XIII SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
ESCA
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 13th INTERNATIONAL CONFERENCE

DESENVOLVIMENTO DE UM FRAMEWORK DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTES DE CLOUDCOMPUTING BASEADO NA ABNT ISO/IEC 27001:2022

DEVELOPMENT OF AN INFORMATION SECURITY FRAMEWORK FOR CLOUDCOMPUTING ENVIRONMENTS BASED ON ABNT ISO/IEC 27001:2022

PAULO SERGIO DE SOUZA
FUNDAÇÃO PEDRO LEOPOLDO (FPL)

WANDERLEY RAMALHO
FUNDAÇÃO PEDRO LEOPOLDO (FPL)

JOSÉ EDSON LARA
FUNDAÇÃO PEDRO LEOPOLDO (FPL)

THAIS ESPINOLA DE OLIVEIRA LIMA

Comunicação:
O XIII SINGEP foi realizado em conjunto com a 13th Conferência Internacional do CIK (CYRUS Institute of Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

Agradecimento à orgão de fomento:
Agradeço o apoio e atenção dispensada ao desenvolvimento e apresentação deste trabalho, especialmente à Fundação Pedro Leopoldo.

DESENVOLVIMENTO DE UM FRAMEWORK DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTES DE CLOUDCOMPUTING BASEADO NA ABNT ISO/IEC 27001:2022

Objetivo do estudo
O presente estudo 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 nuances da segurança em CloudComputing.

Relevância/originalidade
Observa-se uma lacuna retratada pela falta de um modelo capaz de nortear o desenvolvimento de uma estratégia de gestão de segurança da informação no ambiente de computação em nuvem. Este trabalho preenche essa lacuna utilizando uma metodologia estatística apropriada para fazê-lo.

Metodologia/abordagem
A partir da ISO/IEC 27001:2022 e de pesquisa com especialistas, elaborou-se um modelo com três construtos e 34 indicadores. Após questionário aplicado a 110 especialistas, foi aplicado o método de análise fatorial e obtendo-se modelo final com 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 resultado mais relevante foi constatar a necessidade de refinar o modelo analítico sugerido pelo referencial teórico, calculando-se todos os seus coeficientes fatoriais.

Contribuições teóricas/metodológicas
O estudo desenvolveu e testou um modelo analítico extraído do referencial teórico, explicitando 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 construção do modelo.

Contribuições sociais/para a gestão
O presente estudo constitui um instrumento gerencial e de planejamento para a atividade de CloudComputing, mostrando a importância de cada indicador em cada uma das dimensões do modelo analítico contribuindo para um processo de intervenção na realidade da gestão de segurança.

Palavras-chave: Computação em Nuvem, Segurança da Informação, Modelo analítico, Ciber Segurança

DEVELOPMENT OF AN INFORMATION SECURITY FRAMEWORK FOR CLOUDCOMPUTING ENVIRONMENTS BASED ON ABNT ISO/IEC 27001:2022

Study purpose
This study aimed to develop and test an analytical model, including constructs and indicators, to investigate the nuances of Cloud Computing security, grounded in expert perceptions and aligned with the principles and guidelines established by ABNT ISO/IEC 27001:2022.

Relevance / originality
There is a gap due to the lack of a model to guide the development of an information security management strategy in cloud computing environments. This study addresses that gap by applying a suitable statistical methodology to support model development and validation.

Methodology / approach
Based on ISO/IEC 27001:2022 and expert research, a model with three constructs and 34 indicators was developed. After a questionnaire with 110 specialists and factor analysis, the final model resulted in eight dimensions and 34 indicators.

Main results
The overall goal of presenting an analytical model for Cloud Computing security management was achieved. The most relevant result was identifying the need to refine the theoretical model by calculating all its factor loadings to ensure its statistical and conceptual validity.

Theoretical / methodological contributions
The study developed and tested an analytical model based on the theoretical framework, detailing analytical dimensions and indicators for building a Cloud Computing security management strategy. Methodologically, it demonstrated how to apply statistical tools effectively for model construction and validation.

Social / management contributions
This study serves as a management and planning tool for Cloud Computing activities, highlighting the importance of each indicator within the model's dimensions and contributing to effective intervention in real-world information security management processes.

Keywords: CloudComputing, Information Security, Analytical model, Cyber Security

DESENVOLVIMENTO DE UM FRAMEWORK DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTES DE CLOUDCOMPUTING BASEADO NA ABNT ISO/IEC 27001:2022

1 Introdução

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 instalarem suas aplicações em servidores localizados em ambientes de fornecedores da Cloud. 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). 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.

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. 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.

De forma geral, ressente-se, no mercado, da falta de um protocolo que permita às organizações, tendo por base a ISO 27001, enfrentar os novos desafios apresentados pelas nuances 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. Para preencher essa lacuna, este artigo é norteado 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.

2 Referencial teórico

Uma incursão no referencial teórico pertinente ao tema permitirá a extração de um modelo analítico inicial com o qual todo o estudo será desenvolvido.

2.1 Segurança da informação

A segurança da informação, 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. 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.

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.

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 a 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:

2.1.2.1 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.

2.1.2.2 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.”

2.1.2.3 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.

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 1950 , 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 1950 a 1970 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*.

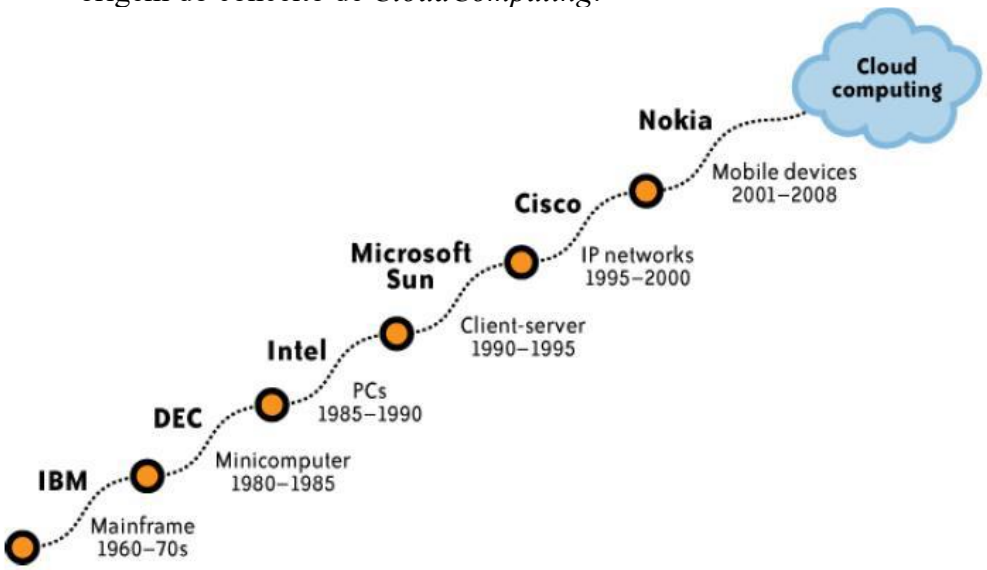

Figura 1
Evolução tecnológica.
Fonte: Mather, T., Kumaraswamy, S., & Latif, S., 2009. *Cloud security and privacy.* s.l.: O'Reilly.

As bibliografias estudadas definem a *CloudComputing* como um modelo de computação que fornece recursos de processamento, 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.

2.2.1 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.

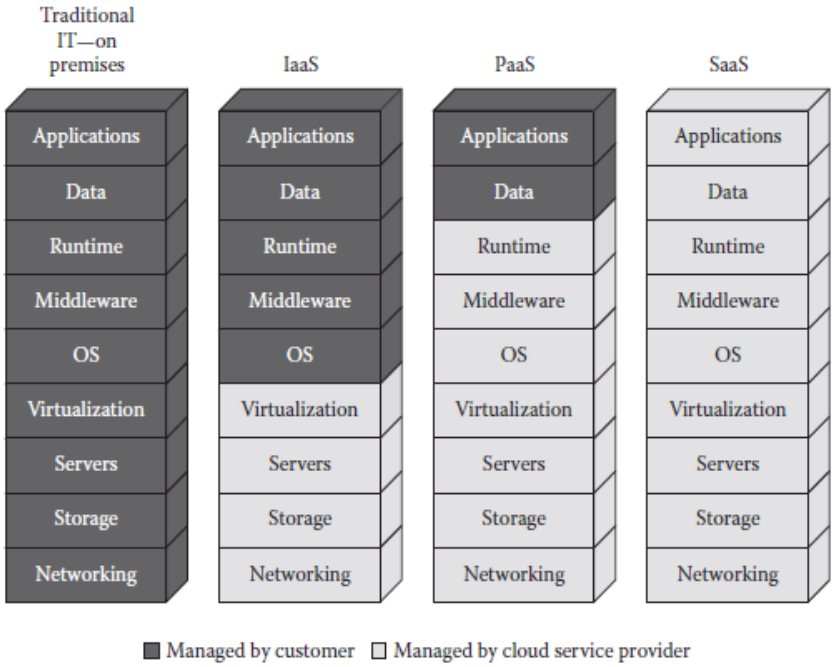

Figura 2
Responsabilidades dos envolvidos, nos diversos modelos.
Fonte: Vacca, J. R. (2016). *Cloud Computing Security*. Foundations and Challenges.

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 (Sistema de Gestão de Segurança da Informação). 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. A norma teve ainda outras duas revisões: em 2013 e, mais recentemente, em 2022, sobre a qual foi desenvolvido esse artigo.

2.3.1 Referências de controles da segurança da informação

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 deste artigo. Esses controles são divididos da seguinte forma:

2.3.2 Controles organizacionais

Aqui são descritos 37 controles 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.

2.3.2.1 Controle de pessoas

São determinados 08 controles 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.

2.3.2.2 Controles físicos

Neste subitem são tratados os 14 controles de acesso físico 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.

2.3.2.3 Controles tecnológicos

Nessa seção são descritos 34 controles de segurança da informação que podem afetar diretamente o cliente contratante do serviço de *CloudComputing*. Dependendo do modelo de contratação, o cliente pode ser totalmente responsável por mantê-los, dependendo da forma de contratação. Estes controles são o ponto central deste estudo, eles serão detalhados mais a diante.

3 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".

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.

4 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 3, que é constituído por três construtos e 34 indicadores que se encontram descritos na Tabela 1.

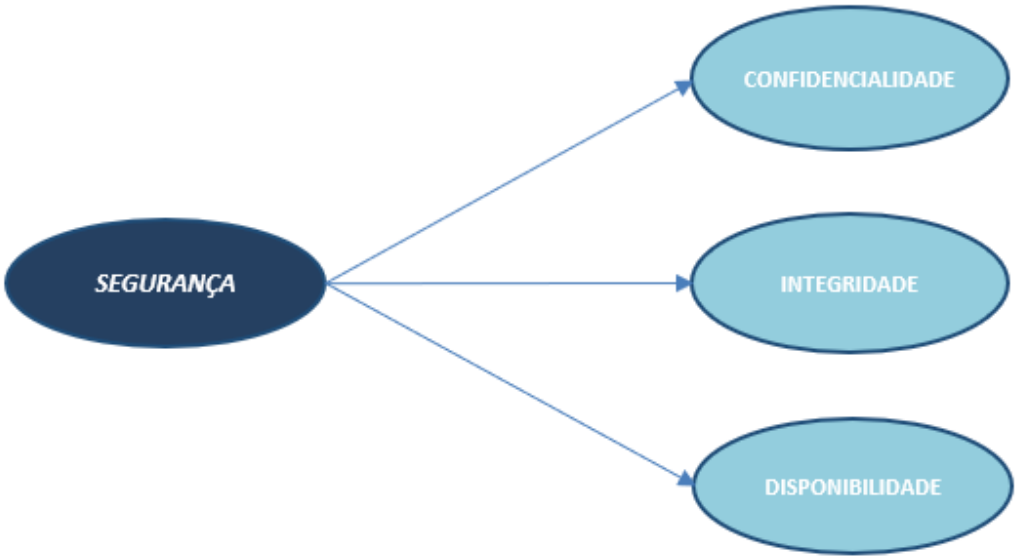

Figura 3
Modelo analítico.
Fonte: do autor.

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.

5 Metodologia

O presente estudo pode ser classificado como quantitativo em decorrência do tipo de variável e dos procedimentos utilizados. A unidade de observação 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.

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 4, 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.

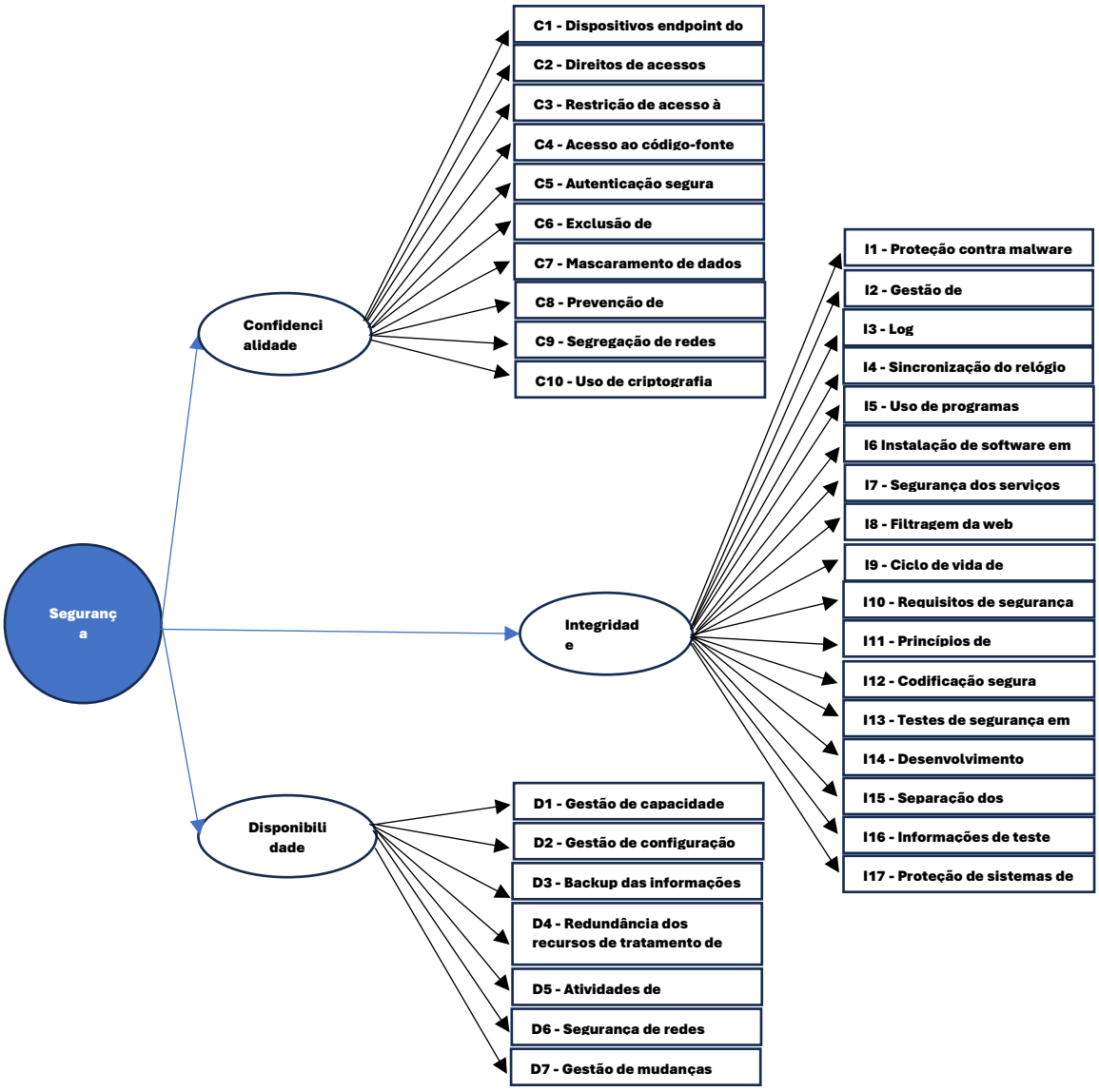

Figura 4
Modelo intermediário
Fonte: dados da pesquisa.

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.

6 Análise dos resultados

O primeiro procedimento metodológico consistiu na utilização da análise multivariada que permitiu testar o modelo proposto pelo referencial teórico bem como explicitar a importância relativa dos indicadores que constituem cada construto desse modelo.

Nesse caso, 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 – (Mignot, 2007), 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). Após uma aplicação de análise fatorial com os indicadores do novo modelo analítico, extraiu-se todos os seus coeficientes fatoriais.

A Figura 5 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.

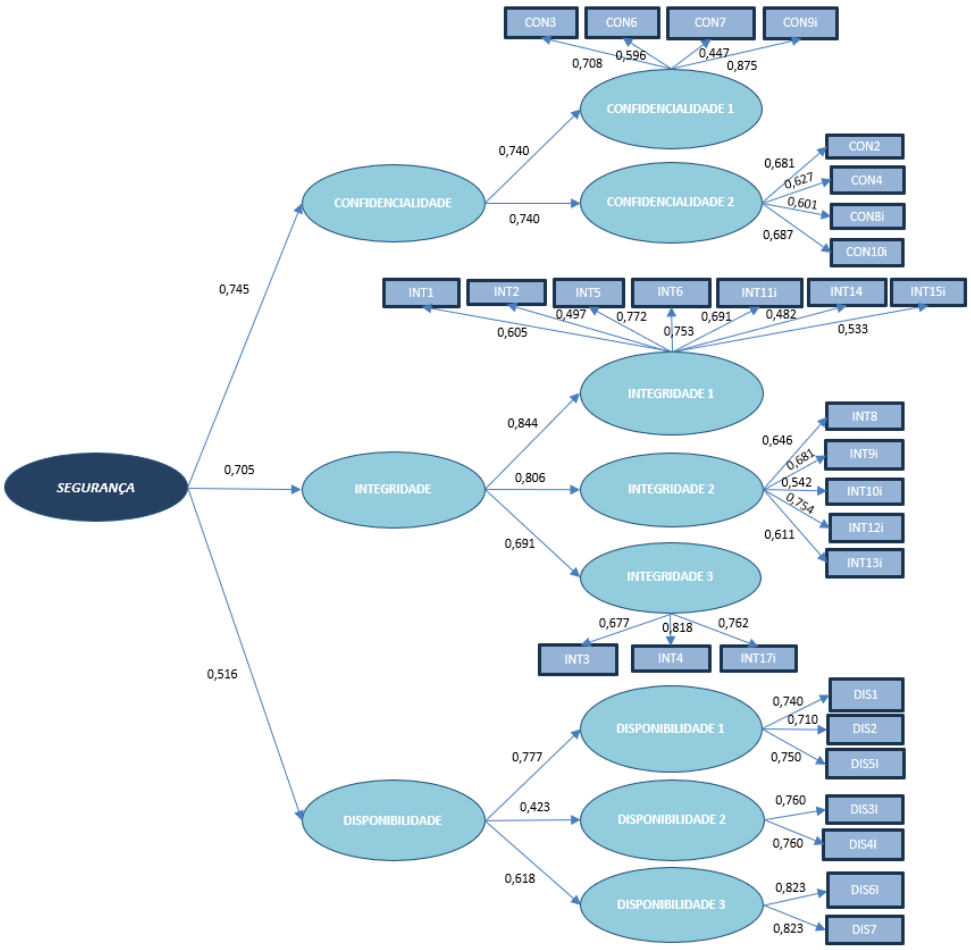

Figura 5
Modelo ajustado.

Fonte: dados da pesquisa.

Um segundo procedimento foi proceder a uma verificação do impacto do "tempo de experiência do profissional" sobre cada construto do modelo analítico final. 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.

Em terceiro lugar, procedeu-se a uma verificação do impacto da variável "cargo ocupado pelo profissional" sobre cada construto. 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.

7 **Considerações Finais**

Este artigo 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 apresentação do modelo analítico final obtido após a aplicação da análise fatorial (Hair,2009) sobre os dados obtidos pela pesquisa de campo preencheu a lacuna identificada e retratada pela inexistência de um *framework* sistematicamente obtido que subsidiasse o desenvolvimento de uma estratégia de segurança em *CloudComputing*. Nesse sentido, apresentou-se a importância relativa (pesos) de cada indicador para o seu respectivo construto por meio dos coeficientes fatoriais mostrados na Figura 5. Adicionalmente, ao analisar-se os impactos das variáveis “tempo de experiência do profissional de segurança” e “cargo desse profissional”, concluiu-se 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.

8 Referências

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.

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.

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/.

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.

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

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.

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.

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

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

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

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

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

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

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

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

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.

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.