PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA E DE ARTES

GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

USO DAS NORMAS NBR ISO/IEC 27017 E 27018 PARA GARANTIR A SEGURANÇA DA COMPUTAÇÃO EM NUVEM

HIANKA RODRIGUES SOUZA

GOIÂNIA

2023

HIANKA RODRIGUES SOUZA

USO DAS NORMAS NBR ISO/IEC 27017 E 27018 PARA GARANTIR A SEGURANÇA DA COMPUTAÇÃO EM NUVEM

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade de Goiás, como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia da Computação
Orientadora: Prof.ª Dr.ª Solange da Silva.

GOIÂNIA

2023

HIANKA RODRIGUES SOUZA

USO DAS NORMAS NBR ISO/IEC 27017 E 27018 PARA GARANTIR A SEGURANÇA DA COMPUTAÇÃO EM NUVEM

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia da Computação, e aprovada em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, em 16 / 12 / 2023 .

Banca examinadora:

Prof.ª Dr.ª Solange da Silva

Prof. Me. Fernando Gonçalves Abadia

Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA

2023

A minha mãe e ao meu pai por sempre me apoiarem na minha jornada.

AGRADECIMENTOS

Agradeço a Deus por estar ao meu lado nos momentos difíceis da minha vida.

Quero agradecer a minha mãe por possibilitar minha graduação na PUC GO e por me incentivar em todos os meus projetos, e ao meu pai por me apoiar em minhas decisões durante essa jornada. A minha irmã, agradeço pelos momentos em que me proporcionou clareza sobre conteúdos acadêmicos.

Agradeço a minha orientadora Solange da Silva pela paciência, dedicação e conselhos dados na orientação deste TCC, buscando junto comigo o sucesso.

Agradeço também todos meus professores da graduação e a todos que de alguma forma contribuíram com o desenvolvimento deste trabalho.

RESUMO

O objetivo deste trabalho foi o de abordar os principais conceitos e características da computação em nuvem, bem como as vulnerabilidades e ameaças relacionadas a segurança do ambiente em nuvem. A computação em nuvem é uma tecnologia que ganhou bastante destaque devido ao fato dela atender alguns dos principais requisitos que as empresas necessitam. Apesar das vantagens de seu uso é importante estar atento a questões de segurança. Nesse contexto há as normas NBR ISO/IEC 27017 e 27018, que são orientações de boas práticas para garantir a segurança no ambiente em nuvem e dos dados privados armazenados nela. De acordo com os procedimentos metodológicos esta pesquisa é bibliográfica. Os estudos permitiram concluir que a implementação das normas ISO/IEC 27017 e 27018 em ambientes de nuvem desempenha um papel fundamental na garantia da segurança e privacidade dos dados, reforça a confiança dos envolvidos e ajuda a manter a conformidade com regulamentações. Ao adotar essas normas, as organizações tornam-se mais preparadas para enfrentar os desafios crescentes associados à gestão de informações na nuvem.

Palavras chaves: Computação em nuvem. Segurança da Informação. Ciberataque. Normas de segurança NBR ISO.

ABSTRACT

The objective of this work was to address the main concepts and characteristics of cloud computing, as well as the vulnerabilities and threats related to the security of the cloud environment. Cloud computing is a technology that has gained a lot of attention due to the fact that it meets some of the main requirements that companies highlight. Despite the advantages of its use, it is important to be aware of security issues. In this context, there are the NBR ISO/IEC 27017 and 27018 standards, which are good practice guidelines to ensure security in the cloud environment and confidential data stored there. According to the methodological procedures, this research is bibliographic. The studies concluded that the implementation of ISO/IEC 27017 and 27018 standards in cloud environments plays a fundamental role in ensuring data security and privacy, reinforces the trust of those involved and helps maintain compliance with regulations. By adopting these standards, organizations become more prepared to face the growing challenges associated with managing information in the cloud.

Key words: Cloud computing. Security. Cyberattack. Data. Standard.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
API	*Application Programming Interface* ou Interface de programação de aplicação
AWS	*Amazon Web Service*
CPU	*Central Processing Unit* ou Central de processamento de dados
DoS	*Denial of Service* ou Negação de serviço
DDos	*Distributed Denial of Service* ou Negação de serviço distribuída
GDPR	*General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados
IaaS	*Infrastructure as a service* ou Infraestrutura como serviço
ICS	*Industry Control Systems* ou Sistemas de controle de Indústrias
IEC	*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional
ISMS	*Information Security Management System*
ISO	*International Organization for Standardization* ou Organização Internacional para Padronização
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
PaaS	*Platform as a service* ou Plataforma como serviço
SaaS	*Software as a service* ou Software como serviço
SGSI	Sistema de Gestão de Segurança da Informação
SGSI-C	Sistema de Gestão de Segurança da Informação para Serviços em Nuvem
SI	Segurança da Informação
SQL	*Structured Query Language* ou Linguagem de consulta estruturada
TCC	Trabalho de conclusão de curso
TI	Tecnologia da informação
ITMF	*Intelligent Traffic Management Finland Oy*

LISTA DE TABELAS

Sumário

1 INTRODUÇÃO

Com o desenvolvimento da sociedade ao longo dos anos, o uso de tecnologias no dia a dia das empresas se tornou algo comum. Tendo em visto o aumento da competitividade do mercado empresarial, houve a necessidade de buscar recursos para garantir a qualidade de seus produtos e serviços e, ao mesmo tempo, diminuindo os gastos (Avinte et al., 2019)

O aumento de informações e dados nos ambientes corporativos trouxe a necessidade de tecnologias com maior capacidade de processamento e armazenamento sem que tivessem que investir em grandes estruturas de hardware e software que ocupariam um extenso espaço na empresa e gerariam gastos com manutenção (Santos, 2018).

Tendo em vista tal necessidade, a computação em nuvem ou *cloud computing*, surgiu com o objetivo de disponibilizar sob demanda um conjunto compartilhado de recursos através da Internet, poupando gastos com, por exemplo, energia, manutenção, espaço de infraestrutura entre outros. Estes recursos podem ser facilmente alocados sem muito esforço de gerência e o cliente paga apenas por aquilo que ele usa (Coutinho et al., 2016).

A computação em nuvem se trata de uma combinação da evolução dos serviços da tecnologia da informação por demanda, também conhecida como *Utility Computing*. Esta tecnologia percursora da computação em nuvem oferece disponibilidade total de recursos por meio de um provedor especializado (Kadhim et al., 2018).

Levando em conta a demanda da empresa, a computação em nuvem oferece três tipos de modelo de serviços, sendo eles Plataforma como serviço (PaaS), Software como serviço (SaaS) e Infraestrutura como serviço (IaaS). Cada um deles tem risco, benefícios e utilidades diferentes (De Paula; Dian, 2021).

A *Amazon Web Services* (AWS) é uma das plataformas de computação em nuvem utilizadas por muitas empresas que buscam eficiência e redução de custos. Esta oferece cera de 200 serviços de datacenters que estão espalhados pelo mundo inteiro (AWS, 2022).

De acordo com os dados de pesquisas realizadas pela *Synergy Research Group* (2022), a Amazon dominou o mercado mundial de computação em nuvem no primeiro trimestre de 2022. A plataforma lidera com cerca de 33% de participação no mercado, e junto com a Microsoft (22%) e Google (10%) controlam cerca de 71% da receita.

Organizações de todos os tipos e portes podem usar computações em nuvem com diversos objetivos finais. A AWS garante uma infraestrutura global segura para atender todos os seus clientes com eficiência. Através dela a plataforma proporciona uma boa performance para os usuários. Além disso, oferece uma grande disponibilidade de rede (AWS, 2022).

Ao utilizar o serviço de computação em nuvem uma questão muito importante é colocada em pauta, a segurança dos dados. Por ser um serviço que reúne informações de um ou mais clientes, ele se torna um alvo para ataques. Tendo acesso aos dados de uma empresa a pessoa ou grupo mal-intencionado pode apagar, modificar ou até mesmo compartilhá-los (Rosy et al, 2019).

Segundo Lima (2018), o fornecedor do serviço deve garantir confidencialidade, integridade e disponibilidade aos dados do cliente. Para isto ter um plano de gerenciamento de risco é fundamental, pois com ele pode-se identificar a ação necessária a ser tomada com objetivo de minimizar os prejuízos.

A norma ABNT NBR ISSO/IEC 27017, dentre outras, estabelece um código de boas práticas para melhorar a segurança de serviços em nuvem para o cliente e para o provedor. Esta norma fornece diretrizes para diferentes tipos de implementações de serviços em nuvem para evitar ameaças. No entanto, para certificar que os serviços estejam seguros é necessário combinar o uso destas normas com outras, que abordem também questões de segurança e computação em nuvem (Gislaine, 2017).

Logo, justifica-se o presente estudo porque houve um grande aumento do uso de serviços de computação em nuvem pelas empresas, a fim de diminuir os custos e aumentar a eficiência. Apesar da grande quantidade de vantagens do uso da computação em nuvem é importante perceber que isso tudo torna o quesito segurança extremamente necessário. Com isso, as práticas de segurança contra riscos

existentes se tornaram algo essencial para evitar perdas, alterações e compartilhamento de dados (LANE, 2018).

Diante deste contexto, este trabalho visa responder a seguinte questão de pesquisa: - Como as normas ABNT NBR ISO/IEC 27017:2015 e 27018:2019 garantem a segurança na computação em nuvem?

O objetivo geral é identificar como as normas de segurança ABNT NBR ISO/IEC 27017:2015 e 27018:2019 garantem a segurança na computação em nuvem no ambiente empresarial e doméstico.

Os objetivos específicos são:

- Realizar uma revisão bibliográfica sobre computação na nuvem;
- Identificar ciberataques no meio empresarial;
- Mapear documentos e normas de segurança na computação em nuvem.
- Apresentar exemplos de usos destas normas no ambiente real.

Espera-se que os resultados deste trabalho possam contribuir com:

- Apresentando as normas existentes que garantem a segurança da computação em nuvem;
- Mostrando a importância das Políticas de Segurança em ambientes corporativos e domésticos;
- Alertando os administradores de nuvem sobre as vulnerabilidades existentes;
- Informando a comunidade sobre os ataques aos dados já conhecidos.

Esta monografia está estruturada da seguinte maneira, no capítulo 1 é introduzido o tema do trabalho, a questão de pesquisa, objetivo e resultados esperados. O capítulo 2 traz o referencial teórico com conceitos, definições, e trabalhos relacionados com o tema. No capítulo 3 é descrito o método, ou seja, como o trabalho foi desenvolvido e o que foi feito para que o objetivo geral fosse atingido. No capítulo 4 é apresentado os ataques mais comuns em ambiente em nuvem, apresentando as vulnerabilidades que os permitiram. Por conseguinte, no capítulo 4 é abordado normas e leis que recomendam boas práticas de segurança para computação em nuvem. No capítulo 5 são apresentados estudos de caso de implementação das normas NBR ISO/IEC 27017 e 27018, com foco nas melhorias experimentadas nas práticas de segurança da informação e proteção de dados. Por

fim, no capítulo 6 é apresentada a conclusão do Trabalho de Conclusão de Curso (TCC).

2 REFERENCIAL TEÓRICO

Este capítulo é composto por duas partes: uma de conceitos e definições e outra de trabalhos relacionados.

2.1 Conceitos e definições

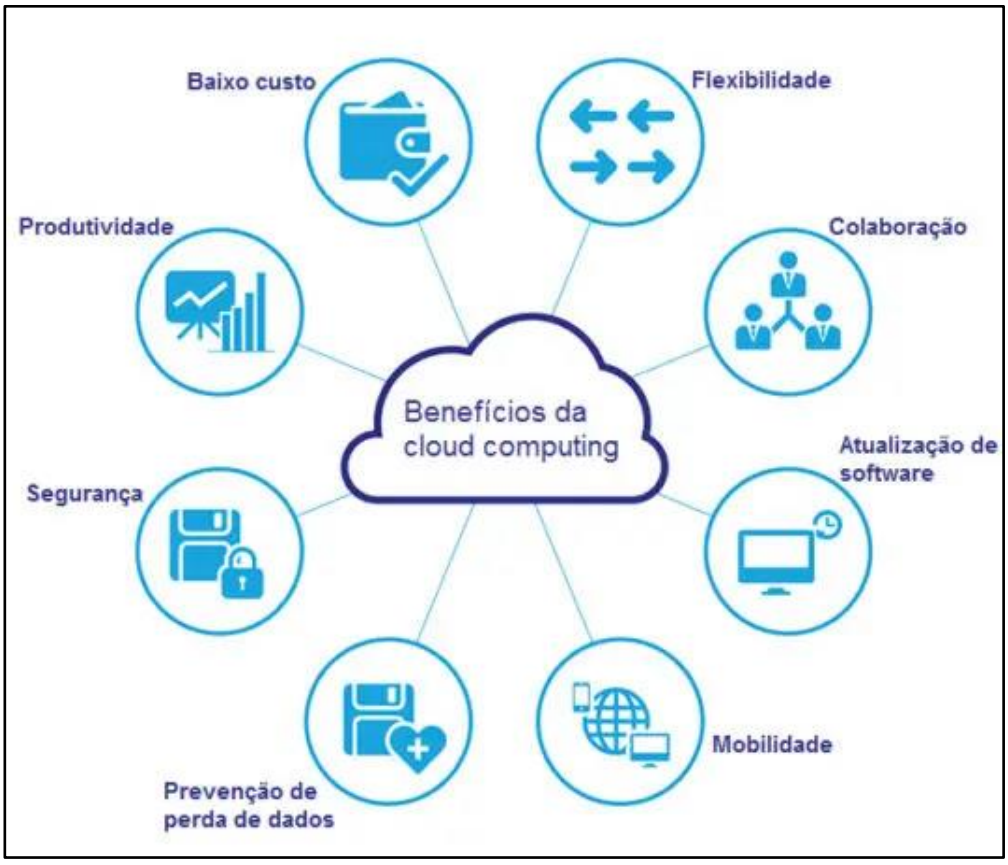
O rápido desenvolvimento e agregação de tecnologias no cotidiano das pessoas pode ser definido pelo termo tecnologia da informação (TI). Alecrim (2019), define este termo como atividades e soluções que foram produzidas por meios tecnológicos possibilitando gerenciar informações.

De acordo do Raju (2023), a computação em nuvem esta dentre um dos desenvolvimentos na área de TI que ganhou bastante destaque devido ao fato dela atender alguns dos principais requisitos que as empresas necessitam, sendo alguns deles: velocidade, inovação e crescimento.

O conceito de computação em nuvem pode ser definido como o fornecimento de recursos de TI, tais como processamento, armazenamento entre outros, através da internet. Tais recursos podem ser alocados de forma rápida e elástica para atender a necessidade dos usuários. O que possibilita o funcionamento dessa tecnologia é a operação em conjunto de diversos servidores, físicos ou virtuais, geralmente espalhados por várias localidades (Uriel et. al., 2022).

A Figura 1 ilustra as principais vantagens da computação em nuvem.

Figura 1 – Vantagens da computação em nuvem



Fonte: TI Open, 2021.

Levando em conta seus benefícios, computação em nuvem se tornou uma das tecnologias mais requisitadas pelas empresas com o passar dos anos. Dentre as várias empresas que oferecem tal serviço, a *Amazon Web Service* (AWS) se destaca como uma das pioneiras deste mercado, tendo iniciado em 2006. Atualmente no ano de 2023, está se encontra dentre as três empresas que lideram o mercado de computação em nuvem (Gupta et. al., 2021).

Não obstante, apesar da grande quantidade de vantagens do uso da computação em nuvem é importante perceber que isso tudo torna o quesito segurança extremamente necessário. Por armazenar e circular muitos dados, garantir a segurança da computação em nuvem tornou-se algo crucial. Nesse sentido, os provedores de nuvem devem buscar conhecer os riscos de ciberataques existem a fim de evitá-los (Araújo, 2020).

Um ciberataque é um crime. Ele consiste em ações não autorizadas dirigidas contra um sistema de informação, com objetivo de prejudicar a pessoa ou organização, de alguma forma. Tais ações podem ser realizadas de diversos tipos como, por exemplo, ataque a banco de dados ou criptografia de dados, buscando extorquir, destruir informações, expor ou alterar dados, entre outros (Martins, 2022).

Governança de TI é o conjunto de padrões e procedimentos que cada organização define para seu departamento de tecnologia da informação. Eles são determinados com base nos requisitos da indústria e nos valores internos da empresa. Esses parâmetros também determinam as responsabilidades de cada departamento e o resultado esperado de cada atividade realizada pela equipe (Lourenço, 2022).

2.2 Modelos de nuvem

Segundo Lorenzi (2022), existem três modelos de implantação da computação em nuvem, sendo eles privada, publica e híbrida. A escolha de qual será usada depende da necessidade de cada cliente, pois cada modelo tem suas vantagens e desvantagens.

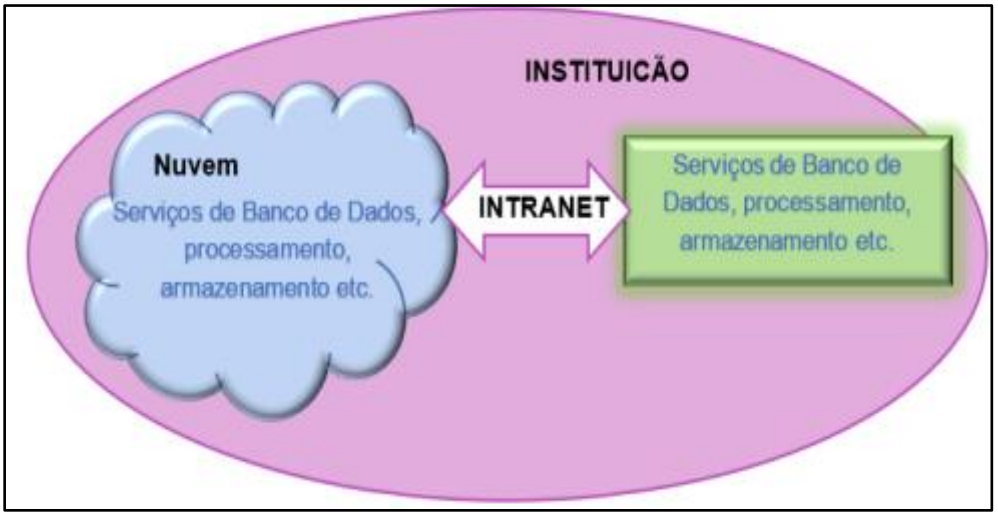
2.3 Nuvem privada

De acordo com Tavbulatova (2020), pode-se definir a nuvem privada como aquela cujo recursos são usados e pertencem a uma organização em particular. Nesse sentido, os serviços fazem parte de uma rede privada de usuários com infraestrutura dedicada a organização. Estes recursos podem ser tanto físicos, hospedados no ambiente da empresa nos *data centers*, quanto terceirizados por um provedor de nuvem.

O uso da nuvem privada traz consigo vantagens, mas a que mais se destaca é a questão de ter maior controle. Devido ao fato de que os recursos são compartilhados apenas com os usuários internos, torna-se possível personalizar e controlar os recursos de acordo com a necessidade da organização para garantir maior produtividade. Ademais, por não ser acessível ao público geral, este modelo oferece mais eficiência e agilidade aos usuários da organização (Nasereddin, 2021).

Outra vantagem é que a nuvem privada garante mais segurança. O tráfego de informações é limitado as operações da organização. Embora não seja impossível, é menos provável que haja tráfego malicioso, já que o público em geral não tem acesso à rede. Quanto a segurança física da nuvem, este modelo de nuvem consegue lidar melhor com isto, pois o equipamento em geral é gerenciado pela organização e os computadores que têm acesso fazem parte de um grupo restrito (Fernandes, 2022). A Figura 2 ilustra o esquema de uma nuvem privada.

Figura 2 – Modelo de nuvem privada



Fonte: Silva, 2019.

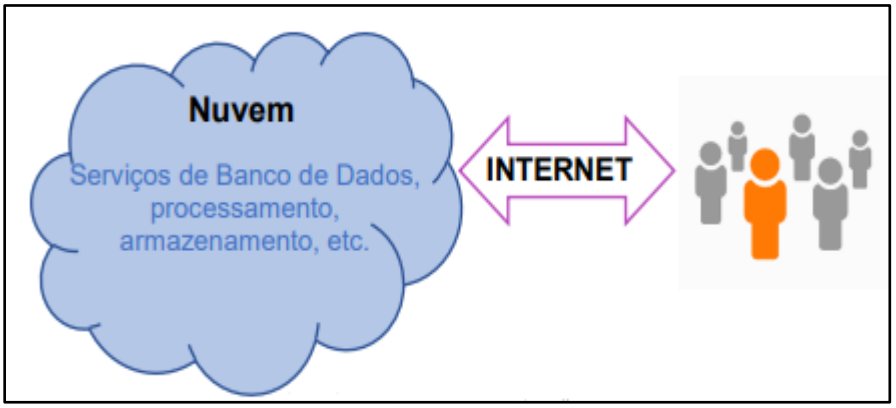
2.4 Nuvem pública

Tendo como uma das principais características uma arquitetura multi-inquilino, o modelo de nuvem pública é gerenciado por um provedor de serviços terceirizado. Por este motivo, a gerência de recursos e infraestrutura é de responsabilidade do provedor, cabendo ao cliente apenas o acesso pela Internet (Lorenzi, 2022).

Este modelo de nuvem oferece serviços do tipo “pague pelo que usar”, os recursos requisitados pelo cliente são sob demanda. Nesse viés, pode-se destacar vantagens como maior escalabilidade de recursos conforme a necessidade do cliente. Ao contrário da nuvem privada, a pública possui uma grande vantagem financeira, ela

reduz de custos da empresa com hardware, software, infraestrutura e manutenção. A Figura 3 mostra o esquema de uma nuvem pública.

Figura 3 - Modelo de nuvem pública



Fonte: Silva, 2019.

2.5 Nuvem híbrida

A nuvem híbrida é uma combinação da privada e pública. O uso deste modelo se destaca pela vantagem de aproveitar pontos positivos de ambas, ao mesmo tempo. As organizações podem aproveitar a infraestrutura de uma nuvem privada garantindo maior segurança e mantendo alguns recursos de baixa prioridade na pública (Silva, 2023).

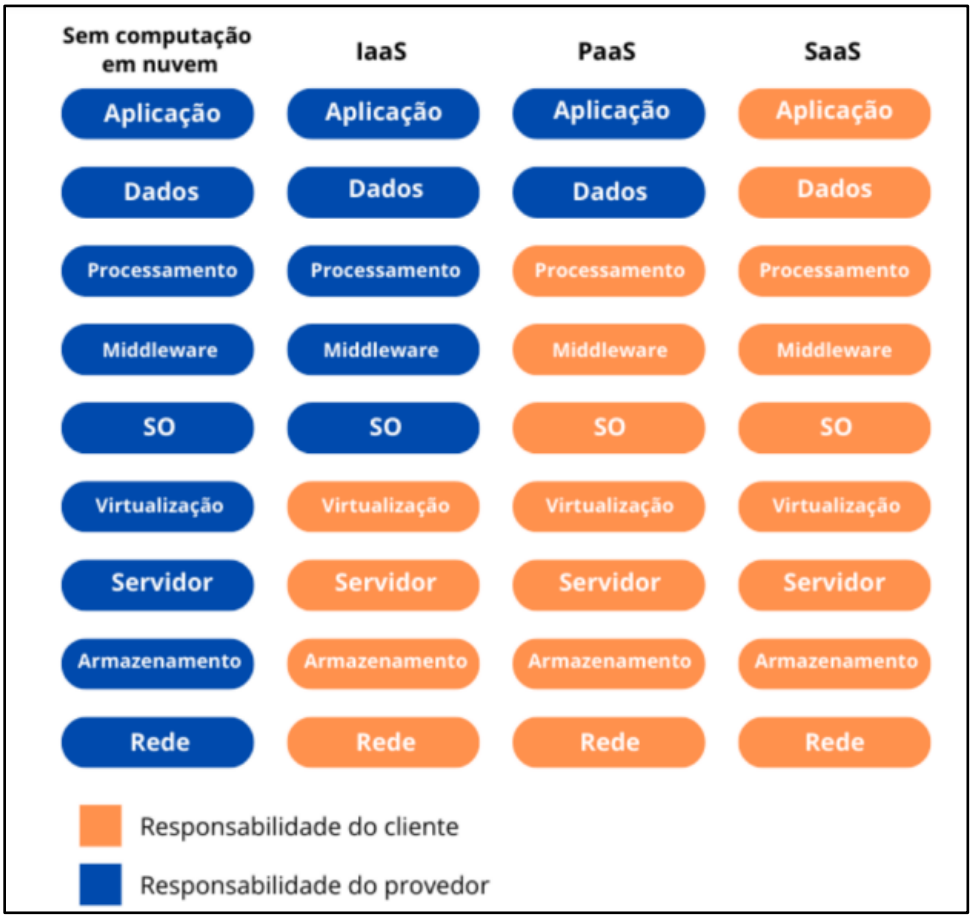
Deste modo, torna-se possível atender necessidades de escalonamentos rápidos para atender alguma demanda, flexibilidade e redução de custo e ao mesmo tempo ter controle sobre seus dados mais sensíveis. No entanto, sua implementação é algo mais complexo. É necessária uma boa equipe de gestão para administrar e integrar as várias plataformas e dados utilizados pela empresa, o que acaba não saindo barato para o cliente (Santos, 2018).

2.6 Modelos de serviço

Se tratando dos serviços oferecidos pela computação em nuvem, pode-se dividi-los em três modelos diferentes, sendo eles Infraestrutura como Serviços ou em inglês *Infrastructure as a service* (IaaS), Software como Serviço ou em inglês *Software*

as a service (SaaS) e plataforma como serviço ou em inglês *Platform as a service* (PaaS). Cada um deste possui suas vantagens dependendo da demanda de serviços da empresa (Rashid, 2019). A Figura 4 mostra uma comparação entre os modelos, destacando os principais itens fornecidos por cada um.

Figura 4 - Comparação dos modelos de serviço



Fonte: Bandeira, 2022.

2.7 IaaS – Infraestrutura como serviço

Para empresas de porte menor, nem sempre era viável financeiramente manter um *datacenter* próprio na organização. Os recursos que tinham disponíveis não eram utilizados totalmente, então manter gastos com hardwares e manutenções não seria o ideal (Avinte, 2019). Nesse sentido, entra a IaaS oferecendo a infraestrutura necessária para o funcionamento da empresa. Esse serviço é possível devido a virtualização. Com ela o cliente pode acessar os recursos adquiridos tais como armazenamento, processamento, máquinas virtuais entre outros pela Internet (Coutinho, 2016).

Este serviço se tornou atraente para as empresas devido a vantagem da redução de gastos. O cliente se livra da responsabilidade de cuidar de equipamentos físicos, alugando apenas aquilo que sua demanda carece pelo tempo que for necessário. A provedora de serviços em nuvem fica sendo a responsável pelo gerenciamento da infraestrutura (Rashid, 2019).

2.8 SaaS – Software como serviço

Esse modelo de negócio é muito buscado pela sua integração simplificada e demais vantagens. Quando se trata de SaaS, o produto oferecido pelo serviço é software, acessado pela Internet, para realização de diversas tarefas. O cliente não precisa se preocupar com licenças, renovações, atualizações etc., pois tudo isso é de responsabilidade do provedor de serviços (Loukis, 2019).

Este serviço SaaS se destacou bastante em relação as empresas de softwares convencionais. Enquanto estas necessitavam que seus clientes instalassem o software localmente, com o SaaS isso foi deixado de lado, passando a ser hospedado na nuvem, permitindo que o usuário acesse o software de qualquer dispositivo pela Internet (Martins, 2019).

Um exemplo de um cenário muito comum no qual se utiliza SaaS no cotidiano das pessoas é o acesso a e-mails. Geralmente, o usuário acessa por meio de um navegador WEB e, com a conta pessoal, é possível ter acesso a tais e-mails. Tanto o software, como os dados são armazenados na rede do provedor de serviço, tornando possível que os usuários acessem seus dados por computadores e celulares, podem ser vários dispositivos diferentes (Raghavan, 2020).

2.9 PaaS – Plataforma como serviço

Buscada principalmente por empresas desenvolvedoras de software, a PaaS diferentemente do SaaS, oferece uma plataforma completa para desenvolvimento na nuvem. Como o próprio nome já diz, o principal item oferecido é uma plataforma bem equipada com ferramentas para desenvolvimento de aplicações (Kolb, 2019).

Os clientes que adquirirem esta tecnologia pagam apenas pelo que usam. Os itens a serem contratados podem variar desde apenas sistemas operacionais á plataformas completas com servidores. Eles possuem a disposição banco de dados, ferramentas de desenvolvimento e segurança, *middlewares* entre outros itens (Martins, 2019).

A principal vantagem é que o cliente possui acesso aos produtos sem a preocupação em gerenciar e manter a infraestrutura responsável pela plataforma. Os usuários do serviço apenas configuram a infraestrutura e suas aplicações (Silva, 2019).

3 TRABALHOS RELACIONADOS

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

3.1 Implementação de um modelo de segurança para mitigação de vulnerabilidades em ambientes de armazenamento em nuvem baseado nas normas ISO 27017 e 27018

Conforme apresentado por Arias (2020), a computação em nuvem apesar das diversas vantagens possui suas vulnerabilidades. A autora analisou dados de instituições internacionais para identificar as vulnerabilidades mais comuns, e a partir destes dados elaborar um modelo de segurança para ser implementado em ambientes de armazenamento em nuvem.

O objetivo do trabalho desenvolvido foi implementar o modelo de segurança para garantir a segurança no ambiente, o controle de acesso e a detecção e resposta a incidentes. Dois senários foram analisados, o primeiro com o uso do modelo em um protótipo de armazenamento em nuvem e o segundo sem o modelo de segurança.

Como resultado foi possível obter um modelo com estratégias de segurança que reduziu em 75% a média da probabilidade de ocorrência de riscos comparada ao não uso do modelo.

3.2 Estudo sobre vulnerabilidades e implementação de um cenário de SQL *Injection*

Machado (2021), apresentou estudos para identificar e descrever as principais formas de ataques cibernéticos conhecidas, apresentando as vulnerabilidades. Como resultado a autora identificou os seguintes ataques: *Port Scanning Attack, Phishing, Spoofing, Sniffing* e *SQL (Structured Query Language* ou Linguagem de consulta estruturada) *Injection*. Os pontos de vulnerabilidade são: portas de rede desprotegidas, falta de conscientização dos funcionários e desenvolvedores, protocolos de segurança fracos e falta de boas práticas de segurança.

Com os resultados conclui-se que não existe uma única solução para evitar os ataques e resolver os problemas de vulnerabilidades de uma organização. Entretanto,

existem formas eficientes de proteção e boas práticas como, por exemplo, o treinamento dos funcionários e manter políticas de segurança em prática. Além disso, ter conhecimento dos principais tipos de ataques e como os ciber criminosos agem são fatores para manter a empresa protegida contra os ataques cibernéticos.

3.3 Gestão da segurança na computação em nuvem

Soares (2017) em seus estudos teve como objetivo discutir o tema segurança na computação em nuvem. Abordou-se como sua utilização cresceu, bem como as questões de segurança no ambiente em nuvem. Por fim, foram apresentados os principais serviços oferecidos.

O levantamento bibliográfico realizado pelos autores discorreu sobre o gerenciamento de redes. Tal gerenciamento é fundamental para compreender como surgiu a necessidade de uma tecnologia como a computação em nuvem e quais são as ameaças existentes. Foi apresentado também os serviços em nuvem sendo eles PaaS, IaaS e SaaS.

Por fim, conclui-se que lidar com a segurança neste ambiente não é algo fácil. As empresas que decidem migrar seus dados para nuvem devem ter isso em mente, é necessário analisar vários passos antes de tomar a decisão da migração a fim de evitar futuros problemas de segurança.

3.4 Sistema de gestão de segurança da informação para serviços em nuvem para a empresa "Massive" da cidade de Quito, baseado na ISO/IEC 27017

Imbat (2021), elaborou um trabalho cujo principal é projetar um Sistema de Gestão de Segurança da Informação para Serviços em Nuvem (SGSI-C) para a "Masiva", uma empresa equatoriana dedicada à prestação de serviços e aplicações na nuvem.

Foi utilizado como base as diretrizes estabelecidas na norma de boas práticas ISO/IEC 27017, que destacam a importância da aplicação de domínios de segurança, políticas, gestão de recursos humanos, controles de acesso e avaliação de riscos.

Primeiramente, foi feito a realização de uma análise dos riscos e vulnerabilidades atuais por meio da utilização de ferramentas de coleta de dados.

Posteriormente, foi realizada a abordagem do SGSI-C com as políticas baseadas nos critérios das normas consideradas aplicáveis para as necessidades da organização. Por fim, realizou-se uma validação através de uma matriz de correlação que indica cada documento que a organização deve cumprir para gerenciar corretamente a segurança da informação de seus serviços em nuvem.

4 MÉTODO

Este trabalho segundo sua natureza é um resumo de assunto. Fundamenta-se em trabalhos da área de conhecimento do projeto, buscando reunir, analisar, avaliar e discutir conhecimentos e informações (Wazlawick, 2014).

De acordo com Pereira *et. al.* (2018), segundo seus objetivos este trabalho classifica-se como exploratório e descritivo. Ele é caracterizado pela explicação dos fatos como eles são sem a interferência do pesquisador e como o primeiro estágio de um processo de pesquisa mais longo.

Segundo Wazlawick (2014), tratando-se dos procedimentos técnicos, este trabalho é bibliográfico. Estuda-se artigo, teses, livros entre outras publicações. Tal pesquisa é necessária, pois é com ela que o pesquisador vai fundamentar-se para prosseguir com sua pesquisa.

De acordo com Gil (2017), uma boa pesquisa bibliográfica segue minunciosamente as seguintes etapas:

- Escolha do tema da pesquisa: Uso das normas NBR ISO/IEC 27017 e 27018 para garantir a segurança da computação em nuvem;
- Levantamento bibliográfico preliminar: foi levado em consideração os últimos cinco anos, para garantir uma pesquisa atualizada, podendo haver exceções de literaturas clássicas;
- Formulação do problema: Como as normas ABNT NBR ISO/IEC 27017:2015 e 27018:2019 garantem a segurança na computação em nuvem?
- Busca das fontes: durante a busca utilizou plataformas como Periódicos CAPES, Google Scholar, entre outros. Foi feito uma filtragem de materiais onde eles foram separados por sua relevância na pesquisa. Essa separação foi feita a partir da leitura do resumo do trabalho para classificá-lo com relevância alta, média ou baixa. Além disso, durante esta etapa o autor pode anotar também bibliografias relevantes usadas nos artigos lidos;

- Leitura do material: tendo este material em mão, agora pode-se fazer uma filtragem selecionando aqueles artigos com maior relação ao tema a ser pesquisado.;
- Fichamento: foram fichados os trabalhos de alta relevância por ser uma etapa importante que, facilita a organização de ideias para a escrita do trabalho;
- Escrita do TCC.

Sendo assim, ao final destas etapas, foi possível realizar a escrita do TCC com uma base bem estruturada.

5 RISCOS E AMEAÇAS

Qualquer serviço conectado à Internet está sujeito a falhas e a vulnerabilidades de segurança, principalmente sobre os dados. Com a computação em nuvem não é diferente, à medida que esta tecnologia foi crescendo o quesito segurança foi ganhando bastante atenção. Por tratar dados de muitos usuários, ter sistemas de segurança robustos não é exagero. Nesse contexto, é importante conhecer os riscos existentes como objetivo de evitá-los (Araujo, 2020).

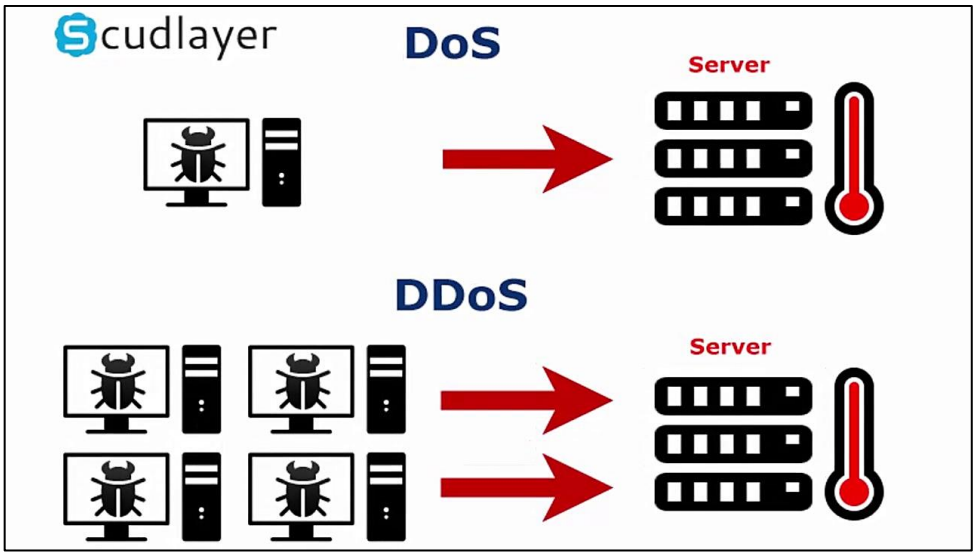
5.1 Ataques cibernéticos

Ataques cibernéticos são tentativa de indivíduos ou grupo de indivíduos mal-intencionados de roubar, destruir, modificar, expor ou usar para extorsão informações de outras pessoas ou organizações (Teixeira, 2021). Existem vários ataques diferentes e serão discutidos os principais que mais ocorrem no ambiente em nuvem.

Um ataque de negação de serviço ou no inglês *Denial of Service* (DoS) é feito com a intenção de impedir que os serviços do provedor sejam entregues. Ele é realizado por meio de várias requisições de um dispositivo ao sistema visando sobrecarregar seu processamento, largura de banca, CPU e memória. Deste modo, fica impedido aos usuários legítimos de usarem o serviço (Bonguet, 2017).

Ademais, este ataque pode ser feito também de forma distribuída, chamado de Negação Distribuída de Serviço ou em inglês *Distributed Denial of Service* (DDos). Em sua forma distribuída o ataque é feito por vários dispositivos, geralmente infectados por *malwares*. Assim que iniciado o ataque, estes vários dispositivos mandam muitas requisições ao servidor para sobrecarregá-lo. Por ser originado de vários lugares é mais difícil de ser detectado (Araújo, 2020). A figura 5 ilustra os ataques do tipo Dos e DDos.

Figura 5 – Ataques Dos e DDos



Fonte: SM!Tech, 2019.

Outro ataque são os *malwares* que são softwares maliciosos. O mais comum no ambiente em nuvem é o ataque de *ransomware*. Bem similar a um sequestro digital, nele o principal objetivo é a extorsão, os dados da vítima são criptografados e para que ela tenha acesso novamente a eles é exigido o pagamento de uma quantia em específico (Fornasier, 2020).

Há também o *phishing*, termo que surgiu da modificação da palavra na língua inglesa *fishing*, que significa pescar, pelo fato de que é deixado várias iscas pela internet para pescar informações confidenciais das vítimas. O golpe consiste em persuadir a vítima por meio de alguma telecomunicação, principalmente o e-mail, para extrair dados privados dela. Geralmente, o site ou e-mail contém mensagens e conteúdos similares a marca legitima, por exemplo, bancos ou sites de compras. Em seguida, é solicitado dados como login e senha ou número de cartões e a vítima acaba os revelando pensando se tratar de uma fonte válida (Pena, 2020).

Os ataques de injeção de SQL são uma das vulnerabilidades mais comuns em aplicativos da Web, porém podem ser explorados em um ambiente de computação em nuvem também. A injeção de SQL ocorre quando um invasor insere um código malicioso em uma consulta SQL enviada a um banco de dados, fazendo com que o banco de dados execute a consulta e retorne informações confidenciais ou execute

ações maliciosas. Essa situação pode ser agravada por falhas em *APIs* (*Application Programming Interface* ou Interface de programação de aplicação), pelo compartilhamento de recursos e a rápida escalabilidade da computação em nuvem, o que permite a rápida propagação de uma vulnerabilidade a vários usuários (Hajj, 2019).

Além disso, outro tipo de ataque que tem recebido muita atenção é o ataque de quebra de autenticação. Esse ataque ocorre quando um invasor consegue burlar ou comprometer o processo de autenticação, permitindo o acesso não autorizado ao sistema. Alguns exemplos de vulnerabilidades de autenticação em ambientes de nuvem incluem senhas fracas ou compartilhadas, autenticação de *API* insatisfatória e gerenciamento de identidade e acesso insatisfatório. Para evitar esses ataques, é importante seguir boas práticas de segurança, como o uso de senhas fortes e exclusivas, autenticação multifatorial, monitoramento de logs e gerenciamento rígido de acesso (David, 2022).

5.2 Vazamento de dados

Apesar das vantagens de armazenar dados em nuvem, estes ficam suscetíveis a possíveis vazamentos. A origem deste problema pode vir de várias áreas. Os ataques cibernéticos é um exemplo de um dos geradores de vazamentos de informações, seu objetivo esta dentre extorsão e exposição e pode ser de vários tipos como *malwares, phising, ramsoware* entre outros (Fernandes, 2022).

Segundo Fernando (2022), a falha humana também é uma questão a ser discutida. A computação em nuvem pode apresentar brechas na segurança por ser programada, configurada e utilizada por pessoas, Tais brechas possibilitam que invasores se aproveitem para roubar dados. De acordo com a Verizon (2021), cerca de 85% dos problemas de vazamento são ocasionados por interação humana, seja ela de um funcionário do provedor de nuvem ou de um cliente.

Nesse contexto, é importante ter em mente que as ameaças à segurança de uma nuvem não vêm apenas de fora da organização. As ameaças internas vêm de dentro das organizações ou empresas que usam serviços em nuvem. Elas podem ser

causadas por funcionários mal-intencionados, negligentes ou fraudulentos, prestadores de serviços terceirizados e parceiros de negócios (Fernando, 2021).

Algumas medidas que podem ajudar a prevenir violações de dados em ambientes de nuvem incluem criptografia de dados, controles de acesso baseados em funções e o uso de firewalls e sistemas de detecção de segurança. Também é importante introduzir práticas de segurança cibernética em todos os níveis da organização, educar os funcionários sobre a importância da segurança dos dados e realizar auditorias de segurança regulares.

6 NORMAS DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM

A segurança da computação em nuvem é um assunto importante, e existem diversas normas e padrões que estabelecem orientações e melhores práticas para garantir a segurança de dados e sistemas em ambientes de nuvem (De Paula, 2021).

6.1 ABNT NBR ISO/IEC 27017:2015

ABNT NBR ISO/IEC 27017:2015 é uma norma que desenvolve diretrizes para segurança da informação (SI) em serviços de computação em nuvem. Foi desenvolvida de acordo com a norma ISO/IEC 27002, que é um conjunto de boas práticas para segurança da informação (Tabosa, 2022).

Esta norma fornece um conjunto de controles de segurança específicos para um ambiente em nuvem, incluindo orientações de como deve ser o gerenciamento de segurança, a governança, o gerenciamento de riscos, o gerenciamento de incidentes, a proteção de dados, privacidade e conformidade. O padrão é aplicado a todos os tipos de serviços oferecidos pela nuvem e se aplica também a organizações e provedores que usam ou fornecem serviços de computação em nuvem (Borges, 2019).

De acordo com a ABNT (2015), o uso da ISO/IEC 27017 auxilia as organizações a manterem as informações seguras em seus ambientes de nuvem, fornecendo uma boa estrutura para a implementação de controles de segurança específicos da nuvem. Além disso, pode ajudar a aumentar a confiança do cliente porque demonstra que as organizações estão tomando as medidas para proteger os dados.

Entre os principais tópicos abordados pela ISO/IEC 27017, pode-se destacar:

- Gerenciamento de segurança: a norma estabelece diretrizes para a definição de políticas e procedimentos para gerenciar a SI em ambientes de nuvem, incluindo a definição de responsabilidades e de papéis.
- Governança: é estabelecido instruções para o estabelecimento de uma estrutura de governança para a SI em ambientes de nuvem, incluindo a

definição de objetivos de segurança e a realização de avaliações de riscos.

- Gerenciamento de riscos: a norma fornece orientação para a gestão de riscos em ambientes de nuvem, incluindo a avaliação de riscos, a seleção de controles de segurança e a implementação de medidas de mitigação.
- Gestão de incidentes: a norma estabelece diretrizes para a gestão de incidentes de segurança em ambientes de nuvem, incluindo a definição de procedimentos para detectar, responder e relatar incidentes.
- Proteção de dados: a norma fornece orientação para a proteção de dados em ambientes de nuvem, incluindo a criptografia de dados em trânsito e em repouso, a definição de políticas para o uso de senhas e a realização de backups regulares.
- Privacidade: a norma estabelece diretrizes para a proteção da privacidade em ambientes de nuvem, incluindo a definição de políticas e procedimentos para o tratamento de informações pessoais.
- Conformidade: a norma fornece orientação para garantir a conformidade com requisitos regulatórios e legais em ambientes de nuvem.

Nesse contexto, a ISO/IEC 27017 é um padrão importante para a SI de serviços de computação em nuvem porque fornece uma estrutura clara para a implementação de controles de segurança específicos da nuvem. Esta norma complementa outras normas da série ISO/IEC 27000, como a ISO/IEC 27001 e a ISO/IEC 27002, que fornecem orientação para a implementação de sistemas de gerenciamento de segurança da informação (Tabosa, 2022).

A ISO/IEC 27017 foi desenvolvida por especialistas em segurança da informação de todo o mundo para ajudar as organizações a enfrentar os desafios específicos da SI em ambientes de nuvem. A norma é aplicável a organizações de todos os setores e portes, podendo ser utilizada em conjunto com outras normas e regulamentações, como a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (De Almendra, 2022).

O uso da ISO/IEC 27017 pode trazer muitos benefícios para as organizações que usam serviços em nuvem, incluindo a redução do risco de violações de segurança, aumento da confiança do cliente e conformidade com os requisitos regulamentares e legais. O padrão também pode ajudar as organizações a aumentar a eficiência operacional e reduzir custos ao estabelecer uma estrutura clara para a implementação de controles de segurança específicos da nuvem (Borges, 2019).

6.2 ABNT NBR ISO/IEC 27018:2019

De acordo com a ABNT (2019), esta norma técnica estabelece requisitos para a proteção da privacidade de dados pessoais em nuvens públicas, com base nos princípios estabelecidos na ISO/IEC 27002 e na LGPD.

É definido um guia composto por um conjunto de diretrizes que os provedores de serviços de computação em nuvem e os clientes devem seguir para garantir a proteção dos dados pessoais armazenados em nuvens públicas. Dentre as principais diretrizes desenvolvidas por esta norma, destacam-se:

- Política de privacidade: uma política clara e compreensível para os provedores de serviços de nuvem pública processarem dados pessoais, incluindo informações como a finalidade do processamento, o tipo de dados coletados, as medidas de segurança aplicadas e os direitos dos titulares dos dados. É importante que as políticas sejam atualizadas regularmente para refletir as mudanças na legislação e na prática de proteção de dados.
- Segurança da Informação: são medidas de segurança, como controles de acesso, criptografia, monitoramento de log e auditoria, para proteger os dados pessoais armazenados em nuvens públicas contra acesso não autorizado ou divulgação de informações. Os provedores de serviços de nuvem pública devem garantir a integridade e a confidencialidade dos dados pessoais e tomar medidas para garantir a disponibilidade dos dados em caso de falha técnica ou desastre natural.
- Gerenciamento de incidentes: estabelece um procedimento claro de notificação de violação de dados, determine a causa raiz de um incidente e implemente ações corretivas para evitar futuras violações. Os

provedores de serviços de nuvem pública devem notificar imediatamente os clientes e departamentos relevantes, em caso de violação de dados e ter planos de contingência para lidar com incidentes de segurança.

- Governança de dados: estabelece uma responsabilidade clara entre provedores de serviços de nuvem pública e clientes e defina práticas para coletar, armazenar e processar dados pessoais. Os provedores de serviços de nuvem pública devem garantir que as práticas de proteção de dados estejam em conformidade com a LGPD e outras leis aplicáveis, além de fornecer relatórios regulares sobre o processamento de dados pessoais.

A implementação da ABNT NBR ISO/IEC 27018:2019 é importante para garantir a privacidade dos dados pessoais na nuvem pública e cumprir as obrigações legais relacionadas à proteção de dados. Ao seguir as diretrizes definidas na norma, os provedores de serviços de nuvem pública podem garantir a confiança e a satisfação de seus clientes, além de proteger sua reputação e evitar sanções legais por violações de privacidade. O padrão também pode ajudar os clientes a escolher um provedor de serviços de nuvem pública confiável e tomar medidas apropriadas de proteção de dados pessoais (Aleixo, 2020).

7 ESTUDO DE CASOS USANDO AS NORMAS

Neste capítulo são apresentados estudos de caso de implementação das normas NBR ISO/IEC 27017 e 27018, com foco nas melhorias experimentadas nas práticas de segurança da informação e proteção de dados. O objetivo deste estudo de caso é analisar como a aplicação dessas normas contribuiu para aprimorar a segurança cibernética e a privacidade dos dados nas organizações.

7.1 *IMPLEMENTING A SECURITY MODEL FOR VULNERABILITY MITIGATION IN CLOUD STORAGE ENVIRONMENTS BASED ON ISO 27017 AND 27018 STANDARDS*

Este estudo foi realizado por Arias (2020). A segurança da informação em ambientes de armazenamento em nuvem é uma grande preocupação. A ISO/IEC 27017 fornece diretrizes para segurança da informação na nuvem, já a ISO/IEC 27018 estabelece diretrizes para proteção de dados pessoais nos ambientes digitais. Este artigo foi estudado para entender como a implementação desses padrões pode ajudar a mitigar vulnerabilidades na nuvem.

Propõe-se melhorar a segurança da informação através da implementação de um modelo de segurança para mitigar vulnerabilidades em ambientes de armazenamento na nuvem. Foi analisado qual o nível de melhoria de segurança com a implementação desse modelo com base nas Normas ISO 27017 e 27018.

A demonstração prática da pesquisa foi realizada em dois protótipos, no primeiro com uma solução de armazenamento em nuvem com a implementação de um modelo de segurança proposto (protótipo 1) e o segundo com um cenário que não considera a aplicação das normas (protótipo 2).

Posteriormente, a eficácia da implementação foi medida entre os dois cenários de teste do modelo de segurança da informação para armazenamento em nuvem.

- Implementação

O autor criou o modelo estabelecendo controles de segurança. Cada controle apresenta detalhes como se há obrigatoriedade ou não em sua implementação. Além

disso, apresentou também qual seu objetivo, quais os componentes relacionados a esse controle, quais os fatores de risco que ele abrange etc.

A tabela 1 apresenta os principais controles de segurança utilizados e seu tipo, ou seja, se é obrigatório ou apenas recomendado.

Tabela 1 – Controles de segurança implementados.

Controle de Segurança	**Tipo**
Proteção da plataforma de virtualização	Obrigatório
Proteção do ambiente de armazenamento em nuvem	Obrigatório
Proteção contra *malware*	Obrigatório
Integridade do banco de dados	Obrigatório
Monitor de integridade de arquivos	Recomendado
Planejamento de resposta a incidentes cibernéticos	Obrigatório
Testes de penetração	Recomendado
Política de senha	Obrigatório
Fortalecimento do Sistema	Obrigatório
Autenticação multifatorial	Obrigatório
Compromissos das partes	Obrigatório

Fonte: Autoria Própria.

Com isso, foram estabelecidos dois cenários de teste para análise de vulnerabilidades, sendo o primeiro contemplado pela aplicação das normas e o segundo não.

- Análise dos resultados.

O autor estabeleceu duas variáveis a serem analisadas sendo a primeira: Implementação de um modelo de segurança para mitigar vulnerabilidades em ambientes de armazenamento em nuvem, do tipo independente. E a segunda: Segurança da informação, do tipo dependente.

Para analisar os resultados da variável independente foram utilizados os seguintes indicadores:

1. Complexidade;

2. Facilidade de projeto e implementação;

3. Tempo de design e implementação;

4. Recursos necessários.

Já para a variável dependente os indicadores utilizados foram:

1. Número de vulnerabilidades;

2. Número de riscos mitigados;

3. Número de registros encontrados.

A partir destes indicadores realizou-se uma análise e classificação do protótipo 1 e 2. Por fim, as conclusões obtidas foram:

Para a variável independente:

Complexidade: o nível de complexidade em relação aos dois protótipos foi baixa, tendo em vista que quando elaborado uma estrutura clara de controles de segurança, o design e a implementação da solução de armazenamento em nuvem ficam simplificada.

Facilidade de projeto e implementação: a facilidade no desenho e implementação em relação à variável do Protótipo I ao II, é pouca pois o Protótipo I possui diretrizes, diretrizes para desenho e implementação enquanto no Protótipo II você tem que analisar uma estratégia para iniciar o desenho e implementação.

Tempo de design e implementação: Pode-se notar que o tempo de projeto e implementação em relação à variável do Protótipo I é muito pequeno comparado ao do Protótipo II, pois conforme mencionado no item anterior, o Protótipo II tem que considerar uma estratégia para iniciar o projeto e exigir implementação, o que exige mais esforço e tempo.

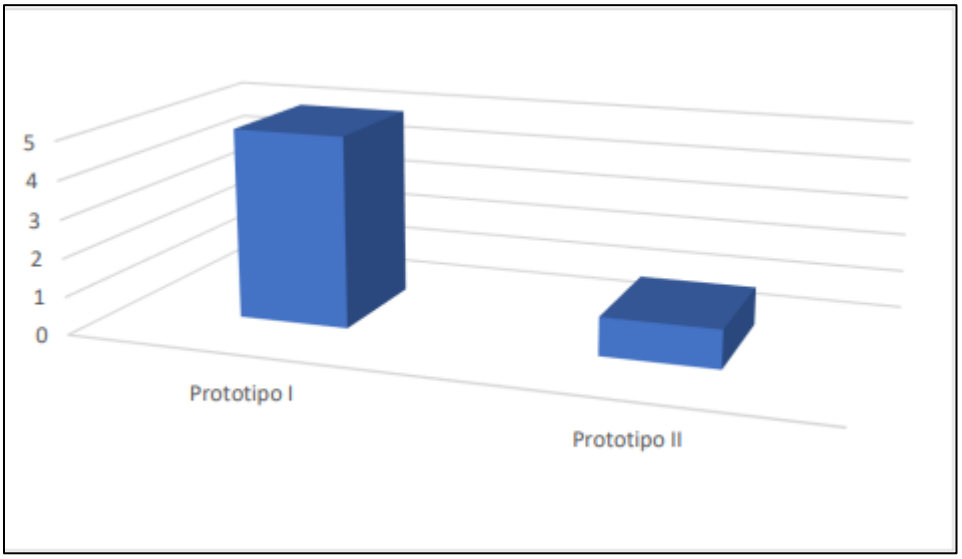
Recursos necessários: Os recursos necessários em relação à variável Protótipo I são muito poucos comparados ao Protótipo II, pois como as diretrizes e orientações a seguir no Protótipo II não são claras, é possível escolher recursos inadequados ou excessivos.

Para comparar os resultados obtidos dos indicadores da variável dependente foi utilizada a escala *Likert* para cada um.

No protótipo l o indicador 1 contabilizou um total de 10 vulnerabilidades, enquanto para o protótipo ll foram contabilizadas um total de 41 vulnerabilidades.

Sendo assim, de acordo com a escala *Likert* os protótipos receberam os códigos 5 e 1, respectivamente. O resultado dessa análise pode ser visualizado na Figura 6.

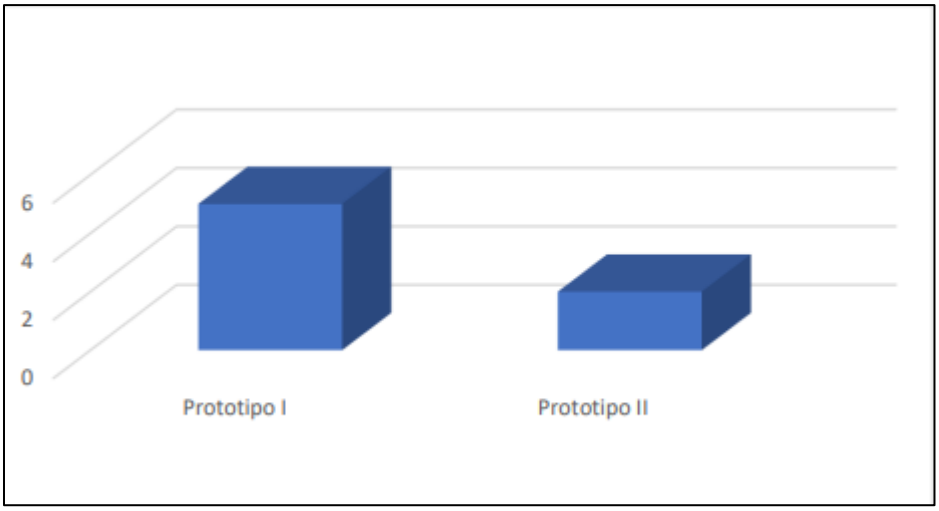
Figura 6 – Resultados obtidos para o indicador 1



Fonte: Tenelema, 2020.

No indicador número 2 foram contabilizados 2 riscos mitigados para o protótipo l, e 7 para o protótipo ll. Estes valores na escala representam 5 para o primeiro e 2 para o segundo. O resultado pode ser visualizado na Figura 7.

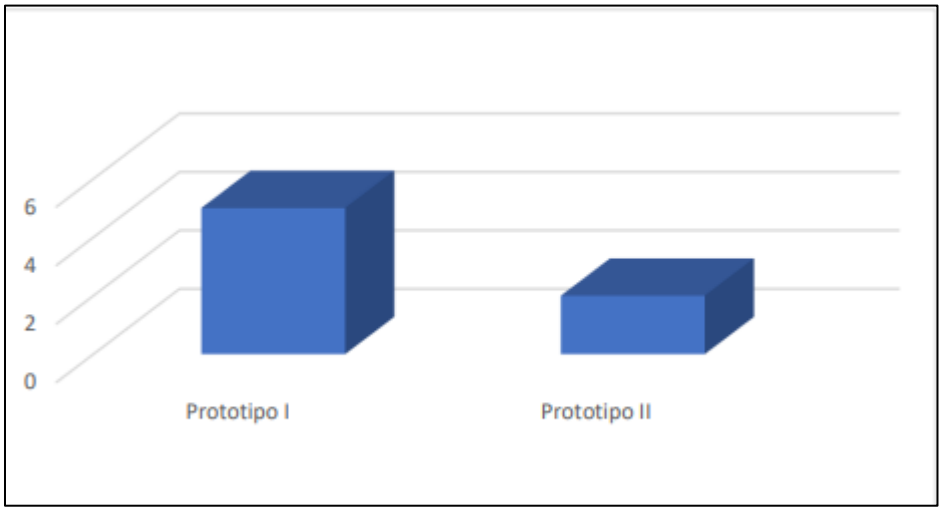
Figura 7 – Resultados obtidos para o indicador 2



Fonte: Tenelema, 2020

Por fim, para o indicador 3 foram contabilizados 8 logs para o primeiro protótipo, enquanto para o segundo foram contabilizados um total de 34 logs. Estes valores na escala representam respectivamente 5 e 2. O resultado pode ser visualizado na Figura 8.

Figura 8 - Resultados obtidos para o indicador 3



Fonte: Tenelema, 2020.

- Avaliação da eficácia das normas NBR ISO/IEC 27017 e 27018 na melhoria da segurança da informação e proteção de dados.

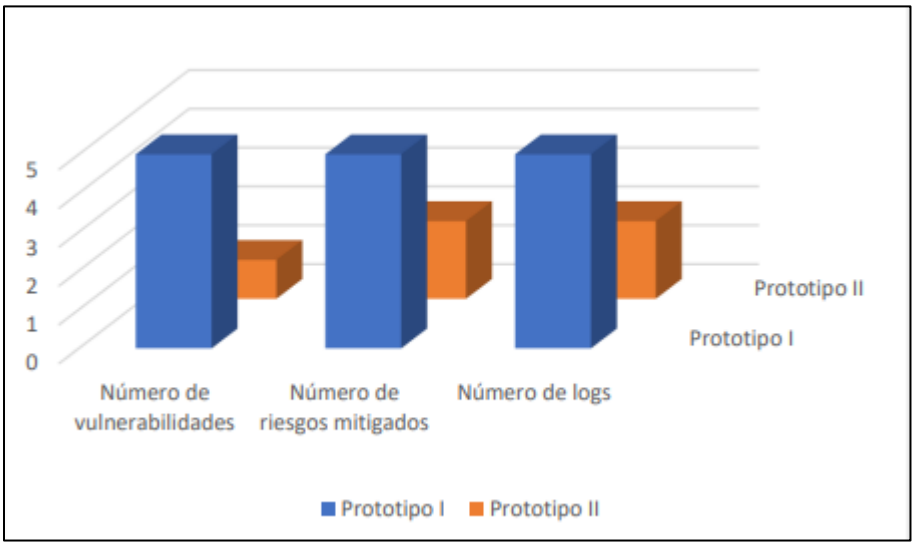
Foram utilizadas estatísticas descritivas e estatísticas inferenciais, considerando como fatores atenuantes:

- População: número de vulnerabilidades

- Amostra: número de vulnerabilidades encontradas com base na escala *Likert*.

A figura 9 mostra a comparação dos resultados obtidos para o protótipo I e para o protótipo 2 por cada um dos indicadores.

Figura 9 –Comparação de resultados dos indicadores



Fonte: Tenelema, 2020

Conclui-se então que a implementação de um modelo de segurança para armazenamento em nuvem implementado no Protótipo I é 75% mais seguro comparado ao Protótipo II que não o considera.

Para verificar a hipótese de pesquisa, foram atribuídos os seguintes valores à variável independente X os seguintes valores:

X = Implementação do modelo de Segurança;

X1 = Melhora a segurança;

X2 = Não melhora a segurança.

Estes valores verificaram o impacto em relação à variável dependente que é o número de vulnerabilidades, riscos mitigados e logs encontrados no Protótipo I e Protótipo II. Para o teste de hipótese proposto foi utilizado o teste qui-quadrado ou X^2 que é um teste não paramétrico através do qual a relação entre a variável dependente e o independente.

Além disso, foram consideradas a hipótese nula Ho e a hipótese de pesquisa Hi.

• Hi: A implementação de um modelo de segurança para mitigar vulnerabilidades em ambientes de armazenamento na nuvem, melhorará o nível de segurança da nuvem.

• Ho: A implementação de um modelo de segurança para mitigar vulnerabilidades em ambientes de armazenamento em nuvem, não melhorará o nível de segurança da nuvem.

Conclui-se que o valor calculado de X2 está no setor de rejeição da hipótese nula H0, e aceita-se a hipótese de pesquisa que for significativa, com nível de significância de α = 5% = 0,05 para obter um nível de confiança de 95%:

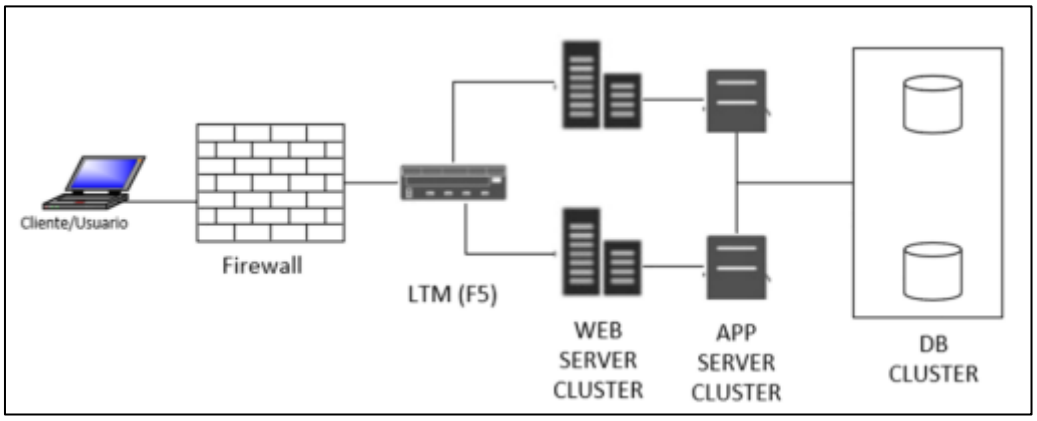
Recomenda-se que este modelo de segurança seja considerado ponto de partida para melhorar os níveis de segurança; pois devido ao constante crescimento de ameaças deve ser atualizado e melhorado.

7.2 *COMPARACIÓN DE MÉTODOS DE SEGURIDAD ENTRE CLOUD COMPUTING Y DATACENTER CONVENCIONALES UTILIZANDO NORMAS ISO 27001 Y 27017*

O autor Patricio (2022) teve como principal objetivo comparar os métodos de segurança entre *Cloud Computing* e *DataCenter* convencionais através das normas ISO 27001 e 27017, para determinar uma possível alternativa de segurança dentro deles.

Foi abordado diversas vantagens e desvantagens acerca da *Cloud* e de um *DataCenter* comum. As figuras 10 e 11 mostram a estrutura de cada um.

Figura 10 – Estrutura de um *DataCenter*

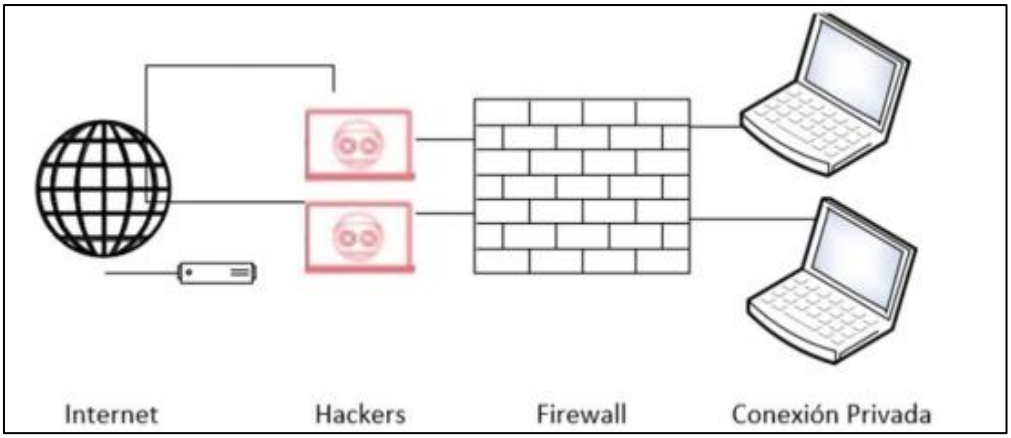


Fonte: Patricio, 2022.

Pode-se destacar entre as vantagens do *DataCenter:*

- Implantação simples sem perda de tempo;
- Escalável de acordo com as necessidades de uma organização;
- Um firewall é muito acessível, diagnosticável e escalonável.

Figura 11 – Estrutura da C*loud Computing*



Fonte: Patricio, 2022.

E algumas vantagens da *Cloud* são:

- Um design de firewall confiável e robusto;
- É necessário o melhor dos firewalls de perímetro e distribuídos para fornecer proteção de alto nível;

- A alta disponibilidade garante um fluxo de serviço contínuo e seguro, fontes de energia redundante e *backup* segurança automática.

Para validar o que foi apresentado no projeto de pesquisa, foram feitas entrevistas com especialistas da área de segurança entre *Cloud Computing* e *DataCenter* convencional utilizando as normas ISO 27001 e 27017.

Analisado as respostas das entrevistas, pode-se concluir que, entre os benefícios, a ISO 27017 fornece controles para provedores de serviços em nuvem e clientes e a ISO 27001 enfatiza a importância da comunicação entre a empresa e os clientes na determinação dos processos de gestão.

Quanto aos protocolos de segurança da informação, são regras ou padrões que garantem a confidencialidade, integridade e disponibilidade das informações. Estas são medidas de segurança tomadas para evitar que pessoas não autorizadas acessem, manipulem ou destruam informações,

Em relação às vantagens dos firewalls, pode-se dizer que esta tecnologia de nuvem pode ser considerada um produto de segurança, como os firewalls tradicionais, filtrando o tráfego de rede potencialmente perigoso. Eles formam uma barreira virtual em torno da plataforma, infraestrutura e aplicativos em nuvem, assim como os firewalls tradicionais formam uma barreira em torno da rede interna de uma empresa.

Os firewalls em nuvem também podem proteger a infraestrutura local. Este dispositivo é recomendado tanto para *Cloud Computing* quanto para *Data Centers* convencionais, pois filtra as informações que navegam na Internet e na rede respectivamente dependendo do serviço que irá prestar. Ao analisar os parâmetros necessários para a segurança dos dados, são criadas tabelas de comparação entre as vantagens, levando à conclusão de que *Cloud Computing* pode ser o mais adequado, pois o tráfego de informações não precisa ser roteado através de dispositivos de hardware, desta forma os ataques cibernéticos são evitados com mais eficiência e ao mesmo tempo gargalos na rede.

7.3 SECURE CLOUD IMPLEMENTATION IN GOVERNMENTAL ORGANIZATIONS

O estudo realizado por Lampikari (2020) fornece uma visão geral das principais questões de segurança que as organizações governamentais devem considerar ao planejar a implementação da computação em nuvem como parte de suas operações. O principal objetivo é esclarecer os principais elementos a serem focados no processo de seleção de um provedor de serviços em nuvem e quais áreas-chave precisam ser avaliadas e controladas da perspectiva do cliente durante e após a implementação da nuvem.

A organização do caso é a *Intelligent Traffic Management Finland Oy* (ITMF). Essa organização é uma subsidiária da *Traffic Management Finland* que opera sob a direção de propriedade do Ministério dos Transportes e Comunicações. A organização é um grupo de atribuição especial, e salvaguarda os serviços de controle de tráfego exigidos pela sociedade e pelas autoridades. Tem como objetivo garantir a fiabilidade das operações em caso de perturbações, tanto em circunstâncias normais como excepcionais, em terra, no ar e no mar.

Muitas das etapas que devem ser seguidas antes de contratar um provedor de serviços em nuvem parecem ser universais. Não existe um jeito específico que você possa usar para selecionar o melhor fornecedor para sua organização. Certificações e padrões são um bom ponto de partida para avaliar candidatos, e os clientes devem procurar provedores de serviços em nuvem com certificações reconhecidas, como a série de padrões ISO 27000.

O primeiro objetivo da pesquisa foi descobrir o que as organizações governamentais devem levar em consideração quando planejam implementar a computação em nuvem em geral. Descobriu-se que muitas das etapas que devem ser tomadas antes de contratar um fornecedor de serviços em nuvem são universais – os mesmos princípios aplicam-se a organizações governamentais e não governamentais e podem ser aplicados como tal à organização do caso.

O segundo objetivo é identificar os principais elementos relacionados ao gerenciamento e controle da segurança na nuvem. O gerenciamento da segurança na nuvem também se baseia na compreensão da responsabilidade compartilhada. A

terceirização para terceiros sempre envolve riscos. Vazamentos de dados, configurações incorretas e controle inadequado de alterações representam grandes ameaças à computação em nuvem. Os processos de auditoria e resposta a incidentes devem estar em vigor, e os clientes da nuvem devem estar cientes de quaisquer questões legais que possam surgir ao mover dados para a nuvem.

Nem sempre é fácil aplicar todas as políticas da sua organização à nuvem, mas é importante manter uma boa segurança. Uma vez introduzida a perspectiva do governo, começam a surgir diferenças e é necessária uma abordagem ligeiramente diferente. Os padrões de gerenciamento de controle e segurança em nuvem do governo visam identificar os tipos de sistemas, aplicativos e informações confidenciais envolvidos e, em seguida, planejar e implementar serviços em nuvem de acordo com os documentos e padrões acima.

O terceiro e último objetivo do estudo foi determinar se havia uma forma de compilar uma lista de melhores práticas que poderiam ser usadas para garantir a adoção da nuvem neste tipo de situações. Uma maneira mais fácil é listar um conjunto de práticas recomendadas e a chave é saber quais seguir. Em termos gerais, o conjunto de padrões da série ISO 27000 fornece uma grande quantidade de detalhes sobre segurança em ambientes de nuvem e quase qualquer organização pode consultá-lo para sua implementação.

Segundo o autor, pesquisas semelhantes nesta perspectiva específica não foram realizadas ou não estão disponíveis publicamente na Finlândia. Uma entrevista conduzida pelo Brigadeiro-General Finlandês Mikko Heiskanen apoiou esta última opinião, observando que as Forças de Defesa Finlandesas começaram recentemente a reavaliar a possibilidade de utilizar serviços em nuvem para apoiar operações.

Internacionalmente, existem vários estudos que avaliam questões semelhantes, mas em contextos ligeiramente diferentes. A maior parte da pesquisa relacionada à segurança na nuvem concentrou-se em questões mais específicas e detalhadas e não está de forma alguma relacionada a agências governamentais. Não está claro o porquê, mas é possível que este tipo de investigação não tenha a intenção de ser visível ao público. A exposição a audiências públicas pode ser prejudicial ao governo, especialmente por se tratar de uma investigação mais detalhada que podem ser expostas em audiências com intenções ilegais.

7.4 CLOUD SECURITY PRE-ASSESSMENT MODEL FOR CLOUD SERVICE PROVIDER BASED ON ISO/IEC 27017:2015 ADDITIONAL CONTROL

O autor Kamaruddin (2020) realizou estudos com o objetivo de aprimorar modelos existentes de avaliação de prontidão em nuvem e modelos de maturidade baseado em SGSI. Foi incorporado sete controles adicionais definidos na ISO/IEC 27017:2015 por meio do desenvolvimento de um pré-modelo de avaliação de prontidão de segurança para fornecedores de serviços em nuvem, fornecendo a eles um método para avaliar seu nível de prontidão em controles de segurança implementados em suas operações, que devem estar em conformidade com os padrões.

Nesse viés, o estudo possibilitou orientar os provedores a identificarem qualquer lacuna na implementação da segurança em nuvem de suas operações de serviços para que seja normalizada antes de enfrentar o processo de auditoria real por uma organização de certificação.

Este estudo utilizou modelos e estruturas que definiram a avaliação da arquitetura de prontidão da segurança da nuvem como linhas de base deste estudo. A seguir estão os modelos existentes de avaliação de prontidão para segurança em nuvem:

Estrutura 1: Estrutura de domínios;
Estrutura 2: Quadro de Avaliação da Preparação para a Nuvem;
Modelo 1: Modelo de Preparação para Sistemas de controle de Indústrias, ou no inglês *Industry Control Systems* (ICS) e *Cloud*;
Modelo 2: Modelo Hexagonal de Segurança em Nuvem.

A Estrutura 1 define critérios de segurança com base em domínios, sendo eles:

1. Organização;
2. Partes Interessadas;
3. Ferramentas e Tecnologia;
4. Política;
5. Cultura;
6. Conhecimento.

Eles são usados como base para avaliar o nível de prontidão da organização. A estrutura elabora 21 controles de segurança importantes retirados do padrão de gerenciamento de segurança da informação na ISO/IEC 27001:2013.

A Estrutura 2 foi construída com base na combinação de perspectivas da Organização-Ambiente Tecnológico, da Difusão de Inovação e do Modelo de Aceitação de Tecnologia. A partir desses critérios citados foi possível produzir 12 fatores de prontidão, sendo eles:

1. Utilidade Percebida;
2. Facilidade de Uso Percebida;
3. Vantagem Relativa;
4. Resultado Observável de Capacidade de Teste;
5. Compatibilidade com Valores e Práticas Existentes;
6. Suporte Executivo;
7. Business Case e Orçamento;
8. Número de Servidores de Prontidão Tecnológica;
9. Idade do Servidor de Prontidão Tecnológica;
10. Virtualização de Prontidão Tecnológica;
11. Conectividade de Rede;
12. Vantagem Competitiva.

O Modelo 1 é composto por quatro estágios que avaliam a segurança da informação nos componentes de ICS e na implantação da computação em nuvem como infraestrutura de TI. As etapas são definidas para alimentar os requisitos de implementação de segurança da informação do sistema ICS para a utilização da computação em nuvem como uma das infraestruturas ICS em seu ecossistema. Estas etapas foram definidas da seguinte forma:

1. Implementação da componente 1 através do método de análise da adequação da organização;
2. Implementação da componente 2 para testar a prontidão organizacional dos instrumentos de valor;
3. Implementação da componente 3 para cálculo do item anterior;
4. Determinar o nível de prontidão da organização.

O Modelo 2 segue os aspectos de segurança em nuvem definindo a importância de alguns elementos básicos na segurança da informação para computação em nuvem, sendo eles:

1. Durabilidade;
2. Disponibilidade;
3. Validade;
4. Confidencialidade;
5. Utilidade;
6. Propriedade;
7. Integridade;
8. Segurança.

Com base nos dois *frameworks* e nos dois modelos mencionados, além dos fatos estudados nas revisões de literatura, foram selecionados sete domínios para o desenvolvimento do protótipo. Este foi desenvolvido por meio de uma combinação de métodos tanto qualitativos como quantitativos, que estão sendo divididos em três fases:

1. Desenvolvimento do modelo preliminar;
2. Verificação do modelo preliminar;
3. Validação do modelo final.

Durante a fase inicial de desenvolvimento, um estudo para mapear os domínios definidos foi realizado, totalizando 44 controles de segurança. A segunda fase do desenvolvimento envolveu o processo de verificação do modelo preliminarmente feito. As atividades abrangem dois processos, que são o de coleta e o de análise de dados. O método utilizado nestes dois processos baseia-se na abordagem qualitativa por meio de entrevistas com especialistas técnicos na área de gestão de segurança da informação e computação em nuvem. Após o *feedback* do especialista, o modelo preliminar será melhorado para a construção do modelo final.

A etapa final é o processo de validação do modelo através de teste do protótipo e questionário em formato de formulário de avaliação. O protótipo foi construído no Microsoft Excel, enquanto o questionário foi desenvolvido no Google Form. A validação foi realizada por 10 representantes formados na área de segurança

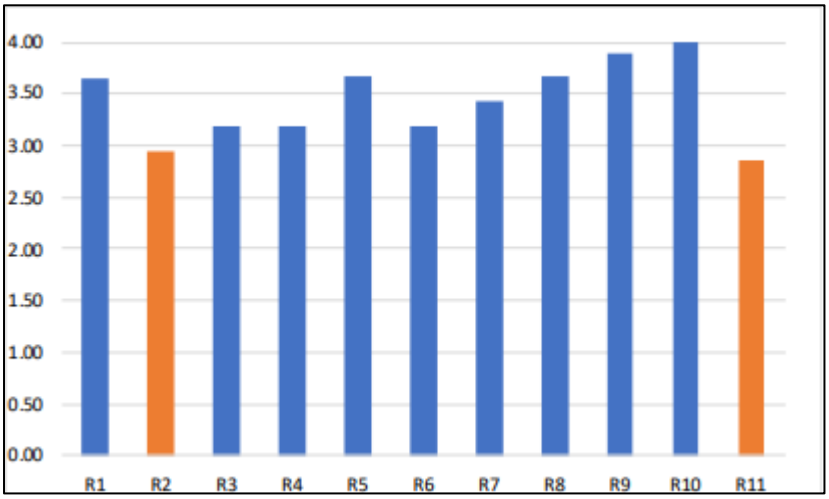
da informação e computação em nuvem. Esses representantes são selecionados com base na organização e no processo de obtenção da certificação ISMS.

O protótipo final construído ficou composto de 44 controles de segurança elaborados na forma de 94 checklists mapeados para 7 domínios definidos. O nível de prontidão foi medido por uma escala de Sim representado pelo valor 1 ou Não representado pelo valor de 0.

O processo de obtenção da verificação do modelo de pré-avaliação envolveu a verificação por especialistas. Eles foram rotulados como Especialista A e Especialista B. Ademais, eles concordaram com o modelo desenvolvido, no entanto, os peritos forneceram recomendações para melhorias nas várias listas de verificação selecionadas das 94 nas subsecções de controle.

A validação do feedback fornecido pelos especialistas veio de profissionais com vasta experiência em tecnologia de nuvem, implementação de segurança em nuvem e SGSI. O processo de validação envolveu os respectivos representantes das organizações para realizar os testes do protótipo e fornecer respostas aos questionários. A pontuação geral do teste do protótipo dos entrevistados é apresentada na Figura 12.

Figura 12 – Pontuação geral do protótipo

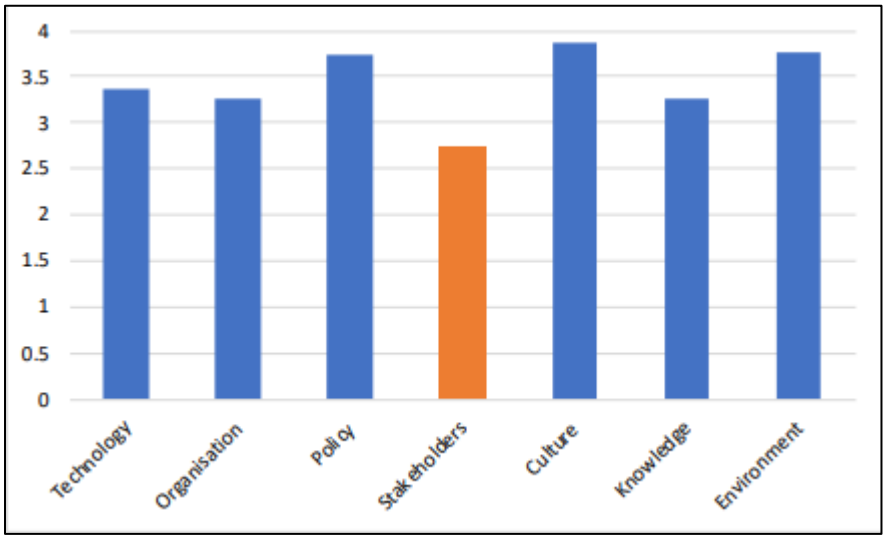


Fonte: KAMARUDDIN, 2020.

Com base nestes resultados, nove entrevistados (R1, R3, R4, R5, R6, R7, R8, R9 e R10) alcançaram um elevado nível de prontidão, enquanto os 2 restantes profissionais (R2 e R11) indicam nível intermediário de prontidão.

Além disso, dos sete domínios listados, constatou-se que seis domínios, nomeadamente tecnologia, organização, política, cultura, conhecimento e ambiente, registaram um elevado nível de preparação. Entretanto, o domínio das partes interessadas registou-se no nível de preparação intermédio. A pontuação média de cada domínio pode ser consultada na Figura 13.

Figura 13 - A pontuação média de cada domínio



Fonte: KAMARUDDIN, 2020.

Dentre os sete domínios definidos, o domínio das partes interessadas está registrado no radar de menor valor em comparação com outras medições entre os outros domínios, em que este domínio obtém nível intermediário de prontidão.

Os resultados obtidos na validação constataram que o protótipo desenvolvido foi respondido com sucesso. Os resultados mostram que 45,5% dos profissionais concordam fortemente com a eficácia do teste do protótipo. Além disso, os resultados mostram que 54,5% dos profissionais concordaram fortemente com o nível de eficiência do teste do protótipo.

No geral, as descobertas do teste e validação do protótipo mostraram que o modelo de pré-avaliação para a avaliação da prontidão da segurança na nuvem é confiável para ajudar provedores de serviços em nuvem a avaliar o nível de prontidão

da segurança do serviço na nuvem de forma eficaz e sem esforço, sem desperdiçar os recursos da organização.

8 ANÁLISE DOS RESULTADOS OBTIDOS E DISCUSSAO

Neste capítulo, foi realizada uma análise dos resultados obtidos a partir do estudo de implementações das normas ISO/IEC 27017 e 27018 em organizações citados no capítulo anterior. A análise levou em conta vários aspectos para fornecer uma visão detalhada do impacto das normas de segurança da informação no ambiente de nuvem.

A primeira parte da análise diz respeito à conformidade das empresas com as normas ISO/IEC 27017 e 27018. Avaliações detalhadas foram realizadas durante a implementação para garantir que todos os requisitos destas normas foram atendidos. Pôde-se observar que, em sua maioria, as organizações alcançaram um alto nível de conformidade com as normas. Os processos para implementar controles de segurança e políticas de privacidade específicos provaram ser eficazes na promoção de uma abordagem mais segura ao uso de serviços em nuvem.

Após uma análise mais detalhada foi possível notar que a implementação das normas teve um impacto significativo na melhoria da segurança da informação de uma organização. Os controles de segurança recomendados pela ISO/IEC 27017 ajudam a reduzir os riscos relacionados à segurança em ambientes de nuvem e garantem princípios como integridade, confidencialidade e disponibilidade dos dados. Além disso, a adoção da orientação ISO/IEC 27018 permite uma abordagem mais estruturada e proativa para proteger a privacidade dos dados pessoais dos clientes.

Outro ponto relevante notado com os estudos realizados é a redução significativa no número de incidentes de segurança desde a implementação das normas. Anteriormente, a organização estava sujeita a uma série de incidentes de segurança em ambientes de nuvem, incluindo vazamentos de dados e tentativas de acesso não autorizado. No entanto, após a implementação das normas, a organização observou uma diminuição notável na ocorrência desses incidentes, demonstrando a eficácia das medidas de segurança implementadas.

Além disso, também foram identificados desafios e limitações. A implementação das normas exigiu uma garantia de recursos e esforços, o que pode ser um desafio em organizações de porte menor. A manutenção da conformidade contínua com essas normas requer que seja feito não só um monitoramento

constante, como também atualizações das práticas de segurança, o que pode ser um processo complexo.

Em síntese, a implementação de ambas as normas teve um impacto positivo na segurança da informação, privacidade dos dados, satisfação do cliente e redução de incidentes de segurança nas organizações. No entanto, também apresentou desafios em termos de recursos e manutenção contínua. No geral, com a análise dos resultados conclui-se que a implementação dessas normas é altamente benéfica para as organizações que desejam fortalecer sua postura de segurança em ambientes de nuvem e garantir a proteção da privacidade dos dados.

8.1 Comparação dos resultados obtidos deste TCC com os trabalhos relacionados

Neste capítulo, foi feito uma análise e comparativa dos trabalhos relacionados com os resultados obtidos nesta pesquisa. A revisão da literatura foi essencial para contextualizar a pesquisa, identificar lacunas no conhecimento existente e destacar as contribuições originais deste trabalho.

Arias (2020) realizou pesquisas com o objetivo de implementar um modelo de segurança para garantir a segurança no ambiente, o controle de acesso e a detecção e resposta a incidentes. Neste TCC foi analisado trabalhos de autores que objetivaram a implementação das normas e que obtiveram resultados similares. Ambos utilizaram dois pontos de vista o primeiro com o uso do modelo e o segundo sem o modelo de segurança.

Machado (2021) apresentou estudos para identificar e descrever as principais formas de ataques cibernéticos conhecidas, apresentando as vulnerabilidades conhecidas. Como resultado a autora identificou ataques que podem ser mitigados com o uso de padrões de segurança. Em comparação com os estudos realizados neste TCC, também se conclui que pontos de vulnerabilidades podem ser evitados com o uso das normas ISSO/IEC 27017 e 27018, apesar de que não existe uma única solução para evitar os ataques e resolver os problemas de vulnerabilidades de uma organização.

Soares (2017) em seus estudos teve como objetivo discutir o tema segurança na computação em nuvem. Abordou-se como sua utilização cresceu, bem como as questões de segurança no ambiente em nuvem. Por fim, foram apresentados os principais serviços oferecidos. Ao longo deste TCC foi abordado sobre o crescimento da tecnologia da computação em nuvem bem como seus serviços, gerenciamento, vantagens e ameaças.

Imbat (2021), elaborou um trabalho cujo principal é projetar um Sistema de Gestão de Segurança da Informação para Serviços em Nuvem (SGSI-C) para a "Masiva", uma empresa equatoriana dedicada à prestação de serviços e aplicações na nuvem. Similarmente, neste TCC abordou estudos de autores que implementaram o uso das normas em organizações destacando a importância da aplicação de domínios de segurança, políticas, gestão de recursos humanos, controles de acesso e avaliação de riscos. Ambas concluindo que a implementação foi eficiente e vantajosa para a organização.

Com base na revisão dos trabalhos relacionados e nas conclusões destacadas, esta pesquisa preencheu algumas das lacunas e contribuiu para uma melhor compreensão da implementação das normas ISO/IEC 27017 e 27018 em ambientes de nuvem.

9 CONCLUSÃO

Este trabalho teve o intuito de responder a seguinte questão: Como as normas ABNT NBR ISO/IEC 27017:2015 e 27018:2019 garantem a segurança na computação em nuvem?

A segurança em nuvem inclui a implementação de medidas de segurança para garantir que os dados armazenados e processados na nuvem sejam protegidos contra acesso não autorizado, roubo, perda de dados e outras ameaças.

Os estudos permitiram concluir que A implementação de medidas de segurança adequadas, como controle de acesso, criptografia, monitoramento e detecção de ameaças, gerenciamento de incidentes e conformidade legal e regulamentar, pode ajudar a manter os dados da nuvem pública seguros e aumentar a confiança na tecnologia de segurança. Deste modo, houve uma diminuição notável na ocorrência de incidentes, demonstrando a eficácia das medidas de segurança implementadas.

O cumprimento das normas demonstra o comprometimento da organização com a proteção dos dados e a privacidade dos indivíduos, o que pode aumentar a confiança dos clientes, parceiros e stakeholders. Há também a contribuição para melhoria contínua dos processos de segurança e privacidade em ambientes de nuvem, promovendo a adaptação às mudanças nas ameaças cibernéticas e nas práticas recomendadas.

Além disso, também foram identificados alguns desafios e limitações no processo. A implementação das normas exigiu uma garantia de recursos e esforços, o que pode ser um desafio em organizações de pequeno porte. A manutenção da conformidade contínua com essas normas requer que seja feito um monitoramento frequente, e atualizações constantes das práticas de segurança, o que pode ser um desafio.

No geral, a implementação das normas é muito benéfica para as organizações que desejam fortalecer sua postura de segurança em ambientes de nuvem e garantir a proteção da privacidade dos dados. No entanto, é importante ressaltar que não existe uma única solução que evite os ataques e resolva os problemas de vulnerabilidades de uma organização.

Para continuidade desta pesquisa, sugere-se como trabalhos futuros:

- Implementar as normas em um ambiente (simulado) e compará-lo a um ambiente sem elas implementadas (simulado);
- Comparar o uso das normas ISSO/IEC 27017 e 27018 com outros padrões de segurança em nuvem;

10 REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas**. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ABNT. Associação Brasileira de Normas Técnicas**. NBR ISO/IEC 27017:2015: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem**. Rio de Janeiro, 2015.

ABNT. Associação Brasileira de Normas Técnicas**. NBR ISO/IEC 27018:2019: Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP**. Rio de Janeiro, 2019.

ALECRIM, Emerson. **O que é tecnologia da informação (TI)?** INFOWESTER, São Paulo. 2019. Disponível em: https://www.infowester.com/ti.php. Acesso em: 28 de fev. de 2023.

ALEIXO, Marina Romano. **Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação**. Tese de Doutorado – Universidade Nova de Lisboa, p.98. 2020. Disponível em: https://run.unl.pt/handle/10362/109742. Acesso em: 13 abr. 2023.

ARAÚJO, Franciele Cassimiro de; ROSSI, Jackeline Magrin. **A evolução dos ataques cibernéticos**. Trabalho de conclusão de curso - Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”. São Paulo, p. 51. 2020. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/5272. Acesso em: 26 mar. 2023.

ARIAS, E. N. **Implementação de um modelo de segurança para mitigação de vulnerabilidades em ambientes de armazenamento em nuvem baseado nas normas ISO 27017 e 27018**. Tese de mestrado - Escola Politécnica de Chimborazo. Riobamba, p.136. 2020. Disponível em: http://dspace.espoch.edu.ec/handle/123456789/14346. Acesso em: 01 mai. 2023.

AVINTE, E. F. ***Cloud computing: reducing costs in small and medium business****. Journal of Engineering and Technology for Industrial Applications*, Manaus, v. 5, n. 18, p. 5-17, 12 jun. 2019.

AWS. ***WHAT is AWS****.* 2022. Disponível em: https://aws.amazon.com/pt/what-is-aws/?nc1=f_cc. Acesso em: 27 set. 2022.

BANDEIRA, Waliff Cordeiro. **Análise do Custo-benefício de Funções como Serviço e Infraestrutura como Serviço**. Trabalho de conclusão de curso – Universidade de Brasília. Brasília, p. 67. 2022. Disponível em: https://bdm.unb.br/bitstream/10483/32446/1/2022_WaliffCordeiroBandeira_tcc.pdf. Acesso em: 20 mar. 2023.

BONGUET, Adrien; BELLAICHE, Martine. ***A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing***. Future Internet, [S.L.], v. 9, n. 3, p. 43, 5 ago. 2017. MDPI AG. Disponível em: http://dx.doi.org/10.3390/fi9030043. Acesso em: 02 abr. 2023.

BORGES, Filipe Afonso Nogueira; SILVA, Gabriel Santos Tavares da. **Proposta de modelo de migração de sistemas *on-premises* para nuvem pública no Brasil**. Trabalho de conclusão de curso – Universidade de Brasília. Brasília, p.54. 2019. Disponível em: https://bdm.unb.br/bitstream/10483/29192/1/2019_FilipeAfonsoBorges_GabrielDaSilva_tcc.pdf. Acesso em: 11 abr. 2023.

COUTINHO, A. A. T. R. et al. **Computação em Névoa: Conceitos, Aplicações e Desafios**. In: XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 34, 2016, Salvador. Anais, Salvador: Sociedade Brasileira de Computação (SBC), 2016, p. 266-315.

DAVID, D. Stalin et al. ***Cloud security service for identifying unauthorized user behaviour***. *CMC-Computers, Materials & Continua*, v. 70, n. 2, p. 2581-2600, 2022. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/72764369/pdf-libre.pdf?1634369667=&response-content-disposition=inline%3B+filename%3DCloud_Security_Service_for_Identifying_U.pdf&Expires=1682953553&Signature=MK88HJdn2~ekjM0qyS5JdTX-q25Gy39igSOkWgzcrVdLKc38RzsJzmfWkCxAhWa5Xor9hsogWQMknQ7xcnotCksjSlM0vVPLQJPNjKGF75Iheu05dVUoSe1fROyyeK8-pB2RwMI1UTrKO1FjMAc2OVu0yiFTSgt1SZorR3xVcYQzmHTo0rMV4syB6~rSPwxmvWhAQmL7dyc4iStJAmbZV97Wi-H5EtrhB-1kz~Nh8AziAyCi9BISxKZByBt2r2QU5DjnTZLsWxQwLt0cCFH65uCP~40C~ZklcjSLRz2pcnNzXpCWMP~tekSfqO2ePLyQGY3Lmr0AGQEy~7WSLYJETQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 29 abr. 2023.

DE ALMENDRA FREITAS, Cinthia Obladen. **Riscos e proteção de dados pessoais.** Revista Rede de Direito Digital, Intelectual & Sociedade, v. 2, n. 4, p. 225-247, 2022. Disponível em: https://revista.ioda.org.br/index.php/rrddis/article/view/74. Acesso em: 15 abr. 2023.

DE PAULA, L.; DIAN, M. de O. **COMPUTAÇÃO EM NUVEM: os desafios das empresas ao migrar para a nuvem.** Revista Interface Tecnológica, [S. l.], v. 18, n. 2, p. 304–315, 2021. DOI: 10.31510/infa. v18i2.1304. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1304. Acesso em: 7 set. 2022.

FERNANDES, Miguel A. P. et al. **Segurança da informação com a utilização de computação em nuvem**. In: MARTINS, Ernane Rosa. Engenharia de produção: tecnologia e inovação em pesquisa. 2 vol. São Paulo: Científica Digital, 2022. p. 106-118. Disponível em: https://www.editoracientifica.com.br/books/livro-engenharia-de-producao-tecnologia-e-inovacao-em-pesquisa-vol2. Acesso em: 17 mar. 2023.

FORNASIER, Mateus O.; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. ***Ransomware* e cibersegurança: a informação ameaçada por ataques a dados.** Revista Thesis Juris, v. 9, n. 1, p. 208-236, 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739. Acesso em: 09 abr. 2023.

GIL. Antonio C. **Como Elaborar Projetos de Pesquisa.** 6ª edição. São Paulo: Atlas, 2017. E-book.

GISLAINE, P. F. **Requisitos para análise de segurança da informação em provedores de serviços em nuvem**. Informação & Tecnologia (ITEC), v.4, n.1,

p.89-109, jan./jun. 2017. Disponível em: <https://brapci.inf.br/index.php/res/download/100678>. Acesso em: 02 nov. 2022.

GUPTA, Bulbul; MITTAL, Pooja; MUFTI, Tabish. ***A review on Amazon web service (AWS), Microsoft azure & Google cloud platform (GCP) services***. In: *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development,* ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India. 2021. Disponível em: https://eudl.eu/pdf/10.4108/eai.27-2-2020.2303255. Acesso em: 14 mar. 2023

HAJJ, H. *et al.* **SQL Injection Attacks and Defense in Cloud Computing: A Systematic Review**. IEEE Access. Vol 7, 2019.

HALLBERG, Fernando. **Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia**. Trabalho de conclusão de curso - 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/13546. Acesso em: 26 abr. 2023.

HUGE. ***Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total****. Synergy Research Group*, 2022. Disponível em: <https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues>. Acesso em: 27 set. 2022.

KADHIM, Q. K. et al. ***A Review Study on Cloud Computing Issues****. Journal of Physics: Conference Series, Kunching*, 2018, vol. 1018, p. 1-10. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1018/1/012006/meta>. Acesso em: 09 set. 2022.

KAMARUDDIN, Nur A. *et al.* ***Cloud security pre-assessment model for cloud service provider based on iso/iec 27017: 2015 additional control***. International Journal of Innovation and Industrial Revolution, v. 2, n. 5, p. 01-17, 2020. Acesso em: 08 out. 2023.

KOLB, Stefan. ***On the Portability of Applications in Platform as a Service****. University of Bamberg Press*, 2019. E-book. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H4uRDwAAQBAJ&oi=fnd&pg=PP1&dq=platform+as+a+service&ots=oq9MOUmELH&sig=pFXdGZgEWakvtDFSl_JzQsFTiXc#v=onepage&q&f=false. Acesso em 25 mar de 2023.

LAMPIKARI, Jan. ***Secure Cloud Implementation in Governmental Organisations***. Tese de mestrado - 2020. Disponível em: https://www.theseus.fi/bitstream/handle/10024/346412/Lampikari_Jan.pdf?sequence=2&isAllowed=y. Acesso em: 01 out. 2023.

LANE, Nicolas Peter; MIERS, Charles Christian. **Análise de segurança em infraestruturas de rede de provedores de nuvens computacionais *OpenStack***. In: Anais da XVIII Escola Regional de Alto Desempenho do Estado do Rio Grande do Sul. SBC, 2018.

LIMA, Adriano Carlos de. **Segurança da computação em nuvem**. 1ª edição. São Paulo: Senac, 2018. E-book.

LORENZI, Uriel Mafra; DE BRITO GREIN, Willian; CORCINI, Luiz Fernando. **Computação em nuvem: conceitos, aplicações e novas tecnologias**. Revista das Faculdades Santa Cruz, v. 13, n. 1, 2022.

LOUKIS, Euripidis; JANSSEN, Marijn; MINTCHEV, Ianislav. ***Determinants of software-as-a-service benefits and impact on firm performance****. Decision Support Systems*, v. 117, p. 38-47, 2019.

LOURENÇO, Flávio Augusto; BARNABÉ, Lucas Adriano. **A Área de Governança de TI: Suas Diretrizes e Processos**. In: FatecSeg-Congresso de Segurança da Informação. 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/62. Acesso em: 01 mai. 2023.

MACHADO, B. C. **Estudo sobre vulnerabilidades e implementação de um cenário de SQL Injection**. Trabalho de conclusão de curso – Universidade Católica de Goiás. Goiânia, p. 93. 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2703. Acesso em : 01 mai. 2023.

MARTINS, Inês Maria Araújo**. A imputação de ciberataques aos Estados**. 2022. Tese de Doutorado - Universidade Católica Portuguesa, p. 41. 2022. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/39892/1/203156218.pdf. Acesso em: 26 mar. 2023.

MARTINS. R. E. **Fundamentos da ciência da computação 2**. v. 2. Ponta Grossa: Atena Editora, 2019.

MGTEK, Assessoria em TI. **Nuvem pública, privada e híbrida: Saiba o que é e entenda suas diferenças**. Disponível em: https://mgtek.com.br/lages/blog/nuvem-publica-privada-e-hibrida-diferencas/. Acesso em: 14 mar. 2023.

NASEREDDIN, H*. **Building of Private Cloud Computing Architecture to Support E-Learning*****.*** *High Technol*. Lett, v. 26, p. 853-860, 2021. Disponível em: https://www.researchgate.net/profile/Hebah-H-O-Nasereddin/publication/348419926_Building_of_Private_Cloud_Computing_Architecture_to_Support_E-Learning/links/5ffe2f2e299bf140888f8be7/Building-of-Private-Cloud-Computing-Architecture-to-Support-E-Learning.pdf. Acesso em: 14 mar. 2023.

PATRICIO, Veloso C. E. ***Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.*** Tese de mestrado – *Universidad Tecnológica Israel*. Equador, p. 46. 2022. Disponível em: http://repositorio.uisrael.edu.ec/bitstream/47000/3369/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-012.pdf. Acesso em: 27 set. 2023

PENA, Braian Henrique; DA SILVA, Anderson Santos; DOS SANTOS, Maicon. **PHISHING**. SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO, v. 2, n. 2, 2020. Disponível em: http://raam.alcidesmaya.edu.br/index.php/SGTE/article/view/271/258. Acesso em: 09 abr. 2023.

PEREIRA, A. S. et al. **Metodologia de pesquisa cientifica**. 1ª edição. Santa Catarina: UFSM/NTE, 2018. E-book.

RAGHAVAN. R. S.; KR, Jayasimha; NARGUNDKAR, R. V. ***Impact of software as a service (SaaS) on software acquisition process.*** *Journal of Business & Industrial Marketing*, v. 35, n. 4, p. 757-770, 2020.

RASHID, Aaqib; CHATURVEDI, Amit. ***Cloud computing characteristics and services: a brief review****. International Journal of Computer Sciences and Engineering*, v. 7, n. 2, p. 421-426, 2019. Disponível em: https://www.researchgate.net/profile/Aaqib-Rashid/publication/331731714_Cloud_Computing_Characteristics_and_Services_A_Brief_Review/links/5c89f6c045851564fadca23f/Cloud-Computing-Characteristics-and-Services-A-Brief-Review.pdf. Acesso em: 21 mar. 2023.

RODRIGUES, Auro de Jesus. **Metodologia científica: completo e essencial para a vida universitária.** 1ª edição. São Paulo: Avercamp, 2006. E-book.

ROSY, M. A. et al. ***Challenges, service models and deployment models of cloud computing*****.** JETIR *Journal,* Gujarat, p. 81-86, set. 2019. Disponível em: <https://www.jetir.org/papers/JETIRDD06016.pdf>. Acesso em: 07 set. 2022.

SANTOS, Tiago. **Fundamentos da computação em nuvem**. 1ª edição. São Paulo: Senac, 2018. E-book.

SILVA, Anderson Trindade. **Computação em nuvem: análise dos atuais modelos.** Trabalho de conclusão de curso – Universidade Federal Fluminense. Niterói, p. 42. 2019. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/12977/TCC_ANDERSON_TRINDADE_DA_SILVA.pdf?sequence=1&isAllowed=y. Acesso em: 18 mar. 2023

SILVA, Anildo Joaquim. **Segurança de informação no ambiente da computação na nuvem**. Revista Primeira Evolução, v. 1, n. 38, p. 13-25, 2023. Disponível em: http://primeiraevolucao.com.br/index.php/R1E/article/view/393. Acesso em: 09 abr. 2023.

SM!Tech. **O que é DoS e DDoS?** Vídeo. Youtube. Disponível em: https://www.youtube.com/watch?v=qNygYNVdSs8. 2019.

SOARES, A. C. B. **Gestão da segurança na computação em nuvem**. Trabalho de conclusão de curso – Universidade Federal Fluminense. Niterói, p. 53. 2017 Disponível em: https://app.uff.br/riuff/handle/1/5621. Acesso em: 03 mai. 2023.

SRIVASTAVA, A. K. ***Adoption of the cloud accelerates innovation, growth for modern business***. Entrevistador: Narasimba Raju. CXOtoday, 2023. Disponível em: https://www.cxotoday.com/interviews/adoption-of-the-cloud-accelerates-innovation-growth-for-modern-business/. Acesso em: 28 fev. 2023.

TABOSA, Fábio Galvão Ferreira. **Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal**. Dissertação de metrado profissional – Universidade de Brasília. Brasília, p. 96. 2022. Disponível em: https://repositorio.unb.br/handle/10482/45369. Acesso em: 13 abr. 2023.

TAVBULATOVA, Z. K. et al. ***Types of cloud deployment****. In: Journal of Physics: Conference Series*. IOP Publishing, 2020. p. 012085. Disponível em:

https://iopscience.iop.org/article/10.1088/1742-6596/1582/1/012085/pdf. Acesso em: 14 mar. 2023.

TEIXEIRA, Cleyson Fernando Araújo. **Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos**. Trabalho de conclusão de curso – Universidade Federal de Ouro Preto. Ouro Preto, p. 94. 2021. Disponível em: https://monografias.ufop.br/bitstream/35400000/3567/1/MONOGRAFIA_Seguran%c3%a7aCibern%c3%a9ticaRedes.pdf. Acesso em: 02 abr. 2023.

TI OPEN. **OwnCloud Sua Nuvem Privada No Linux**. Disponível em: https://www.tiopen.com.br/2021/03/09/owncloud-sua-nuvem-privada-no-linux/. Acesso em: 14 mar. 2023.

VERIZON. ***2022 Data Breach Investigations Report***. 2022. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 07 abr. 2023.

WAZLAWICK. Raul S. Metodologia de Pesquisa Para Ciência da Computação. 2ª edição. Rio de Janeiro: Elsevier, 2014. E-book.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Hianka Rodrigues Souza do Curso de Engenharia da Computação, matrícula 20191003300063, telefone: 62 985516527 e-mail hiankars@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado USO DAS NORMAS NBR ISO/IEC 27017 E 27018 PARA GARANTIR A SEGURANÇA DA COMPUTAÇÃO EM NUVEM , gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 12 de Setembro de 2023.

Assinatura do autor: _ gov.br Documento assinado digitalmente HIANKA RODRIGUES SOUZA Data: 13/09/2023 08:01:13-0300 Verifique em https://validar.iti.gov.br _____

Nome completo do autor: Hianka RodriguesSouza_____

Assinatura do professor–orientador: __SOLANGE DA SILVA

Nome completo do professor-orientador: gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 17/12/2023 10:30:49-0300 Verifique em https://validar.iti.gov.br _