas de trabalho em contêiner no Google Kubernetes Engine, o que permite o monitoramento contínuo da conformidade e relatórios gerados automaticamente para regulamentações e padrões comuns, eliminando longas auditorias manuais (PALOALTONETWORKS, 2022).

Uma integração com a API Security Baseline (Alpha) do Google Cloud Platform permite que os clientes combinem uma visão de sua própria postura de segurança e conformidade com dados da infraestrutura do Google Cloud Platform, que não está disponível em nenhuma outra nuvem pública (MARTINS, 2021).

A integração profunda dos produtos da Palo Alto Networks com o Cloud Security Command Center do Google permite uma visão única dos riscos de segurança e conformidade no Google Cloud Platform. As integrações da Palo Alto Networks enviam alertas de firewalls da série VM, proteção de *endpoint Traps* e RedLock para fornecer uma visão única dos riscos de segurança e conformidade em um ambiente do Google Cloud (GOOGLE, 2022b).

Essa funcionalidade se soma aos já amplos recursos compartilhados que ajudam os clientes do Google Cloud a definir, aplicar, monitorar e manter políticas de segurança consistentes em ambientes locais, de nuvem pública e híbridos. A gama completa de firewalls de última geração da Palo Alto Networks, tanto físicos quanto virtualizados, oferece suporte à conectividade VPN IPsec baseada em padrões para garantir conectividade segura de ambientes locais ao Google Cloud. Além disso, o GlobalProtect Cloud Service oferece conectividade segura ao GCP as a Service, aliviando as organizações da carga associada às implementações de *firewall* (PALOALTONETWORKS, 2022).

Os firewalls virtualizados da série VM da Palo Alto Networks protegem e segmentam as cargas de trabalho na nuvem no Google Cloud Platform para proteção contra ameaças internas e externas e podem ser implantados diretamente do mercado do Google Cloud Platform. O Panorama Network Security Management fornece

gerenciamento unificado de firewalls físicos e da série VM implantados no local e no Google Cloud Platform (SOUSA et al., 2020).

O Traps ajuda a proteger o sistema operacional e os aplicativos em cargas de trabalho no Google Cloud Platform. Um agente de host leve implantado na instância de nuvem detecta todas as explorações de dia zero e garante a integridade do sistema operacional e dos aplicativos. Se os invasores descobrirem vulnerabilidades, a abordagem baseada em agente pode fornecer proteção até que as organizações consigam corrigir as cargas de trabalho na nuvem (QUEIROZ, 2020).

A proteção em linha fornecida pelos dispositivos de firewall da Palo Alto Networks ou pelo GlobalProtect Cloud Service permite que as organizações entendam o uso de SaaS e criem políticas para controlar a exposição ao risco. O usuário pode complementar os recursos de segurança robustos do G Suite com o serviço de segurança Aperture SaaS, que oferece opções adicionais para proteger dados em repouso e monitoramento contínuo da atividade do usuário e das configurações administrativas. As empresas que operam no Google Cloud têm acesso fácil aos recursos de segurança da Palo Alto Networks com recursos avançados disponíveis apenas no Google Cloud (CISOADVISOR, 2020).

As empresas podem fazer uma avaliação gratuita de duas semanas do pacote de VM e aprender como o pacote pode ser implantado no Google Cloud Platform para evitar perda de dados e possíveis interrupções operacionais. As empresas também podem se inscrever para uma avaliação gratuita de duas semanas do RedLock para monitorar e proteger continuamente o ambiente do Google Cloud, identificando ativos vulneráveis e possíveis pontos de ataque (FORTINET, 2022).

No final de 2021, o Google divulgou o primeiro relatório sobre ameaças enfrentadas por usuários típicos de nuvem. O relatório se concentra na segurança do Google Cloud Platform. O serviço oferece aos clientes corporativos a capacidade de construir diversos tipos de sistemas em nuvem, desde simples hospedagem e execução de aplicativos personalizados até a implementação de computação de alto desempenho (MORETTI, 2022).

O relatório explica as causas e consequências dos ataques a instâncias personalizadas do Google Cloud Platform analisando 50 ataques bem-sucedidos recentemente a servidores e aplicativos. Nos casos analisados pelo Google, o sucesso de 48% dos ataques se deveu a uma senha fraca ou mesmo falta de proteção por senha em contas baseadas em servidor. Em 26% dos casos, os *hackers*

exploraram uma vulnerabilidade no *software* do servidor em nuvem. A configuração incorreta de servidores ou aplicativos possibilitou 12% dos ataques e apenas 4% foram resultado de vazamento de senhas ou chaves de acesso (GOOGLE, 2021).

Os vazamentos surgiram em parte devido a um erro comum cometido pelos desenvolvedores: carregar o código-fonte, junto com as credenciais de autenticação, para um repositório público no GitHub ou plataforma similar. Até 5.000 segredos (chaves de API, senha/nome de usuário, certificados, etc.) são carregados no GitHub todos os dias e em 2020 houve 2 milhões de vazamentos (GOOGLE, 2021).

O Google explica que os cibercriminosos geralmente não visam empresas específicas, mas verificam regularmente muitos endereços IP pertencentes à plataforma Google Cloud para procurar instâncias vulneráveis. O que essa automação significa é claro: se um servidor desprotegido estiver acessível pela Internet, provavelmente será invadido e possivelmente rapidamente, em muitos casos, o ataque começou 30 minutos após a criação da nova instância. O tempo entre o ataque de *hackers* e o início da atividade maliciosa é ainda menor, a maioria dos servidores comprometidos é usada para fins ilegais em 30 segundos (MATRIX, 2021).

Na maioria dos casos (86%), um criptominerador, que é um programa que explora os recursos de outros para minerar criptomoedas, foi instalado nos servidores. Normalmente, esses são recursos de CPU/GPU, mas o relatório também mencionou a mineração de criptomoeda Chia, que também inclui o uso de espaço livre em disco (GOOGLE, 2021).

Em 10% dos casos, os servidores comprometidos foram usados para varredura de portas para procurar novas vítimas. Em 8% dos casos, um ataque foi realizado via servidor em outros recursos da rede. Algumas das atividades ilegais menos comuns em servidores de plataforma de nuvem hackeados incluem: hospedagem de *malware* ou conteúdo proibido, ou ambos, execução de ataques DDoS e distribuição de *spam* (GOOGLE, 2021).

Se alguém *hackear* um serviço de nuvem e instalar um criptominerador, a reputação do cliente pode ser prejudicada. Além disso, o cliente também pode receber contas de serviço absurdamente altas, mesmo que a atividade maliciosa dure apenas algumas horas (FORTINET, 2022).

Na maioria dos casos analisados pelo Google, os usuários poderiam ter evitado todo o aborrecimento tomando algumas medidas simples de segurança: usando senhas fortes e fatores de autenticação adicionais, tomando o devido cuidado

ao carregar o código-fonte e atualizando regularmente o software instalado para conhecer as vulnerabilidades de segurança são corrigidos o mais rápido possível (FORTINET, 2022).

Em geral, os sistemas em nuvem exigem as mesmas proteções que qualquer outro tipo de infraestrutura de TI. Os requisitos básicos de proteção incluem auditorias regulares, monitoramento de atividades suspeitas e isolamento de dados críticos (GOOGLE, 2022b).

No entanto, há mais algumas coisas a serem consideradas ao implementar a infraestrutura em um serviço de nuvem pública, e não apenas para organizações que usam o Google Cloud Platform. Uma das medidas mais importantes de acordo com o Google é configurar alertas automáticos que soem um alarme quando o consumo de recursos excede um determinado limite ou quando os custos aumentam repentinamente rapidamente (SOUSA et al., 2020).

O modelo de segurança do Google é em camadas e construído com base em mais de 15 anos de experiência em nuvem. O Google protege os dados do cliente, pastas de e-mail, Pesquisa do Google e outros aplicativos do Google. O Google Cloud Platform permite que aplicativos e dados aproveitem esse modelo de segurança, mantendo todas as informações em uma rede praticamente impenetrável e fechada pelo maior tempo possível (SOUSA et al., 2020).

Esse é um dos motivos pelos quais o Google Cloud é o provedor de serviços em nuvem, *Cloud Solution Provider* (CSP), preferido por empresas globais em uma ampla variedade de setores. Com foco direcionado na entrega eficiente de dados em ambientes multicloud e gerenciamento simples de aplicativos, a gigante da nuvem não apenas causou alvoroço na área de migração e armazenamento de dados, mas também na frente multicloud, tudo em suporte a soluções de negócios modernas (MATRIX, 2021).

A plataforma de nuvem intuitiva do Google Cloud abrange a infraestrutura de nuvem pública do Google, ambientes de computação sem servidor, APIs de aprendizado de máquina e, claro, o Google Workspace, tornou-se sinônimo do futuro da computação em nuvem de código aberto (GOOGLE, 2021).

Os recursos multicloud do Google Cloud Platform foram projetados para permitir que as organizações se transformem. Ao fornecer serviços e ferramentas de nuvem flexíveis em uma infraestrutura inteligente, o Google Cloud Platform facilita a

movimentação e o desenvolvimento de aplicativos em qualquer combinação de ambientes de nuvem (PALOALTONETWORKS, 2022).

Seja distribuindo cargas de trabalho em uma combinação de Google Cloud e AWS, Microsoft Azure, Oracle Cloud e/ou qualquer outro CSP público ou privado ou infraestruturas virtualizadas, as soluções Google Cloud Platform ajudam a simplificar o processo para que o usuário possa usar o melhor das funções e serviços de cada nuvem para o usuário (GOOGLE, 2022a).

O Google Anthos é fundamental para gerenciar multiclouds empresariais no Google Cloud Platform. O Anthos estende os serviços de nuvem do Google em suas diferentes infraestruturas de nuvem, permitindo que sua equipe implante e execute aplicativos em contêiner entre eles e fornecendo visibilidade dos ambientes de nuvem da sua organização para gerenciar adequadamente (PALOALTONETWORKS, 2022).

Uma das grandes vantagens do Google Anthos é seu componente básico, o Google Kubernetes Engine. Esse serviço de conteinerização de código aberto oferece controle total sobre o gerenciamento de infraestrutura e serviços descentralizados usando o Google Cloud (FORTINET, 2022).

Ao fazer upload, upload, entrega, salvar, armazenar, enviar ou receber material para ou por meio dos Serviços, o usuário concede ao Google (e seus associados) uma licença válida em todo o mundo para usar, compartilhar, armazenar, reproduzir, modificar, fazer upload, publicar, apresentar publicamente , exibindo e divulgando esses materiais, bem como criando trabalhos derivados deles, como obras derivadas, por exemplo, traduzindo, adaptando ou outras alterações para que funcionem melhor com os Serviços. O usuário sob esta licença concede direitos com a finalidade limitada de manter, promover e melhorar os Serviços e criar novos. A licença permanece em vigor mesmo depois que parar de usar os Serviços (GOOGLE, 2022a).

Portanto, é teoricamente possível que os arquivos armazenados pelos usuários no Google Drive caiam em mãos erradas ou sejam disponibilizados a terceiros. Tudo com o “consentimento" do usuário expresso como parte da aceitação dos regulamentos de serviço. É claro que é difícil supor que esse seja o caso, especialmente porque o texto afirma que o objetivo da licença concedida ao Google é melhorar o serviço. No entanto, dado o valor e a confidencialidade dos documentos da empresa, essas disposições são muito perigosas (GOOGLE, 2022b).

Em conclusão vale a pena usar o Google Drive como um serviço para empresas de forma limitada, por exemplo, para armazenar dados de trabalho, todos os tipos de materiais de suporte com baixa confidencialidade e valor para terceiros. Devido aos polêmicos regulamentos do serviço e os perigos relacionados, não seria recomendado o uso do Google Drive como repositório de dados confidenciais, como documentos corporativos, faturamento etc.

5 CONSIDERAÇÕES FINAIS

Serviços em nuvem são infraestruturas, plataformas e softwares hospedados por terceiros e disponibilizados aos usuários pela *Internet*. Os serviços de TI da nuvem são dinâmicos e, portanto, podem ser ampliados e reduzidos em curtos períodos de tempo. Dessa forma, o podem ser adaptados prontamente às necessidades do usuário. Então, é possível falar em escalabilidade oportuna dos serviços de TI, já que os usuários podem dimensionar serviços de acordo com suas demandas, personalizar aplicativos e acessar serviços em nuvem de qualquer lugar pela *Internet*.

A infraestrutura de nuvem também pode ser ampliada ou reduzida conforme necessário para dar suporte às cargas de trabalho flutuantes. Os usuários podem escolher armazenamento público, privado ou híbrido dependendo de suas necessidades de segurança e outras considerações.

A nuvem pública é provavelmente a mais fácil de todas as implantações de nuvem: os clientes que precisam de recursos, plataformas ou serviços adicionais simplesmente compram os recursos necessários do provedor de nuvem pública, seja por tempo ou bytes. Infraestrutura, poder de computação, armazenamento ou aplicativos baseados em nuvem são virtualizados por meio do hardware do provedor, combinados em *data lakes*, orquestrados usando software de gerenciamento e automação e disponibilizados ao cliente pela *Internet* ou por meio de uma conexão de rede dedicada.

O cliente não possui as soluções de armazenamento que usa, nem está envolvido na operação do *farm* de servidores que contém o *hardware* ou no *backup* ou gerenciamento de plataformas, aplicativos ou serviços baseados em nuvem. Os usuários de nuvem pública simplesmente contratam, usam e pagam por esses recursos.

A nuvem virtual é uma solução moderna com a qual cada usuário dessa nuvem tem a oportunidade de coletar seus dados em servidores que na versão física pertencem ao provedor de um determinado serviço de nuvem. São os provedores que são totalmente responsáveis pela privacidade, segurança dos dados ali armazenados e pela manutenção de tais servidores. A possibilidade de armazenar dados na nuvem é disponibilizada graças a um aplicativo especial disponível em telefones, *tablets* e computadores.

Graças ao serviço em nuvem, é possível guardar e acessar arquivos nela e em seguida, usar qualquer dispositivo com acesso à Internet para acessá-los em qualquer lugar e a qualquer momento, sem formalidades desnecessárias. Os provedores de serviços em nuvem oferecem uma certa capacidade limitada do disco virtual gratuitamente, mas se o usuário planeja acumular uma grande quantidade de dados no disco virtual, será necessário pagar uma assinatura mensal. Os preços de tal serviço são estritamente dependentes da quantidade de espaço que se quer obter.

Os serviços em nuvem são uma solução cada vez mais popular para coletar e armazenar seus arquivos. De longe, o mais popular é o Google Drive, como parte do qual se obtém uma capacidade gratuita de 5 GB para os documentos, fornecidos com Google Drive ao criar uma conta no e-mail do Gmail.

Como parte do armazenamento Google Cloud Platform é possível compartilhar uma determinada parte dos arquivos com outros usuários que podem apenas visualizar nossas coleções, ou até mesmo editar, dependendo da opção que o usuário escolhe. Outros serviços de nuvem populares incluem Amazon Web Services e Dropbox. Ambos os serviços funcionam como o Google Drive.

As soluções em nuvem são uma das maneiras mais seguras de armazenar os documentos e arquivos particulares ou corporativos. Esta solução é suportada pela grande flexibilidade de acesso aos dados. Juntamente com o aplicativo instalado, é possível acessar qualquer documento do smartphone em questão de segundos, além de ser uma solução muito segura que presta o máximo de atenção à proteção da privacidade de dados.

Quando se trata de proteger seus próprios dados, as empresas levam essa questão muito a sério, e isso é bom. O equívoco de que os servidores locais podem oferecer a mesma proteção que os principais provedores de serviços em nuvem ainda é difundido. No entanto, a segurança na nuvem tem sido um grande tópico há muito tempo e provedores como o Google Cloud já construíram as fortalezas mais seguras com certas precauções.

As precauções de segurança no Google Cloud incluem: rede global segura, detecção de ataques, conformidade e certificações, criptografia de dados. As equipes de engenharia de confiabilidade do site supervisionam a operação dos sistemas da plataforma usando APIs de serviço seguro e acesso autenticado e registros.

Conclui-se que quanto aos benefício estratégico, os serviços em nuvem oferecem aos usuários uma vantagem competitiva, fornecendo a tecnologia mais

inovadora disponível no mercado. Os provedores de serviços em nuvem operam a infraestrutura subjacente, permitindo que os contratantes se concentrem DevOps e em outras prioridades.

REFERÊNCIAS

ANDRIETTA; Murilo Guidetti; GEUS, Paulo Lício de. **Categorização dos Desafios de Segurança em Nuvem relacionados à tecnologia de Virtualização**. Instituto de Computação. Universidade Estadual de Campinas. Campinas-SP, 2021. Disponível em: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-52.pdf. Acesso em: 20 abr. 2022.

ANTUNES, Jonathan Lamim. **Amazon AWS:** Descomplicando a computação na nuvem. Casa do Código, 2016 (eBook Kindle)

ARUNDEL, John; DOMINGUS, Justin. **DevOps Nativo de Nuvem com Kubernetes:** Como Construir, Implantar e Escalar Aplicações Modernas na Nuvem. São Paulo: Novatec, 2019.

BARBIERI, Carlos. **Governança de Dados:** Práticas, conceitos e novos caminhos. São Paulo: Alta Books, 2019.

BARBOSA, Juliana Souza et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. ***Research, Society and Development***, v. 10, n. 2, e40510212557, 2021. Disponível em: https://rsdjournal.org/index.php/rsd/article/download/12557/11384/167309. Acesso em: 15 mar. 2022.

BAUER, Murilo. **Ferramenta para implementação de aplicações para ensino com moderação.** 2021. 47f. Trabalho de conclusão de curso (Graduação - Engenharia de Telecomunicações). Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, São José – SC, 2021. Disponível em: https://wiki.sj.ifsc.edu.br/images/f/f9/Projeto_de_TCC_Murilo_Bauer.pdf. Acesso em: 01 jun. 2022.

BLEFARI, Rodrigo et al. Mecanismo de Priorização em Segurança da Informação para um ambiente de Computação em Nuvem Pública. In: **I FatecSeg - Congresso de Segurança da Informação**, Santana de Parnaíba/SP, 2021. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/download/16/1. Acesso em: 30 mar. 2022.

CHAVES, Bruno Duruteu; CASTRO, Bruno Guilherme Dias de; NASCIMENTO, Leuzimar Júnio Souza. **Estudo comparativo entre cloud computing e infraestrutura de rede local.** 2021. 30f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Centro Universitário do Planalto Central Apparecido dos Santos, 2021. Disponível em: https://dspace.uniceplac.edu.br/handle/123456789/914. Acesso em: 01 jun. 2022.

CHEE, Brian J. S.; FRANKLIN JÚNIOR, Curtis. **Computação em Nuvem** - Cloud Computing: Tecnologias e Estratégias. São Paulo: M.Books, 2013.

CISOADVISOR. **Google amplia segurança de nuvem com memória criptografada** [*on line*], 17/07/2020. Disponível em: https://www.cisoadvisor.com.br/google-amplia-seguranca-em-nuvem-com-memoria-criptografada/. Acesso em: 15 mar. 2022.

COUTINHO, Luís Rafaeli; NEVES, Henrique Pereira Oliveira d'Eça; LOPES, Lecian Cardoso. Abordagens sobre computação na nuvem: uma breve revisão sobre segurança e privacidade aplicada a e-saúde no contexto do Programa Conecte SUS e Rede Nacional de Dados em Saúde (RNDS). ***Brazilian Journal of Development***, Curitiba, v.7, n.4, p. 35152-35170, abr./2021. Disponível em: https://www.brazilianjournals.com/index.php/BRJD/article/download/27732/21936. Acesso em: 01 jun. 2022.

FERNANDES, Daniel Brito. **Projeto de aplicação em cloud computing.** 2021. 44f. Trabalho de Conclusão de Curso (Graduação - Engenharia de Computação). Universidade Federal do Rio Grande do Norte – UFRN. Departamento de Engenharia de Computação e Automação – DCA, Natal, 2021. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/38070/1/ProjetoAplicacaoCloudComputing_Fernandes_2021.pdf. Acesso em: 01 jun. 2022.

FERREIRA, António Miguel. **Introdução ao Cloud Computing. IaaS, PaaS, SaaS, Tecnologia, Conceito e Modelos de Negócio**. São Paulo: FCA, 2015.

FONTES, Edison. **Segurança da Informação:** Gestão e Governança: (Conformidade para a LGPD). São Paulo: Edição do Autor, 2020.

FORTINET. **Google Cloud Security com Fortinet Security Fabric**. [*on line*], 2022. Disponível em: https://www.fortinet.com/br/products/public-cloud-security/gcp. Acesso em: 30 mar. 2022.

GOOGLE. **A proteção da sua privacidade começa com a segurança mais avançada do mundo** [*on line*], 2022a. Disponível em: https://safety.google/intl/pt-BR/security/built-in-protection/. Acesso em: 30 mar. 2022.

GOOGLE. **Segurança e confiança do Google Workspace**. [*on line*], 2022b. Disponível em: https://workspace.google.com/intl/pt-BR/security/?secure-by-design_activeEl=data-centers. Acesso em: 01 jun. 2022.

GOOGLE. **Threat Horizons Cloud Threat Intelligence.** Google's Cybersecurity Action Team. November 2021. Disponível em: https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf. Acesso em: 15 mar. 2022.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação**: com Base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

ITFORUM. **Google Cloud lança novas ferramentas de segurança para o setor público e privado** [*on line*], 21 de julho de 2021. Disponível em: https://itforum.com.br/noticias/pegasus-50-mil-numeros-de-telefone-estao-na-lista-de-possiveis-ataques-com-spyware-israelense/. Acesso em: 01 jun. 2022.

JENSEN, Nikolas; MIERS, Charles C. Uma análise das vulnerabilidades de segurança do Kubernetes. In: 19º Escola Regional de Redes de Computadores (ERRC). In: **Anais [...].** Porto Alegre: Sociedade Brasileira de Computação, 2021. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/18544/18377. Acesso em: 27 abr. 2022.

LIMA, Adriano Carlos de. **Segurança na computação em nuvem**. São Paulo: Senac, 2018. (Série Universitária). eBook Kindle

LIMA, Elton Celestino de. **Uma metodologia para avaliação multicritério da tomada de decisão sobre adoção de serviços de nuvem SaaS ou local.** 2020. 42 f. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores). Universidade Federal do Ceará, Campus de Quixadá, Quixadá, 2020. Disponível em: https://repositorio.ufc.br/handle/riufc/59041. Acesso em: 27 abr. 2022.

LIMA, Geycy Dyany Oliveira. **ARQDEP:** arquitetura de computação em nuvem com dependabilidade. 2014. 172 f. Dissertação (Mestrado em Ciências Exatas e da Terra). Universidade Federal de Uberlândia, Uberlândia, 2014. Disponível em: https://repositorio.ufu.br/handle/123456789/12557. Acesso em: 30 mar. 2022.

LINS, Kennedy Bezerra da Silva. **Estudo para implementação de uma nuvem híbrida na Agência Estadual de Meio Ambiente de Pernambuco - CPRH/PE.** 2020. 55f. Trabalho de conclusão de curso (Graduação – Sistemas de Informação). Universidade Federal de Pernambuco, Recife, 2020. Disponível em: https://www.cin.ufpe.br/~tg/2020-3/TG_SI/tg_kbsl.pdf. Acesso em: 27 abr. 2022.

MARTINS, Antonio Adriano. **CISEF - Segurança Cibernética**: Uma Questão de Sobrevivência. São Paulo: Independently Published, 2021.

MARTINS, Claylson. Google Cloud lança novas ferramentas de segurança. **SempreUpdate** [*on line*], 20/07/2021. Disponível em: https://sempreupdate.com.br/google-cloud-lanca-novas-ferramentas-de-seguranca. Acesso em: 15 mar. 2022.

MATRIX. Flexera. **2021 State Of The Cloud Report**. 2021. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F149480%2F1647516745report-state-of-the-cloud-2021.matrix.pdf. Acesso em: 27 abr. 2022.

MEDEIROS, Thiago; CAMPOS, Carlos Alberto. ARTSIA: Escalabilidade de Aplicações para Sistemas Inteligentes de Transportes em um Ambiente de Computação em Neblina. In: **Simpósio Brasileiro De Engenharia De Sistemas Computacionais (SBESC)**, 10, 2020, Evento Online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 73-80. Disponível em: https://sol.sbc.org.br/index.php/sbesc_estendido/article/view/13093. Acesso em: 30 mar. 2022.

MELO, Henning Barly Summer de. **Uma proposta para o uso de progressive web apps em ambientes de computação móvel em nuvens**. 2020. 79f. Trabalho de Conclusão de Curso (Especialização em Gestão e Qualidade em Tecnologia da Informação e Comunicação). Instituto Federal de Educação, Ciência e Tecnologia, Campus Jaboatão Dos Guararapes, Campus Jaboatão dos Guararapes/PE, 2020. Disponível em: https://repositorio.ifpe.edu.br/xmlui/bitstream/handle/123456789/171/TCC_IFPE_Henning_Summer_2020_GQTIC_CBIM.pdf?sequence=1&isAllowed=y. Acesso em: 27 abr. 2022.

MENDONÇA, Cláudio Márcio Campos de; SOUSA NETO, Manoel Veras de. Serviço da computação em nuvem e sua relação com os arranjos de Governança de TI e o alinhamento estratégico. **Revista de Tecnologia Aplicada (RTA).** v.8, n.2, p. 41-62. mai-ago, 2019.

MIRANDA, Marcelo dos Santos. **Soluções de infraestrutura hiperconvergente em datacenters.** 2020. 20f. Trabalho de Conclusão do Curso (Especialização em Datacenter: Projeto, Operação e Serviços). Universidade do Sul de Santa Catarina, Florianópolis,2020. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/4026/1/MARCELO_DOS_SANTOS_MIRANDA_artigo_ad6_apos_defesa.pdf. Acesso em: 15 mar. 2022.

MOLINARI, Leonardo. **Cloud Computing**: A inteligência na nuvem e seu novo valor em TI. São Paulo: Érica, 2017.

MORETTI, Raphael Hungaro. **Soluções de segurança da informação**. São Paulo: Senac, 2022.

MOURA, Eduardo Henrique de Carvalho. **Autonomic security model for cloud computing with using honeypot**. 2019. 92 f. Dissertação (Mestrado em Engenharia de Computação). Universidade Federal do Maranhão, São Luís, 2019. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/516. Acesso em: 20 abr. 2022.

NEPOMUCENO, Késsia Thais Cavalcanti; NEPOMUCENO, Thyago Celso Cavalcante; SADOK, Djamel Fawzi Hadj. Measuring the Internet Technical Efficiency: A Ranking for the World Wide Web Pages**. IEEE Latin America Transactions**, [S. l.], v. 18, n. 6, p. 1119–1125, 2020. Disponível em: https://latamt.ieeer9.org/index.php/transactions/article/view/1747. Acesso em: 20 abr. 2022.

OLIVEIRA, A. C.; SPOHN, M. Escalonamento de máquinas virtuais baseado em custo e tolerante a anomalias de tráfego de rede para Dados-como-Serviço. **Revista Brasileira de Computação Aplicada**, v. 12, n. 3, p. 85-96, 17 set. 2020. Disponível em: http://seer.upf.br/index.php/rbca/article/view/11220. Acesso em: 15 mar. 2022.

OLIVEIRA, Vinícius Eduardo. **Abordagem baseada em clusterização e em Redes Neurais Artificiais para detecção de intrusão em dispositivos IoT**. 2020. 82 p. Trabalho de Conclusão de Curso (Graduação - Sistema de Informação). Universidade Federal de Santa Catarina, Florianópolis, 2020. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/218116/Monografia.pdf?sequence=1&isAllowed=y. Acesso em: 15 mar. 2022.

PALOALTONETWORKS. **Segurança nativa da nuvem criada para o Google Cloud** [on line], 2022. Disponível em: https://www.paloaltonetworks.com.br/prisma/environments/gcp. Acesso em: 20 abr. 2022.

QUEIROZ, Caio Weliton Nascimento. **Uma comparação entre arquiteturas convencional e serverless utilizando atributos de qualidade em aplicações eHealth.** 2020. 70 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de *Software*). Universidade Federal do Ceará, Campus de Quixadá, Quixadá, 2020.

Disponível em: https://repositorio.ufc.br/handle/riufc/58823. Acesso em: 15 mar. 2022.

REIS, Thiago Nelson Faria dos. **Um Recomendador de Alocação de Recursos em Computação em Nuvem usando Algoritmos Genéticos e SVR**. 2018.73 f. Dissertação (Mestrado em Ciência da Computação/CCET) - Universidade Federal do Maranhão, São Luís. 2018. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/2323. Acesso em: 27 abr. 2022.

RODRIGUES, Melody. **Computação em nuvem: Estudo de viabilidade**. 2011. 54f. Monografia (Especialização em Teleinformática e Redes de Computadores). Departamento de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2011. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/20004/2/CT_TELEINFO_XIX_2011_15.pdf. Acesso em: 30 mar. 2022.

ROSÁRIO, Djan de Almeida do. **Disponibilidade e qualidade Operacional de Datacenters:** Livro Digital. Unisul Virtual: Palhoça, 2016.

SALES, Ricardo Maia de. **Infraestrutura e operação de Datacenter**: levantamento de algumas estratégias para uma gestão mais eficiente. 2020. 24f. Trabalho de Conclusão do Curso (Especialização em Datacenter: Projeto, Operação e Serviços). Universidade do Sul de Santa Catarina, Florianópolis,2020. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/4007/1/%5b66231-64262%5dAD6_artigo_RMS_RevisaoFinal.pdf. Acesso em: 27 abr. 2022.

SANTOS, Tiago. **Fundamentos da computação em nuvem**. São Paulo: Senac, 2018. (Série Universitária). eBook Kindle

SCHIAVO, João Matheus Ampessan. **Cloud Computing**: uma questão de segurança. 2015. 34f. Monografia (Especialização em Gestão de Serviços de Telecomunicações). Programa de MGA, Centro Federal de Educação Tecnológica do Paraná. Curitiba, 2015. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/19362/2/CT-TELECOM-I-2015-03.pdf. Acesso em: 20 abr. 2022.

SILVA, Antônio Carlos. **Uma ferramenta para criação de clusters virtuais para execução de aplicações paralelas e distribuídas em nuvens públicas**. 2020. 41 f. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores)- Universidade Federal do Ceará, Campus de Quixadá, Quixadá, 2020. Disponível em: https://repositorio.ufc.br/handle/riufc/59040. Acesso em: 20 abr. 2022.

SILVA, Jorge Ribeiro Cunha da. **Experiência na implantação de plataforma de aplicativos em nuvem, para agregar novos produtos, serviços ou processos destinados a tecnologias de gestão para aumentar a eficácia e a qualidade às ofertas educacionais**. 2020. 28 f. Trabalhos de Conclusão de Curso (Especialização em Inovação em Educação e Tecnologias. Escola Nacional de Administração Pública (Enap), 2020 . Disponível em: https://repositorio.enap.gov.br/handle/1/6556. Acesso em: 15 mar. 2022.

SILVA, Wermeson Rocha da**. Estudo comparativo do impacto da segurança em ambientes de mobile cloud computing.** 2019. 64f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação). Campus de Crateús, Universidade Federal do Ceará, Crateús, 2019. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49203/1/2019_tcc_wrsilva.pdf. Acesso em: 27 abr. 2022.

SINGH, SK. **Cloud Computing**: Cloud Computing Fundamentals. KnoDAX, 2022. eBook Kindle

SOUSA NETO, Manoel Veras. **Computação em Nuvem.** Rio de Janeiro: Brasport, 2015. (eBook Kindle)

SOUSA, Matheus et al. Big data, machine learning e cloud computing na gestão de obras: uma revisão sistemática da literatura. In: **Encontro Nacional de Tecnologia no Ambiente Construído**, 2020. Anais [...]. Porto Alegre: ANTAC, 2020. p. 1–8. Disponível em: https://eventos.antac.org.br/index.php/entac/article/view/1186. Acesso em: 20 abr. 2022.

SOUZA, Jailson João de**. A importância da gestão e monitoramento de um datacenter.** 2019. 20f. Trabalho de Conclusão do Curso (Especialização em Datacenter: Projeto, Operação e Serviços). Universidade do Sul de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/3994/1/A%20IMPORT%c3%82NCIA%20DA%20GEST%c3%83O%20E%20MONITORAMENTO%20DE%20UM%20DATACENTER%20-%20Jailson%20Jo%c3%a3o%20de%20Souza.pdf. Acesso em: 15 mar. 2022.

TAURION, Cezar. ***Cloud Computing***: computação em nuvem. Rio de Janeiro: Brasport, 2009.

TEIXEIRA FILHO, Sócrates Arantes. **Segurança da Informação Descomplicada**. Curitiba: Clube de Autores, 2019.

TOKUMARU, Marcelo Seiji. **Computação em nuvem e o desafio de inovação das consultorias integradoras de sistemas**. 2019. Dissertação (Mestrado em Empreendedorismo) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2019. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12142/tde-18102019-182108/pt-br.php. Acesso em: 27 abr. 2022.

VARELLA, Walter Augusto**. Arquitetura de solução de computação em nuvem**. São Paulo: Senac, 2019b. (Série Universitária). eBook Kindle

VARELLA, Walter Augusto. **Implementação e migração para computação em nuvem.** São Paulo: Senac, 2019a. (Série Universitária). eBook Kindle

VERAS, Manoel**. Cloud Computing**: Nova Arquitetura de TI. Rio de Janeiro: Brasport, 2015.

VIEIRA, Cláudia Simone. **Computação em nuvem:** fatores que influenciam a adoção pelas empresas no Brasil. 2017. 106 f. Tese (Doutorado - Administração de

Empresas). Escola de Administração de Empresas de São Paulo. Fundação Getúlio Vargas, São Paulo, 2017. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/18024/Tese_Claudia_Vieira.pdf?sequence=1&isAllowed=y. Acesso em: 20 abr. 2022.

WOLLINGER, Sandro. **Datacenter modular abrigado em contêiner: vantagens e desvantagens.** 2020. 24f. Trabalho de Conclusão do Curso (Especialização em Datacenter: Projeto, Operação e Serviços). Universidade do Sul de Santa Catarina, Florianópolis,2020. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/4004/1/SANDRO_WOLLINGER-%5b64262-11299-2-871928%5dSandro_Wollinger_AD6_Datacenter_projeto_opera%c3%a7%c3%a3o_e_servi%c3%a7os.pdf. Acesso em: 30 mar. 2022.

ZAMBIASI, S. P.; RABELO, R. J. Arisa Nest – A Cloud-Based Platform for Development of Virtual Assistant. **Revista de Informática Teórica e Aplicada**, [S. l.], v. 27, n. 2, p. 116–126, 2020. Disponível em: https://www.seer.ufrgs.br/rita/article/view/RITA_VOL27_NR2_116. Acesso em: 15 mar. 2022.