FUNDAÇÃO PEDRO LEOPOLDO

Mestrado Profissional em Administração

Paulo Sérgio de Souza

Desenvolvimento de um *framework* de segurança da informação para ambientes de *CloudComputing* baseado na ABNT ISO/IEC 27001:2022

Pedro Leopoldo

2024

Paulo Sérgio de Souza

Desenvolvimento de um *framework* de segurança da informação para ambientes de *CloudComputing* baseado na ABNT ISO/IEC 27001:2022

Dissertação apresentada ao Curso de Mestrado Profissional em Administração da Fundação Pedro Leopoldo como requisito parcial para obtenção do grau de Mestre em Administração.

Área de concentração: Gestão e Estratégia em organizações.

Linha de pesquisa: Gestão em Organizações, Pessoas e Inovação.

Orientador: Prof. Dr. Wanderley Ramalho.

Pedro Leopoldo

Fundação Pedro Leopoldo

2024

658.406
S729d

SOUZA, Paulo Sergio de
Desenvolvimento de um framework de segurança da informação para ambientes de CloudComputing baseado na ABNT ISO/IEC 27001:2002 / Paulo Sérgio de Souza.
- Pedro Leopoldo: FPL, 2024.

104 p.

Dissertação: Mestrado Profissional em Administração, Fundação Cultural Dr. Pedro Leopoldo, Pedro Leopoldo, 2024.
Orientador: Prof. Dr. Wanderley Ramalho

1. Segurança da Informação.
2. CloudComputing.
3. Modelo Analítico.
I. Título. II. RAMALHO, Wanderley, orient.

.

Dados Internacionais de Catalogação na Publicação
Ficha catalográfica elaborada por Maria Luiza Diniz Ferreira
CRB 6 -1590

FOLHA DE APROVAÇÃO

Título da Dissertação: **"DESENVOLVIMENTO DE UM *FRAMEWORK* DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTES DE *CLOUDCOMPUTING* BASEADO NA ABNT ISO/IEC 27001:2022".**

Nome do Aluno: **Paulo Sérgio de Souza**

Dissertação de mestrado, modalidade Profissionalizante, defendida junto ao Programa de Pós-Graduação em Administração da Faculdade Pedro Leopoldo, aprovada pela banca examinadora constituída pelos professores:

gov.br Documento assinado digitalmente
WANDERLEY RAMALHO
Data: 03/09/2024 17:27:16-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Wanderley Ramalho - Orientador - FPL Educacional

gov.br Documento assinado digitalmente
JOSE EDSON LARA
Data: 04/09/2024 08:35:06-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. José Edson Lara - FPL Educacional

THAIS ESPINOLA DE OLIVEIRA LIMA:47503688904

Profa. Dra. Thaís Espínola de Oliveira Lima – Faculdade de Pinhais - FAPI

Pedro Leopoldo (MG), 19 de agosto de 2024.

A Minha família, em especial minha mãe e meu filho Lucas Davi!

Agradecimentos

Primeiramente, a Deus, que me guiou ao longo desses anos e me permitiu chegar até aqui.

Ao meu orientador, Prof. Dr. Wanderley Ramalho, pela paciência, generosidade e por acreditar no meu potencial.

Aos meus pais, Alfredo de Souza Lima (*in memoriam*) e Maria da Costa Souza Lima, que sempre estiveram em meu coração me dando forças!

Aos meus irmãos, minha ex-esposa, Michelle Aparecida, e especialmente ao meu filho, Lucas Davi de Souza Silva, que sempre esteve a meu lado em todos os momentos mais especiais.

Aos médicos que cuidaram de mim em um momento tão especial durante o desenvolvimento desse trabalho.

Aos amigos, colegas de trabalho e de mestrado com os quais convivi nesse período, que me trouxeram alegrias e desafios para vencer até aqui.

Resumo

Objetivo: a presente dissertação teve como objetivo desenvolver e testar um modelo analítico – construtos e respectivos indicadores – que permita, com base na percepção de especialista do mercado e nos ditames da ABNT ISO/IEC 27001:2022, perscrutar as nuanças da segurança em *CloudComputing*. **Relevância/ originalidade**: tem-se observado uma lacuna retratada pela falta de um modelo analítico capaz de nortear o desenvolvimento de uma estratégia de gestão de segurança da informação no novo ambiente de computação em nuvem. Esta dissertação preenche exatamente essa lacuna e se utiliza de uma metodologia estatística apropriada para fazê-lo. **Metodologia/abordagem:** o exame do referencial teórico pertinente, das diretrizes emanadas da ABNT ISO/IEC 27001:2022 e dos dados obtidos em uma pesquisa prévia com especialistas de mercado ensejou a construção de um modelo analítico constituído inicialmente por três construtos e 34 indicadores que permitiram a elaboração de um questionário ulteriormente aplicado a outros 110 especialistas em *CloudComputing*. Ao banco de dados obtido foi aplicada uma análise fatorial da qual resultou um modelo analítico final constituído de oito dimensões e 34 indicadores. **Principais resultados**: o objetivo geral de apresentar um modelo analítico para a gestão de segurança em *CloudComputing* foi alcançado. O primeiro objetivo específico (teste do modelo sugerido) foi alcançado mostrando que o modelo analítico utilizado foi estatisticamente aprovado. O segundo objetivo específico, que buscou mostrar as importâncias relativas (pesos) de cada indicador para o seu respectivo construto foi representado pelos coeficientes fatoriais. Concluiu-se ainda que apenas para a dimensão Integridade 1 observou-se diferença estatisticamente significativa de percepção entre profissionais de distintos tempo de experiência na área. Nesse caso, a diferença apareceu quando se comparou “intermediário” com “iniciante” e com “especialista”. Quando se considerou o cargo que o profissional desempenha, ocorreram percepções diferentes nas dimensões Confidencialidade 1 e Confidencialidade 2. No primeiro caso as diferenças apareceram quando se comparou o superintendente com o coordenador; no segundo caso as diferenças significativas ocorreram entre o superintendente e o analista/consultor. **Contribuições teórico-metodológicas:** o estudo desenvolveu e testou um modelo analítico extraído do referencial teórico pertinente, explicitando as suas dimensões de análise e respectivos indicadores para desenvolver uma estratégia de gestão de segurança em *CloudComputing*. Em termos metodológicos, mostrou-se como utilizar o instrumental estatístico para a construção do modelo. **Contribuições sociais/para a gestão**: em função do exposto, pode-se afirmar que o presente estudo constitui um instrumento gerencial e de planejamento para a atividade de *CloudComputing*. De fato, além de apresentar um *framework* sistematicamente obtido, o estudo mostra a importância (pesos) de cada indicador em cada uma das dimensões do modelo analítico e perscruta a diferença de percepções ao levar-se em conta o tempo de experiência bem como o cargo do profissional de *CloudComputing*. Desse modo, esse conjunto de conclusões extraídas do estudo permite subsidiar o desenvolvimento de uma estratégia de segurança no campo de *CloudComputing,* contribuindo, desse modo, para um processo de intervenção na realidade da gestão de segurança.

Palavras-chave: *CloudComputing*. Segurança. Modelo analítico.

Abstract

Objective: this dissertation aimed to develop and test an analytical model – constructed and respective indicators – that allows, based on the perception of market experts and the dictates of ABNT ISO/IEC 27001:2022, to examine the nuances of security in cloud computing. **Relevance/originality:** a gap has emerged due to the lack of an analytical model capable of guiding the development of an information security management strategy in the new cloud computing environment. This dissertation completely fills this gap and uses a statistical methodology to do so. **Methodology/approach:** the examination of the relevant theoretical framework, the guidelines issued by ABNT ISO/IEC 27001:2022 and the data obtained in a previous survey with market specialists led to the construction of an analytical model initially consisting of 3 constructs and 34 indicators that allowed the elaboration of a questionnaire later applied to another 110 cloud computing experts. A factor analysis was applied to the database obtained, resulting in a final analytical model consisting of 8 dimensions and 34 indicators. **Main results:** the general objective of presenting an analytical model for security management in cloud computing was achieved. The first specific objective (test of the suggested model) was carried out showing that the analytical model used was statistically approved. The second specific objective that seeks to show the relative importance (weights) of each indicator for its respective construct is represented by the factorial coefficients. It was also concluded (tables 8 and 9 respectively) that only for the Integrity1 dimension is that I observed a statistically significant difference in perception between professionals with different experience in the area. In this case, the difference appears when comparing “intermediate” with “beginner” and “expert”. When considering the workload that the professional performs, different perceptions occur in the Confidentiality1 and Confidentiality2 dimensions. In the first case, differences appear when comparing the superintendent with the coordinator; in the second case, disagreements occurred between the superintendent and the analyst/consultant. **Theoretical/methodological contributions:** the study developed and tested an analytical model, extracted from the relevant theoretical framework, explaining its analytical dimensions and respective indicators to develop a security management strategy in cloud computing. In methodological terms, it was shown how to use statistical tools to build the model. **Social/management contributions:** Based on the above, it can be concluded that the present study constitutes a management and planning instrument for cloud computing activity. In fact, in addition to presenting a systematically developed framework, the study presents the importance (weights) of each indicator in each of the dimensions of the analytical model and examines the difference in perceptions when taking into account time of experience as well as workload. make cloud computing professional. In this way, this set of conclusions drawn from the study allows to support the development of a security strategy in the field of cloud computing, thus contributing to a process of intervention in reality. security management.

Keywords: CloudComputing. Security. Analytical model.

Lista de Abreviaturas e Siglas

AaaS	Serviços de análise como serviço
ABNT	Associação Brasileira de Normas Técnicas
AC	Alfa de Cronbach
ACP	Análise de componentes principais
AIaaS	Serviços de inteligência artificial como serviço
ANPD	Autoridade Nacional de Proteção de Dados
BSI	*British Standards Institution*
CC	Confiabilidade composta
CD	*Compact disk*
CF	Carga fatorial
CGI.br	Comitê Gestor da Internet no Brasil
CID	Confidencialidade, integridade e disponibilidade
Com	Comunalidade
COVID-19	*Disease of coronavirus*
CPD	Centro de Processamento de Dados
CSIRT	*Computer Security Incident Response Team*
DBaaS	Serviços de banco de dados como serviço
DDoS	Ataques de rede distribuídos
DISHO	Divisão de Serviços da Hora Legal Brasileira
DLP	*Data Loss Prevention*
EC2	*Elastic Compute Cloud*
GDPR	Regulamento Geral de Proteção de Dados
GDPR	*General Data Protection Regulation*
HLB	Hora Legal Brasileira
IaaS	Infraestrutura como serviço
IBM	*International Business Machines Corporation*
IEC	*International Eletrotechnical Comission*
ISMS	*Information security management system*
ISO	*International Organization Standardization*
KMO	*Kaiser-Meyer-Olkin*
LGPD	Lei Geral de Privacidade de Dados

NIC	Núcleo de Informação e Coordenação
NIST	*National Institute of Standards and Technology*
OWASP	*Open Web Application Security Project*
PaaS	Plataforma como serviço
PCI DSS	*Payment Card Industry Data Security Standard*
PDCA	Planejamento, execução, verificação e ação
SaaS	*Software* como serviço
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da informação
WSTG	*Web Security Testing Guide*
BACEN	Banco Central do Brasil

Lista de Figuras

Lista de Tabelas

Sumário[1]

[1] Este trabalho foi revisado e formatado de acordo com as Instruções para Formatação de Trabalhos Acadêmicos – Norma APA, 2023.

1 INTRODUÇÃO

Desde o lançamento do primeiro grande computador para uso corporativo, realizado pela *International Business Machines Corporation* (IBM) em 1964, quando apresentou seu *mainframe* nomeado à época como *System*/360, uma onda de inovação tecnológica foi iniciada (https://www.ibm.com/reports/data-breach).

Na década de 1980 observou-se outro grande salto de inovação, com o surgimento dos computadores pessoais e a criação das redes locais que possibilitavam interligá-los em um mesmo ambiente. Conectando também os servidores, que eram máquinas mais robustas, mas menores e com menos capacidade de processamento que os *mainframes*, iniciou-se o modelo conhecido de computação cliente-servidor, em que os computadores de menor porte (as estações de trabalho ou *workstations*) se conectavam aos servidores (*servers*), onde eram executados os sistemas computacionais de forma centralizada. O aumento de poder de processamento dos servidores, a maior oferta de aplicações e a diminuição do preço desses os tornaram mais acessíveis (Veras, 2015). Esses servidores e os *mainframes* eram alocados em lugares adequados e protegidos, os *DataCenters*, ou Centros de Processamento de Dados (CPD), como eram chamados à época.

Nos últimos anos a Internet possibilitou o aumento da oferta de serviços de computação em nuvem de forma descentralizada, ou *CloudComputing* (ou apenas *Cloud*), como *DataCenters* virtuais que permitem às empresas instalar suas aplicações em servidores localizados em ambientes de fornecedores da *Cloud*. Mais recentemente, permitiu utilizar apenas serviços já prontos e disponibilizados pelos fornecedores. Isso tem permitido mais agilidade na criação de estruturas por custo muito mais baixo. Conforme Taurion (2009, p. 24), “embora possa parecer revolucionário, o conceito de computação em nuvem é um passo evolutivo na eterna busca pelo compartilhamento e consequentemente maior aproveitamento dos recursos computacionais”.

As questões técnicas associadas ao uso da *CloudComputing* têm sido amplamente abordadas na literatura, com destaque para os trabalhos de Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica & Zaharia (2010), Buyya,

Broberg & Goscinski (2011) e Mell & Grance (2011). Há, também, alguns estudos relativos ao uso estratégico da *CloudComputing* e aos variados modelos de negócios advindos de sua adoção pelas empresas, como visto em Wirtz, Mory & Piehler (2014).

O mercado de *CloudComputing* foi, com o passar do tempo, centralizado em poucos e grandes fornecedores. Segundo Laudon e Laudon (1999), no atual século XXI os gigantes da comunicação estão envolvidos na maior competição empresarial de todos os tempos, sendo o principal objetivo construir e controlar com segurança a vasta teia de redes e serviços eletrônicos que fornecem informação, educação e serviços a empresas e residências de todo o mundo.

Com o mercado requerendo cada dia soluções mais rápidas, simples, baratas e com acessibilidade a partir de qualquer ponto do mundo, as empresas perceberam que os *DataCenters* virtuais passaram a ser uma excelente opção para todos esses requerimentos. Entretanto, uma vez que a *CloudComputing* disponibiliza os dados remotamente de forma imediata, fora do controle do proprietário, é inevitável que surjam questões relacionadas à segurança da informação.

Segundo Dikakaikos, Smith & Jones (2009), toda a responsabilidade pela proteção do usuário, da sua privacidade e da integridade das informações por ele armazenadas em *Cloud* é da provedora de serviço contratada. Esse pensamento é compartilhado por Wei, Li & Wang (2014), que acreditam que a gestão da segurança e privacidade são os principais desafios associados à implantação da *CloudComputing* em organizações. Todas essas questões são claras, mas, as estruturas atuais de instituições financeiras ainda são grandes usuárias dos sistemas centralizados em *mainframes*. O aspecto técnico de migração não parece ser problema, uma vez que há oferta de estruturas similares em *Cloud*. Nesse contexto, a norma Associação Brasileira de Normas Técnicas, *International Organization Standardization*/ *International Eletrotechnical Comission* (ABNT ISO/IEC) 27001:2022 (ou apenas ISO 27001), mantida pela ABNT e baseada na ISO, emerge como uma referência essencial, sendo um padrão e referência de mercado que fornece diretrizes abrangentes para o estabelecimento de sistemas de gestão de segurança da informação eficazes.

Não obstante esse seu reconhecido e importante papel para a gestão da segurança da informação, a ISO 27001 apresenta-se bastante complexa e desafiadora quando se trata de sua aplicação direta na nuvem, em decorrência das singularidades desse novo ambiente. Na realidade, é lícito afirmar que a adoção dos serviços em nuvem introduz um novo paradigma tecnológico ancorado na virtualização, na escalabilidade dinâmica e na heterogeneidade das infraestruturas. Segundo Silva e Cunha (2021), os próprios provedores de serviços podem oferecer diferentes níveis de segurança em suas estruturas, o que é importante considerar ao implementar-se a ISO 27001. Adicionalmente, é merecedor de ênfase especial o fato de que as tradicionais práticas de segurança não conseguem atender às necessidades bastante específicas que são imperativos de um ambiente em nuvem. Desse modo, as organizações passam a enfrentar dificuldades para o desenvolvimento de uma estratégia de gestão de segurança da informação.

Particularmente, surgem desafios únicos em termos de controle de acesso, compartilhamento de responsabilidades de segurança entre provedores e clientes, a proteção de dados em trânsito e em repouso na nuvem, a gestão adequada de identidades e acessos em ambientes virtualizados, a avaliação de riscos específicos à nuvem e a incorporação de práticas de resposta a incidentes em cenários distribuídos além da continuidade operacional. Santos (2020) acrescenta a necessidade e o desafio constante de se monitorar o ambiente de *CloudComputing*, devido às suas dinâmicas, indicando que o monitoramento constante, como proposto pela ISO 27001, é um processo crucial para garantir que os controles de segurança estejam funcionando de forma eficaz. Cabe destacar que esse conjunto de constatações tem a sua explicação no cenário original no qual nasceu a ISO 27001, o qual não apresentava as imposições implícitas para uma gestão eficaz de segurança tal como a exigida em *CloudComputing*.

Malgrado o reconhecimento da necessidade imperiosa de uma adaptação das melhores práticas de gestão de segurança da informação emanadas da ISO 27001 às novas necessidades surgidas a partir das especificidades trazidas na esteira da *CloudComputing*, não se conta ainda com um estudo sistematizado capaz de ensejar essa adaptação no sentido de priorizar a implementação dos indicadores de segurança propostos pela ISO 27001 em seus respectivos construtos. Em outros

termos, ressente-se da falta de um protocolo que permita às organizações, tendo por base a ISO 27001, enfrentar os novos desafios apresentados pelas nuanças da nova era digital mediante a priorização de esforços propostos por controles baseados em um *framework* norteador de uma gestão de segurança da informação no novo ambiente de nuvem. A relevância de um estudo que incorpore todas essas considerações está em possibilitar o desenvolvimento de uma verdadeira estratégia de gerenciamento da segurança da informação que leve em consideração as transformações havidas no campo computacional, particularmente, aquelas que são inerentes à *CloudComputing*.

Para preencher essa lacuna, esta dissertação é norteada pela seguinte pergunta de pesquisa: que característica deve apresentar um *framework* de gestão da segurança da informação em nuvem estribando-se nos fundamentos apresentados pela ISO 27001?

1.1 Objetivos

O que alcançar para atender à finalidade do estudo é o que se define como “objetivo da dissertação”, ou seja, o que vai ser feito para responder à pergunta de pesquisa. Este, por sua vez, pode ser cindido em um objetivo geral e em objetivos específicos que visam a uma digressão mais detalhada. Eles representam, assim, um desdobramento do que deve ser buscado para que, em seu conjunto, permita alcançar o objetivo geral (Minayo, 2020).

1.1.1 Objetivo geral

Desenvolver um *framework* para a gestão de segurança da informação em nuvem, com base na percepção de especialistas de mercado.

1.1.2 Objetivos específicos

São os seguintes os objetivos particulares a serem alcançados:

a) Testar a validade estatística do modelo analítico obtido por meio da pesquisa de campo.
b) Indicar, usando método estatístico adequado, a importância relativa dos indicadores que retratam as diversas facetas de cada construto (dimensão de análise) do modelo analítico.
c) Estabelecer, para cada construto, a existência de diferença estatisticamente, significativa, dos seus respectivos indicadores quando se consideram **profissionais com distintos tempos de atuação na área.**
d) Estabelecer, para cada construto, a existência de diferença estatisticamente, significativa, dos seus respectivos indicadores quando se consideram **profissionais com distintos cargos em que atuam na área.**

1.2 Estrutura do trabalho

Este trabalho está organizado em cinco capítulos. O primeiro é constituído por esta introdução, apresentando e contextualizando o tema segurança em *CloudComputing*, a relevância da pesquisa e a pergunta que a norteou.

O segundo capítulo traz todo o arcabouço conceitual e teórico do qual foi possível extrair a base que gerou um modelo de análise que foi o ponto crucial para entendimento e condução desta pesquisa.

No terceiro capítulo são descritos os procedimentos metodológicos utilizados na pesquisa, a saber, todo o processo de coleta, tratamento e análise dos dados, além dos métodos utilizados para a obtenção dos resultados.

O quarto capítulo analisa os resultados da pesquisa após a aplicação da metodologia estatística ao banco de dados obtido por meio de um questionário extraído do modelo analítico utilizado.

No quinto capítulo são tecidas as considerações finais, destacando-se a sua relevância tanto do ponto de vista acadêmico quanto do ponto de vista gerencial.

O sexto capítulo apresenta sugestões para estudos futuros.

2 Referencial Teórico

Este capitulo visa trazer uma base teórica para melhor compreensão dos conceitos e do objetivo do trabalho, dividindo-se em duas seções. Na primeira são abordados os conceitos acerca do tema segurança da informação, a fim de demonstrar sua importância para a empresa estudada de forma geral. A segunda seção apresenta as informações a respeito da norma ISO 27001 que traz um arcabouço de recomendações para se estabelecer controles e um sistema de gestão de segurança da informação que assegurem que os dados da empresa e de seus clientes alcancem e mantenham um nível adequado de proteção.

2.1 Segurança da informação

A segurança da informação, ao longo de sua história, tem evoluído correlativamente aos avanços tecnológicos e às crescentes ameaças cibernéticas. No contexto global, desde os primórdios da comunicação humana, métodos de criptografia foram utilizados para proteger informações sensíveis, como os algoritmos criptografia modernos desenvolvidos por Diffie & Hellman (1976), que afirmaram que a segurança absoluta é praticamente impossível. Contudo, complementam os autores, um dos propósitos da criptografia é fornecer um melhor nível de segurança em comunicações por canais considerados inseguros, a exemplo do cenário atual da Internet. Com o advento da computação e das redes de comunicação, novos desafios surgiram, destacando-se a importância da proteção dos dados digitais armazenados e da infraestrutura tecnológica utilizada.

No Brasil, a preocupação com a segurança da informação ganhou destaque à medida que o país se integrou à economia global e adotou tecnologias digitais em larga escala. Conforme Rodrigues (2013), a Lei Brasileira nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, que tipifica crimes cibernéticos como invasão de dispositivos informáticos e violação de dados, representou um marco importante na legislação brasileira ao tipificar e estabelecer punições para crimes cibernéticos, fornecendo assim uma base legal sólida para combater as violações de segurança digital no país. No entanto, o país ainda

enfrenta desafios como a falta de investimentos em capacitação e infraestrutura tecnológica adequada.

Nos últimos anos, observou-se crescente interesse na proteção da privacidade e dos dados pessoais, tanto em nível global quanto no Brasil. A implementação do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a criação da Autoridade Nacional de Proteção de Dados (ANPD, 2016) no Brasil são exemplos de medidas adotadas para fortalecer a segurança da informação e a privacidade dos cidadãos. Estudo realizado por Almeida, Mendes e Figueiredo (2020) destaca a importância da Lei 13.709, de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), como um instrumento essencial para garantir a privacidade dos dados e a conformidade das organizações com as normas de proteção de dados. A implementação eficaz da LGPD requer o comprometimento das empresas em adotar medidas adequadas de segurança da informação e em promover uma cultura de respeito à privacidade dos indivíduos.

Em suma, a história da segurança da informação reflete a constante busca por soluções que garantam a confidencialidade, integridade e disponibilidade das informações em um mundo cada vez mais conectado digitalmente.

2.1.1 Evolução global da segurança da informação

A história da segurança da informação remonta aos primórdios da comunicação humana, quando métodos rudimentares de criptografia eram utilizados para proteger mensagens importantes. Conforme Hintzbergen, Hintzbergen, Smulders e Baars (2018, p. 07):

> De fato, as raízes da segurança de TI têm mais de 2.000 anos de idade. Por exemplo, os egípcios utilizavam hieróglifos não padronizados esculpidos em monumentos e os romanos inventaram a chamada cifra de César para criptografar mensagens.

Mais recentemente, com o advento da computação e das redes de comunicação, o campo da segurança da informação passou por diversas e rápidas transformações.

Um marco significativo foi a proposição da criptografia de chave pública por Diffie & Hellman (1976), abrindo caminho para a proteção de dados em ambientes digitais. A partir daí surgiram diversas técnicas e protocolos para garantir a segurança das informações.

No entanto, com a popularização da Internet nas décadas seguintes, novos desafios surgiram. Rosenzweig & Kuhn (2015) afirmam que um dos principais desafios surgidos é a crescente sofisticação dos ataques cibernéticos. Com o aumento do número de dispositivos conectados à Internet, os cibercriminosos têm mais oportunidades para explorar vulnerabilidades e realizar ataques em larga escala. Desde ataques de negação de serviço distribuído (DDoS) até ataques de *phishing* e *ransomware*, as ameaças cibernéticas se tornaram mais complexas e difíceis de serem mitigadas.

2.1.2 Conceitos de segurança da informação

Apesar de ser uma preocupação antiga, visto que o tratamento de dados em sistemas computacionais já ocorre há décadas, os conceitos de segurança da informação foram descritos de modo sistemático há pouco tempo. Por se tratar de uma área relativamente nova que cada vez mais vem se desenvolvendo dentro das corporações, a segurança da informação vem formando rapidamente uma base bastante sólida de profissionais, construída com base no envolvimento de especialistas de várias áreas do conhecimento (não só da informática), sobre a qual sustenta seu desenvolvimento.

Atualmente esses conceitos têm como principal referência a norma ISO 27001, que define a segurança da informação como a proteção dos ativos de informação de uma organização contra ameaças e riscos internos e externos. Os ativos de informação podem ser dados, sistemas, aplicações, infraestrutura e pessoas. Dessa forma, a segurança da informação é um campo essencial na era digital, que visa proteger os dados contra acesso não autorizado, uso indevido, alteração ou destruição. Neste texto são explorados os conceitos fundamentais da segurança da informação, discutindo sua importância, os princípios básicos que a norteiam e as medidas de proteção que podem ser implementadas. A crescente digitalização de

informações e processos em diversos setores da sociedade torna a segurança da informação uma preocupação crucial. Como observado por Whitman & Mattord (2019), a segurança da informação é essencial para garantir a proteção adequada contra ameaças internas e externas.

2.1.3 Princípios básicos da segurança da informação

Existem diversos princípios que orientam a segurança da informação. Um dos mais fundamentais é o princípio da confidencialidade, integridade e disponibilidade (CID), como salientam Pfleeger & Pfleeger (2018). Esse princípio estabelece que os dados devem ser acessíveis apenas por pessoas autorizadas, não devem ser alterados indevidamente e sem autorização e devem estar disponíveis quando necessário. Os autores descrevem esses princípios da forma que se segue:

2.1.3.1 Confidencialidade

É o princípio que visa garantir que a informação seja acessível apenas a pessoas autorizadas. Pfleeger & Pfleeger (2018) enfatizam a importância de mecanismos de controle de acesso, criptografia e proteção física para garantir a confidencialidade.

Para Hintzbergen *et al*. (2018, p. 33), “a confidencialidade assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada”.

Como alguns exemplos de medidas de confidencialidade sobressaem-se a limitação de acesso baseada na necessidade da função desempenada, as políticas de mesa limpa a fim de evitar a exposição de informações sensíveis e a separação de funções e de ambientes - como os de produção, de desenvolvimento e de testes.

2.1.3.2 Integridade

Visa assegurar que a informação não seja alterada sem autorização ou que seja corrompida indevidamente. A integridade significa que a informação é completa, perfeita e intacta, não necessariamente correta. Hintzbergen *et al*. (2018, p. 35)

propõem que “a informação pode ser incorreta ou não autêntica, mas possuir integridade, ou ser correta e autêntica, mas faltar integridade.”
Coelho, Araújo e Bezerra (2014, p. 6) citam:

> A perda de integridade surge no momento em que uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

2.1.3.3 Disponibilidade

Esse princípio se refere à acessibilidade da informação quando for necessária por usuários autorizados. Realça-se a importância de medidas de redundância, tolerância a falhas e planos de recuperação de desastres para garantir a disponibilidade da informação.

Para a garantia desses princípios, Whitman & Mattord (2019) defendem que os usuários devem ter acesso apenas às informações e recursos necessários para realizar suas funções. Isso ajuda a reduzir o risco de acesso não autorizado e minimiza o impacto em caso de comprometimento de contas de usuário.

Há ainda que se entenderem dois elementos muito importantes, que podem ser considerados essenciais para o alcance dos objetivos da corporação em termos de segurança. São eles: autenticação e legalidade, que Sêmola (2003, p. 46) define como:

a) Autenticação – processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controle de identificação desses elementos.
b) Legalidade – característica das informações que possuem valor legal dentro de um processo de comunicação em que todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

Com todos esses conceitos, constata-se que há parâmetros e requisitos claramente definidos para se chegar ao entendimento de quando determinado nível de segurança é alcançado, ou seja, deve-se considerar que há controles que garantam a confidencialidade, a integridade e a disponibilidade dos ativos de informação para que sejam considerados, então, seguros. O nível de segurança requerido depende, sempre, do grau de risco que a empresa decide estabelecer. Para atividades críticas, como aquelas que tratam dados de saúde, por exemplo, o grau de segurança pode ser diferente daquelas informações não sensíveis, como informações sobre clima, tempo, ou outras que em caso de comprometimento não comprometam as operações das empresas ou de seus clientes.

2.1.4 Ciclo de vida da informação

Para se identificarem os riscos aos quais as informações estão expostas, é muito importante entender os momentos pelos quais essas informações passam. Durante cada um desses momentos elas participam de processos diferentes envolvendo diferentes agentes que podem vulnerabilizá-las. Sêmola (2003, p. 9-12) define esses quatro momentos como:

a) Manuseio: momento da criação e manipulação da informação. Tem forte participação do agente humano, que apresenta grande potencial de risco, uma vez que tem inúmeras vulnerabilidades.
b) Armazenamento: envolve em grande parte o agente tecnológico, pois geralmente as informações devem ser armazenadas com alguma tecnologia que garanta seus atributos básicos de segurança, mesmo que seja de forma escrita em papel.
c) Transporte: momento quando a informação corre grande risco, pois está em tráfego entre dois pontos. A captura de tráfego é hoje um alto risco para a informação, pois se ampara em tecnologias que nem sempre são aplicadas adequadamente para garantir sua segurança. Como exemplos têm-se as conversas ao telefone, o envio de *e-mail* e as transações hoje feitas pela Internet, entre outros.
d) Descarte: quando a informação já utilizada corre risco devido à forma de destruição do meio no qual está armazenada. Informações impressas em

papel, gravadas em *compact disks* (CD) ou mesmo quando gravadas em discos rígidos devem ter tratamento adequado para descarte, pois são vulneráveis a vários tipos de ataque, sendo alguns muito simples.

Após entender cada um desses momentos, fica mais fácil imaginar as técnicas pelas quais uma ameaça pode explorar a sua vulnerabilidade. A Figura 1 demonstra a interação entre os momentos de forma mais clara:

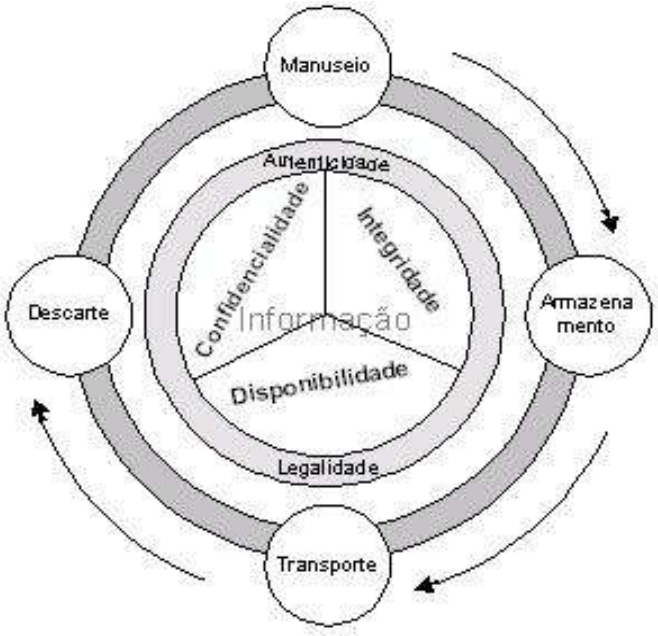

Figura 1
Ciclo de vida da informação e conceitos básicos de segurança.
Fonte: Sêmola, M. (2003). *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Campus (p. 11).

Como se pode notar, os conceitos de segurança da informação e seus aspectos complementares, antes vistos, acompanham todo o ciclo de vida da informação e devem ser observados constantemente. A garantia de segurança deve, então, ser observada em todos os momentos, desde sua criação até seu descarte. Para isso, medidas de proteção devem ser aplicadas em todos esses momentos.

2.1.5 Segurança da informação no contexto brasileiro

No Brasil, a preocupação com a segurança da informação ganhou destaque com a crescente integração do país à economia global e a adoção massiva de tecnologias digitais. Nunes (2020, p. 125) preleciona que:

> Os desafios da segurança da informação no Brasil são muitos e complexos, exigindo medidas abrangentes e multifacetadas para garantir a proteção de dados e sistemas no país. Entre os principais desafios, podemos destacar: a falta de uma cultura de segurança da informação enraizada na sociedade brasileira; a infraestrutura digital precária do país; o marco regulatório em desenvolvimento; a escassez de profissionais qualificados; os investimentos insuficientes em segurança da informação; a desigualdade digital; e os desafios socioeconômicos.

No Brasil o Cert.br, um *Computer Security Incident Response Team* (CSIRT) nacional de último recurso, mantido pelo NIC.br, presta serviços na área de gestão de incidentes de segurança da informação para qualquer rede que utilize recursos administrados pelo NIC.br. O NIC.br é um Núcleo de Informação e Coordenação criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil (CGI.br), que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no país.

O CERT.br divulga regularmente informações sobre as notificações de incidentes de segurança no Brasil, conforme mostra a Figura 2.

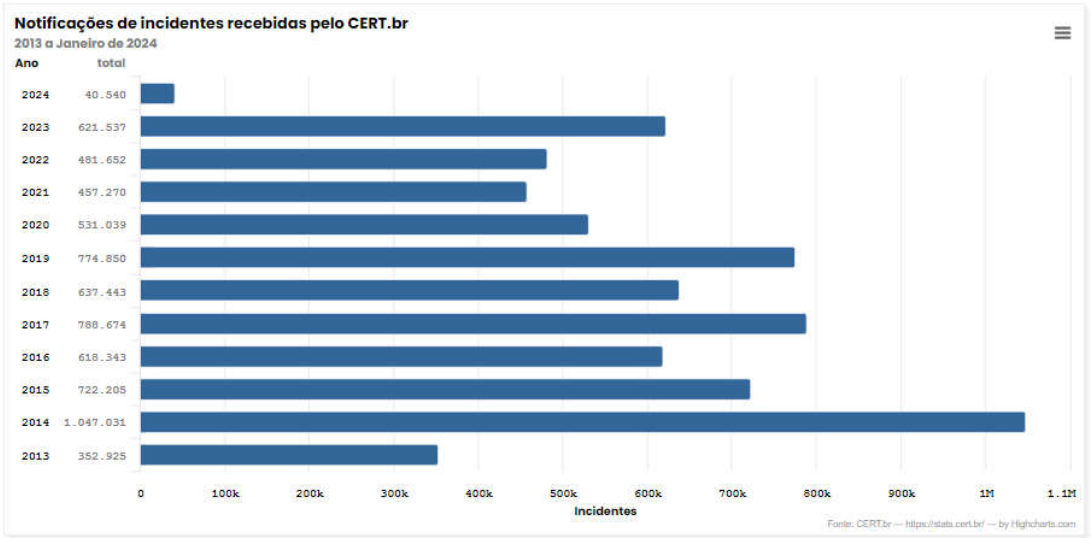

Figura 2
Notificações de incidentes recebidos pelo CERT.br anualmente.
Fonte: https://stats.cert.br/incidentes/.

2.1.6 Desafios e avanços recentes

Nos últimos anos, tem-se observado uma série de avanços significativos no campo da segurança da informação em todo o mundo. A ascensão da inteligência artificial e da aprendizagem de máquina tem possibilitado a detecção mais eficaz de ameaças cibernéticas, enquanto regulamentações como o GDPR na União Europeia têm promovido conscientização sobre a privacidade dos dados.

Historicamente:

> O Brasil apresenta alguns avanços na área de segurança da informação. A criação da Política Nacional de Segurança da Informação e Comunicação (PNSIC) em 2004, a aprovação da Lei do Marco Civil da Internet em 2014 e a criação do Comitê Gestor da Internet no Brasil (CGI.br) são exemplos de iniciativas que demonstram o compromisso do governo brasileiro com a segurança da informação (Pontes & de Sousa, 2018, p. 205)

No Brasil, a criação da Autoridade Nacional de Proteção de Dados (ANPD) e a adoção de padrões de segurança cibernética pelo setor financeiro representam passos importantes na proteção das informações pessoais.

A criação da ANPD representa um marco na evolução da segurança da informação no Brasil. A ANPD tem atuado na regulamentação da Lei Geral de Proteção de Dados (LGPD), na edição de normas e procedimentos, na orientação de empresas e na aplicação de sanções em caso de descumprimento. A ANPD ainda está em fase de desenvolvimento, mas já demonstra impacto positivo na proteção de dados pessoais no país (Autoridade Nacional de Proteção de Dados, 2023).

2.1.7 Medidas de proteção em segurança da informação

Até há pouco tempo, para se proteger um banco bastava ter guardas armados, controle de acesso à agências e um sistema interno de monitoramento por televisão eficiente. Atualmente o dinheiro físico está cada vez menos presente no mercado brasileiro, dando lugar às transações financeiras digitais. Em 2022, de acordo com a Pesquisa Febraban de Tecnologia Bancária 2023, oito em cada 10 transações financeiras realizadas no Brasil foram feitas por meios digitais, como *mobile banking* e internet *banking* (Federação Brasileira de Bancos - Febraban, 2023a; 2023b).

Segundo a pesquisa, 66% das transações foram realizadas por *mobile banking*, ou seja, por aplicativos em *smartphones* e *tablets*; 24% das transações foram feitas por internet *banking*, por meio de *sites* dos bancos. Os 10% restantes se dividem entre caixas eletrônicos, terminais de autoatendimento e outros canais.

Vale ressaltar que esse índice representa crescimento de 30% em relação ao ano de 2021. A pandemia da *disease of coronavirus* 19 (COVID-19) acelerou a adoção dos canais digitais para transações financeiras, impulsionando essa tendência. O Brasil se destaca como um dos países com maior uso de serviços bancários digitais na América Latina.

Com a digitalização da economia, quando o dinheiro passou a circular de forma digital, o foco dos atacantes mudou e apenas a proteção física passou a não ser mais tão eficiente. Com essa transformação do físico para o virtual, outras medidas de segurança passaram a ser propostas e implementadas para proteger a informação contra ameaças, não bastando mais os guardas nas agências e os grandes cofres físicos. Uma delas é o uso de *firewalls*, que ajudam a filtrar o tráfego

de rede e impedir acessos não autorizados (Stallings & Brown, 2015). Além disso, a criptografia desempenha papel crucial na proteção dos dados em trânsito e em repouso, tornando-os ilegíveis para pessoas não autorizadas (Schneier, 2015). A educação e conscientização dos usuários também são aspectos importantes da segurança da informação. Treinamentos regulares podem ajudar os funcionários a reconhecer e evitar ameaças como *phishing* e engenharia social, reduzindo o risco de comprometimento de sistemas e dados (Whitman & Mattord, 2019).

A segurança da informação é um campo multifacetado e dinâmico, essencial para garantir a proteção dos dados em um mundo digital cada vez mais interconectado. Compreender os conceitos básicos da segurança da informação e implementar medidas de proteção adequadas são passos essenciais para mitigar os riscos e garantir a integridade, confidencialidade e disponibilidade das informações.

Outras medidas de proteção são mais amplamente discutidas nos próximos tópicos, à medida que forem abordadas as recomendações da norma ISO 27001.

2.1.8 Sistema de gestão de segurança da informação

O Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto estruturado de políticas, processos e procedimentos que visa proteger os ativos de informação de uma organização. Sua implementação garante confidencialidade, integridade e disponibilidade da informação, mitigando riscos e assegurando a conformidade com requisitos legais e regulatórios.

Ter um SGSI bem definido é um ponto crucial para o sucesso de qualquer organização na era digital, cuja informação é um ativo estratégico. Como visto no tópico anterior, as ameaças à segurança da informação são muitas e estão em constante evolução, tornando a implementação de um SGSI uma medida essencial para proteger os dados contra acesso não autorizado, uso indevido, divulgação, perda ou destruição.

2.1.8.1 Abordagem de um SGSI

O SGSI deve ser estruturado sob uma abordagem de gestão de riscos, conforme preconizado por autores como Galup (2015) e Stoneburner, Goguen & Feringa (2004). Essa abordagem identifica, classifica e avalia os riscos à segurança da informação, priorizando a implementação de medidas de controle para mitigar os riscos em um nível aceitável para a organização.

2.1.8.2 Ciclo de gestão do SGSI

Deming (1986) já propunha que a gestão contínua do SGSI é realizada a partir do ciclo planejamento, execução, verificação e ação (PDCA). Segundo o autor, esse ciclo garante a revisão e atualização periódica do SGSI, assegurando sua efetividade e adequação às necessidades e contexto da organização.

Comparando versões anteriores, conforme Hintzbergen *et al*. (2018), a ISO 27001:2005 exigia o modelo PDCA como a base geral para a implementação e a manutenção do ciclo de gestão do SGSI, assim como a versão revisada da norma em 2013. Watkins (2022) ressalta que, a partir da versão de 2022, a ISO modificou essa definição, porque percebeu que a maioria das organizações já possui seu próprio ciclo de gestão de negócios, sendo ou não baseado no PDCA. Algumas vezes o PDCA pode não ser compatível com o ciclo de gestão adotado por uma empresa em particular. Por essa razão, na ISO 27001:2022 o texto mudou para a obrigação de a organização estabelecer, implementar, manter e melhorar continuamente o sistema de gerenciamento da segurança da informação, em conformidade com os requisitos dessa norma. A norma apresenta requisitos para estabelecer o *information security management system* (ISMS). Embora a obrigação de utilizar o ciclo PDCA tenha sido revista e retirada, o conceito pode ser utilizado como referência e, por isso, será detalhado adiante.

Coelho *et al.* (2014, p. 74) esclarecem que o modelo PDCA compõe um conjunto de ações sequenciais, cuja sigla é composta basicamente por: P (*plan*: planejar), D (*do*: fazer, executar), C (*check*: verificar, controlar) e finalmente o A (*act*: agir, atuar

corretivamente). Os autores explicam um pouco mais cada uma dessas atividades da seguinte forma:

Plan (estabelecer o SGSI): define que se deva estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação, para produzir resultados de acordo com objetivos globais de uma organização, ou seja, deve haver um alinhamento estratégico desde o início dos trabalhos, quando as ações são planejadas.

Do (implementar e operar o SGSI): requer que a política, controles, processos e procedimentos do SGSI sejam implementados e operados adequadamente.

Check (monitorar e analisar criticamente o SGSI): requer que haja um procedimento para avaliar e, quando aplicável, medir o desempenho de um processo frente à política, aos objetivos e experiência prática do SGSI, e que os resultados sejam acrescentados à direção, para a análise crítica.

Act (manter e melhorar o SGSI): nessa etapa devem-se executar as ações corretivas e preventivas baseadas nos resultados de um processo de auditoria interna do SGSI e na análise crítica realizada pela direção, durante a checagem, buscando a melhoria contínua do SGSI.

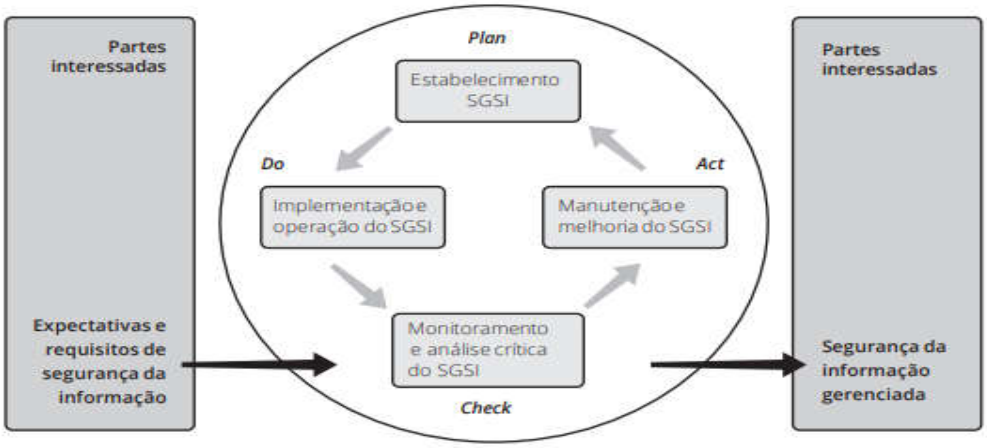

Figura 3
Ciclo PDCA aplicado ao SGSI.
Fonte: Coelho, F. E. S., Araújo, L. G. S., Bezerra, E. K. (2014). *Gestão da Segurança da Informação NBR 27001 e NBR 27002*. Rio de Janeiro: Escola Superior de Redes (p. 74).

2.1.8.3 Conformidade com normas

A implementação do SGSI pode ser orientada por normas internacionais como a ISO 27001, como sugerem Bezerra, Souza e Oliveira (2019), pois esta fornece requisitos específicos para a gestão de segurança da informação. A certificação em normas, como a própria ISO 27001, demonstra o compromisso da organização com a segurança da informação e pode trazer benefícios como aumento da confiança dos clientes e parceiros, redução de custos e melhor reputação.

2.1.8.4 Considerações adicionais sobre o SGSI

a) Liderança e compromisso: o sucesso do SGSI depende do engajamento e compromisso da alta gerência e de todos os colaboradores da organização, como enfatizam De Haes, S., & Van Grembergen, W. (2009).
b) Comunicação e conscientização: a importância da segurança da informação deve ser comunicada a todos os colaboradores, com treinamentos e campanhas de conscientização, como recomendam Pfleeger & Pfleeger (2018).
c) Revisão e atualização: o SGSI deve ser revisado e atualizado periodicamente para garantir sua efetividade e adequação às necessidades e contexto da organização.

2.2 O conceito de *CloudComputing*

O conceito de *CloudComputing* pode ser compreendido como uma evolução das tecnologias disponíveis atualmente. Os fundamentos desse modelo têm suas origens na década de 50, quando as organizações e instituições de educação deram prioridade à otimização dos grandes computadores utilizados à época, permitindo o acesso por meio de terminais, de forma a compartilhar a capacidade de processamento disponível. Desde então, podem-se identificar seis fases de desenvolvimento, cada uma muito relevante no seu tempo (Berger, 2009):

a) Primeira fase: nas décadas de 50 a 70 havia computadores centrais com grande capacidade de processamento para a época e que eram acessados

por meio de terminais. Os terminais eram computadores simples que não dispunham de capacidade de processamento, ou seja, tudo acontecia de fato no processador do computador central.

b) Segunda fase: nos anos 1980 iniciou-se o movimento de popularização dos computadores pessoais, que ganharam capacidade de processamento por um preço acessível e permitiu a expansão do uso dos computadores de forma diferente.
c) Terceira fase: os computadores pessoais passaram a ser conectados a servidores centrais, sendo interligados por redes locais.
d) Quarta fase: as redes locais evoluíram e deram origem a uma rede global, a Internet, que viabilizou o compartilhamento de recursos entre computadores remotos de forma global.
e) Quinta fase: marcada pela capacidade de se compartilhar o processamento e o armazenamento dos computadores, conhecido como computação em grade ou *grid computing*.
f) Sexta fase: a partir da computação distribuída no modelo de grade, da melhoria com novos protocolos de compartilhamento, são criadas as condições que permitiram a origem do conceito de *CloudComputing*.

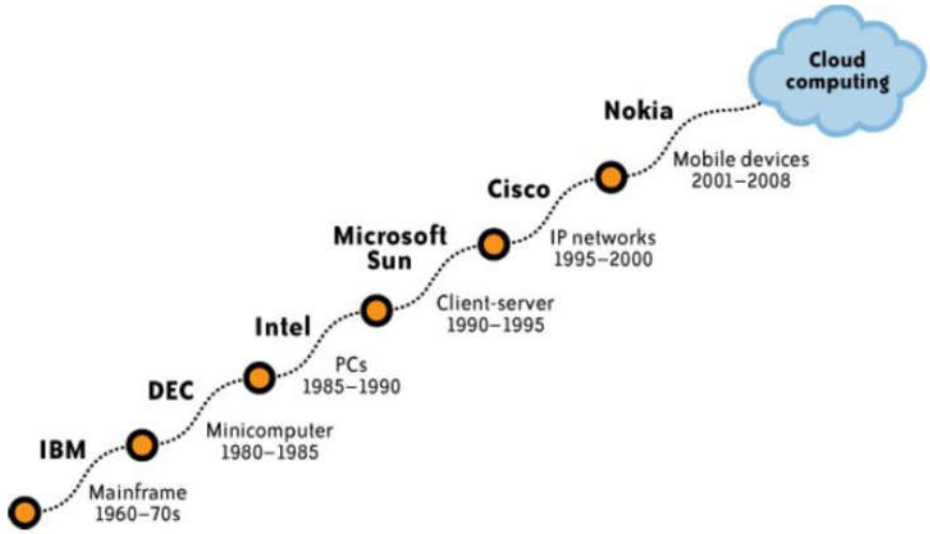

Figura 4
Evolução tecnológica.
Fonte: Mather, T., Kumaraswamy, S., & Latif, S., 2009. *Cloud security and privacy.* s.l.: O'Reilly.

Alguns marcos históricos na etapa inicial da evolução dos serviços de *Cloud* são citados a seguir (Mohamed, 2009).

Em 1999 foi realizado o lançamento da primeira solução de aplicação empresarial oferecida via Internet de forma mais popular: o *salesforce*.

Em 2002 a Amazon lançou seu modelo de serviços via Internet, conhecido como *Amazon Web Services*, um dos principais serviços ofertados até a atualidade, disponibilizando uma série de serviços, iniciando por modelos de armazenamento, processamento e agregando inteligência humana.

Em 2006, novamente puxado pela *Amazon,* foi lançada uma novidade em sua aplicação comercial, *Elastic Compute Cloud* (EC2), que basicamente é uma oferta de plataforma na qual os clientes passaram a conseguir executar suas próprias aplicações de forma remota.

Em 2009 foi lançado o conceito de *Web* 2.0, que abriu o mercado para o aparecimento de outros fornecedores de serviços de *Cloud*, como o *Google* e a *Microsoft*.

O *National Institute of Standards and Technology* (NIST, 2011) define *CloudComputing* como um modelo de computação em que recursos computacionais, como redes, servidores, armazenamento, aplicativos e serviços, são fornecidos como um serviço por um provedor de nuvem para clientes que podem acessá-los pela Internet.

Essa definição refere-se a vários modelos e características, cuja relação é ilustrada na Figura 5:

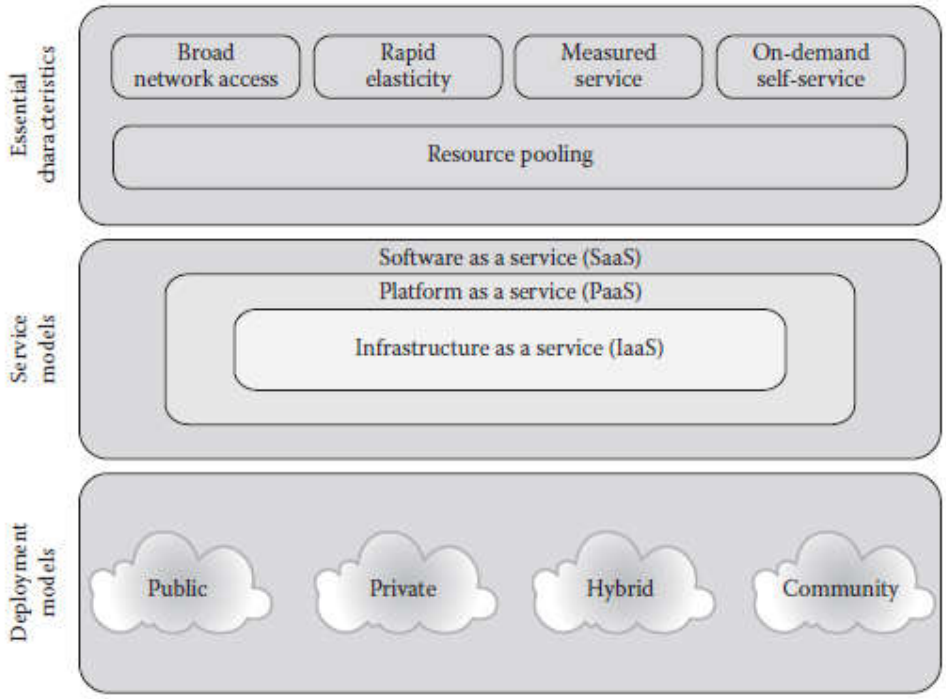

Figura 5
Elementos da *CoudComputing* segundo o NIST (2011).
Fonte: https://www.nist.gov/cyberframework.

2.2.1 Elementos essenciais de CloudComputing

Ainda segundo o NIST (2011), o modelo de *CloudComputing* agrega as seguintes características essenciais:

a) Amplo acesso à rede: recursos disponíveis pelas redes a partir de mecanismos padronizados e que promovem o uso por plataformas heterogêneos como telefones celulares, *laptops*, *desktops* ou outros serviços de *software* baseados em nuvem.
b) Elasticidade rápida: o modelo de *CloudComputing* oferece a capacidade de expandir e reduzir recursos de acordo de acordo com sua necessidade de serviço específica. Uma empresa pode precisar de representativo número de servidores durante determinada época do ano, sendo liberados após passada tal necessidade.
c) Utilização do serviço: aqui é necessário controlar e otimizar o uso de recursos aproveitando uma capacidade de medição em algum nível de abstração

apropriado ao tipo de serviço, proporcionando transparência tanto para o fornecedor quanto para o consumidor do serviço utilizado.

d) Autoatendimento sob demanda: um consumidor pode unilateralmente provisionar recursos como servidores e armazenamento em rede, de forma automática e conforme necessário, sem exigir interação humana com cada prestador de serviço.
e) Agrupamento de recursos: o provedor pode oferecer recursos agrupados para atender vários consumidores, usando um modelo multiclientes, com diferentes recursos físicos e recursos virtuais atribuídos dinamicamente e reatribuídos de acordo com a demanda do consumidor.

2.2.2 Modelos de oferta dos serviços de Cloud

Embora o mercado de *Cloud* seja algo bastante difundido mundialmente, a oferta dos serviços ocorrem basicamente em quatro modelos específicos:

2.2.2.1 *Cloud* pública

Esse é o modelo mais amplamente utilizado e conhecido em termos de *Cloud*, uma vez que é o que se encontra disponível a qualquer indivíduo ou organização, bastando um acesso à Internet para se conectar, e pode ser acessado de forma quase imediata. O NIST (Mell & Grance, 2011; NIST, 2011) define esse modelo como uma infraestrutura localizada dentro da propriedade do fornecedor que é ofertada para uso aberto ao público em geral.

Nesse modelo, a gestão da segurança e operações diárias é atribuída ao fornecedor, deixando pouco ou nenhum controle ou conhecimento acerca da segurança física e lógica da infraestrutura subjacente aos clientes (Mather & Kumaraswamy, 2009).

Segundo Krutz & Vines (2010, p. 45), o uso de uma *Cloud* pública, muitas vezes chamada também de *Cloud* externa, pode proporcionar economias de custos quase imediatas para uma organização. O fato de contar com infraestrutura compartilhada, hospedagem remota e licenciamento e provisionamento dinâmicos é forte atrativo

para uma empresa contratante. A implementação da *Cloud* pública também pode ser uma grande ajuda na remoção da carga paralisante de manutenção da infraestrutura nas organizações de tecnologia da informação (TI). A Figura 6 exemplifica esse modelo.

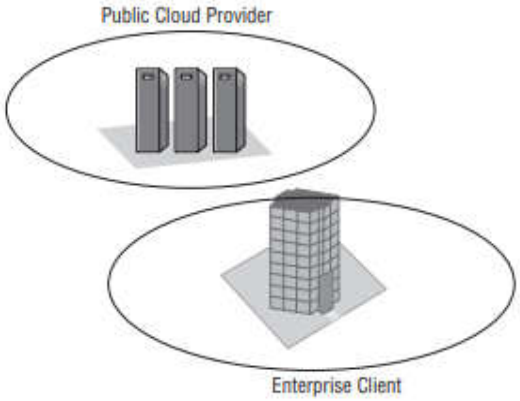

Figura 6
Exemplo de *Cloud* pública.
Fonte: Krutz, R. L., & Vines, R. D. (2010). *CloudSecurity: A comprehensive guide to secure cloud computing.* Wiley Publishing.

2.2.2.2 *Cloud* privada

Nesse modelo, a infraestrutura subjacente é desenvolvida e gerida exclusivamente para um cliente específico, podendo o fornecedor pertencer à mesma organização ou a *Cloud* pertencer à organização. Seus recursos podem estar alocados na infraestrutura da organização ou hospedada exteriormente numa infraestrutura gerida por terceiros. Uma *Cloud* privada oferece ao cliente mais controle sobre a infraestrutura e sobre os recursos computacionais (Jansen & Grance, 2011) que o modelo de *Cloud* pública.

Krutz & Vines (2010, p. 48) esclarecem:

> As nuvens privadas diferem das nuvens públicas porque a infraestrutura associada a uma nuvem privada é normalmente dedicada a uma única empresa e não é partilhada com nenhuma outra empresa. Essa infraestrutura pode incluir muitos escritórios corporativos, parceiros de negócios, clientes/fornecedores de Intranet, revendedores ou quaisquer outros grupos envolvidos em um relacionamento comercial com a empresa.

Comparando os modelos, a segurança é considerada mais rigorosa numa implementação de *Cloud* privada do que *Cloud* nuvem pública. Claramente para essa afirmação se sustentar, as melhores práticas de segurança devem ser seguidas, mas uma empresa que tenha preocupações de segurança, risco ou conformidade pode certamente querer exercer o controle que uma *Cloud* privada pode oferecer, já que ela possui a infraestrutura e tem controle sobre como os aplicativos são implantados nela. A Figura 7 demonstra esse modelo:

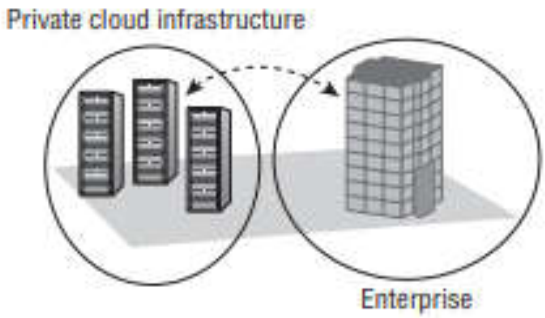

Figura 7
Exemplo de *Cloud* privada.
Fonte: Krutz, R. L., & Vines, R. D. (2010). *CloudSecurity: A comprehensive guide to secure cloud computing.* Wiley Publishing (p. 49).

2.2.2.3 *Cloud* híbrida

Já no modelo de *Cloud* híbrida tem-se a junção de dois ou mais dos modelos tratados anteriormente. Essa abordagem pode trazer benefícios ao cliente *Cloud,* por permitir o uso de diferentes tipos de *Cloud* para diferentes objetivos. Permite, ainda, quando necessário, recorrer a recursos que podem aumentar a capacidade de acordo com picos de acordo com necessidades específicas, temporariamente, liberando uma capacidade extra de um fornecedor de *Cloud* (Buyya *et al*., 2011).

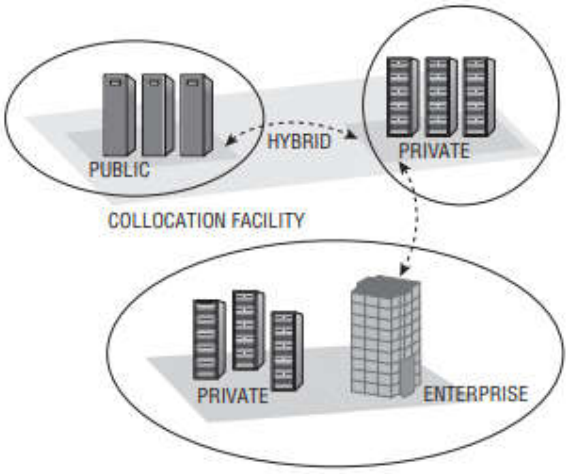

Figura 8
Exemplo de *Cloud* híbrida.
Fonte: Krutz, R. L., & Vines, R. D. (2010). *CloudSecurity: A comprehensive guide to secure cloud computing.* Wiley Publishing (p. 50).

2.2.2.4 *Cloud* comunitária

Esse é um modelo que fica, conceitualmente, entre os modelos de *Cloud* pública e privada. Ainda de acordo com o NIST (Mell & Grance, 2011; NIST, 2011), uma *Cloud* comunitária é uma infraestrutura partilhada por várias organizações, pertencendo a uma comunidade específica e partilhando objetivos. A gestão pode ser efetuada pelas organizações ou por terceiros e a sua localização pode ser interna ou externa.

Existem alguns tipos de serviço de nuvem disponíveis atualmente, enumerados na sequência.

Como citado anteriormente, a *CloudComputing* é um modelo de computação que fornece recursos de computação, armazenamento e rede sob demanda, acessados pela Internet. O NIST (2011) preceitua que os serviços de *CloudComputing* são divididos em três categorias principais:

a) Infraestrutura como serviço (IaaS): fornece recursos de infraestrutura de TI, como servidores, armazenamento e rede. Os clientes podem provisionar e gerenciar esses recursos por conta própria.

b) Plataforma como serviço (PaaS): fornece uma plataforma de desenvolvimento e implantação de aplicativos. Os clientes podem usar essa plataforma para criar e executar aplicativos sem precisar se preocupar com a infraestrutura subjacente.
c) *Software* como serviço (SaaS): fornece *software* como um serviço. Os clientes podem acessar aplicativos e dados pela Internet, sem precisar instalá-los ou administrá-los localmente.

Além dessas categorias Hurwitz, Blosch, Nugent & Ray (2010) mencionam a existência, também, de outros serviços de *CloudComputing* especializados, como:

a) Serviços de banco de dados como serviço (DBaaS): fornecem bancos de dados como um serviço. Os clientes podem usar esses bancos para armazenar e gerenciar dados.
b) Serviços de análise como serviço (AaaS): fornecem serviços de análise de dados. Os clientes podem usar esses serviços para analisar dados para obter *insights*.
c) Serviços de inteligência artificial como serviço (AIaaS): fornecem serviços de inteligência artificial. Os clientes podem usar esses serviços para criar e implantar aplicações de inteligência artificial.

2.2.3 Responsabilidade em cada modelo de serviço

Sobre a responsabilidade em termos de riscos de segurança da informação em ambientes de *CloudComputing*, Winkler (2011) afirma que estão diretamente ligados ao modelo de serviço prestado, seja SaaS, PaaS ou IaaS. O grau de risco aumenta nessa mesma sequência, o que aumenta o grau de responsabilidades do cliente na gestão da segurança da informação e dos riscos associados.

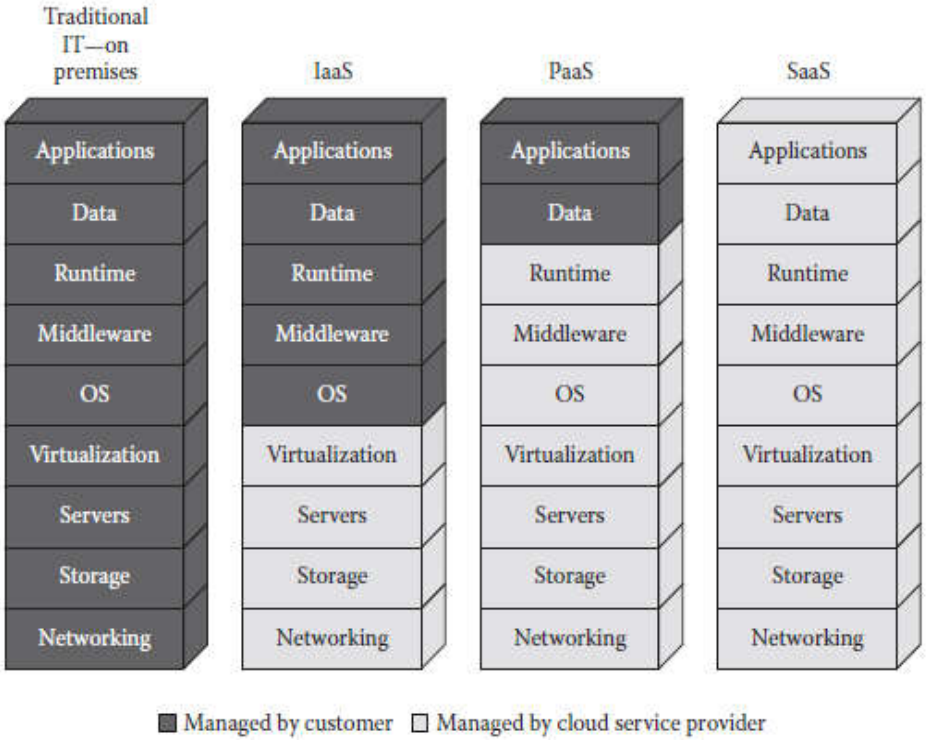

Figura 9
Responsabilidades dos envolvidos, nos diversos modelos.
Fonte: Vacca, J. R. (2016). *Cloud Computing Security*. Foundations and Challenges.

2.2.4 Benefícios da CloudComputing

Mesmo com os riscos mencionados, há de se observar que os serviços de *CloudComputing* oferecem uma variedade de benefícios para as organizações, incluindo:

a) Redução de custos: os serviços de *CloudComputing* podem ajudar as organizações a reduzir os custos de infraestrutura de TI.
b) Flexibilidade: os serviços de *CloudComputing* permitem que as organizações escalem ou reduzam seus recursos conforme necessário.
c) Agilidade: os serviços de *CloudComputing* permitem que as organizações lancem novos produtos e serviços mais rapidamente.
d) Segurança: os serviços de *CloudComputing* são projetados para serem seguros e confiáveis.

A tecnologia de *CloudComputing* vem passando por rápida evolução, com novos serviços sendo lançados constantemente. As organizações que desejam aproveitar os benefícios da *CloudComputing* devem avaliar seus requisitos cuidadosamente para escolher os serviços certos, buscando a segurança e a independência da tecnologia dos grandes representantes dessa tecnologia atualmente. Dessa forma, o ambiente de *CloudComputing* carece de uma visão de segurança da informação bastante focada e estruturada. Embora haja diversos *frameworks* de segurança aplicáveis, este trabalho considera a norma ISO 27001.

2.3 A norma ABNT ISO/IEC 27001:2022

A norma ISO 27001 é uma evolução da norma BS7799, que foi publicada pela primeira vez em 1995 pela *British Standards Institution* (BSI). A BS7799 era um código de prática que fornecia orientação para a implementação de um sistema de gestão da segurança da informação (SGSI).

A primeira versão da norma ISO 27001 foi publicada em 2005 e constituiu um padrão internacional que estabelecia os requisitos básicos para um SGSI. Esse padrão incorporou os requisitos da BS7799 e adicionou novos requisitos, como a necessidade de uma abordagem de risco e a necessidade de melhoria contínua.

Em 2006, a norma foi traduzida e publicada pela Associação Brasileira de Normas Técnicas (ABNT), com o nome de ISO/IEC 27001:2005 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos.

Krebs (2021) reconhece que a ISO 27001 é um marco na evolução da segurança da informação. É um padrão globalmente aceito que fornece um *framework* abrangente para a proteção de ativos de informação.

No início, a adoção da norma no Brasil foi lenta, mas vem crescendo nos últimos anos. Em 2023, o número de organizações certificadas pela ISO 27001 no Brasil é estimado em 1.500.

Na introdução da norma ISO 27001 há uma afirmação de que:

> [...] o documento foi elaborado para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação. A adoção de um sistema de gestão de segurança da informação constitui uma decisão estratégica para uma organização. O estabelecimento e a implementação do sistema de gestão de segurança da informação de uma organização são decorrências de suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados e tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo (ISO, 2022, s.p.)

Dessa forma, os controles recomendados podem ser definidos e implementados em qualquer tipo de ambiente, independentemente de sua natureza, embora esta tenha grande influência nas definições que serão tomadas para a implementação dos controles e do próprio sistema de gestão de segurança da informação adotado.

No Brasil, a adoção da norma emergiu como consequência de vários fatores, entre os quais se podem pontuar:

a) A crescente importância da segurança da informação para as organizações, devido ao aumento da dependência das organizações das tecnologias da informação.
b) A crescente importância da questão concernente à segurança da informação em decorrência da recorrente dependência das tecnologias conexas.
c) A necessidade de atender a requisitos legais e regulatórios, como a Lei Geral de Proteção de Dados (LGPD).
d) A busca por vantagem competitiva, uma vez que a certificação pela ISO 27001 pode ajudar as organizações a se diferenciarem de seus concorrentes e aumentar sua confiabilidade.

2.3.1 A crescente conscientização sobre os benefícios da norma

Hadnagy (2022 como citado em Krebs, 2021) afirma que a ISO 27001 é um requisito fundamental para qualquer organização que deseja proteger seus dados e sua reputação. Baseado nas suas afirmações, a adoção da ISO 27001 oferece uma série de benefícios para as organizações, incluindo: mais proteção das informações;

redução do risco de incidentes de segurança; melhoria da conformidade com requisitos legais e regulatórios; redução de custos; melhoria da imagem da organização.

2.3.2 ISO 27001– princípios

Conforme definição da própria norma:

> A ISO/IEC-27001 é um padrão internacional que fornece um conjunto de requisitos para a implementação, manutenção e melhoria contínua de um sistema de gestão de segurança da informação (SGSI). É uma ferramenta valiosa para organizações de todos os tamanhos e setores que buscam proteger seus ativos de informação contra ameaças e riscos (*International Organization for Standardization* - ISO, 2022, s.p.).

Na perspectiva de Mitnick (2002, p. 1):

> A ISO/IEC-27001 é uma ferramenta poderosa que pode ajudar as organizações a proteger seus ativos de informação. É um processo holístico que aborda todas as dimensões da segurança da informação, desde a gestão de riscos até a implementação de controles. A certificação na ISO 27001 é um investimento que vale a pena para qualquer organização que valoriza a segurança de seus dados..

2.3.3 Conceitos e pilares da ISO 27001

A norma ISO 27001 define três pilares da segurança da informação que, conforme pode ser notado, reflete o que autores citados orientam e os próprios conceitos, já citados anteriormente, de segurança da informação:

a) Confidencialidade: a informação deve ser acessível apenas a pessoas autorizadas.
b) Integridade: a informação deve estar correta e completa.
c) Disponibilidade: a informação deve estar disponível quando for necessário.

Para garantir esses pilares, a norma ISO 27001 institui um conjunto de requisitos para o estabelecimento, implementação, manutenção e melhoria contínua de um SGSI, cumprindo a função para a qual foi desenvolvida: determinar um conjunto de

processos, políticas, procedimentos e controles que visam proteger os ativos de informação de uma organização.

Como a norma ISO 27001 é uma ferramenta extremamente eficaz para possibilitar às organizações proteger seus ativos de informação, a certificação nessa norma demonstra o compromisso da organização com a segurança da informação e pode funcionar como um diferencial competitivo no mercado.

Krebs (2019) sugere que o princípio de abordagem de risco é o mais importante da ISO 27001. Ele garante que as organizações tomem medidas para proteger seus ativos de informação contra ameaças e riscos.

Mitnick (2002) esclarece que os controles de segurança, que são a base ISO 27001, são as medidas que as organizações devem implementar para proteger seus ativos de informação.

Cabe destacar que a implementação de controles de segurança da informação em uma organização exige sopesar os riscos e custos envolvidos, ou seja, impõe uma atuação de forma equilibrada.

2.3.4 ISO 27001 – visão geral dos requisitos

Para o desenvolvimento deste trabalho, faz-se importante um entendimento geral acerca da estrutura da norma ISO 27001. Ela se baseia no conceito da tríade confidencialidade integridade e disponibilidade (CID) e determina os requisitos principais, que são divididos em cinco seções básicas. Entre as três primeiras seções estão as questões estruturais da própria norma, como a primeira seção, que traz a definição de escopo do documento. Esta deixa claro que os requisitos estabelecidos são genéricos e podem ser aplicados a qualquer tipo de organização.

Já na segunda seção a norma traz referências normativas: na norma ISO 27001, a referência é a norma ISO/IEC 27000, que é a norma internacional que trata das técnicas de segurança para gestão de sistemas de informação.

A terceira seção contém os termos e definições da própria norma, que também referenciam os mesmos termos da norma ISO 27001. A partir daqui, cabe uma explicação mais detalhada, com os conceitos e orientações da própria norma ISO 27001, sobretudo até a seção 08, por serem o principal foco desta pesquisa.

2.3.4.1 Seção 4: contexto da organização

Os requisitos do domínio 4 são essenciais para garantir que o SGSI seja adequado às necessidades da organização. A organização deve entender seu contexto, incluindo seus objetivos, suas partes interessadas e seus riscos, para poder implementar um SGSI eficaz.

Requisito 4.1: Entendendo a organização e seu contexto
Nesse ponto, a norma define que a organização deve determinar todas as questões, sejam internas ou externas, relevantes ao seu propósito e que possam afetar sua capacidade de alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

Requisito 4.2: Entendendo as necessidades e as expectativas das partes interessadas
A organização deve compreender as necessidades e expectativas de suas partes interessadas, incluindo as relacionadas à segurança da informação.

Requisito 4.3: Definindo o escopo do SGSI
A organização deve definir o escopo do seu SGSI, ou seja, os limites de aplicabilidade, incluindo os ativos de informação, os processos e as atividades abrangidos e os itens citados no requerimento anterior. Hadnagy (2010) defende que essa sessão traz as definições dos primeiros e principais passos para implementar um SGSI eficaz. Com esses controles a organização assegura a compreensão do seu contexto antes de poder implementar controles de segurança.

Requisito 4.4: Sistema de gestão da segurança da informação (SGSI)
Determina que a organização deva estabelecer, implementar, manter e melhorar continuamente um SGSI, incluindo todos os processos necessários e suas interações, de acordo com os requisitos trazidos pela norma.

2.3.4.2 Seção 5: liderança

Krebs (2019) alerta que essa seção, ou domínio, é o coração do SGSI. Ela visa garantir que as organizações estejam comprometidas e que determinem recursos para o apoio necessário a fim de se implementar e manter um SGSI eficaz.

Requisito 5.1: Liderança e comprometimento
A alta direção deve demonstrar liderança e compromisso com o SGSI, assegurando que a política de segurança e os objetivos de segurança da informação da empresa estejam compatíveis com a direção da organização, assegurando a integração dos requisitos do SGSI aos processos da organização, garantindo os recursos necessários ao SGSI e comunicando a importância do sistema aos colaboradores, orientando as pessoas a contribuir para sua eficácia e promovendo a melhoria contínua.

Requisito 5.2: Política de segurança da informação
Conforme Caruso & Steffen (1999, p. 49), “política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção que será dada aos ativos de informação.” Apesar de ser uma definição antiga, seu conceito é ainda válido nos dias de hoje e está totalmente alinhado ao que pretende a norma ANBT NBR ISO/IEC 27001:2022. Nesse sentido, a norma orienta que organização deva estabelecer uma política de segurança da informação que defina seu compromisso com a proteção dos ativos de informação que seja apropriada aos propósitos da organização. Fontes (2012, p. 12) defende que:

> É estrutural que a organização tenha uma política de segurança da informação para que o processo de proteção da informação possa ser elaborado, implantado e mantido. Esta política (ou conjunto de políticas) definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação.

Requisito 5.3: Papéis, responsabilidades e autoridades organizacionais
Na versão de 2013 a norma ISO/IEC 27001 definia apenas que a organização deveria definir a estrutura organizacional para o SGSI. Na versão revisada de 2022, a definição é mais completa e detalhada, orientando que a alta direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídas e comunicadas dentro da organização, devendo estruturar e atribuir também as responsabilidades e autoridades para relatar sobre o desempenho do plano dentro da organização.

2.3.4.3 Seção 6: planejamento

Hadnagy (2022) postula que a seção 6 visa garantir que as organizações implementem processos para identificar e mitigar os riscos de segurança da informação antes de implementar os controles requeridos de segurança.

Requisito 6.1: Ações para abordar riscos e oportunidades
A organização deve definir objetivos de segurança da informação que sejam alinhados com seus objetivos gerais. Esse requerimento faz referência aos itens do domínio 04, mais especificamente os requerimentos 4.1 e 4.2, especialmente para assegurar os resultados do SGSI a partir de um processo de gestão de riscos que vise prevenir e reduzir os efeitos indesejados, além de planejar as ações para abordar os riscos e oportunidades, avaliando sua eficácia e alcançando a melhoria contínua.

Requisito 6.1.2: Avaliação de riscos de segurança da informação
A organização deve avaliar os riscos de segurança da informação que podem afetar seus ativos de informação. Conforme Hintzbergen *et al*. (2018, p. 37), “um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios”.

Requisito 6.1.3: Tratamento de riscos
Os requisitos do domínio 6 são essenciais para garantir que a organização tenha uma abordagem proativa à segurança da informação. A organização deve identificar e mitigar os riscos antes de eles causarem danos.

Nesse sentido, a ISO 27001 recomenda que todo o processo de tratamento dos riscos de segurança da informação seja orientando para estratégias que evitem sua materialização, que podem ser de redução do risco, retenção, se evitar o risco ou ainda transferi-lo. Alinhado a essas recomendações, Hintzbergen *et al*. (2018) reforçam que uma decisão de tratamento do risco precisa ser tomada para cada um dos riscos que a organização identificar, de forma individual. Os possíveis controles para o tratamento do risco incluem, entre outros: aplicar os controles adequados que ajudem a reduzir os riscos, não permitindo ações que possam causar riscos, evitando-os ou transferindo os riscos associados a outras partes, por exemplo, seguradoras ou fornecedores. O autores também orientam a uma estratégia de aceite do risco, contanto que esteja alinhado aos objetivos de negócio da organização. Essa não é uma estratégia recomendada na ISO 27001.

A Figura 10 representa graficamente o processo de tratamento de risco definido pela ABNT na norma ISO/IEC 27005:2023, que é específica para o tratamento dos riscos, citando as estratégias e fluxos recomendados:

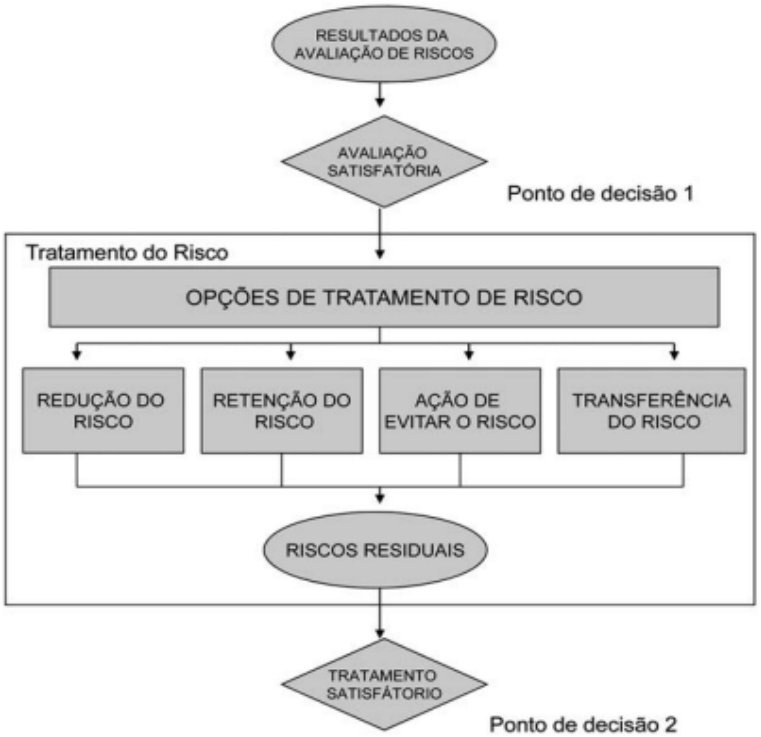

Figura 10
Processo de tratamento do risco.
Fonte: Associação Brasileira de Normas Técnicas – ABNT. (2023). *ABNT NBR ISO/IEC 27005:2023 - Gestão de riscos na segurança da informação*. Rio de Janeiro: ABNT.

Requisito 6.2: Objetivos da segurança da informação e planejamento para alcançá-los

Conforme Hintzbergen *et al*. (2018), a segurança da informação deve ser alcançada a partir da implementação de um conjunto de controles que precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, visando assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos. Tudo isso deve ser feito em conjunto com outros processos de gerenciamento de negócio.

Os objetivos de segurança da informação não podem, então, estar em conflito com os objetivos do negócio. Portanto, precisam ser consistentes com a política de segurança da informação definida, ser mensuráveis, monitorados, estar sempre atualizados e ser comunicados e disponibilizados a todos os envolvidos formalmente.

Requisito 6.3 Planejamento de mudanças

O objetivo desse requisito é garantir que todas as mudanças necessárias no SGSI sejam conduzidas de forma planejada.

2.3.4.4 Domínio 7: apoio

O principal objetivo desse domínio é garantir a implementação de um SGSI eficaz, pelo envolvimento das pessoas envolvidas na manutenção da segurança do ambiente, tendo definidas as responsabilidades, os programas de divulgação e conscientização. Esse foi o domínio que sofreu mais alterações se se compararem as versões das normas ABNT IEC 27001 de 2013 e de 2022. Nesse sentido, a nova versão da norma reforça que a “organização deve determinar e prover recursos necessários para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação” (ISO, 2022). Em resumo, a organização deve definir as competências das pessoas envolvidas no SGSI, estando cientes de sua responsabilidade, o que é recomendado por intermédio de um programa de conscientização com um processo consistente de comunicação e baseado em documentações sempre atualizadas.

Fontes (2012) adverte que todo usuário que tenha acesso a um sistema de informação da organização deve passar por um processo em que seja conscientizado e treinado em segurança da informação, uma vez que o aspecto humano é o fator positivo no processo de proteção da informação. Para isso, a organização deve manter um programa ativo de conscientização, de forma estruturada e registrada, a fim de garantir a proteção adequada e que também poderá atender aos requerimentos de conformidade com processos de auditoria.

2.3.4.5 Domínio 8: operação

Esta seção faz a referência direta e prática aos controles dos processos que devem ser estabelecidos pelas organizações, para atendimento dos requerimentos da Seção 06, citada anteriormente. Esses controles são o principal foco desta pesquisa e serão tratados de forma bastante detalhada mais adiante.

De forma resumida, esse domínio especifica que deva haver um processo para planejamento e controle operacionais, para avaliação e também para tratamento de riscos de segurança da informação. Referem-se basicamente a todos os controles tecnológicos que são recomendados a fim de tratar os possíveis riscos identificados pelas organizações, sendo organizados em 34 requerimentos técnicos, citados em um anexo da norma.

2.3.4.6 Seção 9: avaliação de desempenho

Krebs (2019) afirma que essa seção é essencial para garantir que o SGSI seja eficaz e que a organização deva monitorar, medir, analisar e avaliar seu SGSI regularmente. A afirmação do autor está bastante alinhada aos próprios itens de controle definidos na norma, que traz as orientações específicas e requerimentos para monitoramento, medição, análise e avaliação e para a auditoria interna. Da mesma forma, deve-se estabelecer um processo de análise crítica pela alta direção, de maneira a analisar se o SGSI está adequado, pertinente e eficaz.

Nesse sentido, cabe à organização planejar, estabelecer, implementar e manter um programa de auditoria interna que tenha frequência, métodos e responsabilidades

definidos, assim como os critérios de execução e de demonstração à gestão pertinente.

Watkins (2022, p. 19) assim se posiciona:

> As auditorias internas podem ser utilizadas para diversos fins, mas um dos principais motivos da implantação de um programa interno de gestão de auditoria é monitorar a conformidade entre os requisitos do sistema de gestão e a prática de trabalho. As auditorias internas são encomendadas pela organização e proporcionam uma oportunidade de rever o nível de conformidade e eficácia do SGSI.

2.3.4.7 Seção 10: melhoria

Esta é a última seção da norma ISO 27001. Apesar de o modelo PDCA, já visto anteriormente, não ser uma referência obrigatória para implementação de um SGSI, a orientação de um processo que seja continuamente avaliado e melhorado se mantém. Conforme a própria norma traz, isso garante a pertinência e a eficácia do SGSI. Nesse processo de melhoria, toda não conformidade identificada deve gerar uma ação para controlá-la e corrigi-la, além de lidar com as consequências, garantindo uma documentação completa para se evidenciarem as características dessas não conformidades, como a natureza, as ações tomadas pela organização e o resultado das ações corretivas.

2.3.5 Referências de controles da segurança da informação

Como pode ser notado, os requisitos da norma ISO 27001 são inter-relacionados e devem ser implementados de maneira integrada para garantir a segurança dos ativos de informação de uma organização.

Esses requerimentos foram definidos para serem implementados em qualquer ambiente. Como se pode verificar a partir da leitura da norma, não há qualquer referência direta a um ambiente de *CloudComputing*. Então, as empresas devem adaptar os controles para que atendam aos requisitos e consigam cumprir o objetivo, o que depende de vários pontos, inclusive o risco a que aquele ambiente é exposto e os recursos disponíveis para controle.

A norma traz ainda um anexo com as referências de controles de segurança da informação, que são o principal foco desta pesquisa. Esses controles são divididos da seguinte forma:

2.3.5.1 Controles organizacionais

Aqui são descritos 37 controles que têm referência direta com a seção 05 citada anteriormente, como a definição de política de segurança da informação, papéis e responsabilidades, segregação de funções, contatos com autoridades e outros, todos voltados a estabelecer uma estrutura de governança para a segurança do ambiente organizacional. São recomendações, documentações e processos de forma geral.

2.3.5.2 Controle de pessoas

São determinados oito controles que, como o próprio nome já deixa claro, são aplicados às pessoas envolvidas no ciclo de vida da informação, desde processos de contratação, acordos de confidencialidade, planos de conscientização às mais recentes necessidades de trabalho remoto e as recomendações para que ocorra de forma segura. Esses controles têm também uma referência direta com a seção 06 da norma, como citado anteriormente.

2.3.5.3 Controles físicos

Neste subitem são tratados os 14 controles de acesso físico, com relação direta à seção 07 da norma, voltados para a segurança das instalações de forma geral, como os requisitos de monitoramento, tratamento de mídias, segurança no cabeamento, manutenção de equipamentos e serviços de infraestrutura, entre outros. Normalmente, dependendo da forma e do serviço ofertado pelo provedor de *CloudCompting*, essa é a parte em que o cliente normalmente não é envolvido, pois o próprio provedor é o responsável pela garantia da segurança física de seu ambiente. Ao cliente cabe avaliar o provedor e solicitar as comprovações, muitas vezes feitas por meio de relatórios de conformidade com padrões de segurança ou legislações, de que os requerimentos básicos são atendidos.

2.3.5.4 Controles tecnológicos

Nessa seção são descritos 34 controles de segurança da informação que podem afetar diretamente o cliente contratante do serviço de *CloudComputing*. Esses controles, que são ligados diretamente à seção 08 da norma, podem afetar a confidencialidade, a integridade ou a disponibilidade dos dados dos contratantes.

Dependendo do modelo de contratação, o cliente pode ser totalmente responsável por mantê-los, dependendo da forma de contratação. Alguns provedores de *CloudComputing* já ofertam os serviços de consultoria para manutenção desses controles, mas são, normalmente, serviços contratados à parte e específicos para cada controle descrito, implementados de acordo com a definição de prioridades do contratante, conforme orientado pelas consultorias.

Dado que esses controles são o ponto central deste estudo, eles serão detalhados a seguir, trazendo as orientações da própria norma ISO 27001, com alguns comentários e referências de autores para aqueles mais relevantes e que necessitem de mais detalhamento, a fim de se esclarecer o objetivo de cada controle. São eles:

- Dispositivos *endpoint* do usuário - os itens dos equipamentos que contenham mídia de armazenamento devem ser verificados para assegurar que quaisquer dados sensíveis e *software* licenciado tenham sido removidos ou sobrescritos com segurança antes do descarte ou reutilização.
- Direitos de acessos privilegiados - a atribuição e o uso de direitos de acessos privilegiados devem ser restritos e gerenciados.
- Restrição de acesso à informação - o acesso às informações e a outros ativos associados deve ser restrito de acordo com a política específica por tema sobre controle de acesso. Coelho *et al.* (2014, p. 97) observam que “a restrição de acesso é uma medida preventiva”.
- Acesso ao código-fonte - os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de *software* devem ser adequadamente gerenciados. Coelho *et al.* (2014, p. 82) defendem que “para manter aplicações e sistemas seguros contra alterações não autorizadas ou

acidentais, é importante também ter controles de acesso rígidos ao código-fonte e a informações afins". Os autores complementam que o controle de acesso ao código-fonte é também importante para "proteger qualquer propriedade intelectual que seja usada para desenvolver sistemas e aplicativos".

- Autenticação segura - Tecnologia e procedimentos de autenticação segura devem ser implementados, com base em restrições de acesso à informação e à política específica por tema de controle de acesso. Esse controle requer cuidados especiais ao processo de autenticação e ao princípio de mínimo privilégio, a fim de garantir que apenas os acessos necessários sejam concedidos. Não apenas em termos de tecnologia, mas ao próprio processo de autenticação, que muitas vezes pode conter fragilidades. Nesse sentido, Coelho *et al.* (2014, p. 82) destacam que "a concessão de informação de autenticação seja controlada por um processo de gerenciamento formal".
- Gestão de capacidade - o uso dos recursos deve ser monitorado e ajustado de acordo com os requisitos de capacidade atual e esperada. Hintzbergen *et al*. (2018, p. 105) ressaltam que "o gerenciamento da capacidade também é sobre definir e monitorar desempenho e espaço de bancos de dados e consumo de memória. Um cuidado especial deve ser dado aos sistemas críticos".
- Proteção contra *malware* - proteção contra *malware* deve ser implementada e apoiada pela conscientização adequada do usuário. Humphreys (2016, p. 105) apregoam:

> A proteção contra *malware* precisa de processos e controles de gerenciamento adequados. Para começar, a organização deve produzir uma política que proíba o uso de *software* não autorizado e depois implementar controles para prevenir ou detectar o uso de tal *software*. A organização também deve ter uma política relativa ao *download* ou recebimento de arquivos e *software*.

- Gestão de vulnerabilidades técnicas - informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas; a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas. A norma ISO/IEC-27002:2022 (2022, p. 126) orienta que:

As organizações estabeleçam procedimentos de emissão de relatórios de vulnerabilidade, formulários de emissão de relatórios *on-line* e uso de fóruns apropriados de inteligência de ameaças ou compartilhamento de informações. Convém que as organizações também considerem programas de recompensa por *bugs,* em que as recompensas sejam oferecidas como um incentivo para ajudar as organizações na identificação de vulnerabilidades, a fim de corrigi-las adequadamente.

- Gestão de configuração - as configurações, incluindo configurações de segurança, de *hardware*, *software*, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente. Conforme a norma ISO/IEC-27002:2022 (2022, p. 129), o objetivo desse controle é “assegurar que o *hardware*, o *software* , os serviços e as redes funcionem corretamente com as configurações de segurança necessárias e que a configuração não seja alterada por alterações não autorizadas ou incorretas”. Sem uma gestão de configuração adequada, baseada em ferramentas e processos determinados pela organização, o risco de haver configurações equivocadas, desnecessárias ou que tragam risco ao ambiente aumentam. O Relatório de Segurança em Nuvem da *Check Point Software*, que entrevistou 775 profissionais de cibersegurança, revelou que 77% das violações de dados em *Cloud* são causados por configurações incorretas. O relatório também indica aumento de 10% nos incidentes de segurança na nuvem em relação ao ano anterior (https://www.convergencia digital.com.br/Cloud-Computing/Incidentes-de-seguranca-na-nuvem-cresceram-154%25-em-12-meses-65920.html?User ActiveTemplate=mobile).
- Em estudo de 2021, a IBM divulgou que 95% das violações de dados em nuvem podem ser evitados com medidas adequadas de segurança. O estudo também identificou que as configurações incorretas são um dos principais vetores de ataque em ambientes de nuvem. (https://www.ibm.com/reports/ data-breach).
- Exclusão de informações - as informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias. Essa medida visa diminuir o risco de que informações que não sejam mais necessárias possam ser expostas. A organização deve estabelecer uma política e processos que

garantam que essas informações sejam excluídas com segurança após um período predeterminado.

- Mascaramento de dados - o mascaramento de dados deve ser usado de acordo com a política específica por tema da organização sobre o controle de acesso e outras políticas específicas por tema relacionadas e requisitos do negócio, levando em consideração a legislação aplicável.
- Prevenção de vazamento de dados - as medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações sensíveis. Em um estudo de 2021, o Gartner previu que, até 2025, 75% das grandes empresas utilizarão ferramentas para prevenção contra vazamento de dados, conhecidas pela sigla DLP (*Data Loss Prevention*), para proteger seus dados confidenciais. O estudo também identificou que essas ferramentas podem ajudar as empresas a reduzir até 50% do risco de violações de dados (https://www.gartner.com/en).
- O *National Institute of Standards and Technology* (NIST) publicou também um *framework* de segurança da informação que indica que ferramentas contra vazamento de dados constituem um controle essencial para proteger dados confidenciais. A instituição fornece diretrizes para a implementação de ferramentas DLP em diversos ambientes, incluindo físicos, em *endpoints* e na nuvem (https://www.nist.gov/cyberframework). Essas ferramentas podem ajudar a identificar e bloquear o acesso não autorizado a dados confidenciais, reduzindo o risco de violações de dados.
- *Backup* das informações - cópias de *backup* de informações, *software* e sistemas devem ser mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*. Conforme Coelho *et al.* (2014, p. 104):

  > As cópias de segurança (*backups*) são uma importante ferramenta de apoio à continuidade dos serviços e, por consequência, dos negócios; todavia, riscos associados a procedimentos inadequados de *backup* regular causam impactos como desperdício de tempo e recursos e, por conseguinte, perdas financeiras.

Humpreys (2016, p. 130) cita o principal motivo pelo qual os *backups* são necessários para uma organização ou mesmo para usuários comuns: é o de se recuperarem informações perdidas ou corrompidas por conta de alguma falha, desastre ou comprometimento do sistema. Muitas organizações sofrem algum tipo de perda de informações em algum momento. Essa é uma experiência desagradável e comum compartilhada por muitas organizações ou usuários de TI.

- Redundância dos recursos de processamento de informações - recursos de processamento de informações devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade. Dependendo da disponibilidade requerida para o negócio, alguns componentes-chave no processamento das informações devem ser projetados para atuar em regime de alta disponibilidade, contando com ao menos um recurso reserva, que pode estar funcionando de forma ativa ou passiva.
- *Log* - *logs* que registrem atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados. Esse é um recurso-chave que viabiliza o processo de monitoramento, próximo a ser discutido. Segundo Coelho *et al.* (2014, p. 140):

  > *Logs* de auditoria devem ser mantidos de forma a registrar as atividades dos usuários, problemas de segurança, alterações de configuração dos sistemas, todos os acessos realizados, por um período de tempo adequado às atividades de auditoria e monitoramento.

  Um cuidado especial deve ser tomado em relação ao armazenamento e acesso seguros às *logs*. É necessário que seja garantida a integridade desses registros e que o acesso seja restrito apenas a pessoas que possuem a necessidade de negócios justificada, uma vez que as próprias *logs* devem ser consideradas como informações críticas, embora não devam conter dados sensíveis, como senhas.
- Atividades de monitoramento - as redes, sistemas e aplicações devem ser monitoradas quanto a comportamentos anômalos, e ações apropriadas devem ser adotadas para avaliar possíveis incidentes de segurança da informação.

- Coelho *et al.* (2014, p. 55) esclarecem que as atividades de monitoramento "têm por objetivo detectar atividades não autorizadas de processamento da informação de forma a registrar eventos e gerar evidências". Em questão de segurança, as atividades de monitoramento contam, hoje, fundamentalmente com os registros de eventos (*logs*). Esse controle está intimamente ligado, então, ao controle anterior, que diz respeito à necessidade de se manterem *logs* de atividades executadas no ambiente, e com o posterior, que orienta à sincronização dos relógios, recurso sem o qual não se pode garantir com exatidão a ordem de acontecimentos, que podem ser de extrema importância em uma investigação de incidente de segurança.
- Sincronização do relógio - os relógios dos sistemas de processamento de informações utilizados pela organização devem ser sincronizados com fontes de tempo aprovadas. No Brasil, a orientação é de se utilizar como fonte confiável o relógio atômico da Divisão de Serviços da Hora Legal Brasileira (DISHO) do Observatório Nacional que, conforme a própria instituição divulga em seu *site* oficial (http://pcdsh01.on.br/), "é a única instituição legalmente designada para gerar, conservar e disseminar a hora legal brasileira (HLB), bem como realizar pesquisa e desenvolvimento no campo da metrologia de tempo e frequência."
- Uso de programas utilitários privilegiados – o uso de programas utilitários que possam ser capazes de se sobreporem a controles de sistema e de aplicações deve ser restrito e rigorosamente controlado. Assim como qualquer acesso privilegiado no ambiente, a execução de programas que potencialmente possam impactar a segurança dos dados e do ambiente também deve seguir o princípio de privilégio mínimo, sendo permitido apenas mediante justificativas de negócio e utilizado apenas por usuários previamente determinados e autorizados.
- Instalação de *software* em sistemas operacionais - procedimentos e medidas devem ser implementados para gerenciar com segurança a instalação de *software* em sistemas operacionais. O próprio controle de acesso é uma das primeiras e principais barreiras à instalação indevida de *softwares* em sistemas operacionais das organizações, uma vez que os perfis de acesso são determinados. Portanto, a instalação de *softwares* em sistemas operacionais deve ser restrita aos administradores. Conforme alertado por

Coelho *et al.* (2014, p. 26), “se a integridade de um sistema de controle de acesso a um sistema operacional for violada, também será violada a confidencialidade de seus arquivos”. Ou seja, pode haver impacto ao ambiente ou diretamente aos dados ali tratados.

- Segurança de redes - redes e dispositivos de rede devem ser protegidos, gerenciados e controlados para proteger as informações em sistemas e aplicações. Esse é um controle preventivo e detectivo. Os dispositivos devem contar com políticas e procedimentos para configuração segura, desabilitando todos os serviços desnecessários e configurando adequadamente aqueles serviços que forem necessários.
- Segurança dos serviços de rede - mecanismos de segurança, níveis de serviço e requisitos de serviços de rede devem ser identificados, implementados e monitorados. A ISO/IEC 27002 (2022) recomenda, nesse ponto, que é necessário que sejam definidas as regras sobre o uso de redes e de serviços de rede, de forma a determinar os recursos que podem ser acessados, quais mecanismos de autenticação devem ser utilizados para o acesso, os procedimentos para utilizar tais serviços e os recursos para proteger as conexões necessárias, além dos mecanismos para monitoramento do uso desses serviços.
- Segregação de redes - grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização. É uma técnica muito utilizada e que visa determinar perímetros de segurança, em que o tráfego de entrada e saída seja controlado de maneira a mitigar o risco de acessos indevidos. Em alguns padrões de segurança do mercado, como no PCI DSS (*Payment Card Industry Data Security Standard*), que é aplicável ao mercado de meios de pagamentos eletrônicos de cartões bandeirados, a segregação de redes não é um requerimento obrigatório, mas, se aplicado, pode diminuir o escopo de verificação de riscos e de validação dos demais controles. Isso porque a segregação garante que apenas outras sub-redes que tenham necessidade e que também estão segregadas tenham acesso à sub-rede que armazene, processe ou transmita os dados sensíveis de cartão de crédito (https://www.pcisecuritystandards.org/).

- Filtragem da *web* - o acesso a *websites* externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso. Conforme Watkins (2022) acredita que há aproximadamente 10 controles que focam na segurança da rede e dos sistemas, garantindo que a implantação e a manutenção deles é apropriada. Entre esses, a implantação de filtragem da *web*.
- Uso de criptografa - regras para o uso efetivo da criptografa, incluindo o gerenciamento de chaves criptográficas, devem ser definidas e implementadas. O tema criptografia é extremamente interessante e é possível descrever todo o histórico, tipos de criptografia, algoritmos, tamanhos de chaves e seus cálculos. Entretanto, como esse não é o objeto deste estudo, há uma limitação apenas aos processos de controle requeridos na norma ISO 27001 e às recomendações de uso. Coelho *et al.* (2014, p. 104) orientam que:

  > Em termos do uso de criptografia, deve-se considerar o tipo e a qualidade de algoritmos adequados às necessidades. É aconselhável elaborar uma política específica que elucide o modo correto de uso, reduzindo os riscos de uso inadequado, por exemplo.
  >
  > Os autores também esclarecem que os controles devem se estender à segurança das chaves de criptografia, uma vez que elas são o principal componente dos recursos de criptografia em termo de garantias de confidencialidade das informações (Coelho *et al.,* 2014, p. 182).

- Ciclo de vida de desenvolvimento seguro - regras para o desenvolvimento seguro de *software* e sistemas devem ser estabelecidas e aplicadas. A norma ISO 27002 preconiza que o desenvolvimento seguro é um requisito para construir serviço, arquitetura, *software* e sistema seguros e que sejam considerados aspectos como metodologia de desenvolvimento seguro, diretrizes de codificação segura para cada linguagem utilizada, inclusão de pontos de verificação de segurança nos projetos, testes de segurança, verificação de código e testes de invasão, entre outros.
- Requisitos de segurança da aplicação - requisitos de segurança da informação devem ser identificados, especificados e aprovados ao desenvolver ou adquirir aplicações. Watkins (2022, p. 35) reforça:

A criação, implantação, manutenção e descomissionamento de *software* e sistemas seguros, bem como arquitetura e serviços, são abordados em aproximadamente sete controles que incluem a necessidade de ser claro sobre os requisitos de segurança desde o início, testando esses requisitos em vários estágios de desenvolvimento e pré-lançamento, tendo ambientes separados para desenvolvimento, testes e produção, bem como medidas apropriadas de gestão de mudanças.

Alguns desses são tratados a seguir, como orientações da própria ISO 27001.

- Princípios de arquitetura e engenharia de sistemas seguros - princípios para engenharia de sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados a qualquer atividade de desenvolvimento de sistemas.
- Codificação segura - princípios de codificação segura devem ser aplicados ao desenvolvimento de *software*. O documento N1255, CERT C *Programming Language Secure Coding Standard*, da *Carnegie Melon University* (2007, p. 06), cita que “o desenvolvimento de um padrão de codificação seguro para qualquer linguagem de programação é uma tarefa difícil que requer um envolvimento significativo da comunidade”. O documento cita várias preocupações, como o tratamento de dados de entrada, como lidar com chaves de criptografia, o tratamento de erros e formas de se evitarem vulnerabilidades na etapa de codificação, entre outros.
- Testes de segurança em desenvolvimento e aceitação - processos de teste de segurança devem ser definidos e implementados no ciclo de vida do desenvolvimento. O PCI DSS v4, em seu requisito 06, define que testes de segurança sejam realizados antes da entrada de um novo sistema em produção, assim como garantir que a sua própria implementação não traga risco a outros processos já implementados no ambiente, Nesse ponto, o padrão de segurança sugere alguns testes que devem ser realizados para evitar os ataques de injeção, ataques às estruturas de dados, aos mecanismos de autenticação e o estabelecimento de um processo para que qualquer vulnerabilidade identificada de alto curso seja tratada adequadamente. Aniche (2015, p. 46) explica uma técnica conhecida como *Test-Driven Development*, explicitando que:

Em primeiro lugar, escrevemos um teste; rodamos e o vimos falhar; em seguida, escrevemos o código mais simples para passar o teste; rodamos novamente, e dessa vez ele passou; por fim, refatoramos nosso código para que ele ficasse melhor e mais claro.

Ou seja, o teste de código é escrito antes do código, o que, no entendimento do autor, garante que o código já seja criado e de certa forma testado.

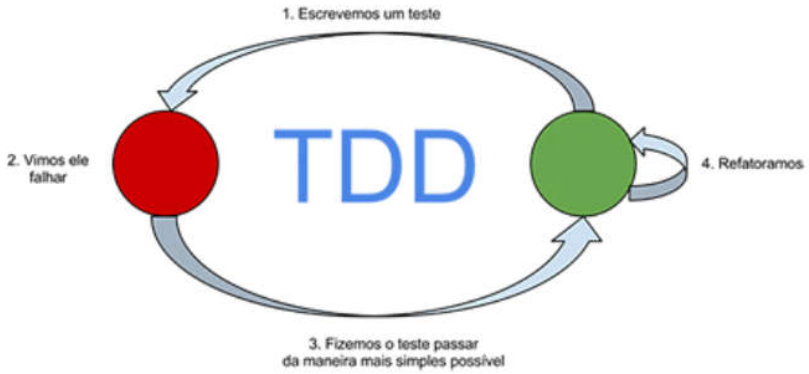

Figura 11
Test-Driven Development.
Fonte: Aniche, M. (2015). *Testes automatizados de software: um guia prático*. São Paulo: Casa do Código Livros para o Programador (p. 46).

- Desenvolvimento terceirizado - a organização deve dirigir, monitorar e analisar criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas. Nesse sentido, a organização deve estender os controles que aplica em seu ambiente aos terceiros contratados para desenvolvimento em seu nome. A capacidade técnica para aplicação de métodos de codificação segura deve ser validada antes da contratação, assim como deve ser combinada a forma como será demonstrada a segurança do código escrito por terceiros.
- Separação dos ambientes de desenvolvimento, teste e produção - ambientes de desenvolvimento, testes e produção devem ser separados e protegidos. Fontes (2012, p. 107) complementa que “cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma falta grave”. Assim, é esperado que equipes de desenvolvimento ou testes de *software* tenham acesso limitado ao ambiente de produção. Esses devem ter

um ambiente próprio em que possam desenvolver e testar aplicações, sem impactar o ambiente de produção.

- Gestão de mudanças - mudanças nos recursos de tratamento de informações e sistemas de informação devem estar sujeitas a procedimentos de gestão de mudanças. Humphrey (2016, p. 117) detalha que o processo de gestão de mudanças envolve modificações nos processos de negócio, sistemas e serviços que suportam o processamento de informações em um ambiente operacional, devendo ser executadas com a concordância e aprovações necessárias e após uma avaliação criteriosa desse possível impacto, tomando as ações necessárias para implementá-la com segurança.
- Informações de teste - informações de teste devem ser adequadamente selecionadas, protegidas e gerenciadas. O *Open Web Application Security Project* (OWASP) descreve em seu guia de testes de segurança para a Internet, o *Web Security Testing Guide* (WSTG), que o uso de dados de produção em ambiente de testes é restrito por leis e regulamentações como a *General Data Protection Regulation* (GDPR) e *o Payment Card Industry Data Security Standards* (PCI DSS), podendo ser entendido como uma violação. Para os casos de necessidade, orienta que os dados passem por processos de anonimização ou mascaramento.
- Proteção de sistemas de informação durante os testes de auditoria - testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais devem ser planejados e acordados entre o testador e a gestão apropriada. Esse é um controle que visa garantir que auditorias nos sistemas não sejam um fato que possa gerar algum impacto negativo. Nesse sentido, a norma ISO/IEC 27002 (2022, p. 161 e 162) orienta que as auditorias sejam acordadas com a gestão apropriada, controlando o escopo dos testes de auditoria técnica, limitando o acesso apenas à leitura de dados, estabelecendo e verificando os requisitos de segurança antes de permitir os acessos para testes, por exemplo. A norma complementa ainda que os testes que possam afetar a disponibilidade devem ser realizados fora do horário comercial, sendo monitorados e registrados.

2.4 Análise crítica da aplicabilidade da ISO 27001 em ambiente de Cloud

Segundo Gartner (2023, s.d.), "o desafio mais crítico para as organizações que migram para a nuvem é a segurança dos dados (https://www.gartner.com/en).

Outras instituições, como *Forrester Research* (2022, https://inthecloud.withgoogle.com/forrest-whitepaper-ptbr/relatorio.pdf, p. 6), reforçam que "ao avaliar fornecedores de serviços na nuvem, os tomadores de decisões dão prioridade a soluções que melhoram a facilidade de utilização, as capacidades técnicas, a segurança e a conformidade".

Já a *International Data Corporation* (IDC, 2023, s.p., https://www.idc.com/latam_pt) concorda em dizer que "as iniciativas estratégicas de TI se concentram na evolução das aplicações de negócio e da infraestrutura para seguir avançando com segurança para a nuvem".

Essas instituições mostram que a segurança dos dados é um desafio para a migração para a *CloudComputing,* porque as organizações precisam transferir seus dados para um ambiente de terceiros, que pode estar fora de seu controle físico. Isso pode gerar preocupações sobre a segurança dos dados.

Como já citado anteriormente, entende-se que a norma ISO 27001 seja um padrão internacional de segurança da informação que fornece um *framework* para a implementação de um sistema de gestão de segurança da informação (SGSI), sendo aplicável a organizações de todos os portes e setores, e é amplamente utilizada por empresas de todo o mundo.

A aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing* é uma questão que tem sido amplamente discutida por especialistas. Alguns autores acreditam que a norma é perfeitamente aplicável ao ambiente de *CloudComputing*, enquanto outros acreditam que existem algumas limitações.

Entre os autores que defendem a aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing* destacam-se Rodrigues (2015), que entende que a norma ISO

27001 seja perfeitamente aplicável ao ambiente de *CloudComputing*, necessitando apenas que sejam feitas algumas adaptações, e Souza (2017), que defende a aplicabilidade da norma ISO 27001 ao ambiente de *CloudComputing*, mas destaca a necessidade e importância de uma avaliação de riscos específica e no contexto desse ambiente.
Há ainda autores que salientam as limitações da aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing*, destacando-se Souza (2019), que defende que "a norma ISO 27001 é aplicável ao ambiente de *CloudComputing*, mas apresenta alguns desafios que precisam ser considerados". Ainda, de acordo com Souza e Costa (2020), "a norma ISO 27001 é um importante instrumento para a gestão da segurança da informação em ambientes de *CloudComputing*".

Compreende-se, a partir da leitura desses artigos que, em geral, a aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing* é uma questão complexa, que depende de uma série de fatores, como o tipo de serviço contratado, as características da organização e os requisitos específicos de segurança da informação para cada cenário, além do próprio apetite ao risco a que cada organização se dispõe.

Com base nesses mesmos artigos, são apresentadas algumas considerações sobre a aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing*:

A norma ISO 27001 é um *framework* genérico, que pode ser aplicado a diferentes ambientes. No entanto, é importante realizar uma avaliação de riscos específica para o ambiente *Cloud*, para identificar os riscos específicos que devem ser mitigados.

A norma ISO 27001 não considera todos os aspectos específicos do ambiente *Cloud*. No entanto, existem documentos complementares, como a ISO/IEC 27017 e a ISO/IEC 27018, que fornecem orientações específicas para o ambiente *Cloud*.

A implementação da norma ISO 27001 em ambiente de *CloudComputing* exige a colaboração entre a organização e o provedor de serviços *Cloud*. É importante que esses dois atores definam claramente as responsabilidades de cada um em relação à segurança da informação.

Conclui-se, nesse ponto, que a aplicabilidade da norma ISO 27001 em ambiente de *CloudComputing* é uma questão que deve ser avaliada caso a caso, levando-se em consideração os fatores específicos do ambiente de *CloudComputing*. No entanto, a norma pode ser um importante instrumento para a gestão da segurança da informação em ambiente de *CloudComputing*.

2.4.1 Desafios de segurança em ambientes de nuvem

Com tanta atratividade, vantagens e facilidade para se implementar um novo ambiente, ou mesmo migrar para um ambiente de *CloudComputing*, a disciplina segurança da informação precisa acompanhar o ritmo dessas vantagens e necessidades geradas, para não se tornar um impedimento à evolução. A ideia desta dissertação é justamente propor um *framework* para segurança dos dados em um ambiente de *CloudComputing*, usando como base a norma ISO 27001), uma vez que esta traz um dos materiais de referência mais abrangentes sobre o tema, especificando requisitos possíveis de serem avaliados pelas empresas e, inclusive, certificados por outras instituições independentes e especialistas.

Nesse aspecto, o intuito é avaliar dentro dos controles propostos quais são os aplicáveis e qual a prioridade, de acordo com as avaliações coletadas no estudo que será conduzido, a partir do preenchimento de um formulário no qual será aplicado um método de pesquisa quantitativa. Essa parte deve completar a ideia de preencher a lacuna mostrada antes da pergunta de partida.

Souza e Costa (2020) discutem os desafios de segurança associados à adoção de *CloudComputing*, incluindo:

a) A necessidade de confiança entre o provedor de serviços em nuvem e o cliente.
b) A complexidade dos ambientes de *CloudComputing*.
c) A dificuldade de manter a conformidade com as regulamentações de segurança.

Souza (2019) traz ainda outros desafios associados à adoção de *CloudComputing*, incluindo:

a) A transferência de controle sobre os dados e sistemas para o provedor de serviços em nuvem.
b) A dificuldade de monitorar e auditar a segurança dos ambientes de *CloudComputing*.
c) O risco de ataques direcionados a infraestruturas de *CloudComputing*.

Esses são apenas alguns exemplos dos autores que discutem os desafios de segurança associados à adoção de *CloudComputing*. A segurança é uma preocupação importante para qualquer organização que considere adotar *CloudComputing*. Eles indicam ser importante realizar uma avaliação de riscos completa antes de adotar esse modelo para garantir que a organização esteja preparada para os desafios de segurança associados à tecnologia.

Além desses autores, Gartner (2023), *Forrester Research* (2022) e o IDC (2023) trazem alguns dos principais desafios de segurança enfrentados pelas organizações durante a migração para a *CloudComputing*:

a) Autenticação e autorização: as organizações precisam garantir que apenas usuários autorizados tenham acesso aos dados na nuvem.
b) Criptografia: os dados na nuvem devem ser criptografados para proteger contra acesso não autorizado.
c) Controle de acesso à rede: as organizações precisam restringir o acesso à rede da nuvem para evitar ataques.
d) *Backup* e recuperação de desastres: as organizações precisam ter um plano de *backup* e recuperação de desastres para proteger seus dados em caso de falha ou ataque.
e) Conformidade: as empresas geralmente operam sob fortes regulamentações de entidades reguladoras, que especificam requisitos de operação que podem limitar até mesmo a localização de onde os dados podem ser tratados. Vide exemplo do Banco Central do Brasil (BACEN), pelas suas resoluções, como a 15 e a 4893, que especificam os controles para contratação de prestação de

serviços de *CloudComputing*, limitando aos países onde houver acordo de cooperação entre o BACEN e seu equivalente naquele país.

Para superar esses desafios, as organizações devem implementar medidas de segurança rigorosas, passíveis de auditoria e medição. Esse é o grande motivo de se adotar um *framework* reconhecido pelo mercado, para que haja um padrão na definição e implementação de controles.

2.5 Modelo analítico

A incursão no referencial teórico sobre segurança em *CloudComputing* e na norma ISO 27001, anteriormente realizada, sugere um modelo analítico mostrado na Figura 12, que é constituído por três construtos e 34 indicadores que se encontram descritos na Tabela 1.

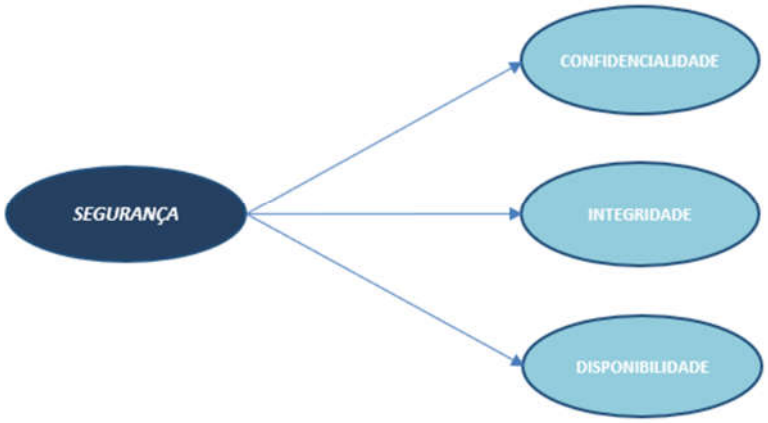

Figura 12
Modelo analítico.
Fonte: do autor.

A Tabela 1 detalha, para cada construto, o conjunto de indicadores que o adentramento no referencial teórico realçou como traduzindo as suas diversas nuanças. Cumpre lembrar que um construto representa uma variável latente que não pode ser medida diretamente e sim por meio de indicadores que representam os diversos aspectos de sua natureza multifacetada.

Tabela 1

Indicadores dos construtos do modelo analítico

Construtos	Itens	Descrição
CONFIDENCIALIDADE	CON1	Dispositivos *endpoint* do usuário
	CON2	Direitos de acessos privilegiados
	CON3	Restrição de acesso à informação
	CON4	Acesso ao código-fonte
	CON5	Autenticação segura
	CON6	Exclusão de informações
	CON7	Mascaramento de dados
	CON8	Prevenção de vazamento de dados
	CON9	Segregação de redes
	CON10	Uso de criptografia
INTEGRIDADE	INT1	Proteção contra *malware*
	INT2	Gestão de vulnerabilidades técnicas
	INT3	*Log*
	INT4	Sincronização do relógio
	INT5	Uso de programas utilitários privilegiados
	INT6	Instalação de *software* em sistemas operacionais
	INT7	Segurança dos serviços de rede
	INT8	Filtragem da *web*
	INT9	Ciclo de vida de desenvolvimento seguro
	INT10	Requisitos de segurança da aplicação
	INT11	Princípios de arquitetura e engenharia de sistemas seguros
	INT12	Codificação segura
	INT13	Testes de segurança em desenvolvimento e aceitação
	INT14	Desenvolvimento terceirizado
	INT15	Separação dos ambientes de desenvolvimento, teste e produção
	INT16	Informações de teste
	INT17	Proteção de sistemas de informação durante os testes de auditoria
DISPONIBILIDADE	DIS1	Gestão de capacidade
	DIS2	Gestão de configuração
	DIS3	*Backup* das informações
	DIS4	Redundância dos recursos de tratamento de informações
	DIS5	Atividades de monitoramento
	DIS6	Segurança de redes
	DIS7	Gestão de mudanças

Fonte: dados da pesquisa.

3 Metodologia

Neste capítulo são descritos a caracterização da pesquisa, a descrição da unidade de análise e de observação, o processo da coleta e do tratamento dos dados bem como o conjunto de métodos estatísticos utilizados para estratégia de análise dos resultados.

3.1 Caracterização da pesquisa

O presente estudo pode ser classificado como quantitativo em decorrência do tipo de variável e dos procedimentos utilizados. Para Mattar (1993), o estudo é descritivo ao se considerar que o pesquisador está certo do que deve ser medido, como fazê-lo e por que a medição se faz necessária. Por outro ângulo, a dissertação é, segundo Marconi e Lakatos (2003), do tipo argumentativa por demandar interpretações e posicionamento do pesquisador. Existe uma profusão de classificações das pesquisas, pois diferentes autores lançam mão de critérios diversos para proceder a essas classificações.

Seguindo um pequeno protocolo de valorização de pesquisa sugerido por Marconi e Lakatos, podem-se destacar quatro aspectos concernentes ao presente estudo:

a) Viabilidade: o banco de dados resultante do *survey* utilizado permite responder ao problema de pesquisa.
b) Relevância: o estudo apresenta um "*plus*" de conhecimento novo, uma vez que faz uma fusão de um arcabouço teórico conceitual e métodos de estatística multivariada.
c) Novidade: desenvolve-se, de modo sistematizado, um modelo para analisar a segurança com a *CloudComputing* e quantifica os parâmetros desse modelo.
d) Exequibilidade: o estudo apresenta conclusões fundamentadas e é passível de aplicação prática.
e) Oportunidade: o estudo atende a interesses tanto teóricos quanto práticos.

3.2 Unidade de análise

A unidade de análise foi constituída basicamente por profissionais da área de segurança da informação da região Sudeste do Brasil, principalmente Minas Gerais e São Paulo, que possuem experiência em projetos que envolvem *CloudComputing* e na implementação dos controles recomendados pela ISO/IEC 27001. Os profissionais envolvidos na pesquisa são os principais influenciadores e decisores dos controles a implementar em suas prioridades, já que eles acompanham diariamente os acontecimentos e incidentes que ocorrem nos ambientes corporativos e suas principais causas.

3.3 Unidade de observação

Deve-se, nesse caso, considerar duas fases de coleta das informações. Em primeiro lugar, solicitou-se a 35 especialistas em segurança em *CloudComputing* que associassem, a cada construto extraído do modelo analítico decorrente do exame do referencial teórico, um conjunto de indicadores que eles entendiam ser mais representativos de tais construtos. Do procedimento de análise do referencial teórico resultou a Figura 12, que passou a constituir o modelo analítico final a ser utilizado para extrair, ulteriormente, a percepção dos especialistas que constituíram uma amostra de 110 respondentes a respeito de suas percepções da importância de cada indicador na formação do construto.

A coleta das informações para essa fase foi efetuada na plataforma *Google* (*Google Forms*) a profissionais selecionados em grupos de *Whatsapp* formados por gestores de segurança da informação experientes, aos quais foi solicitado distribuir os 34 indicadores tecnológicos propostos pela norma ISO 27001 entre os construtos, de acordo com as suas percepções de pertencimento a cada um deles. Em outros termos, cada gestor foi instado a associar a cada construto um conjunto de indicadores que, de acordo com a sua respectiva percepção, melhor representava o conjunto de facetas que o retratava.

Para melhor explicitar o que estava sendo efetivamente solicitado, foi apresentado o seguinte esclarecimento no início do formulário:

> Considerando a contratação de um ambiente de *Cloud* no Brasil no modelo onde a manutenção de ativos e controles de segurança seja sua responsabilidade parcial ou total, para instalação de serviços de missão crítica em regime 24x7x365 e que trate dados sensíveis, com sua experiência em segurança da informação, avalie qual das propriedades de segurança da informação (CID), de acordo com a ISO-27001:2022, melhor justifica a necessidade dos controles listados.

As Figuras 13 e 14 mostram o perfil dos 35 especialistas que permitiram gerar o modelo analítico final.

Figura 13
Tempo de experiência dos respondentes questionário fase 01.
Fonte: dados da pesquisa.

Considerando que o tempo de experiência é um dos fatores preponderantes para uma pesquisa de percepção sobre requerimentos técnicos, verifica-se a senioridade dos respondentes, uma vez que 52,8% destes possuem no mínimo nove anos de experiência na área e 57,2%, mais de 16 anos.

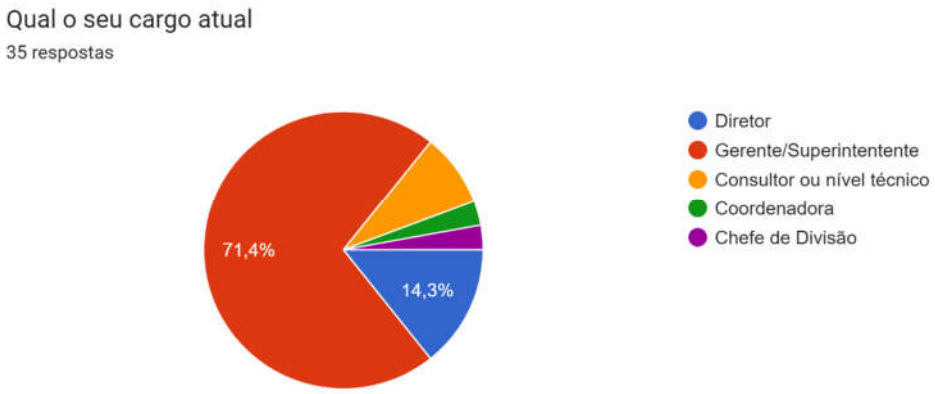

Figura 14
Posição ocupada pelos respondentes questionário fase 01.
Fonte: dados da pesquisa.

Outro ponto importante observado é o conhecimento técnico e vivência acerca do assunto, considerando que 91,4% possuem cargos com poder de decisão ou de orientação sobre a implementação de controles em suas empresas. A maioria dos respondentes possui cargo de gerência ou superintendência, o que também corrobora a demonstração de experiência em gestão de segurança da informação. Conforme citam Whitman & Mattord (2019), os gestores de segurança da informação possuem perfil planejador, implementador e gerenciador do programa de segurança da informação da organização, com foco na proteção da confidencialidade, integridade e disponibilidade dos dados.

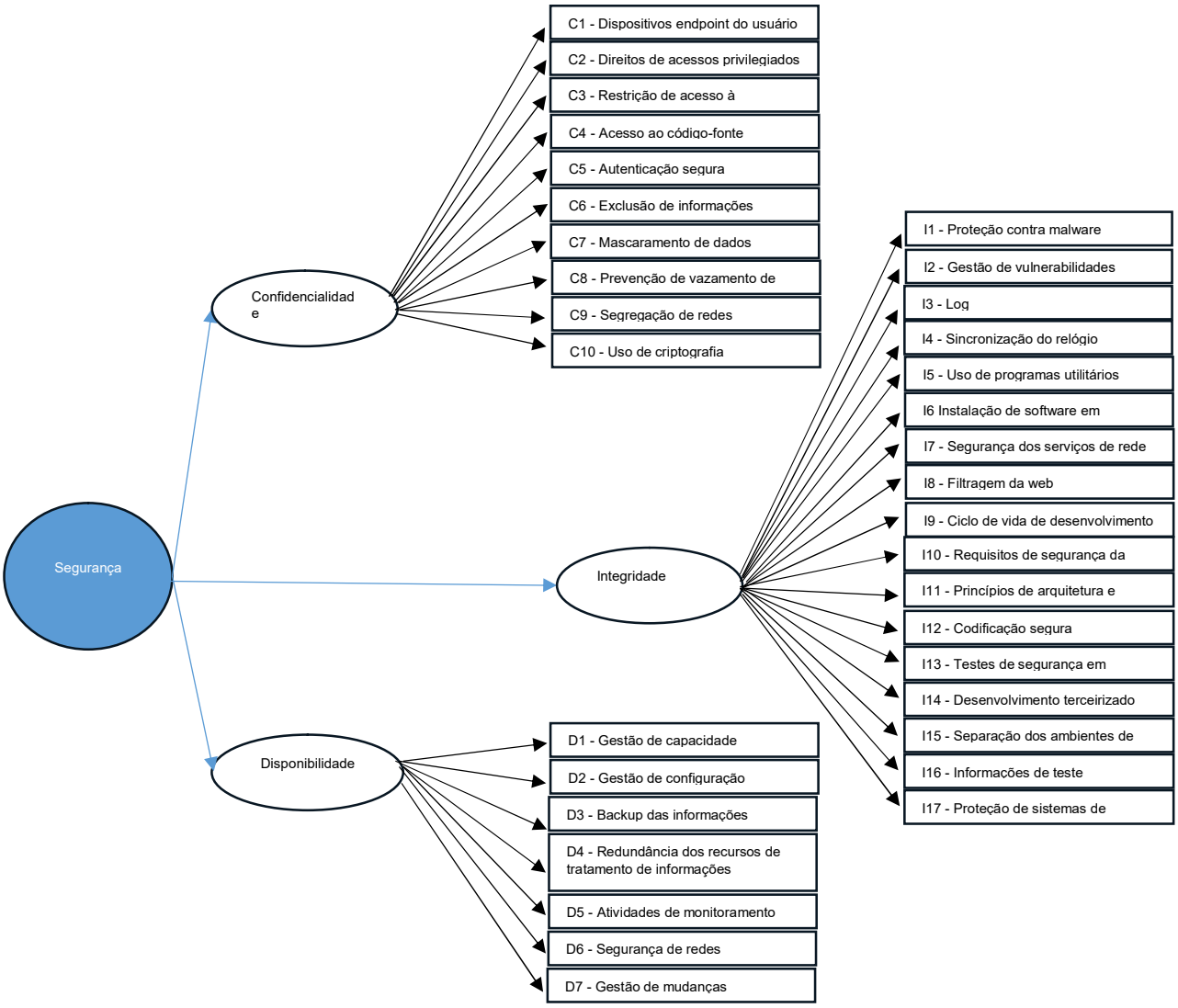

Figura 15
Modelo intermediário
Fonte: dados da pesquisa.

Com a aplicação do questionário aos 35 especialistas selecionados, foi possível se obter uma distribuição dos indicadores em seus respectivos construtos mais relevantes, de acordo com a percepção do grau de relevância dessa relação, conforme mostrado na figura 15.

Na segunda fase, a qual constitui a coleta final das observações, trabalhou-se com a amostra de 110 indivíduos, aos quais foi solicitado que procedessem a uma hierarquização dos indicadores em cada construto levando-se em conta as suas percepções sobre a importância de cada um deles em sua representatividade. De

outro modo, cada respondente foi instado a valorar os indicadores concernentes a cada um dos construtos que compõem o modelo analítico.

3.4 Pré-teste do questionário

Como recomenda a boa prática de pesquisa, procedeu-se a um pré-teste do questionário, visando evitar dúvidas, desinteresse ou má interpretação das assertivas a serem valoradas. A ideia é a de assegurar que a ferramenta de coleta possa fornecer dados fidedignos no sentido de apresentar respostas às características que os indicadores dos construtos buscam efetivamente retratar (Ramalho, 2006).

Nesse sentido, utilizou-se uma amostra de 10 especialistas em segurança em *CloudComputing* para a verificação da adequabilidade da terminologia utilizada na elaboração de cada uma das questões constitutivas do questionário. No presente caso não foi constatado qualquer problema no entendimento das questões propostas, o que permitiu manter o questionário em sua forma original.

3.5 Estratégia de tratamento inicial do banco de dados

O fato de cada indicador estar em uma escala diferente sugeriu uma padronização de maneira que todos eles passassem a variar dentro do intervalo zero a um, sendo "zero" o representante de uma característica considerada a de menor prioridade possível para o respondente e "um" representando uma característica entendida como a de maior prioridade.

A fórmula (A) a seguir permite essa padronização:

$$X_{novo} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad \text{(A)}$$

Dessa forma, intervalos estritamente menores que 0,5 indicam que os respondentes tendem a julgar aquele indicador como pouco prioritário, enquanto que intervalos

estritamente maiores que 0,5 sinalizam que os respondentes tendem a julgar aquele indicador como muito prioritário.

O banco de dados obtido era composto de 34 indicadores correspondentes aos três construtos de primeira ordem do modelo analítico (confidencialidade, integridade e segurança), duas variáveis de categorização (tempo de experiência e cargo) e 110 respondentes, o que, supostamente deveria corresponder a 3.740 respostas. Entretanto, constatou-se que quatro respondentes não forneceram informações solicitadas para mais de 15% das questões. Nesse caso, a literatura concernente sugere excluí-los da amostra a ser trabalhada. Assim, a amostra final ficou com 106 respondentes.

Foi também examinada uma possível existência de *outliers*, observações que apresentam um padrão de resposta que destoa significativamente das demais e pode prejudicar a aplicação da análise multivariada. Podem-se classificar, de acordo com Hair, Black, Babin, Anderson e Tatham (2009), quatro tipos de *outliers*: a) erros na tabulação dos dados ou falhas na codificação; b) observações decorrentes de algum evento extraordinário; c) observações extraordinárias para as quais o pesquisador não tem explicação; e d) observações que estão no intervalo usual de valores para cada variável, mas são únicas em sua combinação de valores entre as variáveis.

Não foram encontrados valores fora do intervalo da escala de sua respectiva variável, não evidenciando o tipo de *outlier* relacionado a erro na tabulação dos dados. Além disso, buscou-se verificar a existência de *outliers* univariados, que consiste na verificação de alguma resposta “divergente” com base em cada uma das variáveis do modelo, e os multivariados, que apresentam um padrão de resposta “estranho” considerando todas as variáveis ao mesmo tempo. Para o primeiro caso, o diagnóstico é feito por meio da variável padronizada

$$\boldsymbol{Z} = \frac{(X - \overline{X})}{\boldsymbol{s}} \qquad \text{(B)}$$

São considerados *outliers* univariados observações com valores |z| >4 (Hair *et al*., 2009). Utilizando esse critério foram encontradas apenas cinco (0,14%) observações consideradas atípicas de forma univariada.

Para o exame de existência de *outliers* multivariados, foi utilizada a distância D^2 de Mahalanobis. Hair *et al*. (2009) acreditam que tal medida verifica a posição de cada observação comparada com o centro de todas as observações em um conjunto de variáveis, sendo que, ao final, é realizado um teste qui-quadrado. Os indivíduos que apresentam significância da medida inferior a 0,1% são considerados *outliers* multivariados. Com base nesse método, não foram encontradas observações consideradas atípicas do ponto de vista multivariado.

Por se acreditar que as observações podem ser casos válidos da população e que, caso fossem eliminadas, podem limitar a generalidade da análise multivariada, apesar de possivelmente melhorar seus resultados (Hair *et al*., 2009), optou-se por não excluir algum dos casos.

Finalmente, antes de se iniciarem as análises descritiva e inferencial do banco de dados, examinou-se a linearidade dos dados, o que constitui uma característica importante para a aplicação das técnicas multivariadas. Inicialmente, foram analisadas as correlações das variáveis par a par, uma vez que um coeficiente de correlação significativo no nível de 5% é indicativo da existência de linearidade. A partir da matriz de correlação de Spearman, foram observadas 152 de 516 relações significativas no nível de 5%, o que representa aproximadamente 27,09% das correlações possíveis.

Adicionalmente, foi realizado o teste de Bartlett (Mignoti, 2007) para verificar a linearidade em cada construto. Para todos os construtos foram observados p-valores menores que 0,05, indicando que existem evidências significativas de linearidade dentro dos construtos.

3.6 Procedimentos metodológicos

Fundamentalmente, utilizou-se tanto estatística descritiva quanto estatística inferencial, como detalhado a seguir.

Adicionalmente, foi realizado o teste de Bartlett (Mignoti, 2007) para verificar a linearidade em cada construto. Para todos os construtos foram observados p-valores menores que 0,05, indicando que existem evidências significativas de linearidade dentro dos construtos.

4 Análise dos Dados

4.1 Análise descritiva dos dados

Neste tópico apresenta-se, por um lado, o perfil da amostra trabalhada mediante uma tabela de frequência das duas variáveis de caracterização utilizadas no cabeçalho do questionário aplicado, constatando-se que: a maior parte dos indivíduos (45,58%) tinha mais de 20 anos de experiência; 49,6% dos respondentes eram coordenadores ou gerentes e 4,72% (5) eram presidentes.

Tabela 2

Análise descritiva das variáveis de caracterização

Variável	Categoria	N	%
Tempo de experiência	Menos de 3 anos	4	3,77
	De 3 a 5 anos	5	4,72
	De 6 a 8 anos	3	2,83
	De 9 a 11 anos	9	8,49
	De 12 a 14 anos	8	7,55
	De 15 a 17 anos	14	13,21
	De 18 a 20 anos	15	14,15
	Mais de 20 anos	48	45,28
Cargo	Analista / Consultor	12	11,32
	Coordenador / Gerente	52	49,06
	Superintendente	13	12,26
	Diretor	24	22,64
	Presidente	5	4,72

Por outro lado, a Tabela 3 apresenta as estatísticas descritivas concernentes aos indicadores dos três construtos do modelo analítico inicial extraído do referencial teórico e explicita os seguintes pontos:

No construto confidencialidade, os indivíduos tenderam a considerar a maioria dos itens como moderadamente prioritária. Ao observar os intervalos de confiança, o item CON6 ("exclusão de informações") apresentou uma prioridade significativamente maior que a dos demais itens. O item CON5 ("autenticação segura") foi considerado menos prioritário, com média de 0,201, indicando menor percepção de sua relevância em comparação aos outros aspectos da confidencialidade.

No construto integridade, os indivíduos tenderam a considerar a maioria dos itens como moderadamente prioritários. Ao observar os intervalos de confiança, os itens INT16 ("informações de teste"), INT17 ("proteção de sistemas de informação durante os testes de auditoria") e INT14 ("desenvolvimento terceirizado") apresentaram prioridade significativamente maior que a dos demais, refletindo alta percepção de relevância nesses aspectos. Os itens INT1 ("proteção contra *malware*") e INT2 ("gestão de vulnerabilidades técnicas") foram considerados menos prioritários, com médias de 0,135 e 0,127, respectivamente, indicando menos ênfase na prioridade desses itens em relação aos outros elementos da integridade.

No construto disponibilidade, os indivíduos tenderam a considerar a maioria dos itens como moderadamente prioritários. Ao observar os intervalos de confiança, o item DIS3 ("*backup* das informações") foi reconhecido significativamente menos prioritário que os outros, com média de 0,291, indicando que os indivíduos entendem o *backup* das informações como um aspecto menos crítico em relação aos demais fatores que afetam a disponibilidade.

Tabela 3

Estatísticas descritivas dos indicadores dos construtos

Construtos	Itens	Média	DP	IC 95%[1]
CONFIDENCIALIDADE	CON1	0,469	0,329	[0,41;0,54]
	CON2	0,231	0,208	[0,19;0,27]
	CON3	0,308	0,228	[0,27;0,35]
	CON4	0,649	0,257	[0,60;0,70]
	CON5	0,201	0,196	[0,17;0,24]
	CON6	0,825	0,195	[0,78;0,86]
	CON7	0,679	0,238	[0,63;0,72]
	CON8	0,519	0,272	[0,46;0,57]
	CON9	0,627	0,286	[0,57;0,68]
	CON10	0,493	0,300	[0,44;0,55]
INTEGRIDADE	INT1	0,135	0,205	[0,10;0,17]
	INT2	0,127	0,125	[0,10;0,15]
	INT3	0,327	0,251	[0,28;0,37]
	INT4	0,556	0,290	[0,50;0,61]
	INT5	0,402	0,194	[0,36;0,44]
	INT6	0,458	0,201	[0,42;0,50]
	INT7	0,333	0,203	[0,30;0,37]
	INT8	0,491	0,244	[0,45;0,54]
	INT9	0,420	0,212	[0,38;0,46]
	INT10	0,436	0,211	[0,40;0,48]
	INT11	0,409	0,251	[0,36;0,46]
	INT12	0,569	0,210	[0,53;0,61]
	INT13	0,636	0,210	[0,60;0,67]
	INT14	0,855	0,120	[0,83;0,88]
	INT15	0,559	0,292	[0,51;0,61]
	INT16	0,890	0,143	[0,86;0,92]
	INT17	0,897	0,173	[0,86;0,93]
DISPONIBILIDADE	DIS1	0,517	0,299	[0,47;0,58]
	DIS2	0,563	0,295	[0,51;0,62]
	DIS3	0,291	0,295	[0,24;0,35]
	DIS4	0,442	0,337	[0,38;0,51]
	DIS5	0,530	0,309	[0,47;0,58]
	DIS6	0,542	0,370	[0,47;0,61]
	DIS7	0,615	0,330	[0,55;0,67]

[1] Intervalo *Bootstrap*.

4.2 Análise multivariada do banco de dados

A utilização da análise multivariada permitiu testar o modelo proposto pelo referencial teórico bem como explicitar a importância relativa dos indicadores que constituem cada construto desse modelo.

A primeira providência metodológica foi verificar a dimensionalidade de cada um dos três construtos de primeira ordem, que são aqueles que se encontram diretamente relacionados aos seus indicadores. Nesse sentido, foi utilizado o critério de retas paralelas (Horn, 1965), que retorna o número de dimensões que se extrai de um dado conjunto de indicadores. Em seguida, aplicou-se a análise de componentes principais (ACP), que permitiu constatar que o conjunto de indicadores correspondentes aos três construtos iniciais sugeridos pelo modelo analítico retratava efetivamente duas dimensões para o construto confidencialidade (C1 e C2), três dimensões para o construto integridade (I1, I2 e I3) e três para o construto disponibilidade (D1,D2 e D3).

Cumpre ressaltar que os itens CON5, CON8, CON9 e CON10 do construto confidencialidade; INT9, INT10, INT11, INT12, INT13, INT15, INT16 e INT17 do construto integridade; e DIS3, DIS4, DIS5 e DIS6 do construto disponibilidade estavam em sentido contrário aos demais itens de seus respectivos construtos, sendo necessária a sua inversão. A partir desse momento, eles passaram a ser denotados com um “i” à frente.

Tabela 4

Análise de componentes principais dos indicadores

Construtos	Itens	PC1	PC2	PC3
CONFIDENCIALIDADE	CON1	-0,180	0,570	-
	CON2	0,000	0,570	-
	CON3	0,720	-0,150	-
	CON4	0,370	0,480	-
	CON5i	0,490	0,010	-
	CON6	0,500	0,110	-
	CON7	0,410	-0,320	-
	CON8i	-0,240	0,670	-
	CON9i	0,770	-0,090	-
	CON10i	0,490	0,600	-
INTEGRIDADE	INT1	0,660	0,170	-0,160
	INT2	0,570	0,020	-0,210
	INT3	-0,250	0,080	0,760
	INT4	-0,010	-0,070	0,860
	INT5	0,650	0,240	-0,010
	INT6	0,530	0,300	0,170
	INT7	-0,130	0,640	-0,280
	INT8	0,240	0,560	-0,220
	INT9i	0,010	0,720	-0,040
	INT10i	0,280	0,300	0,230
	INT11i	0,440	0,330	0,210
	INT12i	0,060	0,580	0,310
	INT13i	-0,090	0,480	0,400
	INT14	0,750	-0,320	-0,170
	INT15i	0,570	-0,410	0,210
	INT16i	0,280	0,010	0,080
	INT17i	0,150	-0,260	0,590
DISPONIBILIDADE	DIS1	0,760	0,190	0,090
	DIS2	0,800	0,320	-0,190
	DIS3i	0,160	0,680	0,270
	DIS4i	0,150	0,810	-0,100
	DIS5i	0,640	-0,450	-0,030
	DIS6i	0,260	-0,290	0,680
	DIS7	-0,220	0,210	0,900

Na Tabela 5 são apresentados as cargas fatoriais, as comunalidades e os pesos da análise fatorial, destacando-se que:

a) No construto confidencialidade 1, o item CONi5 (“autenticação não segura”) teve que ser removido, pois prejudicava a validação do construto. No modelo final, o item mais importante para a formação do conceito foi o CON9i (“não segregação de redes”), seguido pelo CON3 (“restrição de acesso à informação”).
b) No construto confidencialidade 2, o item CON1 (“dispositivos *endpoint* do usuário”) teve que ser removido, pois estava prejudicando a validação do construto. No modelo final, o item mais importante para a formação do conceito foi o CON10i (“não uso de criptografia”), seguido pelo CON2 (“direitos de acessos privilegiados”).
c) No construto confidencialidade, ambos os itens foram mantidos, sendo igualmente importantes para a formação do conceito.
d) No construto integridade 1, o item INT16i (“não informações de teste”) teve que ser removido, pois estava prejudicando a validação do construto. No modelo final, o item mais importante para a formação do conceito foi o INT5 (“uso de programas utilitários privilegiados”), seguido pelo INT6 (“instalação de *software* em sistemas operacionais”).
e) No construto integridade 2, o item INT7 (“segurança dos serviços de rede”) teve que ser removido, pois estava prejudicando a validação do construto. No modelo final, o item mais importante para a formação do conceito foi o INT12i (“codificação não segura”), seguido pelo INT9i (“ciclo de vida de desenvolvimento não seguro”).
f) No construto integridade 3, nenhum item teve que ser removido. No modelo final, o item mais importante para a formação do conceito foi o INT4 (“sincronização do relógio”), seguido pelo INT17i (“não proteção de sistemas de informação durante os testes de auditoria”).
g) No construto integridade, nenhum item teve que ser removido. No modelo final, o item mais importante para a formação do conceito foi o integridade, seguido pelo integridade 2.
h) No construto disponibilidade 1, nenhum item teve que ser removido. No modelo final, o item mais importante para a formação do conceito foi o DIS5i (“não atividades de monitoramento”), seguido pelo DIS1 (“gestão de capacidade”).

i) No construto disponibilidade 2, nenhum item teve que ser removido, sendo eles igualmente importantes.

j) No construto disponibilidade 3, nenhum item teve que ser removido, sendo eles igualmente importantes.

k) No construto disponibilidade, nenhum item teve que ser removido. No modelo final, o item mais importante para a formação do conceito foi o disponibilidade 1, seguido pelo disponibilidade 3.

l) No construto segurança, nenhum item teve que ser removido. No modelo final, o item mais importante para a formação do conceito foi o confidencialidade, seguido pelo integridade.

Tabela 5

Análise fatorial dos indicadores

Construtos		Modelo Inicial				Modelo Final		
		Itens	CF¹	Com²	Peso (α)	CF¹	Com²	Peso (α)
CONFIDENCIALIDADE	Confidencialidade 1	CON3	0,735	0,541	0,383	0,708	0,501	0,388
		CON5i	0,439	0,193	0,229			
		CON6	0,544	0,296	0,283	0,596	0,355	0,327
		CON7	0,446	0,199	0,232	0,447	0,200	0,246
		CON9i	0,833	0,693	0,433	0,875	0,766	0,480
	Confidencialidade 2	CON1	0,475	0,225	0,265			
		CON2	0,579	0,336	0,323	0,681	0,463	0,403
		CON4	0,562	0,315	0,313	0,627	0,393	0,371
		CON8i	0,657	0,431	0,366	0,601	0,361	0,356
		CON10i	0,696	0,485	0,388	0,687	0,472	0,407
	Confidencialidade	Confidencialidade 1	0,740	0,548	0,676	0,740	0,548	0,676
		Confidencialidade 2	0,740	0,548	0,676	0,740	0,548	0,676
INTEGRIDADE	Integridade 1	INT1	0,602	0,362	0,211	0,605	0,366	0,219
		INT2	0,480	0,231	0,168	0,497	0,247	0,179
		INT5	0,767	0,588	0,268	0,772	0,596	0,279
		INT6	0,752	0,565	0,263	0,753	0,567	0,272
		INT11i	0,692	0,479	0,242	0,691	0,478	0,250
		INT14	0,494	0,244	0,173	0,482	0,232	0,174
		INT15i	0,509	0,260	0,178	0,533	0,284	0,192
		INT16i	0,358	0,128	0,125			
	Integridade 2	INT7	0,487	0,237	0,216			
		INT8	0,639	0,408	0,283	0,646	0,417	0,305
		INT9i	0,717	0,514	0,317	0,681	0,463	0,322
		INT10i	0,492	0,242	0,218	0,542	0,293	0,256
		INT12i	0,690	0,476	0,305	0,754	0,568	0,356
		INT13i	0,618	0,382	0,274	0,611	0,373	0,289
	Integridade 3	INT3	0,677	0,458	0,396	0,677	0,458	0,396
		INT4	0,818	0,669	0,479	0,818	0,669	0,479
		INT17i	0,762	0,580	0,446	0,762	0,580	0,446
	Integridade	Integridade 1	0,844	0,713	0,459	0,844	0,713	0,459
		Integridade 2	0,806	0,650	0,438	0,806	0,650	0,438
		Integridade 3	0,691	0,477	0,375	0,691	0,477	0,375

continua

Tabela 5

Análise fatorial - conclui

Construtos		Modelo Inicial				Modelo Final		
		Itens	CF[1]	Com[2]	Peso (α)	CF[1]	Com[2]	Peso (α)
DISPONIBILIDADE	Disponibilidade 1	DIS1	0,740	0,547	0,458	0,740	0,547	0,458
		DIS2	0,710	0,504	0,440	0,710	0,504	0,440
		DIS5i	0,750	0,562	0,465	0,750	0,562	0,465
	Disponibilidade 2	DIS3i	0,760	0,578	0,658	0,760	0,578	0,658
		DIS4i	0,760	0,578	0,658	0,760	0,578	0,658
	Disponibilidade 3	DIS6i	0,823	0,677	0,608	0,823	0,677	0,608
		DIS7	0,823	0,677	0,608	0,823	0,677	0,608
	Disponibilidade	Disponibilidade 1	0,777	0,603	0,623	0,777	0,603	0,623
		Disponibilidade 2	0,423	0,179	0,339	0,423	0,179	0,339
		Disponibilidade 3	0,681	0,464	0,547	0,681	0,464	0,547
Segurança		Confidencialidade	0,745	0,555	0,565	0,745	0,555	0,565
		Integridade	0,705	0,497	0,535	0,705	0,497	0,535
		Disponibilidade	0,516	0,266	0,391	0,516	0,266	0,391

[1] Carga fatorial; [2] Comunalidade.

A Tabela 6 mostra os resultados das análises da validade convergente, confiabilidade e dimensionalidade dos construtos. Logo, conclui-se que:

a) Todos os construtos atingiram os níveis exigidos de confiabilidade, dado que os índices de confiabilidade Alfa de Cronbach (AC) ou confiabilidade composta (CC) foram superiores a 0,60.
b) Pelo critério de retas paralelas, todos os construtos foram unidimensionais.
c) Os valores das AVEs foram superiores a 0,40 em todos os construtos, evidenciando assim a validação convergente desses valores.
d) Em todos os construtos o ajuste da análise fatorial foi adequado, uma vez que todos os *Kaiser-Meyer-Olkins* (KMO) foram superiores a 0,50.

Tabela 6

Validação dos construtos

Construtos	Itens	A.C.[1]	C.C.[2]	Dim.[3]	AVE4	KMO5
CONFIDENCIALIDADE 1	4	0,579	0,692	1	0,455	0,560
CONFIDENCIALIDADE 2	4	0,541	0,675	1	0,422	0,461
CONFIDENCIALIDADE	2	0,181	0,612	1	0,550	0,500
INTEGRIDADE 1	7	0,719	0,764	1	0,400	0,740
INTEGRIDADE 2	5	0,670	0,729	1	0,423	0,726
INTEGRIDADE 3	3	0,587	0,707	1	0,569	0,631
INTEGRIDADE	3	0,642	0,742	1	0,613	0,615
DISPONIBILIDADE 1	3	0,554	0,688	1	0,538	0,623
DISPONIBILIDADE 2	2	0,292	0,641	1	0,586	0,500
DISPONIBILIDADE 3	2	0,510	0,710	1	0,672	0,500
DISPONIBILIDADE	3	0,249	0,593	1	0,409	0,499
SEGURANÇA	3	0,354	0,628	1	0,439	0,532

[1] Alfa de Cronbach, [2] Confiabilidade Composta, [3] Dimensionalidade, 4Variância Extraída; 5 KMO.

A Figura 16 ilustra o modelo final ajustado, o qual passou a contar com oito construtos de primeira ordem e quatro de segunda ordem. É merecedor de ênfase especial o fato de que ele representa um desdobramento do modelo original sugerido pelo referencial teórico após a aplicação das técnicas de análise multivariada, que mostraram, com base nos dados coletados, ter sido necessário um refinamento do primeiro modelo.

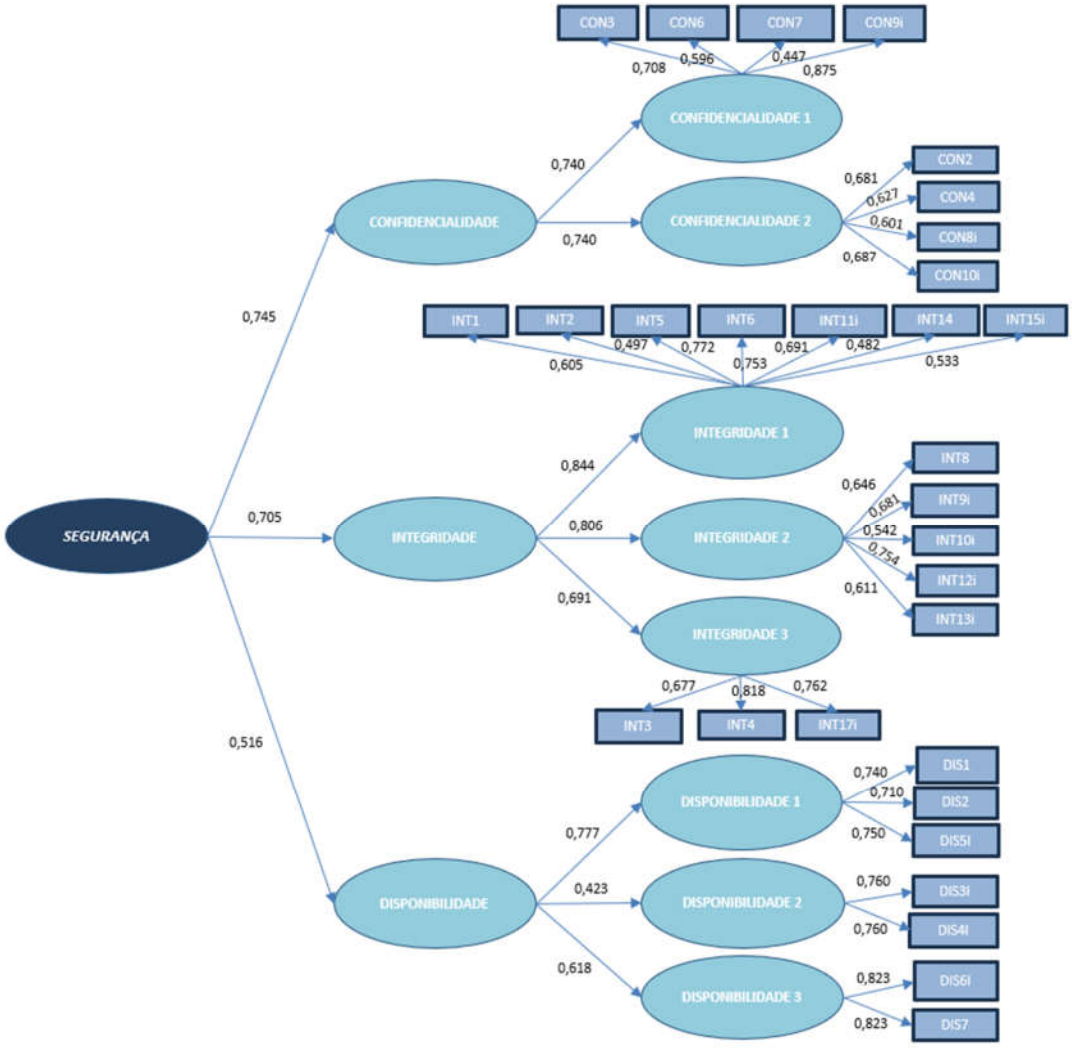

Figura 16
Modelo ajustado.
Fonte: dados da pesquisa.

4.3 Descrição dos construtos criados

Na Tabela 7 encontra-se a descrição dos construtos criados a partir da análise fatorial e mostra que o construto disponibilidade 2 apresentou média significativamente maior que a dos demais, ocorrendo situação inversa para o construto integridade 3.

Tabela 7

Descrição dos construtos de primeira ordem criados

Variáveis	Média	DP	IC - 95%	1Q	2Q	3Q
CONFIDENCIALIDADE 1	0,51	0,17	[0,48; 0,55]	0,36	0,49	0,68
CONFIDENCIALIDADE 2	0,46	0,17	[0,43; 0,49]	0,32	0,48	0,58
INTEGRIDADE 1	0,40	0,13	[0,38; 0,43]	0,29	0,38	0,51
INTEGRIDADE 2	0,48	0,15	[0,46; 0,51]	0,37	0,47	0,55
INTEGRIDADE 3	0,34	0,18	[0,30; 0,37]	0,19	0,32	0,47
DISPONIBILIDADE 1	0,52	0,22	[0,48; 0,56]	0,38	0,55	0,72
DISPONIBILIDADE 2	0,63	0,24	[0,59; 0,68]	0,50	0,67	0,83
DISPONIBILIDADE 3	0,54	0,29	[0,48; 0,59]	0,25	0,58	0,75

[1] Intervalo Bootstrap.

4.4 Relação entre os construtos e as variáveis de caracterização

A Tabela 8 faz a comparação entre os tempos de experiência para cada construto. Os tempos foram agrupados em iniciante (menos de três anos), intermediário (de três a cinco anos, de seis a oito anos), avançado (de nove a 11 anos, de 12 a 14 anos) e especialista (de 15 a 17 anos, de 18 a 20 anos, mais de 20 anos). Os destaques são:

Observou-se diferença significativa (valor p=0,019) de percepção da hierarquização ao se considerar o tempo de experiência do profissional apenas para o construto integridade1. Ao se realizarem as comparações múltiplas, apurou-se significativa diferença do intermediário quando comparado aos níveis iniciante (valor p=0,040) e especialista (valor p=0,023), sendo que os respondentes do nível Intermediário apresentaram valores mais altos de integridade1.

Tabela 8

Comparação entre os tempos de experiência para cada construto

Variáveis		N	Média	DP	1ºQ	2ºQ	3ºQ	Valor-p[1]	Comparações múltiplas[2]		
									Iniciante	Intermediário	Avançado
Confidencialidade 1	Iniciante	4	0,54	0,05	0,50	0,53	0,58	0,411	-	-	-
	Intermediário	8	0,58	0,16	0,47	0,56	0,71		1,000	-	-
	Avançado	17	0,53	0,14	0,42	0,51	0,55		1,000	1,000	-
	Especialista	77	0,50	0,18	0,36	0,48	0,69		1,000	1,000	1,000
Confidencialidade 2	Iniciante	4	0,49	0,10	0,42	0,51	0,56	0,718	-	-	-
	Intermediário	8	0,51	0,12	0,47	0,52	0,58		1,000	-	-
	Avançado	17	0,45	0,21	0,28	0,48	0,54		1,000	1,000	-
	Especialista	77	0,45	0,17	0,32	0,46	0,60		1,000	1,000	1,000
Integridade 1	Iniciante	4	0,32	0,07	0,27	0,32	0,37	0,019	-	-	-
	Intermediário	8	0,54	0,10	0,50	0,53	0,62		0,040	-	-
	Avançado	17	0,40	0,14	0,29	0,39	0,52		0,842	0,116	-
	Especialista	77	0,39	0,13	0,28	0,37	0,47		0,842	0,023	0,842
Integridade 2	Iniciante	4	0,47	0,09	0,41	0,47	0,53	0,309	-	-	-
	Intermediário	8	0,55	0,16	0,41	0,52	0,69		1,000	-	-
	Avançado	17	0,44	0,11	0,36	0,39	0,48		1,000	0,399	-
	Especialista	77	0,49	0,15	0,36	0,47	0,55		1,000	1,000	0,861
Integridade 3	Iniciante	4	0,30	0,14	0,20	0,25	0,39	0,584	-	-	-
	Intermediário	8	0,41	0,16	0,26	0,42	0,54		1,000	-	-
	Avançado	17	0,34	0,21	0,11	0,32	0,49		1,000	1,000	-
	Especialista	77	0,33	0,18	0,19	0,32	0,43		1,000	1,000	1,000
Disponibilidade 1	Iniciante	4	0,61	0,27	0,39	0,67	0,84	0,485	-	-	-
	Intermediário	8	0,58	0,20	0,42	0,63	0,75		1,000	-	-
	Avançado	17	0,54	0,24	0,38	0,61	0,73		1,000	1,000	-
	Especialista	77	0,50	0,22	0,38	0,51	0,67		1,000	1,000	1,000

Continua

Tabela 8

Comparação entre os tempos de experiência para cada construto - conclui

Variáveis		N	Média	DP	1ºQ	2ºQ	3ºQ	Valor-p[1]	Comparações múltiplas[2]		
									Iniciante	Intermediário	Avançado
Disponibilidade 2	Iniciante	4	0,69	0,11	0,63	0,67	0,75	0,156	-	-	-
	Intermediário	8	0,72	0,24	0,58	0,79	0,92		1,000	-	-
	Avançado	17	0,53	0,23	0,42	0,58	0,75		0,817	0,338	-
	Especialista	77	0,65	0,25	0,50	0,67	0,92		1,000	1,000	0,338
Disponibilidade 3	Iniciante	4	0,65	0,34	0,42	0,75	0,88	0,633	-	-	-
	Intermediário	8	0,55	0,33	0,25	0,63	0,79		1,000	-	-
	Avançado	17	0,55	0,35	0,17	0,75	0,83		1,000	1,000	-
	Especialista	77	0,53	0,27	0,33	0,58	0,67		1,000	1,000	1,000

[1] Teste de Kruskal-Wallis; [2] Teste de Mann-Whitney.

A Tabela 9 compara os cargos para cada construto. Sobressaíram-se:

Houve diferença significativa (valor p=0,014) na percepção da hierarquização dos indicadores ao se considerar o cargo do profissional no construto confidencialidade1. Ao se realizarem as comparações múltiplas, detectou-se diferença significativa do cargo de superintendente quando comparado ao de coordenador/ gerente (valor p=0,005), sendo que os respondentes do nível superintendente exibiram valores mais baixos de confidencialidade.

Houve diferença significativa (Valor p=0,033) na percepção da hierarquização dos indicadores ao se considerar o construto confidencialidade2. Ao serem feitas as comparações múltiplas, percebeu-se diferença marginalmente significativa do superintendente em relação ao nível analista/ consultor (valor p=0,060), sendo que os respondentes do nível superintendente relataram valores mais baixos de confidencialidade.

Tabela 9

Comparação entre os cargos para cada construto

Variáveis		N	Média	DP	1ºQ	2ºQ	3ºQ	Valor-p[1]	Comparações múltiplas[2]			
									1	2	3	4
CONFIDENCIALIDADE 1	Analista / Consultor (1)	12	0,49	0,10	0,43	0,48	0,55	0,014	-	-	-	-
	Coordenador / Gerente (2)	52	0,55	0,16	0,41	0,53	0,72		1,000	-	-	-
	Superintendente (3)	13	0,37	0,13	0,29	0,36	0,37		0,086	0,005	-	-
	Diretor (4)	24	0,52	0,20	0,34	0,57	0,69		1,000	1,000	0,334	-
	Presidente (5)	5	0,54	0,18	0,39	0,50	0,71		1,000	1,000	0,415	1,000
CONFIDENCIALIDADE 2	Analista / Consultor (1)	12	0,52	0,16	0,47	0,54	0,61	0,033	-	-	-	-
	Coordenador / Gerente (2)	52	0,47	0,17	0,33	0,48	0,58		1,000	-	-	-
	Superintendente (3)	13	0,34	0,15	0,25	0,32	0,40		0,060	0,104	-	-
	Diretor (4)	24	0,45	0,17	0,32	0,47	0,60		1,000	1,000	0,353	-
	Presidente (5)	5	0,54	0,14	0,48	0,60	0,61		1,000	1,000	0,155	1,000
INTEGRIDADE 1	Analista / Consultor (1)	12	0,44	0,18	0,29	0,42	0,61	0,815	-	-	-	-
	Coordenador / Gerente (2)	52	0,40	0,12	0,31	0,38	0,51		1,000	-	-	-
	Superintendente (3)	13	0,38	0,11	0,28	0,33	0,45		1,000	1,000	-	-
	Diretor (4)	24	0,39	0,14	0,27	0,35	0,51		1,000	1,000	1,000	-
	Presidente (5)	5	0,46	0,16	0,39	0,44	0,50		1,000	1,000	1,000	1,000
INTEGRIDADE 2	Analista / Consultor (1)	12	0,52	0,13	0,47	0,50	0,57	0,450	-	-	-	-
	Coordenador / Gerente (2)	52	0,47	0,15	0,35	0,44	0,55		1,000	-	-	-
	Superintendente (3)	13	0,46	0,14	0,39	0,46	0,55		1,000	1,000	-	-
	Diretor (4)	24	0,49	0,13	0,41	0,47	0,53		1,000	1,000	1,000	-
	Presidente (5)	5	0,56	0,18	0,47	0,51	0,68		1,000	1,000	1,000	1,000
INTEGRIDADE 3	Analista / Consultor (1)	12	0,28	0,11	0,19	0,25	0,37	0,141	-	-	-	-
	Coordenador / Gerente (2)	52	0,33	0,18	0,17	0,32	0,47		1,000	-	-	-
	Superintendente (3)	13	0,25	0,11	0,17	0,23	0,32		1,000	0,870	-	-
	Diretor (4)	24	0,41	0,23	0,20	0,41	0,68		0,870	0,870	0,584	-
	Presidente (5)	5	0,39	0,08	0,32	0,39	0,44		0,584	1,000	0,432	1,000

Continua

Tabela 9

Comparação entre os cargos para cada construto – conclui

Variáveis		N	Média	DP	1ºQ	2ºQ	3ºQ	Valor-p[1]	Comparações múltiplas[2]			
									1	2	3	4
DISPONIBILIDADE 1	Analista / Consultor (1)	12	0,61	0,24	0,55	0,67	0,78	0,468	-	-	-	-
	Coordenador / Gerente (2)	52	0,51	0,22	0,36	0,51	0,72		1,000	-	-	-
	Superintendente (3)	13	0,48	0,20	0,33	0,44	0,61		1,000	1,000	-	-
	Diretor (4)	24	0,50	0,23	0,36	0,47	0,67		1,000	1,000	1,000	-
	Presidente (5)	5	0,53	0,22	0,39	0,61	0,67		1,000	1,000	1,000	1,000
DISPONIBILIDADE 2	Analista / Consultor (1)	12	0,60	0,21	0,58	0,58	0,67	0,872	-	-	-	-
	Coordenador / Gerente (2)	52	0,66	0,24	0,50	0,67	0,92		1,000	-	-	-
	Superintendente (3)	13	0,63	0,30	0,42	0,67	0,92		1,000	1,000	-	-
	Diretor (4)	24	0,60	0,24	0,42	0,63	0,75		1,000	1,000	1,000	-
	Presidente (5)	5	0,60	0,31	0,33	0,58	0,92		1,000	1,000	1,000	1,000
DISPONIBILIDADE 3	Analista / Consultor (1)	12	0,61	0,31	0,29	0,71	0,83	0,720	-	-	-	-
	Coordenador / Gerente (2)	52	0,53	0,28	0,25	0,63	0,75		1,000	-	-	-
	Superintendente (3)	13	0,49	0,27	0,25	0,58	0,67		1,000	1,000	-	-
	Diretor (4)	24	0,53	0,30	0,29	0,58	0,75		1,000	1,000	1,000	-
	Presidente (5)	5	0,55	0,30	0,33	0,58	0,75		1,000	1,000	1,000	1,000

Teste de Kruskal-Wallis; ² Teste de Mann-Whitney.

5 Considerações Finais

Esta dissertação se propôs ao desenvolvimento de um *framework* que disponibilizasse às organizações um ambiente seguro para se trabalhar com *CloudComputing*. Nesse sentido, o estudo estribou-se em um regramento metodológico constituído de quatro etapas, a saber:

a) Eleição inicial de um modelo analítico (construtos e indicadores) extraído mediante a fusão de um referencial teórico pertinente e orientações emanadas da ISO 27001.
b) Pesquisa inicial com 35 especialistas em *CloudComputing* para uma definição final da associação dos indicares sugeridos pela etapa anterior a cada um dos construtos do modelo analítico
c) Aplicação de um questionário construído com o modelo sugerido na etapa **b** a uma amostra de 110 especialistas de mercado.
d) Aplicação de uma análise fatorial aos dados obtidos, que mostrou a necessidade do desdobramento do modelo inicialmente constituído por três construtos em um modelo final sugerido com oito construtos.

A explanação anteriormente apresentada (item 4.2) permite concluir que ambos os objetivos, geral e específicos, foram devidamente alcançados.

O primeiro (objetivo geral) foi alcançado com a apresentação da Figura 16, que mostra o modelo analítico final obtido após a aplicação da análise fatorial sobre os dados obtidos pela pesquisa de campo. Desse modo, ficou preenchida a lacuna identificada e retratada pela inexistência de um *framework* sistematicamente obtido que subsidiasse o desenvolvimento de uma estratégia de segurança em *CloudComputing*.

O primeiro objetivo específico (teste do modelo sugerido) foi alcançado com a apresentação da Tabela 6.

O segundo objetivo específico que buscou mostrar a importância relativa (pesos) de cada indicador para o seu respectivo construto foi representado pelo coeficiente fatorial mostrado na Figura 16.

O terceiro e quarto objetivos específicos foram também alcançados e mostrados nas Tabelas 8 e 9, respectivamente. O que se conclui é que apenas para a dimensão integridade1 é que se observou diferença estatisticamente significativa de percepção entre profissionais de distintos tempos de experiência na área. Nesse caso, a diferença apareceu quando se comparou “intermediário” com “iniciante” e com “especialista”. Quando se considerou o cargo que o profissional desempenha, as percepções foram diferentes nas dimensões confidencialidade1 e Confidencialidade2. No primeiro caso, as diferenças apareceram quando se comparou o superintendente com o coordenador; no segundo caso, as diferenças significativas foram entre o superintendente e o analista/consultor.

Em função do exposto, e à guisa de síntese, pode-se afirmar que o presente estudo pode ser utilizado como um instrumento gerencial e de planejamento para a atividade de *CloudComputing*. De fato, além de apresentar um *framework* sistematicamente obtido, realçou a importância (pesos) de cada indicador em cada uma das dimensões do modelo analítico e perscrutou a diferença de percepções ao se levar em conta o tempo de experiência bem como o cargo do profissional de segurança em *CloudComputing*. Esse conjunto de conclusões extraídas do estudo permite subsidiar o desenvolvimento de uma estratégia de segurança no campo de *CloudComputing*; e fornece, assim, uma contribuição para intervenção.

Do ponto de vista acadêmico, ou seja, em termos de contribuição para a compreensão do fenômeno, o estudo apresenta uma incursão robusta no referencial teórico pertinente e sugere um tratamento estatisticamente embasado para uma geração objetiva de um modelo analítico com parâmetros quantificados e testados.

Do ponto de vista pessoal, permitiu ao mestrando um importante crescimento tanto teórico como prático em sua área de atuação profissional, cuja característica fulcral é a de um dinamismo inovador e recorrente.

6 Recomendações para Estudos Futuros

Cumpre por último enfatizar a necessidade da atualização constante do estudo aqui apresentado, uma vez que o tema tratado se renova exponencialmente, exigindo aperfeiçoamento ininterrupto do modelo sugerido para captar novas dimensões de análise que certamente surgirão. Essa atualização deve ocorrer tanto por meio do acompanhamento sistemático do referencial teórico, que se renova velozmente, quanto mediante novas pesquisas de campo para captar alterações nas percepções dos novos profissionais que adentrarão nessa opção profissional.

Referências

Almeida, M. A., Mendes, I. A. D., & Figueiredo, J. C. (2020). A nova lei geral de proteção de dados pessoais (LGPD) e sua relação com a segurança da informação. *Revista Direito, Estado e Sociedade*, *16*(3), 1-24.

Aniche, M. (2015). *Testes automatizados de software: um guia prático*. São Paulo: Casa do Código Livros para o Programador (p. 46).

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, L., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*. http://doi.acm.org/10.1145/1721654.1721672.

Associação Brasileira de Normas Técnicas. Norma Brasileira. International Organization for Standardization. International Eletrotechnical Comission. ABNT/ NBR/ISO/IEC *27005:2023 - Gestão de riscos na segurança da informação*. Rio de Janeiro: ABNT.

Autoridade Nacional de Proteção de Dados (2023). *Lei Geral de Proteção de Dados Pessoais* (LGPD). Recuperado de: https://www.gov.br/anpd/pt-br: https://www.gov.br/ anpd/pt-br

Berger, I. W. (2009). *Cloud: The emergence of a new model of computing.* Recuperado de: http://blog.irvingwb.com/blog/2009/04/cloud-the-emergence-of-a-new-model-of-computing.html.

Bezerra, F. H. G., Sousa Jr, R. T., & de Oliveira, J. C. (2019). Análise da maturidade da gestão de segurança da informação em empresas de consultoria de TI do Nordeste brasileiro. *Revista Administração em Diálogo, 21*(2), e2122.

Buyya, R., Broberg, J., & Goscinski, A. (2011). *CloudComputing: principles and paradigms.* s.l.: John Wiley & Sons.

Carnegie Mellon University. (2007). D*ocumento n. 2155, CERT C Programming Language Secure Coding Standard*. Retrievedf from: https://www.cmu.edu/.

Caruso, C., & Steffen, F. D. (1999). *Segurança em informática e de informações*. São Paulo: Campus (367 p.).

Coelho, F. E. S., Araújo, L. G. S., Bezerra, E. K. (2014). *Gestão da Segurança da Informação NBR 27001 e NBR 27002*. Rio de Janeiro: Escola Superior de Redes.

De Haes, S., & Van Grembergen, W. (2009). An exploratory study into it governance implementations and its impact on business/IT Alignment. *Information Systems Management, 26*(2), 123-137.

Deming, W. E. (1986). *Out of the crisis*. Cambridge, MA: MIT Press.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE *Transactions on Information Theory, 22*(6), 644-654.

Dikakaikos, N., Smith, J., & Jones, A. (2009). The impact of social media on consumer behavior. *Journal of Marketing Research*, *46*(3), 321-335.

Federação Brasileira dos Bancos. Febraban. (2023a). *Mobile representa dois terços das transações bancárias no Brasil, revela Febraban*. Recuperado de: https://www.mobiletime.com.br/noticias/28/06/2023/mobile-representa-dois-tercos-das-transacoes-bancarias-no-brasil-revela-febraban/.

Federação Brasileira dos Bancos. Febraban. (2023b). *Pesquisa Febraban de Tecnologia Bancária 2023.* Recuperado de: : https://portal.febraban.org.br/ noticia/3950/pt-br/.

Fontes, E. (2012). *Políticas e normas para a segurança da informação*. Brasport.

Galup, S. L. (2015). *Risk management guide for information technology systems*. NIST Special Publication 800-30. [URL inválido removido].

Hadnagy, C. (2010). *The art of deception: Controlling the human element of security*. Wiley Publishing (2. ed.).

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Análise multivariada de dados*. Porto Alegre: Bookman.

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos da segurança da informação: com base na ISO 27001 3 na ISO 27002*. São Paulo, Brasport (3. ed. rev.).

Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika, 30*(2), 179-185, 1965. Doi: 10.1007/BF02289447.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard*. (2. ed.). ISBN 13: 978-1-60807-930-8 ©

Hurwitz, J., Blosch, M., Nugent, C., & Ray, S. (2010). *The essential CloudComputing handbook: A complete guide for business, technology, and IT professionals*. McGraw-Hill Osborne Media.

International Organization for Standardization. (2022). *ISO 27001:2022 - Information security management systems - Requirements*. International Organization for Standardization.

Jansen, W. & Grance, T., 2011. *Guidelines on security and privacy in public CloudComputing,* s.l.: NIST - National Institute of Standards and Technology.

Krebs, B. (2021, Jan. 25). *The ISO 27001 framework: A comprehensive approach to information security*. Krebs on Security.

Krebs, B. (2019). *The ISO 27001 Security Standard: Everything You need to know*. San Francisco, CA: No Starch Press (1. ed.).

Krutz, R. L., & Vines, R. D. (2010). *CloudSecurity: A comprehensive guide to secure cloud computing.* Wiley Publishing.

Laudon, K. C., & Laudon, J. O. (1999). *Sistemas de informação com internet*. Rio de Janeiro: LTC (4. ed.).

Marconi, M. A., & Lakatos, E. M. (2001). *Metodologia do trabalho científico*. São Paulo: Atlas.

Mather, T., Kumaraswamy, S., & Latif, S., 2009. *Cloud security and privacy.* s.l.: O'Reilly.

Mattar, F. N. (2011). *Pesquisa de marketing*. São Paulo; Atlas (v. 1).

Mell, P., & Grance, T. (2011). NIST, 2011. *The NIST definition of CloudComputing,* s.l.: National Institute of Standards and Technology.

Mignoti, S. A. (2007 jan.). *Análise de dados através de métodos de estatística multivariada: uma abordagem aplicada*. Belo Horizonte: UFMG (1. ed., 297 p.).

Minayo, M. C. S. (2016). *Pesquisa social: teoria, método e criatividade*. Petrópolis: Vozes. (3ª. reimp.; Série Manuais Acadêmicos).

Mitnick, K. (2002). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York, NY: Simon & Schuster (1. ed.).

Mohamed, A. (2009). *A history of cloud computing*. Recuperado de: http://www.computer weekly.com/feature/Ahistoryofcloudcomputing.

National Institute of Standards and Technology (NIST) (2011). The NIST definition of *CloudComputing*. *National Institute of Standards and Technology, 53*(6), 50.

Nunes, J. C. (2020). Segurança da informação no Brasil: desafios e perspectivas. *Revista Brasileira de Gestão de Negócios, 22*(1), 124-140.

Pfleeger, C. P., & Pfleeger, S. L. (2018). *Security in computing*. Boston, MA: Pearson (5. ed.).

Pontes, H. M. V., & Sousa, F. A. S. (2018). A segurança da informação no Brasil: desafios e oportunidades. *Revista Administração em Diálogo, 20*(2), 201-222.

Rodrigues, A. A. (2013). *Comentários à Lei Carolina Dieckmann - Lei nº 12.737/12: crimes cibernéticos*. Curitiba: Juruá (1. ed.).

Rodrigues, R. (2015). A ISO 27001 e a *CloudComputing*: uma análise crítica. *Revista Brasileira de Gestão e Tecnologia da Informação, 13*(3), 1-16.

Rosenzweig, P., & Kuhn, D. R. (2015). *Cyber warfare: Techniques, tactics and tools for security practitioners.* Elsevier.

Santos, R. (2020). *Segurança da informação em ambientes de CloudComputing*. Elsevier.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Sêmola, M. (2003). *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Campus (184 p.).

Silva, L., & Cunha, J. (2021). *Segurança da informação em ambientes de CloudComputing*. São Paulo, Senac.

Souza, J. C. (2017). A ISO 27001 e a *CloudComputing*: desafios e oportunidades. *Revista Eletrônica de Sistemas de Informação, 16*(2), 44-60.

Souza, J. C., & Costa, A. M. (2020). A ISO 27001 e a *CloudComputing*: desafios e perspectivas. *Revista de Gestão e Tecnologia da Informação, 19*(2), 1-18.

Souza, M. V. (2019). A ISO 27001 e a *CloudComputing*: uma visão crítica. *Revista de Administração de Empresas, 59*(3), 269-282.

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice*.* Pearson.

Stoneburner, G., Goguen, A., & Feringa, A. (2004). *Risk management framework for information systems and organizations*. NIST Special Publication 800-3

Taurion, C. (2009). *CloudComputing*: *computação em nuvem*. Rio de Janeiro: Brasport.

Vacca, J. R. (2016). *CloudComputing Security*. Foundations and Challenges.

Veras, M. (2015). *Computação em nuvem: nova arquitetura de TI*. Rio de Janeiro: Brasport (174 p.).

Watkins, S. G. (2022). *ISO/IEC 27001:2022 An introduction to information security and the ISMS standard*. IT Governance Publishing.

Wei, J., Li, Y., & Wang, X. (2014). The impact of social media on consumer behavior. *Journal of Marketing Research*, *51*(2), 215-232.

Whitman, M. E., & Mattord, H. J. (2019). *Princípios de segurança da informação.* Cengage Learning.

Winkler, V. (2011). *Securing the Cloud - Cloud Computer Security Techniques and Tactics.* s.l.: Syngress.

Wirtz, B. W., Mory, L., & Piehler, R. (2014). Web 2.0 and digital business models. *In:* F. J. Martínez-López (Ed.). *Handbook of strategic e-business management* (pp. 751-766). Springer.