UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA
ELÉTRICA E DE COMPUTAÇÃO

AMANDIO FERREIRA BALCÃO FILHO

FTACSP: *FRAMEWORK* PARA AVALIAÇÃO DE CONFIANÇA DE PROVEDORES DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

FTACSP: FRAMEWORK FOR TRUST ASSESSMENT OF CLOUD SERVICE PROVIDERS

Campinas
2023

AMANDIO FERREIRA BALCÃO FILHO

FTACSP: *FRAMEWORK* PARA AVALIAÇÃO DE CONFIANÇA DE PROVEDORES DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

FTACSP: FRAMEWORK FOR TRUST ASSESSMENT OF CLOUD SERVICE PROVIDERS

Tese submetida à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Doutor em Engenharia Elétrica, na área de Engenharia de Computação.

Dissertation *submitted to the School of Electrical and Computer Engineering, University of Campinas, in partial fulfillment of the requirements to obtain the Doctorate degree in Electrical Engineering, in the area of Computer Engineering.*

Supervisor/Orientador: Prof. Dr. Mario Jino

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO AMANDIO FERREIRA BALCÃO FILHO, E ORIENTADA PELO PROF. DR. MARIO JINO.

Campinas

2023

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

F189f

Balcão Filho, Amandio Ferreira, 1959-
FTACSP: Framework para avaliação de confiança de provedores de serviços de computação em nuvem / Amandio Ferreira Balcão Filho. – Campinas, SP : [s.n.], 2023.

Orientador: Mario Jino.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Computação em nuvem. 2. Confiança do consumidor. 3. Design centrado no usuário. 4. Métricas de segurança. I. Jino, Mario, 1943-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações Complementares

Título em outro idioma: FTACSP: Framework for trust assessment of cloud service providers
Palavras-chave em inglês:
Cloud computing
Consumer confidence
User - Centered design
Security metrics
Área de concentração: Engenharia de Computação
Titulação: Doutor em Engenharia Elétrica
Banca examinadora:
Mario Jino [Orientador]
Romis Ribeiro de Faissol Attux
Plínio Roberto Souza Vilela
Nandamudi Lankalapalli Vijaykumar
Elcio Hideiti Shiguemori
Data de defesa: 13-09-2023
Programa de Pós-Graduação: Engenharia Elétrica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-8386-0484
- Currículo Lattes do autor: http://lattes.cnpq.br/5891652594120801

COMISSÃO EXAMINADORA – TESE DE DOUTORADO

Candidato: Amandio Ferreira Balcão Filho RA: 098964

Data da Defesa: 13/09/2023

Título da Tese: “FTACSP : Framework para Avaliação de Confiança de Provedores de Serviços de Computação em Nuvem” (*FTACSP: Framework for Trust Assessment of Cloud Service Providers*)

Prof. Dr. Mario Jino - (Presidente, FEEC-UNICAMP)

Prof. Dr. Romis Ribeiro de Faissol Attux - (FEEC - UNICAMP)

Prof. Dr. Plínio Roberto Souza Vilela - (FT - UNICAMP)

Prof. Dr. Nandamudi Lankalapalli Vijaykumar - (INPE)

Prof. Dr. Elcio Hideiti Shiguemori - (ITA)

A ata de defesa, com as respectivas assinaturas dos membros da Comissão Julgadora, encontra-se no SIGA (Sistema de Fluxo de Dissertação/Tese) e na Secretaria de PósGraduação da Faculdade de Engenharia Elétrica e de Computação.

DEDICATÓRIA

Dedico este trabalho de maneira especial à minha esposa Euzeli e à minha filha Amanda, que me apoiaram, foram pacientes e tolerantes e sempre me incentivaram a continuar até a conclusão deste trabalho. Foi de grande aprendizado para todos da família, que a dedicação e persistência apesar dos obstáculos e dificuldades levam a alcançar os sonhos.

AGRADECIMENTOS

Ao meu orientador, professor Dr. Mario Jino, foi uma grande honra para mim ser orientado por uma pessoa tão especial, uma referência na área de Engenharia de Software do nosso país.

Aos membros da banca examinadora, professores Plínio Roberto Souza Vilela, Romis Ribeiro de Faissol Attux, Nandamudi Lankalapalli Vijaykumar e Elcio Hideiti Shiguemori pelas importantes sugestões de melhoria.

Aos professores e funcionários da UNICAMP, que sempre foram gentis e competentes, prontos a nos atender.

Agradeço ao Centro de Tecnologia da Informação Renato Archer (CTI) e a todos os colegas servidores pela oportunidade e pelo apoio que me foram dados para que eu pudesse desenvolver este trabalho concomitantemente com minhas atividades de pesquisador e servidor público.

Em especial ao amigo Ferrucio Rosa que dedicou parte de seu tempo em me ouvir, incentivar, dar opinião e buscarmos soluções conjuntas para a conclusão deste trabalho de doutorado.

Aos amigos Luiz Otávio Duarte, Antônio Theóphilo, Rodrigo Bonacin, Guilherme Ruppert, Walcir Cardoso, Rodrigo Ruiz e Rogério Winter, que foram importantes para a conclusão desta tese.

Agradeço à Profa. Nilde Balcão pelas inestimáveis contribuições para esta tese.

Enfim, agradeço a todos que contribuíram direta ou indiretamente com este trabalho.

Sobretudo a Deus por ter me permitido ter saúde e determinação para não desanimar durante a realização deste trabalho.

*"De fato, a confiança tornou-se a **nova moeda** da economia global. É a base sobre a qual muitas pessoas fazem negócios ou não"*

Stephen Covey e Greg Link

(pág. 22 do livro A Confiança Inteligente)

RESUMO

Os consumidores de serviços de computação em nuvem não possuem informações confiáveis suficientes sobre características críticas de seus provedores, como desempenho, segurança, confiança e privacidade, conformidade com leis e regulamentos, entre outras. Esta tese aborda esses problemas, apresentando um framework de avaliação de confiança que integra três domínios: Governança, Transparência e Informação sobre a Segurança. A abordagem proposta é centrada no consumidor e lida com aspectos de confiança da perspectiva do usuário final. Indicadores são usados para comunicar os resultados, que visam a representar a expressão de governança, transparência e informações sobre a segurança dos serviços em avaliação. A tese inclui uma proposta de implementação, protótipo e prova de conceito, onde o framework foi aplicado em três cenários do mundo real e foi executada uma simulação de uso de 18 meses para verificar sua aplicabilidade, sensibilidade e robustez. O framework é destinado a consumidores de computação em nuvem que buscam conhecer e mensurar níveis de segurança da informação, proteção de privacidade, transparência de segurança e altos níveis de qualidade em seus serviços e infraestrutura. Os resultados principais desta tese são: um framework que fornece uma avaliação de confiança baseada no ponto de vista do consumidor final do serviço de Nuvem; um método que calcula os Indicadores que os consumidores usarão para tomar suas decisões; um questionário com questões que os consumidores usam para avaliar os serviços de nuvem que estão usando; um protótipo de software que entrega como resultado o cálculo dos Indicadores e gráficos de evolução destes. Também foi realizada uma Prova de Conceito com dois avaliadores avaliando três aplicativos reais que usam serviços de computação em nuvem e uma simulação de 18 meses.

Palavras-chave - Computação em Nuvem. Avaliação de Confiança. Métricas. Centrado no Consumidor. Segurança. Privacidade. Estrutura.

ABSTRACT

Cloud computing services consumers do not have enough reliable information about critical characteristics of their providers, such as performance, security, trust and privacy, compliance with laws and regulations, among others. This dissertation addresses these problems by presenting a trust assessment framework that integrates three domains: Governance, Transparency, and Security Information. Our approach is consumer-centric and deals with trust aspects from the end-user's perspective. We use Indicators to communicate the outcomes, which aim to represent the expression of cybersecurity, manageability, and transparency of services under assessment. The dissertation includes an implementation proposal, a prototype, and proof of concept, in which the framework was applied in three real-world scenarios and executed over a 18 months usage simulation to verify its applicability, sensitivity, and robustness. Our study is intended for use by consumers of cloud computing who seek to know and measure levels of cybersecurity, protection of privacy, transparency of security, and high levels of quality in their services and infrastructure. The main results of this dissertation are a framework that provides a trust assessment based on the point of view of the end consumer of the Cloud service; a method that calculates the Indicators that consumers will use to make their decisions; a questionnaire with questions that consumers use to evaluate the cloud services they are using; a software prototype that delivers the calculation of Indicators and graphs of their evolution as a result. A Proof of Concept was also carried out with two evaluators evaluating three real applications that use cloud computing services and an 18-month simulation.

Keywords - Cloud Computing. Trust Assessment. Metrics. Consumer-centric. Security. Privacy. Framework.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
API	Application Programming Interface
AWS	Amazon Web Services
CASB	Cloud Access Security Broker
CAIQ-CSA	CSA Consensus Assessments Initiative Questionnaire
CCAK	Certificate of Cloud Auditing Knowledge
CCM	Cloud Controls Matrix – Versão 4
CCSK	Certificate of Cloud Security Knowledge
COBEI	Comitê Brasileiro de Eletricidade, Eletrônica, Iluminação e Telecomunicações
CSA	Cloud Security Alliance
CSCC	Cloud Security Command Center do GCP
CSP	Cloud Service Providers
CSU	Cloud Service Users
CTP-CSA	Cloud Trust Protocol - CSA
FTACSP	Framework for Trust Assessment of Cloud Service Providers
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation, (UE) 2016/679
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IoT	Internet of Things
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
ISO	International Organization of Standardization
LAI	Lei de Acesso a Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
Nuvem	Computação em Nuvem
PaaS	Platform as a Service
PI	Personal Information
PII	Personally Identifiable Information

PoC	Proof of Concept
QoS	Quality of Service
RB	Relationship Bonus
SaaS	Software as a Service
SGBD	Sistema de Gerenciamento de Banco de Dados
SI	Segurança da Informação
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOC	Security Operation Center
STAR	Security, Trust, Assurance and Risk
TI	Tecnologia da Informação
TPA	Third Party Auditor
TTP	Trusted Third Party
TV	Televisão

SUMÁRIO

1 INTRODUÇÃO

O objeto desta tese é a computação em nuvem. O principal desafio desta tese é a mensuração da confiança que um consumidor deposita no serviço de computação em nuvem que utiliza. Como medir essa confiança? A hipótese é que existem várias maneiras de diminuir as preocupações dos usuários da Nuvem. O problema, portanto, a ser pesquisado, é como fornecer medidas de confiança e indicadores, projetados para medir a confiança do consumidor nos provedores de serviços de computação em nuvem.

O termo "Nuvem é usado com o mesmo significado de serviços de computação em nuvem ou computação em nuvem.

As vidas das pessoas estão cheias de diferentes tipos de sistemas tecnológicos. A vida moderna depende de nossa confiança nesses sistemas especialistas e essa confiança não decorre do amplo conhecimento desses sistemas; em vez disso, está baseada na experiência de que tais sistemas funcionam como se espera que funcionem, como já afirmava o sociólogo britânico Giddens (1991).

O objetivo da tese é contribuir por meio de um modelo conceitual, um *framework* FTACSP (*Framework for Trust Assessment of Cloud Service Providers*) e um protótipo de software para avaliação da confiança em serviços de computação em nuvem. A abordagem está baseada em uma perspectiva centrada nas necessidades e expectativas dos consumidores dos serviços de Nuvem, e usa indicadores numéricos para representar a confiança depositada nos serviços contratados.

O FTACSP é o *framework* que proporciona solucionar o problema de avaliação da confiança do usuário nos serviços de Nuvem; fornecendo soluções de um mesmo domínio de problema, permitindo a reutilização de seu código. Um *framework* para avaliação de confiança em provedores de serviços de computação em nuvem é apresentado. Indicadores numéricos são propostos para que forneçam aos consumidores de serviços de Nuvem um meio de avaliar a confiança no CSP (*Cloud Service Providers*). A melhoria da confiança dos consumidores em ambientes de Nuvem é uma tarefa árdua; são exigidos novos critérios e indicadores relacionados a dados sensíveis, suportados por métricas adequadas.

No modelo proposto, a segurança da informação é entendida como um

conceito que deve considerar também a privacidade. O modelo de avaliação da confiança deve ser entendido no seu significado amplo, não apenas na aceitação de credenciais de autenticação ou autorização emitidas por federação de entidades confiáveis entre si.

Nesse sentido, são necessários modelos mais abrangentes, baseados em um conjunto de critérios representativos como os inspirados em (Saaty & Ergu, 2015). Esses modelos devem considerar vários aspectos, incluindo: reputação, desempenho, recomendação, políticas, regulamentos, conformidade com legislação e normas, credenciamento por auditores independentes e divulgação obrigatória de incidentes de segurança da informação.

O *framework* é proposto para ser utilizado pelos usuários dos serviços de Nuvem, sendo que os usuários não precisam ser especialistas em segurança da informação para realizar a avaliação e formar uma opinião sobre os provedores de serviços de computação em nuvem. Essa opinião será baseada em evidências e informações objetivas e subjetivas. Esta é uma nova abordagem.

Os serviços de computação em nuvem são compostos por sistemas-de-sistemas, ou seja, um conjunto de sistemas interdependentes de modo a formar um todo organizado. Computação em nuvem é uma quebra de paradigma no modelo de negócios de tecnologia da informação (TI), que traz novas exigências, tais como: visibilidade e transparência da segurança da informação; conquista da confiança dos consumidores; significado e relevância das informações providas para esse novo modelo de negócios. As oportunidades que a Nuvem oferece são claras para os setores de negócios e consumidores. No entanto, confiança e segurança são dois dos obstáculos mais críticos para a adoção e crescimento da Nuvem hoje (Meixner & Buettner, 2012).

Segurança e privacidade constituem aspectos cruciais da confiança que os consumidores depositam em um provedor de serviços de computação em nuvem - CSP (*Cloud Service Provider*). Na Nuvem, as funções e responsabilidades de segurança e privacidade são distribuídas entre diferentes atores. Os consumidores de serviços de computação em nuvem não têm informações suficientes sobre essas questões nem sobre o cumprimento de leis e regulamentos. Mesmo quando os consumidores estão cientes, as informações recebidas têm pouco significado e relevância para eles (Habib et al., 2014). A comunicação é um obstáculo a ser

superado, pois nem sempre a informação está disponível e em formato adequado. Nesses ambientes também há pouco controle sobre os níveis de serviço, com base em informações, métricas, leis e regulamentos. Portanto, os clientes logo percebem fragilidades em relação ao desempenho, confiabilidade, segurança da informação e privacidade, dentre outras questões (Pearson, 2013).

Garantia de segurança é um conceito mais amplo do que segurança, pois inclui metodologias para coletar e validar evidências que suportam propriedades de segurança (Ardagna et al., 2015). Estudos apontam que os impedimentos para a adoção da Nuvem provavelmente são atitudinais e não tecnológicos (Carr, 2005).

Os serviços de Nuvem podem ser mais bem explorados se o envolvimento de clientes e provedores na gestão da segurança for aprofundado, aumentando a confiança nesses serviços. Nesse sentido, as técnicas de garantia de segurança aumentam a transparência da Nuvem (Ardagna et al., 2014) e aumentam a confiança dos atores da Nuvem de que seus serviços se comportam conforme o esperado.

Os consumidores exigem métodos e sistemas eficazes que apoiem os processos de avaliação de confiança. Por exemplo, mecanismos de avaliação de confiança, processos de *feedback*, privacidade dos participantes, etc., são questões em aberto a serem estudadas (Noor, Sheng, Maamar, et al., 2016).

Em (Nicol et al., 2010), os autores destacam que “A confiança é um estado mental que compreende:

a) Expectativa – o consumidor espera por um comportamento específico do provedor, como fornecer informações válidas ou efetivamente realizar ações cooperativas;

b) Crença – o consumidor acredita que o comportamento esperado ocorre com base na evidência de competência e boa vontade do fornecedor;

c) Disposição para assumir riscos – o consumidor está disposto a assumir riscos por essa crença.

O equilíbrio entre confiança e risco aceitável é estabelecido por meio da credibilidade de sistemas especialistas, expertise e sistemas contingentes projetados para mitigar os impactos de possíveis incidentes (Giddens, 1991). Confiança é uma

questão de calcular vantagens e riscos em determinadas circunstâncias, onde especialistas responderão aos incidentes de segurança.

A privacidade é outra preocupação importante que não é abordada de forma efetiva pelos modelos recentes. A privacidade tem influência expressiva na decisão dos usuários de utilizar serviços de nuvem (Asadullah et al., 2015). Os serviços da Web que violam as expectativas de privacidade do usuário são penalizados por um declínio nos níveis de confiança (Martin, 2017).

Os contratos com os CSPs devem ser transparentes e deixar claras as questões de segurança, bem como definir responsabilidades relevantes no relacionamento comercial com seus clientes (T. Branco & Santos, 2016). A transparência depende de informações e dados fornecidos pelos provedores de nuvem. O monitoramento é outro aspecto fundamental da confiança e geralmente é realizado usando métricas impostas pelos próprios provedores desses serviços.

Do ponto de vista dos usuários de serviços de Nuvem, a tomada de decisão é uma combinação de transparência da segurança, confiança e interpretação dos dados coletados. Um modelo de confiança abrangente, relevante e significativo deve considerar todos esses aspectos (Ardagna et al., 2015). A tomada de decisões depende de sistemas que coletam e processam continuamente esses dados.

Falhas na proteção de privacidade e vazamento de dados causam danos aos usuários da Nuvem, e a divulgação obrigatória de falhas e incidentes podem induzir os consumidores a aumentar seu nível de cuidado, reduzindo assim seus danos (Romanosky et al., 2010).

Um sistema de gerenciamento de confiança eficaz deve oferecer suporte aos usuários para que possam avaliar seus provedores de serviços de computação em nuvem. Mecanismos de avaliação de confiança, *feedbacks* duvidosos, privacidade dos participantes e falta de integração de *feedbacks* são exemplos de questões em aberto, que ainda precisam ser investigadas (Noor et al., 2013a). Palavras-chave como *Cloud Computing, Edge Computing, Fog Computing*, Internet das Coisas (IoT) são bastante conhecidas e já não causam estranheza no público mais ligado às questões tecnológicas. Esses serviços de tecnologia são fortemente dependentes da computação em nuvem sob suas várias formas de modelos de serviço. No entanto, os usuários desses serviços geralmente não conhecem quais são as condições e

garantias oferecidas pelos serviços que estão usando.

Buscando atender essas exigências, propõe-se um modelo conceitual que aborda o tema da perspectiva do consumidor dos serviços e de suas necessidades de visibilidade da segurança e de confiança nos provedores de serviços de computação em nuvem. Faz-se necessária a investigação de novas formas de comunicação e divulgação eficiente de informações, considerando sua relevância e significado para os usuários finais. Indicadores podem ser definidos para contemplar esses aspectos, apontando tendências e considerando parâmetros quantitativos e qualitativos. Esses indicadores podem servir como métricas de resultados de ações e processos do CSP.

Adicionalmente, um protótipo de software foi desenvolvido e o *framework* proposto foi aplicado em cenários do mundo real. Os resultados empíricos mostram a aplicabilidade, sensibilidade e robustez do *framework*.

Com base no exposto, os seguintes **objetivos** são realizados:

Objetivo Geral

- Elaborar um *Framework* para avaliação de confiança em CSPs (FTACSP – *Framework for Trust Assessment of Cloud Service Providers*).

Objetivos Específicos

- Propor uma Arquitetura Funcional em Camadas do *Framework* que proporcione uma visão geral da abordagem e apresente os Indicadores de Confiança (Amândio Balcão Filho et al., 2020), (Colombo et al., 2012).
- Desenvolver um Protótipo de Software para aplicação da abordagem em um contexto real. O código fonte do protótipo (Versão 1.0) pode ser encontrado no repositório GitHub[1].
- Realizar uma Prova de Conceito, aplicando o *Framework* em três serviços reais e em uma simulação (Balcão Filho et al., 2023).
- Uma simulação do *Framework*, para um período de 18 meses, a fim

[1] Código fonte do FTACSP (Versão 1.0): https://github.com/FTACSP/prototype

de simular uma situação que levou à quebra de confiança do usuário no provedor.

Esta tese está organizada da seguinte forma:

- No **Capítulo 2** – definições e conceitos sobre computação em nuvem;
- No **Capítulo 3** – apresenta fundamentos sobre confiança e segurança da informação;
- No **Capítulo 4** – modelos de confiança em computação em nuvem e os trabalhos relacionados são discutidos;
- No **Capítulo 5** – processo de engenharia e os cálculos do *Framework*;
- No **Capítulo 6** – Prova de Conceito (PoC), onde o *Framework* proposto foi aplicado em três serviços do mundo real e em uma simulação, utilizando o protótipo de software;
- No **Capítulo 7** – discussão sobre os resultados da aplicação do PoC, conclusões, limitações e trabalhos futuros, além dos resultados técnico-científicos da pesquisa.

2 DEFINIÇÕES E CONCEITOS DE COMPUTAÇÃO EM NUVEM

Neste capítulo, são apresentados conceitos sobre Computação em Nuvem, e um histórico de seu desenvolvimento e seus impactos na Tecnologia da Informação.

2.1 Computação em Nuvem: uma quebra de paradigma

Muito se tem falado sobre a quebra de paradigma que a Nuvem trouxe para o cenário de TI. Pode-se fazer analogias com outras quebras de paradigmas que ocorreram em outras áreas como forma de entender e antecipar os impactos que a computação em nuvem proporcionará.

Um paralelo, do ponto de vista da estruturação, entre a utilização da energia elétrica no mundo moderno e o atual cenário da computação em nuvem foi publicado em um polêmico artigo (Carr, 2005). Nele, o autor afirma que, no futuro, as empresas vão comprar de fornecedores externos a TI como um serviço de utilidade. Seu argumento é que ambos, TI e eletricidade, tornaram-se recursos escaláveis, padronizado e acessível à maior parte das pessoas. Atualmente, vemos o retorno à produção de energia elétrica descentralizada a partir da energia solar, porém integrada ao sistema centralizado.

Outro paralelo, do ponto de vista do conteúdo e serviços, foi o que ocorreu com o teatro versus a televisão, pois, com o surgimento da televisão, houve uma transposição da linguagem do teatro para a TV. Com a Nuvem, ocorreu uma transposição da infraestrutura tradicional para a Nuvem, embora a Nuvem ofereça serviços e conteúdos somente possíveis em ambientes da Nuvem. As diversas formas de geração de eletricidade ou as diversas formas de entretenimento não desapareceram; ao contrário, uma suporta e contribui para o desenvolvimento da outra. Supõe-se que será assim com a Nuvem versus a computação tradicional, haja vista que as tecnologias proporcionadas pela Internet estão revolucionando, por exemplo, todos os tipos de entretenimento.

Uma das consequências é a redução de recursos humanos e financeiros na computação tradicional e a migração de recursos de capital para recursos operacionais. Essas consequências impactarão fortemente a cultura das

organizações e pessoas.

A computação em nuvem aproveitou muitos anos de desenvolvimento da computação distribuída, grade computacional, *Service Oriented Architecture* (SOA) e *Web Services* para se consolidar. Seu sucesso baseia-se na virtualização total de servidores, na implementação de técnicas de armazenamento virtual e na virtualização de redes. Técnicas que são aplicadas de forma sistemática em um centro de dados.

Ao se juntar o auto-provisionamento e o auto-dimensionamento, criou-se a infraestrutura básica da computação em nuvem. É a combinação de tecnologias facilitadoras essenciais e um modelo de negócios sob demanda, que possibilitam o desenvolvimento de sistemas de aplicação altamente escaláveis, em escala de peta-bytes. Desde o final dos anos 1990, as empresas Oracle e Dell EMC já ofereciam soluções privadas com características da Nuvem.

Em 2006, é lançado o Amazon Web Service (AWS), uma base de "computação utilitária", termo este usado quando do lançamento do *Whitepaper* do AWS[2] em 2002. Quando a Amazon viu crescer o interesse pelas tecnologias que usava para gerir seus recursos internos de computação, disponibilizou uma *Application Programming Interface* (API) para que outros pudessem desenvolver e implantar aplicações que usavam os recursos do seu centro de dados, resultando num enorme crescimento dos serviços *Amazon Elastic Compute Cloud* (EC2)[3] e Amazon S3 (S3)[4].

A computação em nuvem trouxe novas preocupações de segurança de TI que se somaram a questões já existentes anteriormente. Como a tecnologia de Nuvem está em pleno desenvolvimento e ainda em consolidação, muitas questões estão abertas a novas propostas de abordagem e resolução. A visibilidade ou transparência das práticas e garantias adotadas pelos provedores de Nuvem para a segurança da informação é uma dessas questões que é abordada no desenvolvimento.

Computação em nuvem é uma quebra de paradigma, principalmente no modelo de negócios de TI. A Nuvem é mais fácil de ser adotada por pessoas, pequenas e médias empresas que estejam iniciando seus negócios, ou iniciando

---

[2] Overview of amazon Web Services AWS Whitepaper – https://docs.aws.amazon.com/whitepapers/lates/aws-overview/introduction.html.
[3] Amazon Elastic Compute Cloud (EC2) e do Amazon S3 (S3) - https://aws.amazon.com/pt/ec2.
[4] Amazon S3 (S3) – https://aws.amazon.com/pt/s3.

novos serviços de TI. Ao ser oferecida comercialmente para pequenas empresas e usuários individuais essa tecnologia se popularizou, sendo agora amplamente adotada por muitas empresas e pessoas.

2.2 Visão geral da Computação em Nuvem

A computação em nuvem é um paradigma em evolução. O objetivo desta seção é identificar e descrever as principais características da Nuvem.

Segundo o relatório "*The NIST Definition of Cloud Computing*" (Mell & Grance, 2011), computação em nuvem é um modelo para permitir conveniente acesso ubíquo à rede, sob demanda, a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados e liberados com um esforço mínimo de gerenciamento ou interação com o provedor de serviços. Este modelo de Nuvem é composto de cinco características essenciais, três modelos de serviço e quatro modelos de implantação. Esta definição é a mais conhecida e bastante similar às definições de ITU-T e ISO/IEC sobre computação em nuvem. A Figura 2.1 ilustra esse modelo.

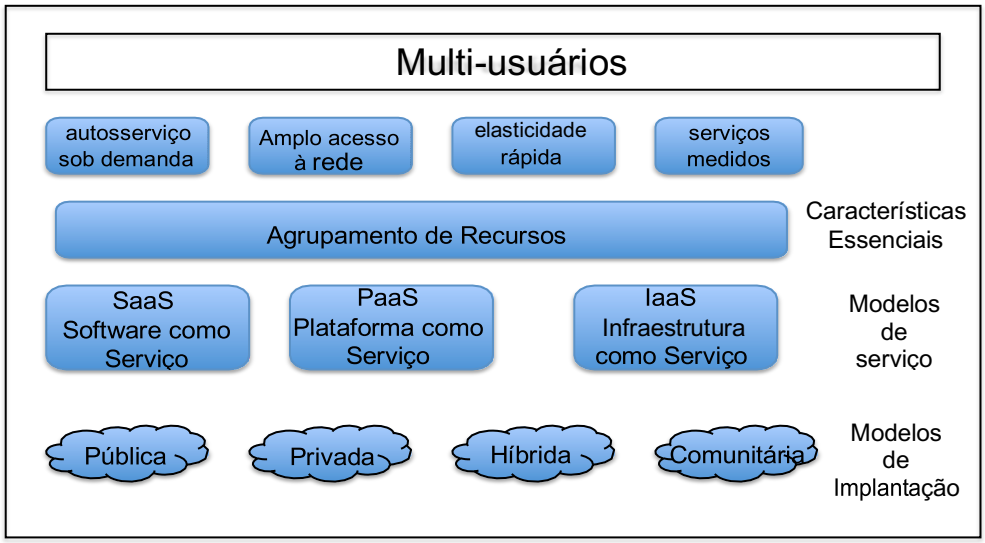


Figura 2.1- Modelo Conceitual da Nuvem

As características essenciais são:

a) autosserviço sob demanda,

b) amplo acesso à rede,

c) elasticidade rápida,

d) serviços medidos e pagos pelo uso,

e) conjunto de recursos compartilhados com múltiplos usuários num modelo multi-arrendamento.

Os modelos de serviço são:

a) Software como Serviço (SaaS),

b) Plataforma como Serviço (PaaS),

c) Infraestrutura como Serviço (IaaS).

Há outras possibilidades e capacidades de serviço que mesclam dois ou mais desses modelos, como armazenamento como serviço, desktop como serviço.

Os modelos de implantação de Nuvem são:

a) pública – a infraestrutura e os serviços de computação são gerenciados por um provedor terceirizado e compartilhados entre várias organizações;

b) privada – a infraestrutura é dedicada a uma única organização do usuário;

c) comunitária – Nuvem para uso exclusivo de uma comunidade específica de consumidores e organizações que compartilham os mesmos fins e objetivos, as mesmas preocupações;

d) híbrida – este modelo é uma composição de dois ou mais modelos de implantação.

A infraestrutura de Nuvem é uma coleção de hardware e software que possibilita a implantação de uma solução de computação em nuvem, integrados por uma *suite* de software chamada orquestrador. São exemplos de orquestradores: Apache CloudStack[5], OpenStack[6], VMWare vCloud Suite[7], dentre outros.

---

[5] CloudStack - https://cloudstack.apache.org

[6] OpenStack - https://www.openstack.org

[7] VMWare vCloud Suite – https://www.vmware.com/content/dam/digitalmarketing/vmware/pt/pdf/products/vCloud/vmware- vcloud-suite-datasheet.pdf.

A infraestrutura de Nuvem pode ser vista como contendo uma camada física e uma camada de abstração. A camada física é composta pelos recursos de hardware que são necessários para apoiar o serviço de Nuvem a ser prestado; normalmente, inclui servidores, armazenamento e componentes de rede. A camada de abstração consiste no software implantado sobre a camada física, onde se manifestam as características essenciais de Nuvem. Conceitualmente, a camada de abstração fica acima da camada física.

2.2.1 Modelo de Referência Conceitual

A Figura 2.2 apresenta uma visão geral da arquitetura de referência de computação em nuvem, segundo Liu et al (2011), que identifica os principais atores, suas atividades e funções na computação em nuvem.

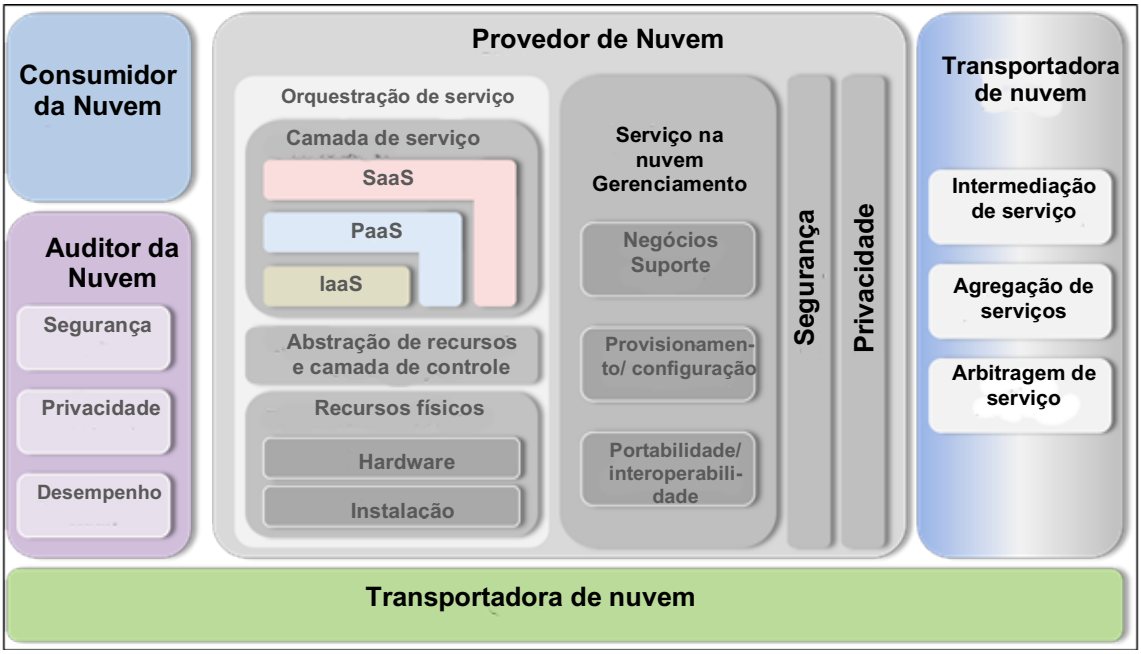


Figura 2.2 – Modelo de Referência Conceitual - adaptado de (Liu et al., 2011)

O diagrama mostra uma arquitetura genérica de alto nível e destina-se a facilitar o entendimento dos requisitos, usos, características e padrões de computação em nuvem. Observa-se na figura a existência de cinco atores principais: consumidor, auditor, provedor, corretor (*broker*) e o provedor de rede; são mostradas as principais atividades de cada um.

2.2.2 Complexidade do Contexto

Prover Segurança da Informação é uma atividade dependente do contexto, principalmente do tipo de informação, de onde está armazenada e como será utilizada (a classificação de sigilo: e.g.). Um mesmo consumidor pode ter necessidades diferentes de segurança para os seus diversos tipos de dados. Mesmo quando os consumidores pertencem a uma mesma organização-cliente, há exigências distintas entre os consumidores.

No modelo de implantação pública os conflitos tendem a aumentar, pois existe a dinâmica de entrada e saída de consumidores; esta dinâmica não enxerga a diferença de interesses entre as organizações que se hospedam nessa Nuvem. Este dinamismo torna as mensurações de segurança pouco repetíveis e com validade de projeção para o futuro muito curta (Jansen, 2009).

A pouca integração e coordenação entre provedor e consumidor cria um contexto dos mais complexos para a avaliação de um ambiente de Nuvem, dadas as necessidades de um consumidor específico.

Os mais diversos aspectos da segurança da informação como métricas, controles, políticas, normas etc. têm um baixo significado para os usuários leigos no assunto, clientes ou mesmo administradores não técnicos da Nuvem. Essas informações sobre segurança encontram pouca ressonância junto a esse público (Barabanov et al., 2011).

A principal atração da Nuvem é a eficiência de custos possibilitada pela economia de escala, reutilização e padronização. Para manter essa eficiência, os provedores têm que sacrificar a flexibilidade de opções à disposição dos clientes. Integrar as atividades de segurança nessas soluções é muitas vezes entendida como torná-las menos flexíveis. Essa rigidez se manifesta na incapacidade de manter paridade com os controles que existem na computação tradicional em comparação com a Nuvem.

2.2.3 Dinâmica da Segurança e Privacidade na Computação em Nuvem

Quando se abordam aspectos de segurança e privacidade na computação

em nuvem, devem ser considerados questões sobre a transversalidade destes aspectos, implicações do modelo de implantação, além do compartilhamento de responsabilidades.

Transversalidade da Segurança. Segurança é um dos aspectos transversais da arquitetura, se estende por todas as camadas, indo da segurança física à segurança das aplicações. Portanto, as atividades de gestão da segurança são de responsabilidade de todos os atores envolvidos. Destaca-se que há uma assimetria entre o poder de um provedor e o do consumidor, especialmente dos domésticos e de pequenas e médias empresas. Isto deve colocar nos ombros dos provedores maiores responsabilidades. Contratos e regulamentações precisam expressar essa maior responsabilização dos provedores.

Transversalidade da Privacidade. A questão da privacidade merece uma discussão à parte do restante da segurança. Segurança e privacidade são dois aspectos e requisitos fundamentais de um ambiente de Nuvem confiável: se juntam e se apoiam mutuamente para proteger os dados pessoais. Do ponto de vista da conformidade, a segurança representa um importante facilitador da privacidade, uma base necessária que permite que as empresas protejam os dados pessoais. A proteção à privacidade precisa garantir que as informações privadas e os dados derivados dessas informações sejam usadas apenas para os fins para os quais foram coletados. Esta é uma questão que remete claramente à necessidade de normatização e controle via legislação. A proteção à privacidade se estende para as informações corporativas que podem ser derivadas ou observadas das atividades do cliente, tais como tendências de negócios, relacionamentos e comunicação com outros parceiros, níveis e padrões de atividades, dentre outras possibilidades. Os provedores de Nuvem devem assegurar que os dados pessoais estão protegidos adequadamente durante o processo de manipulação (i.e., coleta, processamento, comunicação, uso e alienação). A Nuvem coloca muitos desafios adicionais para a proteção dos dados dos consumidores que utilizam seus serviços. Os “dados pessoais” (ou “informações que permitem a identificação pessoal”) referem-se às informações que podem ser usadas para identificar, contatar ou localizar uma pessoa natural, ou que podem ser usados em conjunto com outras fontes para identificar essa pessoa natural. As etapas mais importantes para proteger as informações pessoais são:

a) limitar a coleta e retenção dos dados;

b) proteger os dados de possíveis adulterações ou violações;
c) limitar o acesso interno, classificando os dados e estabelecendo um controle de acesso;
d) priorizar a privacidade, incorporando as melhores políticas e práticas na preservação da privacidade.

Implicações do modelo de implantação. Devem-se considerar as implicações que a escolha do modelo de implantação (pública, privada, comunitária ou híbrida) tem sobre os aspectos de segurança. Uma Nuvem pública tem inquilinos dos mais diversos tipos e necessidades de segurança, enquanto uma Nuvem privada é exatamente o oposto, tem somente uma organização-cliente com necessidades uniformes. Portanto, a escolha do modelo de implantação deve estar em consonância com as necessidades de isolamento entre as cargas de trabalho dos consumidores. Também o estabelecimento do perímetro se dá por meio de *firewall* virtual na Nuvem pública, enquanto na Nuvem privada é adotado *firewall* físico que provê maior controle e flexibilidade.

Compartilhamento das responsabilidades. O provedor e o consumidor de Nuvem compartilham os controles dos recursos em um sistema de Nuvem. Como ilustrado na Figura 2.3, diferentes modelos de serviço afetam os controles da organização sobre os recursos computacionais e, portanto, o que pode ser feito em um sistema em Nuvem. A figura mostra essas diferenças usando uma notação de pilha de camadas de software composta de aplicativos, *middleware* e sistemas operacionais. O esboço dos controles sobre a pilha de software ajuda a compreender o alcance das responsabilidades das partes envolvidas na gestão dos mais diversos aspectos da Nuvem. Observa-se na figura que o modelo de implantação (pública, privada etc.) e o modelo de serviço (IaaS, PaaS, SaaS) alteram profundamente as atribuições dos diferentes atores na Nuvem. Numa organização de TI tradicional os administradores têm controle sobre toda a pilha de recursos de computação e de todo o ciclo de vida dos sistemas. Na computação em nuvem, os provedores e os consumidores controlam de forma colaborativa o projeto, a implantação, a operação e a desativação dos sistemas baseados em Nuvem. A divisão de controle significa que todas as partes envolvidas agora têm a responsabilidade de fornecer proteção adequada aos sistemas baseados na Nuvem. Os provedores e os consumidores têm diferentes graus de controle sobre os recursos, notadamente os recursos de

segurança, que é uma atividade transversal à Nuvem. Esses controles mudam de mãos em função do modelo de serviço e de implantação; por exemplo, o gerenciamento da autenticação e autorização dos clientes aos recursos da Nuvem, ou o gerenciamento das regras do *firewall* para isolar a carga de trabalho entre os diversos clientes.

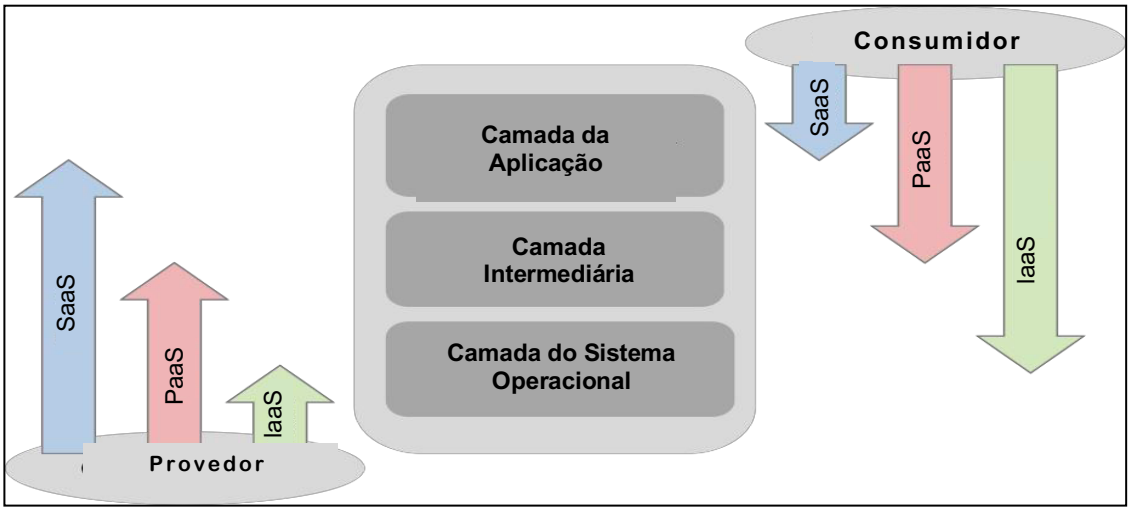


Figura 2.3 – Escopo de Controle do Provedor e do Consumidor - adaptado de (Liu et al., 2011)

2.3 Considerações Finais

Neste capítulo, apresentou-se uma visão geral da computação em nuvem, destacando que essa tecnologia representou uma quebra de paradigma, onde os usuários passam a ser clientes de empresas que oferecem os serviços de tecnologia da informação que os usuários precisam. Não há investimento na compra de equipamentos, mas sim em contratos de prestação de serviços de empresas terceiras. A segurança da informação é muito dependente do contexto, tornando a privacidade e a segurança muito dinâmicas e aumentando a complexidade das soluções.

3 FUNDAMENTAÇÃO SOBRE CONFIANÇA E SEGURANÇA DA INFORMAÇÃO

Este capítulo aborda e discute o conceito “confiança”, no domínio da tecnologia da informação (TI) e seu uso como conceito base, que é utilizado para a formulação do *framework* de avaliação proposto na tese, com vistas a acompanhar como a Segurança da Informação é alcançada pelos serviços de computação em nuvem prestados. Apresenta-se o significado da palavra confiança no contexto geral e como a confiança é construída no contexto dos serviços de TI, mais especificamente nos serviços providos pela computação em nuvem.

Nesta tese, as questões são abordadas a partir da perspectiva do consumidor (ou cliente) da computação em nuvem, ou seja, sob a perspectiva de um profissional de TI que não é especialista ou tenha grandes conhecimentos sobre Segurança da Informação (SI).

A computação em nuvem é uma tecnologia complexa que permite o acesso remoto a recursos computacionais, como armazenamento de dados e processamento de informações por meio das redes de comunicação de dados. No entanto, a adoção da computação em nuvem é muitas vezes limitada pela preocupação com a segurança dos dados e a confiança nas empresas que fornecem esses serviços. Neste contexto, faz-se necessário discutir o conceito de confiança na computação em nuvem e as estratégias que podem ser usadas para aumentar a confiança dos usuários dessa tecnologia.

Em (Schneier, 2012), discorre-se sobre os desafios e problemas que os avanços tecnológicos trazem para a nossa sociedade. A tecnologia tem melhorado continuamente, tornando as coisas existentes mais fáceis e baratas. No entanto, esses avanços tecnológicos resultam numa série de parâmetros que podem ser ajustados das mais diversas maneiras; mais pessoas terão acesso a esses parâmetros que interferem em diferentes sistemas.

A rápida mudança tecnológica faz com que a lacuna de segurança também seja maior. As pessoas e os grupos aprendem a lidar com as novas tecnologias em seu próprio ritmo, algumas com mais facilidade do que outras. As mudanças sociais e políticas trazidas pela tecnologia da informação estão causando problemas de

segurança e confiança em todo o mundo, como já afirmava (Schneier, 2012). A computação em nuvem é um desses avanços que ainda está sendo absorvido pela sociedade como um todo.

A confiança na Nuvem é um conceito complexo que envolve a confiança nas empresas que fornecem os serviços, na segurança dos dados armazenados e na disponibilidade dos recursos computacionais. A confiança é essencial para a adoção da computação em nuvem, uma vez que os usuários precisam confiar na integridade e na capacidade das empresas de fornecerem serviços seguros e confiáveis (Dhillon & Torkzadeh, 2006).

3.1 Significado do Conceito Confiança

Segundo o Dicionário Online de Português[8], a palavra “confiança” pode ser definida como: i) Sentimento de quem confia, de quem acredita na sinceridade de alguém; e ii) Convicção ou segurança em relação a alguma coisa. Segundo o Tradutor Online do Google[9], em uma pesquisa à palavra *trust* obtém-se: *Trust: firm belief in the reliability, truth, ability, or strength of someone or something.*

Atualmente, nossas vidas estão cheias de diferentes tipos de sistemas especialistas. A vida moderna depende da nossa confiança nesses sistemas e essa confiança não decorre do amplo conhecimento desses sistemas; em vez disso, é baseado na experiência de que tais sistemas funcionam como se espera que funcionem. Portanto, a conquista da confiança é essencialmente influenciada pelas expectativas e percepção da segurança da informação que o usuário – agora cliente da Nuvem – tem em relação à segurança da informação dos serviços contratados.

A confiança depende da expectativa, da crença e da disposição em correr riscos. Por expectativa, o cliente espera um comportamento específico do provedor; por exemplo, fornecer informações ou realizar operações cooperativas, com eficácia, para resolver problemas. Por crença, o cliente da Nuvem acredita que o comportamento esperado ocorra, com base nas evidências de competência, integridade e boa vontade do administrador do serviço de Nuvem. Por disposição para

---

[8] Termo Confiança no Dicionário Online de Português: https://www.dicio.com.br/confiancat .

[9] Termo *Trust* no Tradutor Online do Google: https://translate.google.com/?sl=en&tl=pt&text=trust%0A&op=translate:

correr riscos, o usuário da Nuvem sabe que deve mapear e monitorar os riscos que está disposto a correr, em função do contexto e das suas necessidades de segurança da informação.

A confiança do usuário depende da consistência e da confiabilidade. Para desenvolver e fortalecer a confiança do usuário, é fundamental minimizar as interrupções do sistema, fornecer transparência e ser capaz de responder e aprender rapidamente se e quando ocorrerem incidentes. Segurança, conformidade, privacidade e transparência são as bases da confiança na segurança dos serviços de Nuvem que, mediadas pela expectativa e percepção, conquistam os usuários (Huang & Nicol, 2013).

3.2 Segurança e Privacidade na Computação em Nuvem

Segurança e Privacidade são requisitos transversais que atravessam todas as camadas da Nuvem. Essa transversalidade é que impossibilita ao consumidor avaliar quanto das suas necessidades de segurança e privacidade estão sendo atendidas ou não pelos serviços de Nuvem que contratou. Pouco é oferecido a esses consumidores para poderem avaliar e acompanhar a evolução da segurança e privacidade dos serviços que estão utilizando.

As normas técnicas, os *frameworks* disponíveis e os guias de boas práticas têm seu foco no provedor de Nuvem. Ao consumidor final, em especial ao individual e pequenas empresas, avaliar essas questões com as ferramentas disponíveis é uma tarefa demasiada onerosa, quase que impossível; contrariando a premissa de redução de custos.

Nesta seção, são apresentadas definições e conceitos ligados à Segurança da Informação, que foram obtidos de padrões NBR ou ISO/IEC. É consenso que as propriedades essenciais da Segurança da Informação são: a Confidencialidade, a Integridade e a Disponibilidade.

Na Figura 3.1, apresenta-se uma visão particular da inter-relação entre as principais propriedades de segurança da informação; nota-se que foi acrescentada a privacidade como propriedade a ser preservada que vem a influenciar todas demais propriedades.

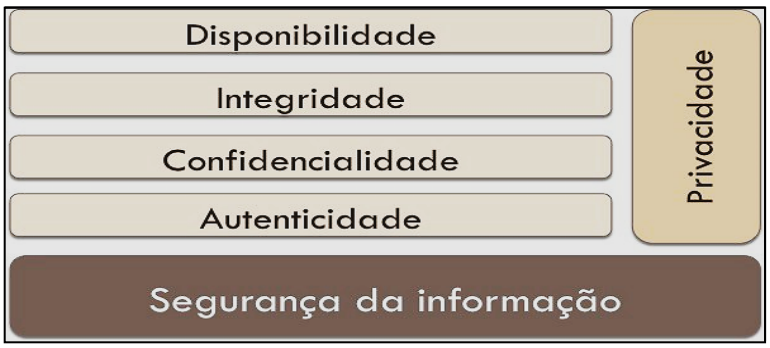


Figura 3.1 – Visão das Propriedades da Segurança da Informação

Outras propriedades também devem ser consideradas quando se avalia os serviços de Nuvem. A seguir são apresentadas definições contidas na Norma ABNT NBR ISO/IEC 27001:2013:

a) Segurança da Informação: preservação das propriedades confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas (Item 3.4 da norma 27001).

b) Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados (Item 3.3 da norma 27001). Sistemas com esta propriedade têm como objetivo limitar o acesso não autorizado a informação ou dados; ela deve permitir que apenas dados e informações sejam revelados apenas àqueles que foram legitimamente autorizados; assim como controlar o tipo de acesso que usuários, processos ou sistemas venham a ter.

c) Integridade: propriedade de salvaguarda da exatidão e completeza de ativos (Item 3.8 da norma 27001). É a propriedade que garante que as informações ou os dados não foram corrompidos ou adulterados, mantendo a sua fidedignidade e correção durante a transferência destes entre os diversos sistemas; ou seja, busca-se a garantia de que os dados não sejam indevidamente alterados. Esta propriedade garante que as características da mensagem original sejam mantidas durante qualquer operação, entre a sua origem e

destino.

d) Disponibilidade: propriedade de a informação estar acessível e utilizável sob demanda por uma entidade autorizada (Item 3.2 da norma 27001). Esta propriedade está relacionada à garantia de que a informação esteja sempre disponível e acessível. Portanto, os usuários autorizados terão acesso às informações de seus interesses sempre que necessário, para uso legítimo, quando requerido.

A seguir são listadas outras propriedades que também devem ser consideradas para uma boa avaliação dos serviços prestados por um provedor de serviços de computação em nuvem.

e) Autenticidade: propriedade que permite garantir que o emissor de determinada informação seja realmente quem alega ser; ou seja, ela garante a identidade, de forma inequívoca, do remetente da informação, assegurando que a mensagem é realmente proveniente da fonte declarada. Esta propriedade não tem definição na ISO/IEC 27001.

f) Irretratabilidade: também conhecida como não-repúdio ou irrefutabilidade. Esta propriedade está relacionada à garantia da impossibilidade de o emissor negar a autoria de determinada mensagem ou transação. Esta propriedade não tem definição na ISO/IEC 27001.

g) Responsabilidade: propriedade que representa que as responsabilidades devem estar definidas, tanto nos sistemas de gestão, quanto dos usuários e demais envolvidos na prestação do serviço de Nuvem. Deve haver evidências do comprometimento dos provedores de serviços de Nuvem com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhorias. Esta propriedade retrata a necessidade de envolvimento da liderança, como exigida nas políticas de Segurança da Informação, onde definem-se as responsabilidades e autoridades (Seção 5 da norma 27001).

h) Confiabilidade*:* probabilidade que representa que um sistema tem que desempenhar suas funções, sob condições especificadas e durante um dado intervalo de tempo, desde que ele esteja funcionando no tempo zero. Portanto, a confiabilidade está relacionada a com que frequência o sistema falha e com os impactos que essas falhas venham a causar. Os serviços e aplicações desenvolvidos para a Nuvem são considerados confiáveis quando mantém os dados intactos ainda que ocorram falhas nesses serviços. A confiabilidade está relacionada à frequência com que o sistema falha e qual o impacto de suas falhas (com perda de dados ou não). As aplicações desenvolvidas para a computação em nuvem devem ser confiáveis, ou seja, elas devem possuir uma arquitetura que permita que os dados permaneçam intactos mesmo quando há falhas. A reputação dos provedores de Nuvem está ligada à sua capacidade de manter os dados seguros utilizando técnicas de backup, criptografia e outros controles. Esta propriedade não tem definição na ISO/IEC 27001.

i) Privacidade: propriedade que representa a busca pela proteção dos dados pessoais, ou quaisquer informações sobre uma pessoa que podem ser usadas para identificá-la; por exemplo, data e local de nascimento, ou registros biométricos. Esta propriedade pode estar incluída dentro da Confidencialidade, porém, num grau muito mais exigente de controle de acesso. A privacidade deve ser assegurada conforme exigido nas legislações aplicáveis, regulamentações e nas cláusulas contratuais (Item A.15.1.4 – Proteção de dados e privacidade da informação pessoal; Controle da ISO/IEC 27701:2019).

3.3 Como o *Framework* Proposto aborda a Segurança da Informação

O *framework* que é proposto neste trabalho (FTACSP – *Framework for Trust Assessment of Cloud Service Providers*) de avaliação deve incorporar incentivos para melhorar a Segurança da Informação dos serviços de computação em nuvem,

deve possuir quesitos que permitam avaliar os domínios de Governança, Transparência e Informações de Segurança. Esses quesitos proporcionariam uma melhor percepção do estado da segurança da informação dos serviços de Nuvem contratados e quais expectativas sobre eles.

Governança, Transparência e Informações de Segurança são conceitos inter-relacionados, que podem proporcionar uma boa visão de como está estruturado um serviço de Nuvem, com base em informações e avaliações de usuários e especialistas na área. Nos próximos capítulos da tese, serão discutidos como entende-se e são aplicados os conceitos de Governança, Transparência e Informações de Segurança para estruturar o *framework* de avaliação proposto.

3.4 Leis, Padrões e Guias sobre Computação em Nuvem

Nesta seção são apresentadas leis brasileiras, normas técnicas e guias que se aplicam aos serviços de computação em nuvem, que consideram aspectos relacionados à segurança da informação.

3.4.1 Legislação Brasileira que Afeta a Computação em Nuvem

A seguir é listada a legislação brasileira que versa sobre temas que afetam a computação em nuvem. Todas as leis citadas são regulamentadas por decretos e instruções normativas que não são detalhados nesta tese, pois esse arcabouço legal está em constante mudança e atualização. Abaixo, são listadas as leis mais importantes no contexto deste trabalho:

a) A Lei n. 12.527/2011[10], também conhecida como “Lei de Acesso a Informação (LAI)” regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do parágrafo 3º do art. 37 e no parágrafo 2º do art. 216 da Constituição Federal do Brasil; altera a Lei n. 8112, de 11 de dezembro de 1990; revoga a Lei n. 11.111 de 5 de maio de 2005, e dispositivos da Lei n. 8159 de 8 de janeiro de 1991; e dá

[10] Lei n. 12.527, de 18 de novembro de 2011 - https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

outras providências.

b) A Lei n. 12.737/2012[11], também conhecida como “Lei Carolina Dieckmann”, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848 de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

c) A Lei n. 12.965/2014[12] também conhecida como “Marco Civil da Internet”, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

d) A Lei n. 13.460/2017[13] dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

e) A Lei n. 13.709/2018[14], também conhecida como “Lei Geral de Proteção de Dados Pessoais (LGPD)”, com redação dada pela Lei n. 13.853/2019[15], dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet (Lei n. 12.965). A LGPD aborda o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Todas essas leis cuidam de disciplinar o tratamento de dados que precisam ser protegidos e outros que precisam ser divulgados, trazendo contradições que dificultam o atendimento aos imperativos legais. Cabe observar que empresas que prestam serviços de Nuvem para entidades governamentais devem prever regras específicas e estar em conformidade com as leis acima listadas.

---

[11] Lei n. 12.737, de 30 de novembro de 2012 - https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

[12] Lei n. 12.965, de 23 de abril de 2014 - http://www.planalto.gov.br/CCivil_03/_Ato2011-2014/2014/Lei/L12965.htm.

[13] Lei n. 13.460, de 26 de junho de 2017 - https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm.

[14] Lei n. 13.709, de 14 de agosto de 2018 - https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[15] Lei n. 13.853, de 08 de julho de 2019 - https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

3.4.2 Normas Técnicas Aplicáveis à Computação em Nuvem

Esta seção tem o objetivo de apresentar de maneira sintética as instituições padronizadoras e suas normas técnicas publicadas aplicáveis à computação em nuvem.

A ABNT[16], que é o órgão responsável no Brasil pela normatização técnica, é uma entidade privada, sem fins lucrativos, de utilidade pública, que aprova normas em diversas áreas de interesse técnico e econômico.

O ITU-T[17] é uma organização global que atua no domínio da tecnologia da informação, normatizando, regulamentando e publicando orientações.

A ISO[18] é a maior organização internacional não governamental, independente, que congrega 167 organismos nacionais de normalização. Só pode haver apenas um membro por país; no Brasil é a ABNT, que é membro fundador da ISO. Cada membro representa a ISO em seu país.

A IEC[19] é uma organização global sem fins lucrativos que reúne 170 países e é a organização líder mundial para a preparação e publicação de padrões internacionais para as tecnologias elétricas, eletrônicas e relacionadas. Cada país pode ter apenas um comitê como membro do IEC. No Brasil é o COBEI[20] uma associação civil de direito privado, sem fins lucrativos, que representa as necessidades nacionais de padronização e avaliação de conformidade, no âmbito global da IEC. As Normas ISO/IEC buscam um consenso global sobre soluções para problemas específicos, fornecendo diretrizes que podem ser usadas para garantir que produtos e serviços sejam seguros e adequados ao seu objetivo.

No Apêndice I, são listadas as normas de ABNT e ITU-T sobre computação em nuvem. Na Tabela 1, são apresentadas as 13 normas da ABNT que versam sobre temas que afetam a segurança da informação na computação em nuvem. Na Tabela 2, são apresentadas 5 normas da ABNT que versam sobre temas que afetam a

---

[16] Associação Brasileira de Normas Técnicas (ABNT) - http://www.abnt.org.br/institucional/sobre

[17] ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*) - https://www.itu.int/rec/T-REC-Y/en

[18] *International Organization for Standardization* (ISO) - https://www.iso.org/about-us.html

[19] International Electrotechnical Commission (IEC) - https://www.iec.ch/about-us

[20] Comitê Brasileiro de Eletricidade, Eletrônica, Iluminação e Telecomunicações (COBEI) - http://cobei.org.br/quem-somos/

privacidade na computação em nuvem. Praticamente todas as normas ABNT são traduções das normas publicadas pela ISO/IEC. Na Tabela 3 são apresentadas 36 normas da série Y.3500 da ITU-T sobre o domínio Nuvem. O guia Y.Sup49[21] apresenta o roteiro de cada norma listada, com o objetivo de apoiar o entendimento do uso das normas.

3.4.3 NIST SP-800-144

O NIST[22] é uma instituição de padronização americana. Na publicação NIST SP- 800-144[23], são apresentadas diversas questões e recomendações de segurança e privacidade, em especial sobre Confiança, contendo as seguintes observações e recomendações:

a) Garantir que os acordos de serviço tenham meios suficientes para permitir a visibilidade dos controles e processos de segurança e privacidade empregados pelo provedor de nuvem e seu desempenho ao longo do tempo;

b) Estabelecer direitos de propriedade claros e exclusivos sobre os dados;

c) Instituir um programa de gerenciamento de risco que seja flexível o suficiente para se adaptar ao cenário de risco em constante evolução e mudança para o ciclo de vida do sistema;

d) Monitorar continuamente o estado de segurança do sistema de informação para apoiar as decisões de gerenciamento de risco em andamento.

3.4.4 Guias CSA

A CSA[24] é uma entidade focada nos provedores de computação em nuvem

[21] Y.Sup49: ITU-T Y.3500-series - Cloud computing standardization roadmap - https://www.itu.int/rec/TREC-Y.Sup49-201811-I/en
[22] National Institute of Standards and Technology (NIST) - https://www.nist.gov/about-nist.
[23] Special Publication 800-144 - *Guidelines on Security and Privacy in Public Cloud Computing* - https://csrc.nist.gov/publications/detail/sp/800-144/final
[24] Cloud Security Alliance (CSA) - https://cloudsecurityalliance.org

(CSPs), que fornece aos CSPs uma estrutura para a garantia e conformidade de segurança e privacidade na Nuvem. Ela é a organização líder mundial, sem fins lucrativos, dedicada a definir e aumentar a conscientização sobre as melhores práticas para ajudar a garantir um ambiente de computação em nuvem seguro. A CSA também se dedica a fornecer educação e certificação sobre os usos da computação em nuvem para ajudar a proteger todas as outras formas de computação. Tanto os provedores de serviços de computação em nuvem (CSP) quanto seus usuários (CSU) podem se associar à CSA.

A CSA fornece ferramentas e orientações que ajudam setores industriais e países a construir seu próprio ecossistema de garantia de Nuvem, motivando uma postura de segurança e conformidade das organizações por meio de normas. Dividido em 11 domínios relacionados à computação em nuvem, o CSA *Security Guidance*[25] apresenta um conjunto de melhores práticas propostas por uma comunidade internacional de especialista em segurança e privacidade da informação. Dentre as ferramentas disponíveis destacam-se o CCM [26] e o CAIQ[27], a saber:

a) CCM é um conjunto de controles de segurança cibernética para computação em nuvem. É uma planilha que lista 16 domínios cobrindo os principais aspectos da tecnologia de Nuvem. Os domínios estão divididos em 133 objetivos de controle. CCM pode ser usado como uma ferramenta para avaliar sistematicamente a implementação da Nuvem, fornecendo orientação sobre quais controles de segurança devem ser implementados por qual ator na cadeia de suprimentos da Nuvem. A estrutura de controles está alinhada ao CSA *Security Guidance* e atualmente é considerada um padrão de fato para garantia e conformidade de segurança na Nuvem.

b) CAIQ é uma planilha com perguntas “sim” ou "não” que correspondem aos controles de CCM. Um CSP pode usar o CAIQ para documentar quais controles de segurança existem em seus serviços. Isso aumenta a transparência do controle de segurança para os clientes,

[25] The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 - https://cloudsecurityalliance.org/research/guidance/
[26] Cloud Controls Matrix (CCM) Versão 4 - https://cloudsecurityalliance.org/research/cloud-controlsmatrix/
[27] Consensus Assessment Initiative Questionnaire (CAIQ) - https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/

que podem determinar se os serviços providos pelo CSP são seguros o suficiente para suas necessidades.

O programa STAR[28] da CSA é considerado um dos programas mais influentes para garantia de segurança na Nuvem. O programa STAR possui um registro[29] de acesso público que documenta os controles de segurança e privacidade fornecidos por CSPs. Neste registro é possível conhecer os provedores que se qualificaram para o status *Trusted Cloud Provider*. O programa STAR adota os princípios-chave de transparência, auditoria rigorosa e harmonização de padrões descritos em CCM. A publicação no registro permite que as organizações mostrem aos clientes atuais e potenciais, sob a perspectiva dos CSPs, sua postura de segurança e conformidade, incluindo os regulamentos, padrões e estruturas aos quais estão aderentes.

Com relação a certificações profissionais, a CSA provê as certificações CCSK[30] e CCAK[31], que são reconhecidas como o padrão de especialização de como proteger dados na Nuvem, oferecendo uma compreensão coesa e neutra do CSP.

Um grupo de trabalho (CTP-CSA[32]) foi estabelecido pela CSA para atuar na definição do *Cloud Trust Protocol* (CTP). O objetivo do CTP é melhorar a confiança na Nuvem por meio de transparência e garantia. A última versão do protocolo CTP foi lançada em outubro de 2015. O CTP foi concebido para ser um mecanismo pelo qual os clientes de serviços em Nuvem podem solicitar e receber informações relacionadas à segurança dos serviços que utilizam na Nuvem, promovendo transparência e confiança. Uma Nuvem confiável pode ser definida como um serviço de Nuvem onde o CSP implementa padrões de governança, gerenciamento e segurança, ao mesmo tempo em que atende a um conjunto mínimo de requisitos destinados a aumentar a confiança dos usuários da Nuvem.

3.4.5 Outras Iniciativas de Apoio aos Usuários de Serviços de Nuvem

A confiança na computação em nuvem também pode ser aumentada por

[28] Security, Trust, Assurance and Risk (STAR) - https://cloudsecurityalliance.org/star/
[29] STAR (Registro) - https://cloudsecurityalliance.org/star/registry/
[30] Certificate of Cloud Security Knowledge – CCSK - https://cloudsecurityalliance.org/education/ccsk
[31] Certificate of Cloud Auditing Knowledge CCAK - https://cloudsecurityalliance.org/education/ccak
[32] CTP-CSA - https://cloudsecurityalliance.org/research/working-groups

meio da educação dos usuários. A educação ou treinamento dos usuários aumenta a confiança nos serviços de Nuvem. Pode-se citar como exemplo os ataques aos computadores pessoais; onde a educação dos usuários e o uso de tecnologias anti-invasão têm contribuído para a defesa desses computadores. Os usuários precisam entender as práticas de segurança e privacidade da Nuvem e as medidas que devem ser tomadas para proteger seus dados e recursos, já afirmavam Dhillon & Torkzadeh (2006). Portanto, faz sentido não subestimar os riscos e investir mais em educação e financiamento da segurança da informação.

Desde 2009 a empresa (Sun Microsystems, 2009) já expunha a preocupação em justificar a transferência do controle de seus dados para um provedor de nuvem com base exclusivamente em economia de custos e maior agilidade. Na ocasião, ainda não tinham sido publicadas as normas que viriam a nortear as ações sobre os serviços de Nuvem, por exemplo ISO/IEC 27018 e ISO/IEC 27019. Os provedores de Nuvem podem construir a confiança do cliente alavancando os padrões de segurança da informação e seguindo um conjunto de “Princípios de Segurança Transparentes”. Os clientes ou usuários, por sua vez, devem desenvolver um perfil de risco adequado às suas necessidades e buscar fazer escolhas mais bem informados.

Cloud Access Security Brokers (CASBs)[33] são sistemas ou aplicativos hospedados na Nuvem, ou mesmo localmente, que ficam entre os clientes dos serviços de Nuvem e os provedores desses serviços. A função principal de um CASB é impor políticas de segurança, conformidade e governança para aplicativos em Nuvem. Eles ajudam as organizações a ampliarem os controles de segurança de sua infraestrutura local para a Nuvem.

Grandes provedores publicam material sobre segurança voltado a apoiar usuários de seus serviços, tais como Google (Google Cloud)[34], Microsoft (Azure)[35], Amazon (Amazon Web Services – AWS)[36].

[33] CASB - https://www.infomach.com.br/casb-o-que-e
[34] Google Cloud - https://cloud.google.com/security?hl=pt-br
[35] Microsoft Azure - emos o site https://azure.microsoft.com/en-us/solutions/network-security
[36] Amazon Web Services - https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-andcompliance.html.

3.5 Considerações Finais

Neste capítulo, apresentou-se o conceito “Confiança” utilizado no domínio da tecnologia da informação. Na computação em nuvem, a segurança e privacidade da informação devem ser atendidas em todas as camadas da Nuvem. Também foram apresentadas leis, guias e normas técnicas aplicáveis ao uso da computação em nuvem. Conclui-se que a educação do usuário, ou cliente, deve passar por treinamentos de uso dos recursos, pois as responsabilidades passaram a ser distribuídas entre os atores que atuam na Nuvem.

4 REVISÃO DE LITERATURA E TRABALHOS RELACIONADOS

Neste capítulo, apresenta-se uma síntese da revisão de literatura sobre modelos de confiança em computação em nuvem. Em Balcão Filho et al. (2019) (mapeamento da literatura) e em Balcão Filho et al. (2020), são apresentados os conceitos e trabalhos mais importantes usados na formulação do *framework* conceitual proposto. A revisão de literatura, cujo resultado está contido nos artigos publicados, foi atualizada para incluir outras referências relacionadas ao referencial teórico e conceitual, complementando assim o referencial bibliográfico da tese.

Com respeito à metodologia usada na revisão, foram seguidas as diretrizes para mapeamento sistemático propostas por (Kitchenham, 2004) e (Biolchini et al., 2005). As palavras-chave escolhidas foram: confiança, computação em nuvem, segurança da informação e privacidade; e *strings* de busca foram formuladas para coletar artigos relevantes de bancos de dados científicos bem conhecidos (IEEE Xplore, ACM Digital Library e SpringerLink). A busca foi limitada aos títulos, no idioma inglês, no período 2015 a 2023. A seleção dos artigos foi baseada em sua relevância, de acordo com seus resumos e conclusões. Foi utilizada uma *string* de busca, cuja sintaxe foi adaptada a cada base de conhecimento: *“trust OR confidence” AND “cloud computing” AND “security information OR privacy”.*

A partir das bases de busca foram selecionados 54 artigos. Após análise de seus títulos, palavra-chave, resumo e conclusões, 32 artigos foram considerados adequados para leitura e 25 têm seus resumos apresentados a seguir.

Na revisão de literatura, foram encontrados estudos com foco em aspectos de confiança e transparência de segurança, que consideram essas questões do ponto de vista do consumidor. Poucos artigos tratam da comunicação do consumidor com o CSP, tais como dar visibilidade às práticas de segurança da informação e como possibilitar que o consumidor compreenda essas práticas. Além disso, eles não discutem como fornecer informações significativas e relevantes para investidores em Nuvem, provedores de serviços em nuvem ou tomadores de decisão.

Depreende-se da revisão que falta uma abordagem unificada para lidar com os seguintes problemas:

a) Acesso à informação relativa à segurança dos sistemas em Nuvem;

b) Modelos e métricas para medir a confiança na Nuvem;

c) Disponibilidade de informações sobre gestão, recursos e aspectos de infraestrutura;

d) Disponibilidade de informações sobre incidentes de segurança;

e) Dificuldade, do ponto de vista dos consumidores, em identificar formas objetivas de comunicação com os fornecedores.

Nos estudos apresentados nesta tese, sobre questões de segurança da informação, vários temas foram analisados para desenvolver um entendimento abrangente de “confiança em serviços de computação em nuvem”. Esses temas incluem privacidade, métricas de segurança cibernética, representação do conhecimento por meio de taxonomias ou ontologias e elementos fundamentais de confiança, como auditoria, recomendação e reputação.

A revisão da literatura de modelos de confiança em computação em nuvem fornece uma base para avaliação de confiança de serviços de Nuvem. Artigos que serviram de base teórica e metodológica para o modelo de confiança proposto são apresentados neste capítulo. A Seção 4.1 apresenta uma síntese dos trabalhos que abordam confiança em CSPs e a Seção 4.2 apresenta uma síntese dos trabalhos relacionados, ou seja, trabalhos que propõem modelos de confiança em computação em nuvem ou abordagens similares à proposta nesta tese.

4.1 Síntese dos Trabalhos que Abordam Confiança em CSPs

Estudos sobre métricas de segurança mostram a importância de tratar metodologicamente os problemas de medição de segurança, bem como de atender às expectativas, tais como repetibilidade, reprodutibilidade, relevância, pontualidade e custos. (Littlewood et al., 1993) identificam a conveniência de uma estrutura baseada em probabilidade para medição de segurança da informação. Jansen (2009) apresenta uma visão geral da área de métricas de segurança, no qual analisa os possíveis caminhos de pesquisa que podem ser tomados por pesquisadores de métricas de segurança. Bayuk (2011) recomenda o uso de métricas de segurança para medir a capacidade da Nuvem de resistir a ataques cibernéticos, em seu estudo sobre a literatura das métricas aplicadas a problemas de segurança em Nuvem.

Bayuk & Mostashari (2013) analisam as métricas de segurança do ponto de vista técnico e histórico e elaboram um quadro teórico para a validação da segurança e do sistema visando apoiar que se deparam com questões de segurança no contexto do comércio.

A literatura também enfatiza a importância dos aspectos sociotécnicos para a confiança. Os modelos de classificação e monitoramento visam assegurar e melhorar a confiança nos CSPs. Whaiduzzaman & Gani (2013) propõem uma agência de notação de risco (*Trusted Third Party* – TTP) para classificação de títulos. Neste estudo, um *script* de software é executado em um servidor CSP para identificar possíveis vulnerabilidades de segurança e avaliar sua resiliência, sendo considerados parâmetros não mensuráveis. Como resultado, o sistema fornece um ranking de confiança no CSP.

Uma revisão da literatura de medição de segurança é apresentada em (Barabanov et al.,2011). Segundo os autores, uma abordagem de pesquisa interdisciplinar não é comum nem fácil e os profissionais de segurança da informação muitas vezes se deparam com questões sociotécnicas que não podem ser respondidas abordando apenas metade do problema.

Taxonomias, ontologias e outros mecanismos de representação do conhecimento têm sido utilizados na formalização conceitual de modelos de confiança para computação em nuvem. A padronização e a interoperabilidade são críticas para que os modelos de confiança estabeleçam e avaliem efetivamente a confiança entre consumidores e CSPs (Kanwal et al., 2015). Chrysikos & Mcguire (2018), propõem uma taxonomia de fatores de risco em ambientes de computação em nuvem, que visa combinar e classificar fontes de informação para avaliação de confiança; essas fontes coletam dados (relacionados a padrões de ataque) de sistemas de avaliação de risco e confiança que operam em CSPs. Uma taxonomia de fatores de confiança e uma estrutura de confiança multifacetada sensível ao contexto (CAMTF) são propostas em (Alhanahnah et al., 2017).

Alhanahnah, Bertok, Tari, & Alouneh (2018) buscam apoiar a seleção de prestadores de serviços, por meio da aplicação de um conjunto de métodos matemáticos que se baseiam em fatores de confiança, características do serviço e confiança do usuário. Os CSPs têm que lidar com cenários onde vários serviços de Nuvem interagem entre si, porém poucas abordagens são capazes de lidar com

segurança, privacidade e confiança em ambientes inter-nuvem. Uma ontologia de segurança baseada em padrão para inter-nuvem (SOFIC) é proposta em (Bernabe et al., 2015) visando formalizar características de segurança que podem ser modeladas na avaliação de segurança de ambientes inter-nuvem. SOFIC é usada como entrada em um sistema para apoiar o processo de tomada de decisão de segurança no contexto da inter-nuvem.

Os trabalhos analisados mostram que a privacidade é outro requisito crítico no processo de construção da confiança. Empresas e usuários finais costumam usar serviços na Nuvem porque oferecem vantagens econômicas, produtivas e inovadoras. No entanto, logo os usuários percebem as fragilidades dos serviços quanto ao desempenho, confiabilidade, privacidade, segurança (Pearson, 2013); (Ruiz et al., 2020). Uma boa comunicação das medidas de segurança e privacidade de dados pode aumentar a confiança dos usuários (Becker et al., 2014).

A literatura também mostra que questões críticas ainda precisam ser abordadas, como mecanismos de avaliação de confiança, *feedback* duvidosos, má identificação e integração de *feedbacks* e privacidade dos participantes (Noor, Sheng, Ngu, et al., 2013). A superfície de segurança da informação é a primeira preocupação na avaliação de serviços de nuvem, mas não é suficiente. Outros aspectos, como transparência, desempenho, privacidade e comunicação, têm peso relevante na avaliação de confiança nos CSPs (Eftekhar et al., 2018).

A falta de transparência e outros problemas de gestão são desafios remanescentes que não são contemplados nos estudos analisados, assim como as soluções de segurança e privacidade existentes não enfrentam esses problemas. Direções de pesquisa para enfrentar esses desafios na pesquisa de segurança e privacidade da computação em nuvem são propostas por Liu et al. (2015).

Junejo et al. (2022) apresentaram um *framework* de computação confiável multidimensional e multifatorial para serviços de nuvem. Os autores calculam a confiança agregando evidências multidimensionais de Qualidade de Serviço (QoS) e Qualidade de Experiência (QoE). Neste trabalho, o desempenho de um CSP é medido pelo tempo médio de resposta e pela taxa de sucesso da tarefa. A credibilidade do feedback é avaliada para prevenir o comportamento malicioso dos usuários da nuvem.

Modelos de confiança para gerenciamento de identidade baseado em

blockchain são apresentados por (Lim et al., 2022). Este artigo fornece a primeira revisão de literatura que aborda a gestão de identidade baseada em *blockchain*. Segundos os autores, o modelo de confiança proposto é formal e abrangente. O trabalho também apresenta lacunas de pesquisa e sugestões para trabalhos futuros na área.

Mehraj & Banday (2022) apresentam uma técnica de média ponderada dinâmica para avaliação de confiança na computação em nuvem. Segundo os autores, a preocupação crítica na avaliação de confiança é a atribuição ideal de pesos a diferentes fatores envolvidos na avaliação. O artigo propõe um método de média ponderada para o paradigma de computação em nuvem em que vários fatores recebem pesos dinamicamente.

Em (Mehraj & Banday, 2022a) propõe-se um sistema de gerenciamento de confiança de mão dupla para computação de nevoeiro (*Fog Computing*). A computação de nevoeiro é a próxima fronteira da computação em nuvem, pois pode calcular e armazenar uma quantidade enorme de dados gerados por dispositivos IoT perto de suas fontes. Foi proposto um sistema de gerenciamento de confiança baseado em lógica bidirecional que permite um solicitante de serviço para verificar se um provedor de Nuvem pode oferecer serviços confiáveis e seguros, bem como permitir que o provedor verifique a confiabilidade do solicitante do serviço.

Gupta et al. (2020) argumentam que os usuários precisam se inscrever nos vários serviços prestados por esses provedores de Nuvem para armazenar ou acessar as informações. Neste artigo, são exploradas as várias possibilidades que poderiam violar a confiança entre o provedor de serviços de nuvem e o usuário. Segundo os autores, o usuário deve confiar em seu provedor de serviços somente se o mesmo garantir várias medidas necessárias para construir a confiança; ou seja, desde a criação de informações até a sua destruição, uma rastreabilidade completa dos dados deve ser provida.

Em (Gupta & Saini, 2021) apresenta-se uma abordagem baseada em inteligência artificial para gerenciar o risco de sistemas de TI na adoção de Nuvem. Os autores propõem um *framework* para gerenciar riscos na adoção da Nuvem baseado na terceirização de dados e processos para uma agência que fará a seleção de provedores de serviços de nuvem adequado às necessidades do usuário; com uma declaração contratual clara quantos aos riscos.

Em (Hasan et al., 2023) são discutidos os desafios à segurança de dados e integridade associados à computação em nuvem. O objetivo é discutir as ameaças e soluções associadas aos problemas de segurança de dados e integridade dos dados com os quais os usuários da computação em nuvem devem lidar. Neste trabalho políticas de segurança são projetadas para garantir a conformidade regulatória, protegendo as informações, aplicativos e infraestrutura associados à Nuvem. Segundo os autores, é fundamental que se forneça segurança de dados através de políticas de segurança abrangentes e uma cultura organizacional consciente da segurança.

Em (Roy & Patil, 2023) apresentam uma pesquisa que reconhece como a segurança da Nuvem é a maior prioridade das pequenas e médias empresa (PMEs). Os desafios existentes na adoção da Nuvem são identificados usando os fatores do *framework* da tecnologia-organização-ambiente (TOE). Os autores também propõem um *framework* que deve ser usado pelas PMEs para avaliar a prontidão da segurança das informações durante a migração para a Nuvem.

4.2 Trabalhos Relacionados

Nesta seção, são descritos e comparados métodos e contribuições de artigos considerados semelhantes (Trabalhos Relacionados) a esta tese. Esses estudos foram selecionados porque propõem *frameworks*, modelos e sistemas para fornecer e avaliar serviços de Nuvem confiáveis.

O *framework* proposto por Rizvi, Ryoo, Kissell, & Aiken (2015) visa a ajudar os Usuários de Serviços de Nuvem (CSUs) a escolherem CSPs confiáveis da seguinte forma:

a) Permitindo que as CSUs forneçam suas preferências de segurança;

b) Fornecendo um mecanismo para validar os controles e políticas de segurança dos CSPs publicados no *Security Trust and Assurance Registry* do banco de dados *Cloud Security Alliance* (STAR-CSA);

c) Mantendo um banco de dados de CSPs juntamente com suas respostas ao Questionário de Iniciativa de Avaliações de Consenso da *Cloud Security Alliance* (CAIQ- CSA).

Rizvi, Karpinski, Kelly, & Walker (2015) incorporam uma auditoria de terceira parte (TPA) ao *framework* para realizar a análise do *Consensus Assessments Initiative Questionnaire* (CAIQ) e para informar os usuários.

Modelos de acordos de gestão de auditoria mútua são cruciais para construir confiança, de modo que uma relação formal possa ser estabelecida entre CSPs e usuários com responsabilidades legais relevantes. Branco e Santos (2015) propõem um modelo de confiança para ambientes de computação em nuvem, que leva em consideração questões legais. A adoção de tecnologias adequadas é outro aspecto fundamental para estabelecer e controlar os requisitos contratuais adequados. Nesse modelo, os próprios provedores de serviços em nuvem e os próprios consumidores devem ter métricas e controles para dar suporte ao gerenciamento de uso da Nuvem.

Um *framework* de gerenciamento de confiança baseada em reputação (CloudArmor), usado para fornecer *Trust as a Service* (TaaS), é apresentado em (Noor, Sheng, Ngu, et al., 2013) e em (Noor, Sheng, Yao, et al., 2016). CloudArmor inclui uma proposta de modelo conceitual que busca medir a credibilidade do *feedback* dos usuários. O objetivo é proteger os serviços em Nuvem de usuários mal-intencionados.

Singh & Sidhu (2017) elaboram um sistema de avaliação de confiabilidade baseado em conformidade com a normatização. Técnicas matemáticas são usadas para fornecer os resultados da avaliação de confiabilidade do ponto de vista dos *stakeholders* (por exemplo, colegas, auditores de Nuvem, corretores de Nuvem). O sistema proposto considera o ponto de vista dos consumidores; no entanto, é limitado por considerar apenas o desempenho e a confiabilidade de acordo com os aspectos do Contrato de Nível de Serviço (SLA) dos serviços em Nuvem; ou seja, questões de segurança e privacidade da informação não são consideradas na avaliação.

Um sistema de rótulo de confiança projetado para comunicar confiança e confiabilidade em serviços de Nuvem é apresentado em (Emeakaroha et al., 2017). Segundo os autores, em um contexto de Nuvem, a incerteza é agravada quando o consumidor percebe a falta de transparência em relação às condições e à qualidade do serviço oferecido pelos CSPs. O sistema proposto permite que os CSPs comuniquem informações selecionadas e atualizadas aos seus clientes. Essas informações ajudam os consumidores a construir sua própria percepção de confiança.

Um modelo de confiança baseado em Nuvem do acordo de nível de confiança é apresentado por Xu (2018) que propõe um modelo hierárquico de modelagem de confiança, que visa a melhorar a percepção da situação de segurança em ambientes de Nuvem. Segundo o autor, os usuários da computação em Nuvem podem tomar boas decisões, pois o método proposto pode reduzir a complexidade de calcular e gerenciar a confiança do serviço.

Lins, Schneider & Sunyaev (2018), propõem uma arquitetura conceitual para auditoria contínua, que destaca componentes e processos importantes que precisam ser implementados. Os autores argumentam que auditorias contínuas são necessárias para garantir que os serviços de Nuvem permaneçam seguros. Como os serviços de Nuvem estão em constante mudança, é necessária uma auditoria contínua dos critérios selecionados para aumentar a confiança nas certificações dos CSPs.

Maher (2018) apresenta um modelo de alto nível que ajuda a alcançar o nível de confiança necessário para uma implantação robusta de Internet das Coisas (IoT). Sugere-se um conjunto de soluções de gerenciamento de confiança que podem oferecer suporte a requisitos de segurança, proteção e privacidade. A solução proposta é centrada no ser humano e sugere o uso de *blockchain* como um oráculo universal confiável.

Com o surgimento da IoT, a computação em nuvem foi combinada com a computação em névoa para diminuir sua latência. Sujana & Revathi (2019) elaboram um modelo de confiança que busca atender aos desafios da IoT, com foco na segurança e no escalonamento de tarefas. Com base no SLA negociado com o CSP, este modelo de confiança visa a garantir que as solicitações dos usuários sejam atendidas com um nível de segurança suficiente. Seu modelo de confiança também considera a relação direta entre confiança e reputação.

Balcão Filho et al. (2020) propuseram um *framework* conceitual centrado no consumidor para avaliação de confiança de ambientes de computação em nuvem. Métricas e indicadores foram propostos para permitir que os consumidores avaliem os CSPs, dentro de três domínios: Governança (GV), Transparência (TP) e Informação sobre Segurança (SI).

Balcão Filho et al. (2023) propuseram um *framework* cuja abordagem é

centrada na avaliação do consumidor dos serviços de Nuvem. Foram utilizados Indicadores para comunicar os resultados com o objetivo de representar a expressão da segurança cibernética, gerenciabilidade e transparência dos serviços sob avaliação. Uma Prova de Conceito (PoC) foi realizada para verificar em três situações do mundo real, a aplicabilidade, sensibilidade e robustez do modelo e do *framework* propostos. O *framework* representa o conjunto dos resultados apresentados nesta tese de doutorado.

A Tabela 4.1 resume e compara métodos e contribuições semelhantes às apresentadas nesta tese. O *framework* FTACSP proposto é mais amplo do que outros, abrangendo as dimensões de Governança, Transparência e Informação sobre Segurança. Os resultados são expressos numérica e graficamente, visando melhorar a comunicação de forma relevante e significativa. Este trabalho também apresenta uma Prova de Conceito e um Protótipo de Software, que dá suporte a especialistas e não especialistas em segurança da informação no uso do *framework* e ajuda a avaliar e formar uma opinião para a escolha de CSPs confiáveis.

O Desempenho é considerado por sete entre os onze estudos analisados. Em seguida estão o Projeto de Segurança, Certificações e Simulação (cinco estudos). Recomendações, Consciência do Contexto e Transparência estão em três. Dois estudos consideram a Reputação. Apenas um aponta os Recursos Envolvidos. A Divulgação das Informações também só é apontada por um estudo, nesse caso, em um trabalho que contou com participação do autor desta tese (Balcão Filho et al., 2020).

Para a elaboração do *framework* proposta nesta pesquisa, as treze características apontadas no estudo, serão consideradas. São elas: desempenho, reputação, projeto de segurança, recomendações, consciência do contexto, garantias contratuais, certificações, recursos envolvidos, transparência, divulgação de informações, protótipo, simulação e estudo de caso.

4.3 Considerações Finais

A revisão da literatura científica e a análise dos trabalhos relacionados mostrou que a preocupação com a necessidade de modelos de confiança nos serviços de computação em nuvem já era apontada em trabalhos anteriores. O modelo

proposto mostra-se mais amplo que os demais, pois além de ser centrado na avaliação que o usuário faz dos serviços que usa, o modelo permite usar de forma mais simples indicadores de confiança que levam em consideração o histórico e o contexto atual.

Tabela 4.1 - Síntese dos Trabalhos Relacionados

Característica / Referência	(Rizvi, Ryoo, et al., 2015)	(Rizvi, Karpinski, et al., 2015)	(T. T. Branco & Santos, 2015)	(Noor, Sheng, Maamar, Zeadally, 2016)	(Singh, Sidhu, 2017)	(Emeakaroha et al., 2017)	(Xu Wu, 2018)	(Lins, Schneider, Sunyaev, 2018)	(Maher, 2018)	(Sujana J. et al., 2019)	(Balcão-Filho et al., 2020)	**Esta Tese**
Desempenho			X	X	X	X	X		X	X		X
Reputação				X						X		X
Projeto de Segurança	X	X	X					X	X			X
Recomendações							X	X		X	X	X
Consciência do Contexto	X				X	X			X			X
Garantias Contratuais			X					X				X
Certificações	X	X						X			X	X
Recursos Envolvidos									X			X
Transparência	X	X			X			X			X	X
Divulgação de Informações											X	X
Protótipo				X		X						X
Simulação	X			X	X	X					X	X
Estudo de Caso												X
Domínio	GV	GV, TP	SI	GV	GV	GV, TP	GV	GV, TP	GV, SI	GV	GV, TP, SI	GV, TP, SI
Tipo de Contribuição	Fr	Fr	Me, Mo	Fr	Fr	Me, Fr	Me	Mo	Mo	Mo	Fr	Mo, Fr
Resultados	NuU, Gr			Nu	Nu, Gr	Nu					Nu	Nu, Gr

1) Tipo de Contribuição: Fr - *Framework*, Mo - Modelo, Me - Métrica.
2) Domínio: GV - Governança, SI - Informações sobre Segurança, TP -Transparência
3) Resultado: Nu - Numérico, Gr - Gráfico.

5 *FRAMEWORK* PARA AVALIAÇÃO DE CONFIANÇA DE PROVEDORES DE SERVIÇOS DE NUVEM (FTACSP)

Neste capítulo, descreve-se o FTACSP (*Framework for Trust Assessment of Cloud Service Providers*), que é centrado no consumidor e aborda aspectos de confiança da perspectiva do consumidor de serviços de nuvem (ou usuário final).

Inicialmente, colocamos questões motivadoras:

a) como os usuários ou consumidores de serviços de nuvem criam confiança nesses serviços?

b) quais são as fontes de confiança?

c) como a segurança afeta a construção da confiança?

d) qual é a relevância da privacidade para construir confiança?

Em relação à Questão (a), os consumidores criam confiança nos serviços de computação em nuvem com base em: competência do CSP; garantias dadas por meio de contratos; força de leis, normas e regulamentos e opinião de terceiros (como auditorias, recomendações de especialistas e avaliações de outros usuários) como exposto no Capítulo 3.

Os serviços de nuvem são dinâmicos, havendo a necessidade de monitoramento contínuo de parâmetros que certifiquem sua qualidade e segurança para lidar com esse dinamismo (Nicol et al., 2010).

Para responder à Questão (b), apresentamos como importantes fontes de confiança, a saber: informações fornecidas pelos prestadores de serviços, notificações obrigatórias impostas por leis e regulamentos, avaliações fornecidas pelo usuário, ferramentas de monitoramento contínuo, auditorias ou laudos periciais, cláusulas de contrato de serviço e certificações formais e credenciamento (Ardagna et al., 2015) (Branco & Santos, 2016).

A Questão (c) é diretamente influenciada pela segurança dos serviços de Nuvem. A falta de detalhes sobre Segurança da Informação tem um impacto negativo na adoção de serviços de computação em nuvem (Rizvi, Ryoo, et al., 2015) (Shaikh & Sasikumar, 2015).

A privacidade, Questão (d), é outra preocupação emergente, especialmente por ser relacionada a dados pessoais, e tem uma influência significativa na escolha dos usuários em utilizar serviços de Nuvem (Asadullah et al., 2015). Privacidade e confiança são conceitos intimamente ligados, conforme Martin (2017).

Para auxiliar os tomadores de decisão na escolha de seus provedores de Nuvem com base em uma medida de confiança, consideramos que um protocolo de decisão eficiente contém os seguintes requisitos (Saaty & Ergu, 2015):

a) um bom entendimento do problema para minimizar dúvidas e incertezas;
b) um *framework* completo para representar todos os fatores envolvendo critérios e alternativas;
c) uma escala numérica para representar julgamentos;
d) uma classificação de prioridade derivada de julgamentos numéricos.

A seguir detalhamos em seis subseções como os requisitos apontados na lista acima, compõem o *framework* proposto. Na Subseção Conceptualização (5.1) é apresentada a formalização do *framework*; em Processo de Desenvolvimento (5.2) a proposta é desenvolvida; em Critérios de Avaliação (5.3) os princípios de avaliação são apresentados; em Arquitetura do Framework (5.4) é apresentada sua estrutura; em Cálculo dos Indicadores (5.5), apresentam-se as métricas para calcular os indicadores; e em Validação do *Framework* (5.6) são apresentados os métodos utilizados para seu desenvolvimento e um Protótipo de Software.

5.1 Conceptualização

A formalização conceitual do *framework* proposto, expressa por meio de uma ontologia leve (Balcão Filho et al., 2020), é apresentada na Figura 5.1. Essa ontologia leve modela a hierarquia de critérios de avaliação de confiança no contexto da computação em nuvem.

São considerados os domínios **Governança** (GV), **Transparência** (TP) e **Informações de Segurança** (SI). Cada domínio é dividido em critérios e subcritérios, que apoiam e contribuem para a compreensão e obtenção de resultados significativos

e relevantes para os consumidores de serviços de Nuvem.

Governança (GV) representa o conjunto abrangente de requisitos que as organizações usam para obter a confiança do cliente e gerenciar os processos do dia a dia, segurança da informação, proteção da privacidade, demandas regulatórias e de negócios.

No questionário, apresentado no Apêndice II, as Questões de 1 a 7 abordam os seguintes quesitos: infraestrutura de segurança, controles e contramedidas, auditorias externas, recomendações realizadas por *experts*, avaliações realizadas pelos usuários, dentre outros, tais como imperativos comerciais.

Transparência (TP) representa a Transparência de Segurança, que é a disseminação apropriada dos aspectos de governança das políticas, práticas e controles de segurança. Em outras palavras, significa revelar informações suficientes para permitir a avaliação dos usuários e ainda garantir que as necessidades de confidencialidade do CSP sejam atendidas.

As Questões de 8 a 14 tratam os seguintes quesitos: o provedor deve divulgar informações sobre sua política de comunicação obrigatória, de atendimento aos requisitos regulatórios, informações sobre incidentes ocorridos, bem como atender às necessidades dos clientes e alertas sobre ameaças ao ambiente do usuário do CSP.

Informações de Segurança (SI) representa a agregação de informações sobre processos, tecnologias e pessoas que apoiarão as organizações na garantia de confidencialidade, integridade e disponibilidade de seus ativos de informação.

As Questões de 15 a 24 apresentam os seguintes quesitos: estrutura de governança de TI; uma plataforma de prestação de serviços de prevenção, detecção e reação a incidentes de segurança (*Security Operation Center* – SOC); recursos tecnológicos de segurança; cláusulas de seguro e de penalidades por descumprir parâmetros dos contratos.

O modelo conceitual proposto na Figura 5.2 para avaliação de confiança em ambientes de computação em nuvem é centrado no consumidor e aborda aspectos de confiança da perspectiva do consumidor.

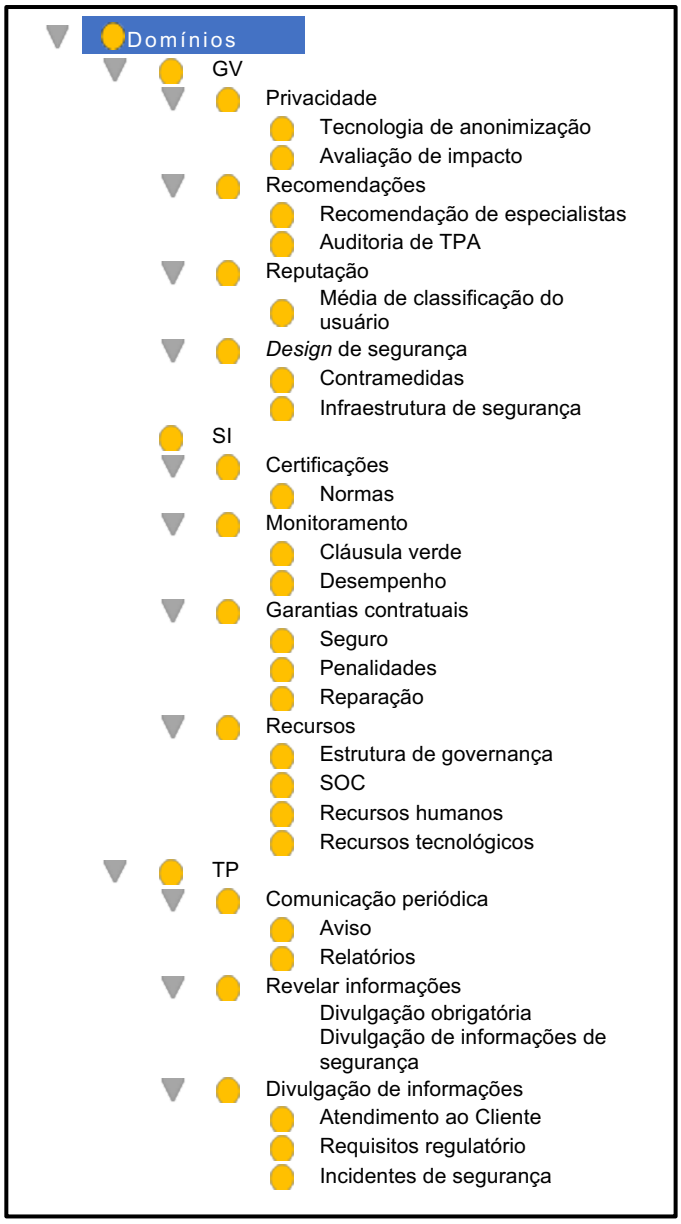


Figura 5.1- Ontologia Leve da Conceptualização do FTACSP - adaptado de (Balcão Filho et al., 2020)

Os modelos são úteis para nos ajudar a identificar as ações mais eficazes para estimar quantidades difíceis de medir, pois levam a um guia das ações mais eficazes para atingir os objetivos propostos. Geralmente são bastante sensíveis aos parâmetros que descrevem as características do sistema modelado. Esses parâmetros não são apenas difíceis de estimar, mas também podem mudar com base no contexto em que o modelo é aplicado. O modelo proposto leva em consideração várias fontes para criar parâmetros de confiança.

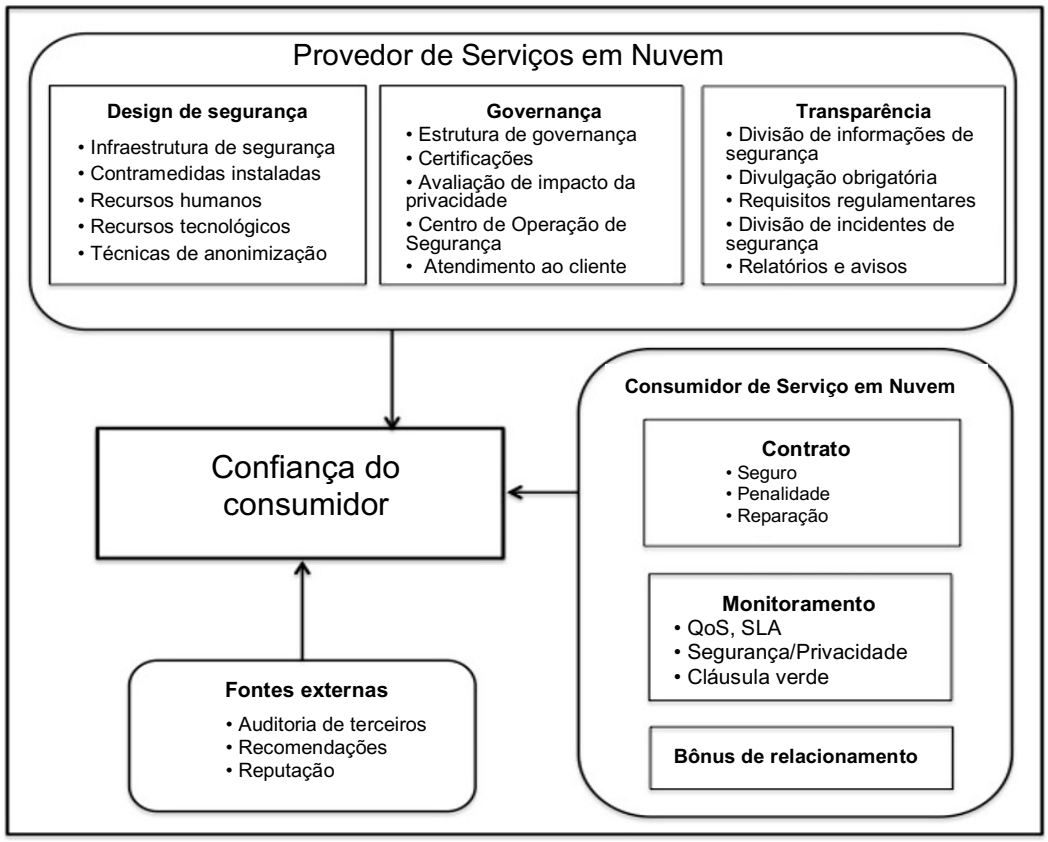


Figura 5. 2– Modelo de Confiança Proposto, adaptado de (Balcão Filho et al., 2020)

Três axiomas compõem a base deste modelo; cada um representa o aumento da confiança dos consumidores nos serviços de nuvem, conforme segue:

a) Axioma 1: A confiança aumenta com fácil acesso e interpretação, informação confiável e comunicação significativa e relevante, ou seja, *"informação sobre o sistema leva à confiança"*.

b) Axioma 2: Segurança de dados, proteção de privacidade e desempenho promovem a confiança, ou seja, *"atender às expectativas do consumidor aumenta a confiança"*.

c) Axioma 3: Boa reputação, auditorias e certificações influenciam a confiança, ou seja, *"opiniões positivas aumentam a confiança"*.

5.2 Processo de Desenvolvimento do *Framework*

Com base no modelo de confiança descrito na Seção Conceptualização,

seguimos o processo de seis etapas proposto por Alabool, Kamil, Arshad, & Alarabiat (2018) para desenvolver o *framework* FTACSP, incluindo as seguintes fases:

a) Planejamento (Etapas 1 a 4),

b) Exame (Etapa 5)

c) Tomada de decisão (Etapa 6).

O desenvolvimento rigoroso do *framework* de avaliação visa a fornecer bons **Indicadores de Confiança** para melhorar o processo de tomada de decisão. A etapa de tomada de decisão (Etapa 6) é bastante complexa, pois depende do contexto e das necessidades dos consumidores.

Etapa 1 – *Selecionar o alvo da avaliação*. Do ponto de vista do consumidor, nesta etapa, seleciona-se o ativo de informação a ser avaliado, que pode ser qualquer serviço de computação em nuvem (e.g., IaaS, PaaS ou SaaS).

Etapa 2 – *Identificar critérios de avaliação*. Critérios e subcritérios de avaliação foram propostos e inseridos no catálogo de critérios de FTACSP (Tabela 5.2), que contém a descrição do domínio, critérios, subcritérios, fontes de informação, além de um questionário detalhado no Apêndice II. Conforme argumentado em (Harker & Vargas, 1987), os termos, critérios e propriedades foram adotados como intercambiáveis.

Etapa 3 – *Definir o padrão de avaliação*. Um padrão de avaliação é uma medida usada para comparar ou julgar um determinado alvo. Esta etapa focou na escolha de uma escala apropriada, que é uma tarefa difícil e dependente do contexto (Harker & Vargas, 1987). No FTACSP propõe-se o uso de uma escala ordenada para representar enunciados verbais, pois é uma alternativa viável quando o avaliador não possui uma compreensão abrangente do problema (Franek & Kresta, 2014). O uso de respostas verbais é intuitivo, mas pode ser ambíguo em comparações não triviais.

Os valores numéricos usados na escala podem afetar as preferências de um indivíduo, pois não há como garantir que um determinado método de avaliação seja totalmente independente da escala de medição. A Tabela 5.1 apresenta a escala adotada inspirada em uma “escala ordinal Likert de 5 pontos” (Joshi et al., 2015). Na escala proposta não existe ponto neutro, pois espera-se uma opinião positiva ou negativa do avaliador.

Tabela 5.1 – Escala Adotada para a Avaliação

	ESCALA
0	Não presença
1	Discordo Fortemente ou Confiança Mínima
2	Discordo ou Confiança Aceitável
3	Concordo ou Boa Confiança
4	Concordo Fortemente ou Alta Confiança

Etapa 4 – *Selecionar e desenvolver a coleta de dados.* Nesta etapa escolhemos as seguintes técnicas de coleta de dados e fontes de dados para apoiar a análise e avaliação dos critérios:

a) Cláusulas contratuais;

b) Informações fornecidas pelo CSP;

c) Opinião de terceiros, como reputação, recomendações de especialistas e auditorias;

d) Demonstração de competência, por meio do monitoramento de desempenho;

e) Aspectos de governança, tais como certificações, recursos técnicos e humanos envolvidos.

Etapa 5 – *Selecionar e desenvolver técnicas de síntese.* Nesta etapa descrevem-se as técnicas e equações de síntese, bem como as atividades e etapas definidas necessárias para incorporar todas as informações coletadas e calcular os **Indicadores**. Esses Indicadores representam avaliações do nível de confiabilidade da meta sob avaliação escolhida na Etapa 1, conforme é descrito na seção sobre o Cálculo dos Indicadores de Confiança.

Etapa 6 – *Processo de tomada de decisão.* Nesta etapa, o usuário avaliador deverá, com base nos valores dos Indicadores, tomar alguma decisão. Caso os valores dos Indicadores indiquem problemas sérios, este terá que tomar alguma atitude. Podem ser atitudes para correção dos problemas ou até mesmo decidir pela troca do CSP. Esta etapa é bastante dependente do contexto, pois depende das necessidades do consumidor daquele serviço sob avaliação.

5.3 Critérios de Avaliação

Embora a segurança da informação seja a primeira preocupação de quem avalia a confiabilidade dos serviços de Nuvem, outros fatores como privacidade, desempenho, transparência e comunicação têm peso significativo (Eftekhar et al., 2018). Todos esses fatores devem ser avaliados por meio de critérios. Os requisitos devem ser analisados e considerados na escolha de critérios consistentes, para que se possa atingir os objetivos pretendidos.

Com base em (Alabool et al., 2018), FTACSP adota três princípios de avaliação:

a) *Clareza* – Os critérios de avaliação são bem definidos, claros, inequívocos, fáceis de entender e significativos para os tomadores de decisão;

b) *Decomponibilidade* – Os critérios de avaliação podem ser decompostos do topo para a base da hierarquia, abrangendo todas as características importantes do problema decisório e simplificando os processos de avaliação;

c) *Confiabilidade* – Os critérios de avaliação são formulados com base em fontes confiáveis e verificados por meio de uma abordagem de verificação formal.

O FTACSP inclui um catálogo de critérios (Tabela 5.2) elaborado por cinco especialistas em segurança da informação. Este catálogo é essencial para a compreensão e aplicação do *framework*.

A Tabela 5.2 mostra como os domínios GV, TP e SI estão divididos em critérios e seus subcritérios, identificados como CGVi, CTPi e CSIi; onde *i* é o índice que identifica o subcritério. A tabela também apresenta uma breve descrição e o número da questão correspondente no questionário apresentado no Apêndice II.

Sete questões foram propostas para abordar o domínio GV, sete questões para o domínio TP e dez questões para o domínio SI. Os critérios e subcritérios propostos foram desenvolvidos levando em consideração os três princípios mencionados acima, o modelo de confiança apresentado na Tabela 5.2, bem como

os axiomas propostos na seção de conceptualização.

Tabela 5.2 – Critérios e Subcritérios com suas Respectivas Fontes de Informação (Balcão Filho et al., 2020)

Domínio	Critério	ID C*xx*i	Subcritério	Questão	Fontes de Informação
Governança	Projeto de Segurança	CGV1	Infraestrutura de Segurança	Q1	CSP
		CGV2	Contramedidas Instaladas	Q2	CSP
	Recomendação	CGV3	Auditoria de Terceira Parte	Q3	Externa/TPA
		CGV4	Recomendação de Especialista	Q4	Externa
	Reputação	CGV5	Avaliação Média dos usuários	Q5	Externa
	Privacidade	CGV6	Avaliação de Impacto de Privacidade	Q6	CSP
		CGV7	Técnicas de Anonimização	Q7	CSP
Transparência	Revelar Informações	CTP1	Divulgação de Informações de Segurança	Q8	CSP
		CTP2	Divulgação Obrigatória	Q9	CSP
	Divulgação de Informações	CTP3	Requisitos Regulamentares	Q10	CSP
		CTP4	Incidentes de Segurança	Q11	CSP
		CTP5	Atendimento ao Cliente	Q12	CSP
	Comunicação Periódica	CTP6	Relatórios	Q13	CSP
		CTP7	Avisos	Q14	CSP
Informações de Segurança	Recursos	CSI1	Recursos Humanos	Q15	CSP
		CSI2	Centro de Operações de Segurança	Q16	CSP
		CSI3	Estrutura de Governança	Q17	CSP
		CSI4	Recursos Tecnológicos	Q18	CSP
	Certificações	CSI5	Normas Técnicas	Q19	Externa/TPA
	Garantias Contratuais	CSI6	Seguro	Q20	CSP
		CSI7	Penalidades (SLA)	Q21	CSP
		CSI8	Reparação	Q22	CSP
	Monitoramento	CSI9	Desempenho (QoS, SLA)	Q23	CSP
		CSI10	Cláusulas Verdes	Q24	CSP/TPA

5.4 Arquitetura do *Framework*

A Figura 5.3 apresenta a arquitetura do FTACSP, que visa a fornecer uma avaliação de confiança dos serviços de computação em nuvem. Na concepção da arquitetura foram consideradas as recomendações de Saaty e Ergu (2015).

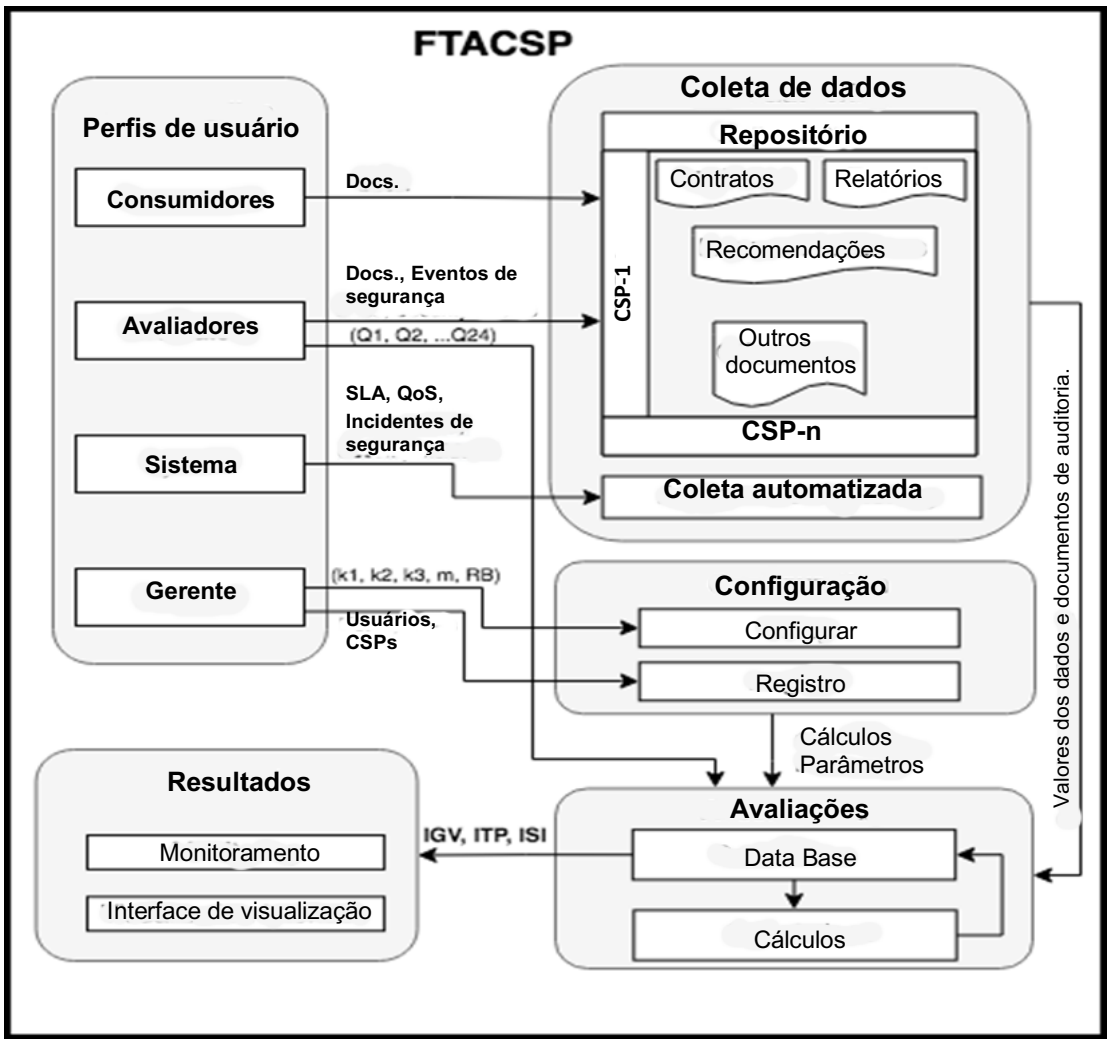


Figura 5.3 – Diagrama Esquemático do FTACSP, adaptado de (Balcão Filho et al., 2023)

A arquitetura de FTACSP possui quatro perfis de usuários, a saber: Gestor, Avaliador, Sistema e Consumidor.

O perfil Gestor tem a função de configurar o *framework* para cada serviço a ser avaliado, definindo os parâmetros k1, k2, k3, RB e m. O gestor também é responsável por cadastrar os provedores de serviços de Nuvem que serão avaliados e

os respectivos avaliadores. O perfil Sistema é responsável por monitorar rotinas e pela coleta automatizada de informações, como SLA, QoS, alertas e avisos de incidentes de segurança e privacidade, para serem utilizados durante uma análise de acompanhamento dos serviços de Nuvem sob avaliação.

O perfil Avaliador é responsável por responder às 24 questões mensalmente, e atribuir uma nota de 0 a 4 para cada uma. Isso deve ser feito para cada serviço. Essas pontuações serão armazenadas e utilizadas, com os demais parâmetros, nas fórmulas que calculam os valores dos indicadores (*IGV, ITP, ISI*).

O perfil Consumidor ou Cliente faz uso dos resultados do FTACSP. Ao ter acesso aos valores dos Indicadores, o consumidor poderá fazer julgamentos sobre a confiança depositada nos serviços avaliados e tomar decisões sobre esses serviços. Consumidor ou cliente de um serviço de Nuvem geralmente não tem experiência nem conhecimento suficientes para responder ao questionário. Portanto, quando nos referimos ao consumidor nos referimos a todas as pessoas que utilizam serviços da Nuvem, tenham elas conhecimento de TI ou não. Já quando nos referimos ao Usuário (ou usuário avaliador) nos referimos às pessoas que têm conhecimento de tecnologia da informação e do uso dos serviços de computação em nuvem. Este tipo de profissional não precisa ser especialista em segurança da informação.

O FTACSP inclui um repositório que armazena os dados coletados das fontes de informação que são consultadas pelos avaliadores, e um banco de dados que armazena todas as informações, incluindo:

a) Registros de usuários e serviços de nuvem sob avaliação;

b) Parâmetros para avaliação de cada CSP;

c) Respostas às questões;

d) Resultados dos cálculos.

Os cálculos são feitos automaticamente pelo sistema, ou seja, sem ações do gestor ou avaliador. Os resultados dos cálculos são disponibilizados em formatos numéricos e gráficos. O objetivo é proporcionar uma melhor visualização da evolução dos indicadores ao longo do período de avaliação.

Para testar e validar o FTACSP uma Prova de Conceito (PoC) foi realizada em três cenários diferentes, aplicando-o em plataformas bem estabelecidas de

computação em nuvem. Esta PoC está descrita no Capítulo 6.

O FTACSP pode ser expandido e aplicado a outros contextos e plataformas, se consideradas suas limitações.

5.5 Cálculo dos Indicadores de Confiança

Segundo Minayo (2009), “indicadores são uma forma de mensuração que aponta tendências e considera parâmetros quantitativos e qualitativos, que servem como métricas para resultados de ações ou processos”.

Os indicadores são ferramentas de gestão importantes para um gestor de Nuvem, pois são essenciais para medir, definir parâmetros e avaliar CSPs. Os indicadores permitem que os administradores atuem em dimensões-chave de sistemas e processos, monitorando situações que devem ser alteradas, incentivadas ou aprimoradas desde o início de uma intervenção, de acordo com a extensão do que foi pretendido e previsto.

Ao usar indicadores, pode-se comunicar de maneira fácil e significativa o progresso da segurança, confiabilidade e outros aspectos de um serviço em Nuvem (Lynn et al., 2016).

Para os consumidores, indicadores são de fácil interpretação e contribuem para a tomada de decisão. Os indicadores auxiliam o consumidor de serviços de Nuvem a tomar melhores decisões além dos aspectos de preço, funcionalidade e *branding*, ou seja, atributos de um produto ou empresa que representam tanto benefícios funcionais como emocionais.

Por exemplo, os rótulos de eficiência energética de produtos são indicadores que incluem informações úteis sobre consumo de energia, classificação energética, valores e cultura da empresa fornecedora. Outro exemplo é a Taxa de Mortalidade Infantil[37] que é um indicador social, mundialmente consagrado, utilizado para medir a qualidade de vida e desenvolvimento por expressar a situação de saúde de uma comunidade e as desigualdades entre grupos sociais.

Os **Indicadores de Confiança da Nuvem** propostos medem

[37] Indicador de Mortalidade Infantil – https://unasus2.moodle.ufsc.br/pluginfile.php/ 33455/mod_resource/content/1/un2/top2_5.html

sinteticamente a consistência e a confiabilidade dos sistemas de computação em Nuvem e representam uma expressão de condições de segurança cibernética, capacidade de gerenciamento e transparência de segurança.

Os resultados do *framework* precisam ser fundamentados em justificativas lógicas e matemáticas. A representação dessa lógica e o raciocínio por trás da teoria subjacente são descritos nos parágrafos seguintes, bem como a formalização das soluções de cálculo adotadas.

5.5.1 Metodologia para calcular os Indicadores Propostos

A seguir apresentamos a sequência de etapas para a avaliação de CSPs usando os indicadores de confiança propostos. É calculado um indicador para cada domínio (GV, TP, SI). A avaliação deve ser realizada mensalmente para possibilitar o acompanhamento do serviço em avaliação ao longo do tempo.

No Apêndice II constam dois Quadros com as questões que são usadas para fazer a avaliação de confiança do serviço de Nuvem. No Quadro 1, estão as questões que foram utilizadas para a realização da Prova de Conceito apresentada na Seção 6. No Quadro 2, estão as mesmas questões, mas corrigidos os erros e melhoradas as redações das questões. Portanto, deve-se usar para as próximas avaliações as questões do Quadro 2.

O processo de cálculo da avaliação começa com um avaliador, que responde a todas as 24 questões do questionário que se encontram no Apêndice II, referentes ao serviço sob avaliação. As Questões de 1 a 7 do questionário referem-se ao Subcritério CGV_i, as Questões de 8 a 14 ao CTP_i e as Questões de 15 a 24 ao CSI_i. Caso haja mais de um avaliador por critério, deve-se calcular a média geométrica para cada subcritério, de forma que apenas um valor entre nos cálculos por subcritério. Segundo Saaty (2008), a média geométrica é a maneira correta de fazer isso, e não a média aritmética.

Na Figura 5.4, a Equação (1) é usada para o cálculo da média por domínio GV, TP e SI, com base nos valores atribuídos às questões. Assim, obtemos os valores de GV_j, TP_j e SI_j, onde *i* refere-se às questões relacionadas aos domínios GV, TP ou SI; e *j* refere-se ao mês de interesse.

Na Figura 5.4, a Equação (2) representa matematicamente o conceito de ter parcelas que expressam a situação atual, de futuro e passado da avaliação. A primeira parcela desta equação é proporcional ao valor atual da avaliação. A segunda parcela representa a tendência, o futuro, indicando se a avaliação é melhor ou pior em relação ao mês anterior. A terceira parcela representa o passado por meio do cálculo da média dos últimos doze meses. Essas parcelas são ponderadas pelos parâmetros k1, k2 e k3, cuja soma deve ser igual a 1.

A primeira parcela da Equação (2) - $k1*GV_j$ - é referente à avaliação do mês corrente, ou seja, é a percepção que o usuário tem de como se comportou o serviço de Nuvem no último mês. Esta parcela é ponderada pelo parâmetro k1.

A segunda parcela da Equação (2) – $k2*(GV_j – GV_{j-1})$ - é referente a expectativa que o usuário tem de como o serviço irá se comportar no futuro. Esta parcela é ponderada pelo parâmetro k2.

A terceira parcela da Equação (2) é k3 que multiplica a média das últimas 12 avaliações feitas; é referente à crença que foi depositada no serviço sob avaliação, nos últimos 12 meses. Esta parcela é ponderada pelo parâmetro k3.

As Equações (1) e (2) são utilizadas para calcular o Indicador IGV; as mesmas fórmulas são aplicadas para calcular os outros dois indicadores, ou seja, ITP e ISI. Para tanto, temos que substituir CGV_j, CTP_j e CSI_j na equação (1) e GV_j, TP_j e SI_j na equação (2).

$$GV_j = \frac{\sum_{i=1}^{n} CGV_i}{n} \quad (1)$$

$$IGV_j = \frac{((k1 * GV_j) + (k2 * (GV_j - GV_{j-1})) + (k3 * \sum_{j-12}^{j} \frac{GV_j}{12})) * RB}{2^m} \quad (2)$$

Figura 5.4 – Equações para Cálculo dos Indicadores de Confiança (Balcão Filho et al., 2023)

Conforme mostrado na Equação (2), o Bônus de Relacionamento RB (*Relationship Bonus)* é uma variável chave, pois o *framework* incorpora a noção de que a confiança depende de um bom relacionamento entre as partes envolvidas. Um bom relacionamento pode compensar problemas de avaliação, pois o prestador de serviço é assertivo e responde bem às necessidades dos clientes. Portanto, propõe-

se que o Indicador possa ser incrementado pela elevação do valor RB, à medida que a relação entre consumidor e CSP se consolida. Esse parâmetro varia de 0% a 100%, ou seja, RB varia entre 1 (0%) e 2 (100%). Assim, o usuário pode compensar a queda dos valores dos Indicadores atribuindo um valor a RB, de modo a aumentar os valores dos Indicadores.

A Equação (2) também incorpora o conceito de que eventos que levam a falhas na prestação dos serviços prejudicam severamente a confiança do consumidor nos CSPs, ou seja, há uma quebra de confiança no CSP. Isso é representado na Equação (2) pelo parâmetro “m”. Divide-se o resultado da avaliação por 2 elevado a m, onde m representa um evento de segurança catastrófico ou muito grave ocorrido no mês, tais como violações de dados, vazamento de informações de clientes, recuperação de desastres etc. O parâmetro “m” é o número de falhas que trouxeram prejuízo ao consumidor daquele serviço que falhou. Normalmente, “m” é igual a zero, mas se ocorrer uma falha, “m” será igual 1; se ocorrerem duas falhas, “m” será igual a 2, e assim por diante.

Após a ocorrência de um evento catastrófico, ou seja, “$m = 1$”, inicia-se uma “etapa de esquecimento” desse evento. O valor de “m” será dividido sucessivamente por 2 nos próximos 3 meses, ou seja: m = 1, m = 1/2, m = 1/4, m = 1/8. Após esta “etapa de esquecimento”, *m* volta a zero. Isso mostra a recuperação da confiança do consumidor no seu provedor de serviços de nuvem.

O resultado da Equação (2), aplicada aos três domínios (GV, TP, SI), é o valor numérico do Indicador para cada domínio – IGV, ITP e ISI. Assim, os indicadores numéricos propostos são proporcionais à avaliação atual, ao histórico de avaliações anteriores, à tendência de confiança do consumidor no serviço de Nuvem, bem como a eventos significativos e a relação de confiança cultivada entre as partes.

O acompanhamento é possibilitado pelo monitoramento mensal dos valores dos indicadores, onde o aumento do valor do indicador evidencia uma melhor avaliação da confiança do consumidor. Quanto maior o valor numérico dos indicadores, melhor a avaliação da confiança.

Os Indicadores visam a permitir uma avaliação da confiança feita pelo consumidor, sendo adaptáveis e extensíveis a outros contextos. Os Indicadores são de fácil comunicação e interpretação se a confiança está aumentando ou não.

5.6 Validação do *Framework* e Protótipo de Software

Como o *framework* é sustentado por avaliações qualitativas e quantitativas, a validação do modelo resultante é essencial; caso contrário, o rigor científico pode ser questionado. Deve-se buscar rigor, confiabilidade e qualidade no desenvolvimento do modelo (Nahid, 2003). A validade de um modelo é baseada nos métodos utilizados durante seu desenvolvimento e na qualidade da própria pesquisa, como transparência e consistência, que juntos constroem a justificativa das interpretações (Ollaik & Ziller, 2012). Esses cuidados foram adotados no desenvolvimento do *framework* proposto. A validação do *framework* proposto é baseada na formulação e desenvolvimento empregados em uma prova de conceito (três avaliações reais e uma simulação), detalhadas no Capítulo 6.

Para apoiar a validação da proposta, foi desenvolvido um protótipo de software que automatiza o cálculo dos Indicadores de Confiança. O código fonte da Versão 1.0 pode ser encontrado no repositório do projeto no GitHub[38]. A Figura 5.5 apresenta uma captura de tela do protótipo, mostrando o Formulário de Avaliação de CSPs, que permite gerenciar todas as avaliações e seus respectivos IGV, ITP e ISI.

O protótipo FTACSP possui um repositório para armazenar os dados coletados das fontes de informação, um banco de dados para manter todas as avaliações, resultados calculados, cadastro de usuários e CSPs em avaliação. O protótipo permite que os consumidores acompanhem a evolução ao longo do tempo das avaliações de confiabilidade dos serviços, por meio de uma interface gráfica de usuário.

[38] Código fonte de FTACSP - https://github.com/FTACSP/prototype

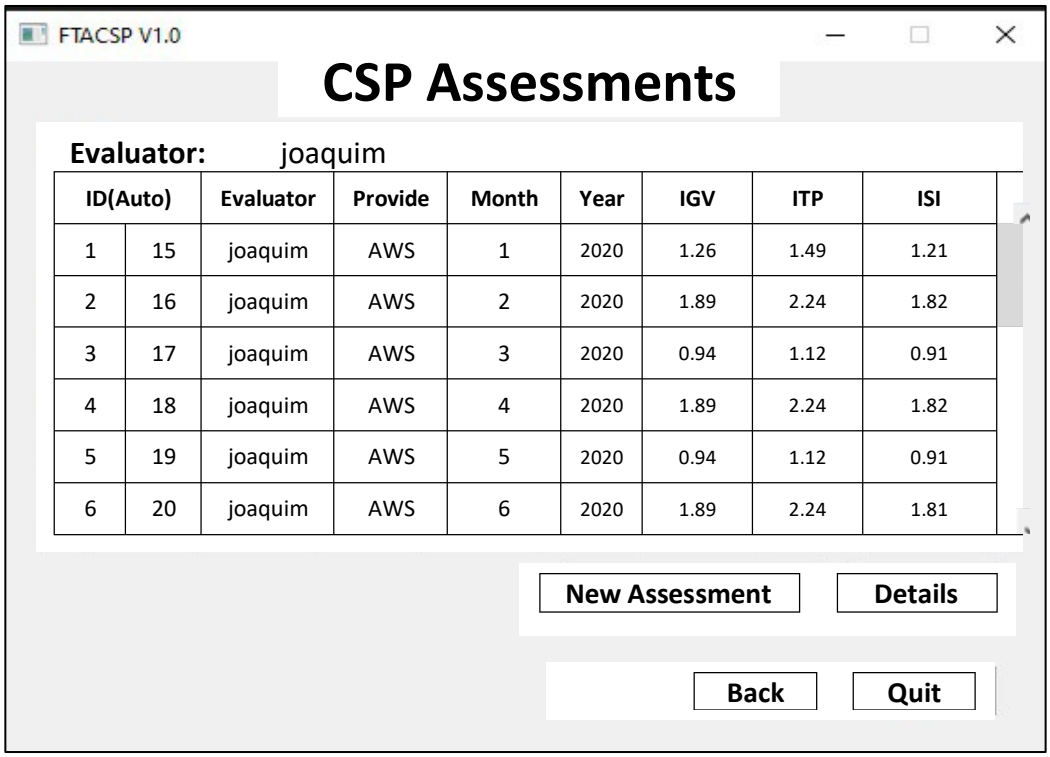


Figura 5.5 – Formulário de Avaliações de CSPs do Protótipo do FTACSP (Balcão Filho et al., 2023)

Para operacionalizar o protótipo de sistema e o ambiente de simulação, foi criado um banco de dados relacional para armazenar as informações que serão utilizadas nos cálculos e na gestão das avaliações. O Sistema Gerenciador de Banco de Dados (SGBD) usado foi o MySQL. A Figura 5.6 apresenta o Modelo Entidade-Relacionamento (MER) do FTACSP.

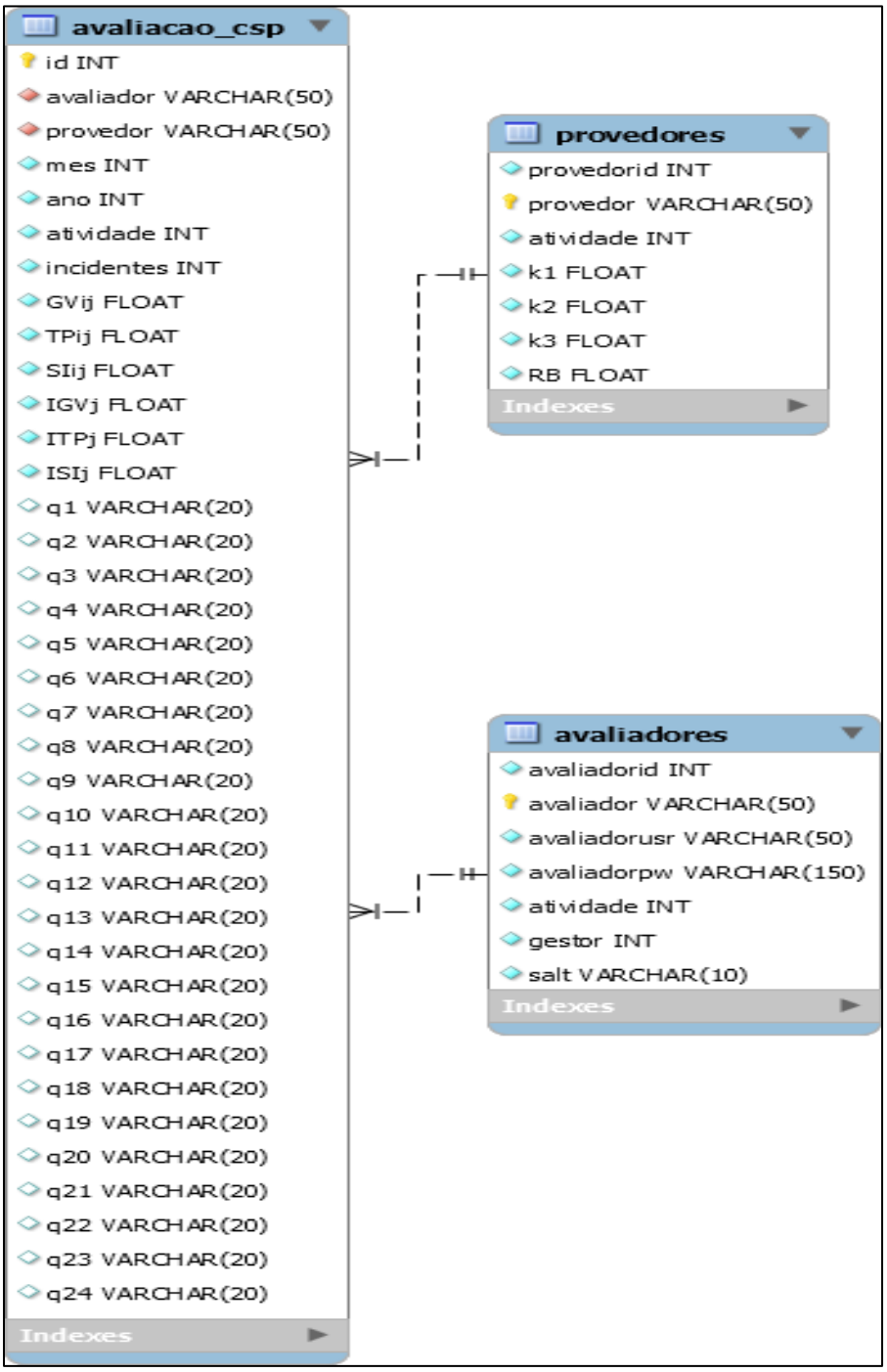


Figura 5.6 – Modelo Entidade-Relacionamento do FTACSP

A entidade "***avaliacao_csp***" armazena informações sobre as avaliações dos CSPs. Seu código identificador (id) é gerado automaticamente pelo SGBD. Esta entidade se relaciona às entidades "*avaliadores*" e "*provedores*". Os campos "*mês*", "*ano*", "*avaliador* ", e "*provedor*" representam unicamente uma avaliação. Os campos "*atividade*" (valor padrão = 1) e "*incidentes*" (valor padrão = *0*), são inseridos

automaticamente a cada avaliação. Se uma avaliação for "*excluída*" no sistema, o campo "*atividade*" será editado para 0 (inativa) e continuará na base de dados. Se o avaliador reportar algum incidente, o campo "*incidente*" será editado para receber o valor 1. Os campos "*GVij*", "*TPij*" e "*SIij*", representam os domínios de Governança, Transparência e Segurança da Informação respectivamente, tendo seus valores calculados e identificados no envio de uma nova avaliação no *framework*. Os campos "*IGVj*", "*ITPj*" e "*ISIj*" armazenam os indicadores, resultantes das parcelas da equação. Os campos de "*q1*" a "*q24*", recebem os valores atribuídos pelos avaliadores a cada uma das 24 questões do formulário de avaliação do FTACSP. Os valores variam de 0 a 4.

A entidade "***avaliadores***" tem como chave primária o campo "*avaliador_id*". O campo "*avaliador*" armazena o nome completo do avaliador. O campo "*avaliadorusr*" armazena o "*usuário de login*" no sistema e o campo "*avaliadorpw*" armazena a senha do usuário. O campo "*atividade*" é usado para gestão da conta do usuário, ou seja, se a conta está ativa (valor = *1*) para poder acessar o *framework*. O campo "*gestor*" indica se o usuário possui credenciais de gestor (valor = *1*) das avaliações.

A entidade "***provedores***" tem como chave primária o campo "*provedor_id*". O campo "*provedor*" armazena o nome do CSP. O campo "*atividade*" é usado para gestão da lista de CSPs, ou seja, se o provedor está ativo para ser listado para avaliações (valor = *1*). Os campos "*k1*", "*k2*" e "*k3*" armazenam os valores utilizados nos cálculos, representando respectivamente a avaliação atual, a tendência e o histórico nos resultados dos indicadores. O campo "*RB*" (*Relationship Bonus*) representa o bônus de relacionamento.

5.7 Considerações Finais

A proposta aborda os problemas de confiança em serviços de Nuvem, apresentando um *framework* de avaliação de confiança que integra três domínios: Governança, Transparência da Segurança e Informações sobre a Segurança dos serviços contratados. O *framework* proposto avalia questões relacionadas à segurança da informação; recomendação de especialistas; reputação do serviço; divulgação obrigatória de eventos relevantes à segurança da informação; estrutura de segurança;

aspectos de governança e cláusulas contratuais. É empregada uma abordagem de avaliação qualitativa dos diversos fatores relacionados a: nível de segurança, reputação, recomendação, desempenho e outros, e os agrega para obter um nível de confiança quantitativo para os serviços de Nuvem. O método retorna um indicador numérico para cada domínio do *framework* – IGV, ITP e ISI.

6 APLICAÇÃO DO FTACSP

Seguindo as diretrizes descritas nas Seções 5.5 e 5.6, as avaliações qualitativas foram conciliadas para obter resultados numéricos, relacionando-os à metodologia utilizada para desenvolver o FTACSP.

É usada uma escala Likert (Tabela 5.1) que usa valores (de 0 a 4) para a realização dos cálculos.

Uma Prova de Conceito foi realizada para verificar, em situações do mundo real, a aplicabilidade, sensibilidade e robustez do modelo e do *framework* propostos. O objetivo principal foi testar se o *framework* atende aos requisitos para os quais foi projetado.

Para avaliar a viabilidade do *framework* proposto, foi realizada uma Prova de Conceito (PoC) em três serviços de Nuvem. Os resultados obtidos permitem discutir a sua eficácia, buscando mostrar que o *framework* pode contribuir para melhorar o nível de confiança dos serviços de nuvem. Também foi efetuada uma simulação de 18 meses para observar como a fase de esquecimento impacta os resultados quando um evento catastrófico ocorre.

6.1 Objetivos da Prova de Conceito

A Prova de Conceito (PoC) realizada visa verificar se o método e o *framework* propostos funcionam conforme projetado, ou seja, analisar em condições reais as propriedades de aplicabilidade, sensibilidade e robustez. A PoC busca essencialmente mostrar se o *framework* contribui para:

a) Evidenciar se a confiança depositada pelos usuários nos serviços de Nuvem sob avaliação contribui para a melhoria destes serviços;

b) Mostrar que o modelo oferece condições para capturar o dinamismo das infraestruturas de Nuvem sob avaliação;

c) Verificar se o modelo é passível de ser empregado de maneira útil aos consumidores dos serviços de Nuvem;

d) Identificar eventuais problemas e propor melhorias ao modelo proposto.

6.2 Cenário da Prova de Conceito

Na realização da PoC seguimos a metodologia descrita no Capítulo 5. Para tanto, dois avaliadores escolheram três cenários reais de uso de serviços de Nuvem, que eles utilizavam para realização de suas atividades profissionais. Para cada cenário, um avaliador respondeu às 24 perguntas em um formulário online. Os questionários foram respondidos mensalmente, durante quatro meses – de novembro de 2019 a fevereiro de 2020. As perguntas do formulário podem ser encontradas no Apêndice II.

Os dois avaliadores possuem o mesmo perfil profissional, ou seja, são profissionais de desenvolvimento de software, atuando (isoladamente) em projetos coordenados remotamente. Ambos os avaliadores dependem da confiabilidade dos serviços contratados para o desempenho de suas funções profissionais e não possuem equipe de apoio. Os três serviços são oferecidos pelos CSPs como serviços padronizados (*off-the-shelf*). Essas características e semelhanças são pontos de interseção que nos permitem comparar os resultados e apresentar algumas conclusões.

Os perfis dos 2 avaliadores que contribuíram na realização da PoC são os seguintes:

a) Avaliador A – Formação na área de Administração de Sistemas com 25 anos de experiência;

b) Avaliador B – Formação na área de Sistemas de Informação (desenvolvimento) com 20 anos de experiência.

O Avaliador A foi responsável por avaliar os Serviços 1 e 2, enquanto o Avaliador B avaliou o Serviço 3. Os serviços de Nuvem avaliados são descritos a seguir:

a) Serviço 1 (Avaliador A) – Refere-se a um ambiente de inteligência de dados (DevOps) que busca avaliar a capacidade dos inadimplentes em quitar suas dívidas, por meio da análise de dados obtidos de fontes abertas e informações fornecidas pelos credores sobre os devedores. O CSP contratado foi a Amazon AWS (EUA). Foram contratados os seguintes serviços de Nuvem: servidor de

mensagens RDS (*Amazon Relational Database Services* – PostgresSQL), S3 (*Amazon File Server*) e SQS (*Amazon Simple Queue Service*) – utilizado na arquitetura de microsserviços, sistemas distribuídos e aplicações *serverless*. O contratante atribui grande importância à confidencialidade e em menor grau à disponibilidade dos serviços.

b) Serviço 2 (Avaliador A) – Refere-se ao ambiente de hospedagem de um software comercial de ensino, que contém funcionalidades de análise de dados e aprendizado de máquina, visando adequar o conteúdo didático entre alunos, pais e professores. O provedor de CSP contratado foi a Locaweb (Brasil). Foram contratados os seguintes serviços: hospedagem de sites HTTP/HTTPS, hospedagem de banco de dados (PostgreSQL), serviços de e-mail (POP3/SMTP). O contratante atribui grande importância à disponibilidade dos serviços e em menor grau à confidencialidade.

c) Serviço 3 (Avaliador B) – Refere-se ao serviço de hospedagem de domínio com banco de dados SQL e execução de APP. Neste caso, foram contratados dois fornecedores. O primeiro provedor contratado apresentou falhas, o que levou o usuário a mudar para um segundo provedor. O segundo provedor contratado foi o SmarterASP.NET (EUA). Foram contratados serviços de hospedagem de domínio, execução de APP, configuração e uso de banco de dados SQL. O contratante priorizou a disponibilidade e facilidade de configuração, seguido pela segurança do banco de dados SQL.

Conforme mencionado acima, para o Serviço 3, o primeiro CSP contratado – já na primeira avaliação – recebeu uma avaliação muito ruim: IGV = 0,57, ITP = 0,14 e ISI = 0,90. Ao aplicar o *framework* ao Serviço 3 o Avaliador B decepcionou-se com o serviço prestado, principalmente em relação ao suporte ao cliente e a falhas de privacidade. Um dos problemas relatados foi que era possível visualizar quais outros consumidores estavam hospedados na mesma instância do banco de dados em uso. Com esse resultado, já se percebe que o *framework* dá visibilidade à insatisfação do consumidor com o serviço, apoiando-o na decisão de trocar de provedor quando os

resultados não forem satisfatórios.

Após o período de implementação da PoC, os avaliadores também deram *feedback* sobre o funcionamento do modelo e do *framework*, descreveram as dificuldades enfrentadas, apresentaram suas impressões sobre o que é mais importante para os usuários finais e quais questões tiveram pouca relevância para eles.

6.3 Análise de Resultados da Prova de Conceito

Os resultados dos quatro meses de avaliação são apresentados nas Tabelas 6.1 e 6.2. A partir dos valores da Tabela 6.1, foram calculados os indicadores para os três serviços, para cada domínio. Na Figura 6.1 é apresentada a evolução das avaliações ao longo dos quatro meses.

As escolhas dos valores para os parâmetros k1, k2, k3, m e RB foram feitas com base nas necessidades dos serviços sob avaliação e na percepção dos avaliadores desses serviços. Ambos os avaliadores, na Prova do Conceito, deram maior importância à parcela referente a avaliação do mês corrente. Por isso a atribuição de k1=0,5. Para a expectativa e crença foram atribuídos k2=k3=0,25.

Como não ocorreram falhas nos serviços sob avaliação nos meses em que foram feitas, o parâmetro m foi fixado em zero (m=0). Como não houve tempo para analisar o relacionamento com o provedor do serviço pelo bom atendimento, RB foi fixada em 1 (RB=1).

Tabela 6.1 – Valores de 4 Meses de Avaliação para os 3 Serviços

Questões	Serviço 1				Serviço 2				Serviço 3			
	k1=0,5; k2,3=0,25; m=0; RB=1				k1=0,5; k2,3=0,25; m=0; RB=1				k1=0,5; k2,3=0,25; m=0; RB=1			
	M1	M2	M3	M4	M1	M2	M3	M4	M1	M2	M3	M4
Q01	1	4	4	3	1	0	1	1	2	2	3	3
Q02	1	3	3	3	0	0	0	1	2	2	3	3
Q03	0	0	0	0	0	0	0	0	0	1	1	1
Q04	0	3	3	3	0	0	2	2	0	0	2	2
Q05	0	3	1	4	0	2	3	1	0	0	1	1
Q06	0	0	3	4	0	0	0	0	2	2	3	3
Q07	0	0	1	1	0	0	0	0	0	2	3	3
Q08	0	2	3	3	1	1	1	1	2	1	3	3
Q09	0	1	3	3	0	1	0	0	0	0	0	0
Q10	0	0	4	4	0	0	1	1	0	0	0	0
Q11	4	3	4	3	0	0	0	0	0	0	0	0
Q12	3	3	3	3	1	2	2	3	2	2	4	4
Q13	1	1	3	3	0	0	0	0	0	0	0	0
Q14	3	3	3	3	0	0	0	0	0	1	0	0
Q15	2	1	1	4	0	3	0	1	2	2	4	4
Q16	3	3	4	3	0	0	0	0	2	2	4	4
Q17	3	1	3	4	0	0	0	0	2	2	3	3
Q18	1	3	4	4	1	1	1	1	3	2	4	4
Q19	0	0	4	0	1	1	0	0	0	0	0	0
Q20	0	4	0	0	0	0	2	0	0	0	0	0
Q21	0	0	0	0	0	0	0	0	0	0	0	0
Q22	0	0	0	0	0	0	0	0	0	0	0	0
Q23	4	4	4	4	2	3	4	3	1	3	4	4
Q24	1	0	4	4	0	0	0	0	0	0	0	0

Tabela 6.2 – Indicadores Calculados para 4 Meses

Serviço	Domínio do Indicador	Mês 1	Mês 2	Mês 3	Mês 4
1	IGV	0,29	1,59	1,50	1,82
2		0,14	0,23	0,68	0,45
3		0,86	1,02	1,76	1,56
1	ITP	1,57	1,43	2,56	2,15
2		0,29	0,46	0,40	0,64
3		0,57	0,43	0,79	0,70
1	ISI	1,40	1,23	1,85	1,61
2		0,40	0,65	0,48	0,35
3		1,00	0,84	1,48	1,32

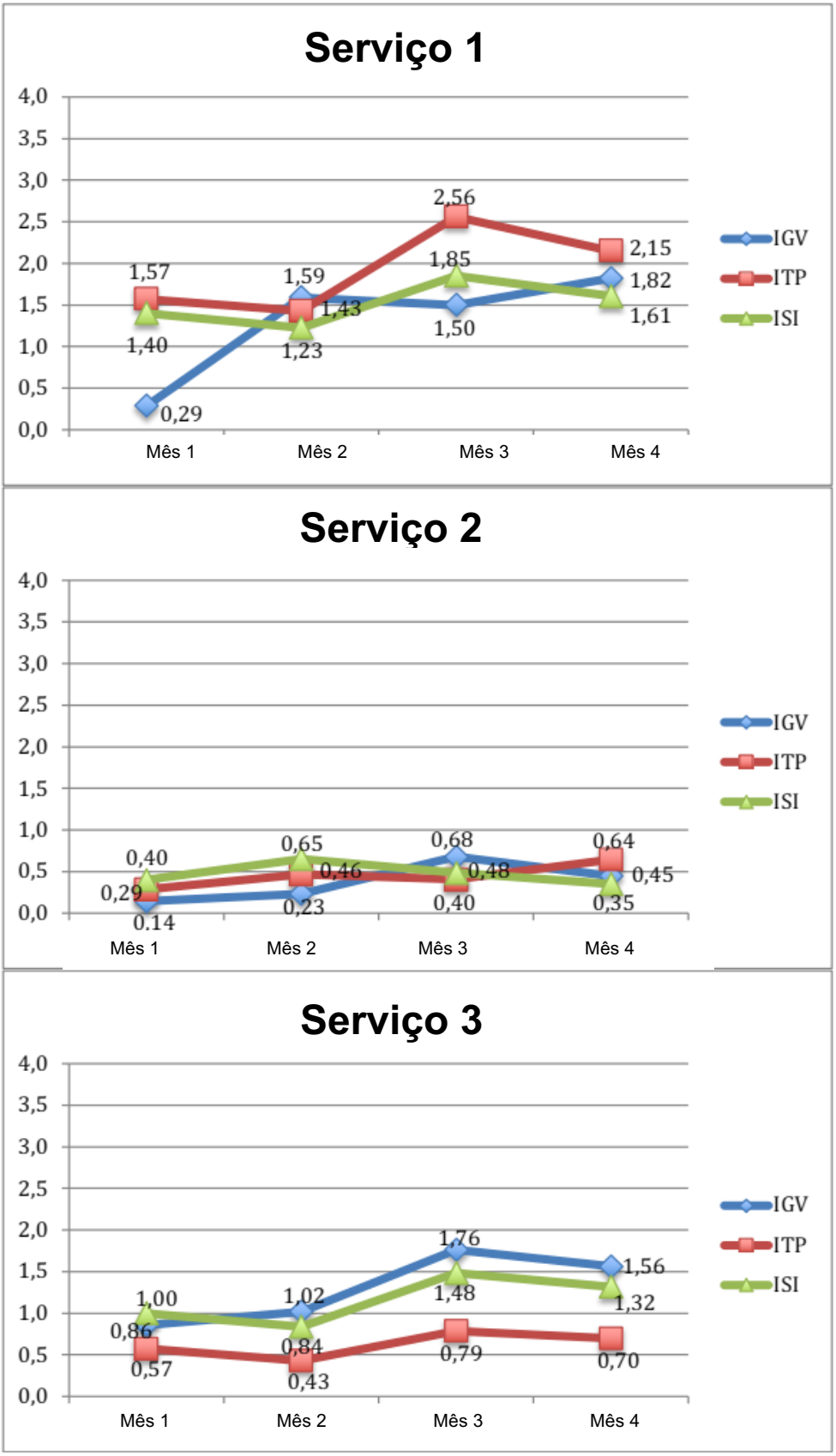


Figura 6. 1 – Evolução dos indicadores para os 3 domínios dos Serviços 1, 2 e 3 – adaptado de (Balcão Filho et al., 2023).

Os CSPs fornecem poucas informações sobre aspectos importantes para a confiança depositada no serviço. A PoC mostra quanta informação é retida pelos CSPs.

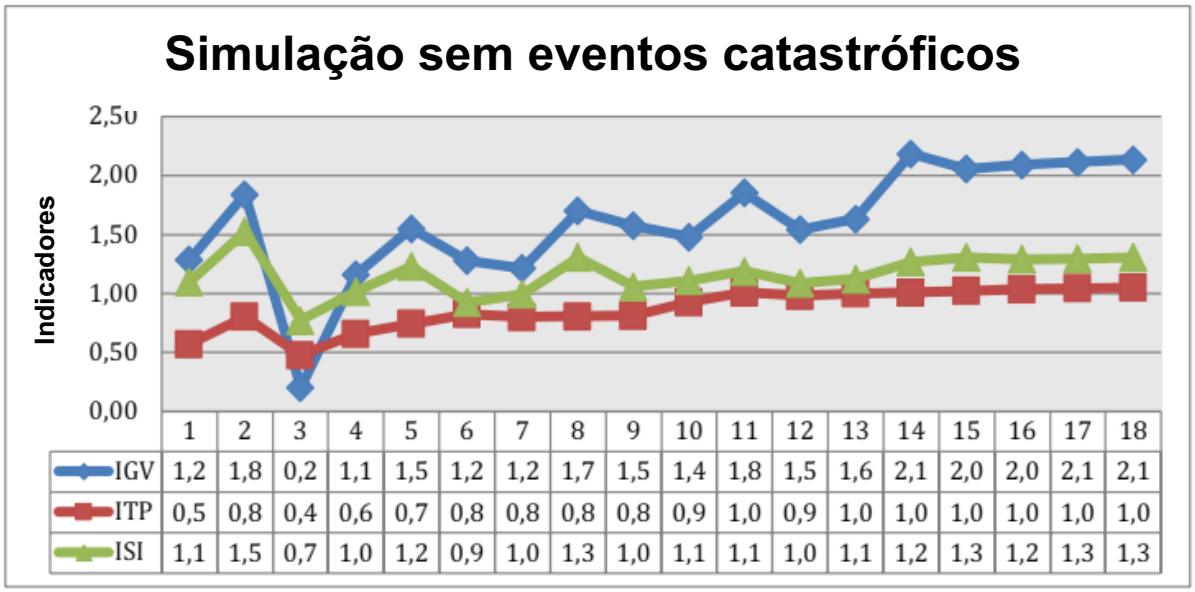
Os três serviços obtiveram resultados abaixo do esperado. Pode-se inferir que isso se deve ao fato de os CSPs fornecerem poucas informações. Foram muitos os valores “0” (Não Presença), pois não foi possível obter informações sobre, por exemplo: seguro, reparo e cláusula verde. Também há pouca informação fornecida pelos CSPs sobre dados de Segurança da Informação (por exemplo, incidentes de segurança). Não há como interagir com provedores de forma automatizada para coleta de dados; apenas SLA (*Service Level Agreement*) e dados de desempenho são fornecidos aos consumidores.

O AWS (Serviço 1) é claramente mais bem avaliado em comparação com os outros dois provedores, que são de porte menor. Os resultados obtidos dos avaliadores foram bastante diferentes. O *framework* também captura a diferença entre os CSPs, conforme mostrado nas avaliações dos Serviços 1 e 2, feitas pelo mesmo avaliador.

O *framework* é capaz de capturar avaliações de confiança em serviços de Nuvem. O fato de ter ocorrido a troca de CSP pelo Serviço 3, logo no início da avaliação, demonstra que ao sistematizar a avaliação, as fragilidades do CSP ficaram evidentes, ou seja, o CSP não estava atendendo às necessidades do consumidor.

A realização da simulação de 18 meses para um cenário hipotético com a ocorrência de um evento catastrófico é mostrada na Figura 6.2, que permite comparar os resultados com e sem o evento catastrófico. O evento catastrófico, m=1, foi inserido durante o 12º mês para simular o comportamento dos indicadores (Figura 6.2, gráfico inferior), bem como exercitar a fase de esquecimento e exemplificar a recuperação dos níveis dos indicadores de confiança.

No gráfico inferior da Figura 6.2, observa-se que após o período de esquecimento (meses 13, 14 e 15), as curvas retornam aos valores anteriores ao evento catastrófico. Para simular o efeito de esquecimento, o parâmetro “m” é reduzido sucessivamente pela metade (1/2, 1/4, 1/8), nos 3 meses subsequentes. O Apêndice III apresenta uma tabela da simulação da avaliação de 18 meses contendo o conjunto completo de dados da simulação.



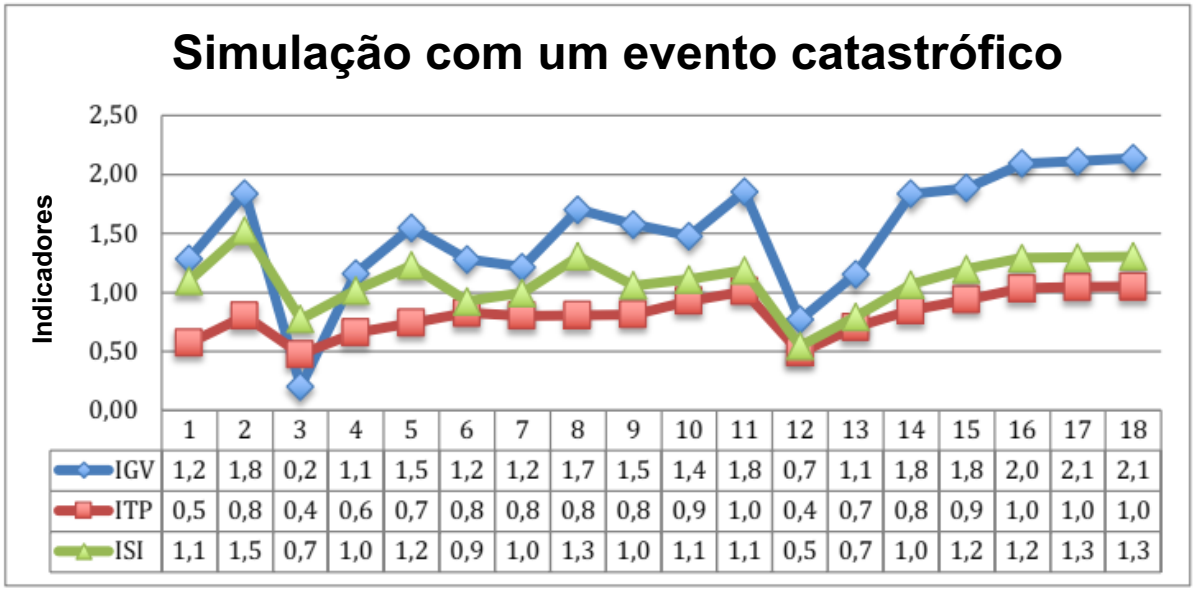


Figura 6.2 – Simulações de 18 meses, com e sem eventos catastróficos, adaptado de (Balcão Filho et al., 2023)

6.4 Conclusões sobre a Prova de Conceito

As entrevistas com os avaliadores revelaram algumas preocupações (por exemplo, onde encontrar as informações que ajudariam a responder o questionário). É difícil obter esse tipo de informação, pois na maioria das vezes elas não existem ou não estão disponíveis para os consumidores de serviços de Nuvem. Diversas questões estão relacionadas a aspectos do contrato, que nem sempre são acessíveis aos usuários finais.

O *framework* se mostrou de fácil aplicação e bastante intuitivo. A maior dificuldade está na obtenção e interpretação das informações. O modelo é sensível às variações e à dinâmica dos serviços de Nuvem. As diferenças entre os critérios de avaliação dos usuários foram reveladas. Também foi possível capturar e comparar as diferenças entre os CSPs.

Os avaliadores apontaram que algumas das 24 questões não são importantes, ou não dizem respeito aos usuários finais; portanto, essas questões não foram avaliadas, recebendo pontuação zero. Segue um exemplo de sugestão dos avaliadores: “Algumas questões poderiam ser respondidas por especialistas, que teriam a expertise para responder tais questões, bem como acesso às informações necessárias”.

A PoC realizada usando três serviços e diferentes avaliadores mostrou que o *framework* de avaliação de confiança pode avaliar de forma eficiente e eficaz a confiança depositada em um serviço de Nuvem. O modelo proposto é de fácil compreensão e fornece medidas relevantes e significativas de aspectos críticos de confiança para usuários de computação em nuvem.

O *framework* mostrou-se capaz de atender a diferentes aplicações, fornecidas por diferentes CSPs, e os avaliadores relataram as mesmas dificuldades na coleta de dados. O *framework* permite que os consumidores acompanhem a evolução da confiança e evidencie antecipadamente a deterioração dessa confiança.

O *framework* foi capaz de dar visibilidade à falta de informações críticas; sem essas informações, os consumidores são obrigados a acreditar nos CSPs. Há uma ênfase muito maior na disponibilidade do que no cuidado com a privacidade, confidencialidade e outros aspectos da governança contratual. Esses contratos são padronizados e não permitem adaptações. Em um mundo que exige cada vez mais cuidados com o ambiente computacional, não há informações sobre esses aspectos.

7 CONCLUSÃO

Os serviços de computação em nuvem formam um conjunto de sistemas interdependentes que se relacionam de modo a formar um todo organizado. Essa tecnologia está em desenvolvimento e não estão consolidadas as possibilidades de alcance dos sistemas.

Por essa razão, há todo um sistema desenvolvido de boas práticas, além da elaboração de regulamentos, normas e leis que orientam tanto a prestação dos serviços como a relação com os contratantes.

No entanto, o consumidor de serviços de Nuvem não tem condições de entender toda a complexidade dessa regulamentação. O usuário final abstrai-se de tudo isso e passa a confiar que o prestador do serviço atenderá a todos os requisitos necessários para a realização do contrato. Cada usuário tem necessidades diferentes entre si, mesmo quando contratam o mesmo tipo de serviço de um mesmo CSP. Para tanto, outra iniciativa necessária é a educação dos usuários para que entendam as práticas de segurança dos serviços de Nuvem e assim possam entender os benefícios e riscos associados ao uso desses serviços.

O desafio que está posto é como “medir” e “monitorar” a confiança de forma simples e factível, por usuários que estão cada vez mais distantes do entendimento de toda a tecnologia envolvida nos serviços que estão contratando. Para isso foi proposto o *framework* apresentado nesta tese.

Pelo disposto na NBR ISO/IEC 27001:2013 a Segurança da Informação deve incluir: a) confidencialidade (controle do acesso aos dados), b) integridade (fidedignidade das informações) e c) a disponibilidade da informação (manter a acessibilidade para quem de direito). São ainda exigidas outras características, tais como autenticidade (garantia de que a identidade declarada é verdadeira), privacidade (confidencialidade de dados pessoais) e resiliência (manutenção integral dos dados ainda que ocorram falhas no sistema).

A governança e a segurança das informações na Nuvem são uma exigência normativa e legal para os provedores e um direito dos clientes. No Brasil, o Marco Civil da Internet (Lei 12.965/2014), que estabelece os princípios, garantias, direitos e deveres para o uso da Internet é bastante recente. O Marco Civil veio depois

da Lei de Acesso à Informação (Lei 12.527/2011). A Lei 12.737/2012 trouxe uma ferramenta para tipificação dos crimes cibernéticos, alterando o código penal (Decreto-Lei 2.848/1940). A Lei 13.460/2017 visa a proteger a participação, proteção e defesa dos direitos do usuário dos serviços públicos. A Lei 13.853/2019 (LGPD) visa a proteção dos dados pessoais. Portanto, a legislação é bastante recente e ainda está em processo de debate e elaboração, conforme os problemas, as denúncias e as reclamações vão ocorrendo.

A transparência na Nuvem aumenta a confiança dos usuários. As empresas prestadoras de serviços podem fornecer informações detalhadas sobre as práticas de segurança e privacidade, incluindo relatórios de auditoria independentes, para fornecer aos usuários a garantia de que seus dados estão seguros.

Nesta tese, questões importantes para a avaliação da confiança nos serviços de computação em nuvem são abordadas, incluindo algumas questões cujas respostas são complexas e dependentes do contexto.

Métricas e indicadores permitem que os consumidores de serviços de computação em nuvem meçam sua confiança nos CSPs. É importante ressaltar que não foram encontrados na literatura científica métodos que utilizem indicadores para representar a confiança do consumidor em serviços de computação em nuvem.

O *framework* proposto fornece uma avaliação de confiança baseada no ponto de vista do consumidor final do serviço de Nuvem, que não precisa ser um especialista em segurança da informação. A estrutura proposta também é mais ampla do que outras encontradas na revisão bibliográfica, abrangendo as dimensões de Governança, Transparência e Informações de Segurança. Os resultados são expressos numérica e graficamente, melhorando a comunicação ao fornecer dados mais relevantes e significativos.

Para responder às questões motivadoras apresentadas no início do Capítulo 5, o *framework* é embasado em axiomas, num modelo de confiança e em critérios de avaliação baseados em boas práticas e literatura da área, além de indicadores.

Sob o domínio da Governança estão os critérios:

(a) projeto de segurança com os subcritérios: infraestrutura de segurança, contramedidas instaladas;

(b) recomendação com os subcritérios: auditoria de terceira parte e recomendação de especialista;

(c) reputação com o subcritério: avaliação média dos usuários;

(d) privacidade com os subcritérios: avaliação de impacto de privacidade e técnicas de anonimização.

Sob o domínio da Transparência estão os critérios:

a) revelar informações com o subcritério: divulgação obrigatória de informações de segurança;

b) divulgação de informações com os subcritérios: requisitos regulamentares, incidentes de segurança, atendimento ao cliente e relatórios;

c) comunicação periódica com os subcritérios: relatórios e avisos.

Sob o domínio das Informações de Segurança estão os critérios:

a) recursos com os subcritérios: recursos humanos, centro de operações de segurança, estrutura de governança e recursos tecnológicos;

b) certificações com o subcritério: normas técnicas;

c) garantias contratuais com os subcritérios: penalidades (SLA), reparação, desempenho (QoS, SLA) e cláusulas verdes.

O FTACSP é composto de:

a) conjunto de questões de avaliação, que está de acordo com os axiomas, confiança, segurança dos dados e boa reputação (Seção 5.1);

b) processo de engenharia, incluindo fórmulas para cálculo dos indicadores e escala em quatro etapas do planejamento (selecionar o alvo, identificar critérios de avaliação, definir o padrão de avaliação e selecionar e desenvolver a coleta de dados) (Seção 5.2);

c) diagrama esquemático, no modelo de confiança (Figura 5.2) fundamentado no modelo de Balcão Filho et. al. (2020);

d) catálogo de critérios, identificando as fontes de informação a serem consultadas conforme os critérios de Governança, Transparência e Informações de Segurança mencionados na (Tabela 5.2).

Os principais obstáculos para realizar as ações propostas no *framework* incluem a dificuldade de acesso aos dados de segurança dos sistemas de computação em nuvem e a dificuldade em identificar alternativas sistemáticas de relacionamento com o CSP.

Essa realidade está mudando, pois os consumidores exigem seus direitos como usuários e são protegidos pelas leis de proteção ao consumidor. Também é necessária uma maior regulamentação legal desses serviços para superar os obstáculos na comunicação com os provedores, bem como para garantir a notificação obrigatória de incidentes significativos para a segurança e confiança nos serviços contratados. A computação em nuvem é essencialmente um serviço e está sujeita às regras e regulamentos do mercado corporativo.

O *Security Trust Assurance and Risk* (STAR) da *Cloud Security Alliance* (CSA) e o *Cloud Security Command Center* (CSCC) do *Google Cloud Platform* (GCP) são exemplos de plataformas que facilitam o acesso às informações exigidas pelo *framework* proposto. O programa STAR oferece registros acessíveis ao público, permitindo que os clientes avaliem seus CSPs para tomar as melhores decisões. O CSCC é uma plataforma voltada ao gerenciamento de risco de segurança de dados para clientes do GCP.

Confiança é o resultado de um processo, ou seja, a conquista da confiança se desenvolve gradativamente. Estabelecer confiança é uma tarefa difícil, pois cresce lentamente e é fácil de se quebrar. Uma vez que a confiança é quebrada, é difícil restaurá-la.

A capacidade de medir a confiança deve ser de grande valor tanto para o progresso científico quanto para o conhecimento prático. Encontrar maneiras melhores e razoavelmente úteis de medir a confiança é um grande desafio.

Quando temos uma decisão complexa envolvendo Benefícios, Oportunidades, Custos e Riscos (BOCR), é necessário um *framework* para construir uma estrutura de decisão abrangente, com profundidade e mérito. A estrutura deve fornecer resultados valiosos para diferentes tipos de decisões e contextos.

A abordagem proposta nesta tese se mostra promissora, pois incorpora tendências e avaliações de diversos atores, além de comunicar resultados de forma simples, por meio de indicadores numéricos. Os indicadores propostos podem comunicar o progresso de segurança, confiabilidade e outros aspectos importantes de um serviço de Nuvem. O *framework* proposto é extensível, pois pode ser aplicado a outros contextos, como IoT, Edge Computing etc., por meio da definição de novos parâmetros de coleta e indicadores numéricos adequados aos novos domínios.

Por fim, a prova de conceito teve como objetivo validar o FTACSP. Avaliações de confiança de serviços de computação em nuvem foram executadas utilizando o *framework*. As principais questões relacionadas aos aspectos de confiança em serviços de Nuvem do mundo real foram identificadas e analisadas. A prova de conceito foi realizada em três serviços de computação em nuvem bem conhecidos.

Uma maior quantidade de avaliação de CSPs é necessária para o aprofundamento dos testes, pois é difícil extrapolar os dados obtidos para outros provedores, principalmente os de pequeno porte. Essa limitação também não permite tirar algumas conclusões, pois os avaliadores são diferentes para cada CSP, que por sua vez são diferentes entre si. Ficou evidente também a falta de preparação dos avaliadores para conduzir avaliações sistemáticas, pois estes nunca foram treinados para esse tipo de atividade ou se preocuparam em requisitar esses tipos de informação aos CSPs.

Os resultados da prova de conceito contribuem para o aprimoramento de modelos de avaliação de confiança para ambientes complexos, como Sistemas-de-Sistemas, por meio de uma abordagem que considera critérios tangíveis (e.g., disponibilidade) e intangíveis (e.g., confiança), além de aspectos sociotécnicos (e.g., vigilância ou monitoramento não autorizados).

A confiança dos consumidores nos serviços de Nuvem é altamente impactada pelos custos, responsabilidades e qualidade fornecidos pelos CSPs.

Ao avaliar sistemas complexos, os consumidores de serviços de Nuvem devem avaliar os aspectos de segurança e privacidade. Essa avaliação é complexa e requer uma equipe de especialistas em segurança. Consequentemente, a tarefa será cara, lenta e desatualizada quando estiver concluída. Nesse contexto, a melhor

abordagem pode ser primeiramente avaliar a confiança depositada no ambiente de computação em nuvem, e posteriormente testar ou avaliar as vulnerabilidades de segurança desse ambiente.

Indicadores de confiança foram propostos e aplicados para desvendar e mensurar as características de confiança dos CSPs de forma sistemática. Ao fazer uso dos indicadores, pôde-se perceber ao longo do tempo o progresso da segurança, confiabilidade, confiança e outros aspectos-chave dos CSPs sob avaliação. O *framework* proposto considera eventos catastróficos em seu cálculo.

O processo de aplicação do *framework* com seus indicadores, bem como cenários de aplicação do mundo real, são outras contribuições desta tese para a literatura científica.

Nesta tese, buscamos abordar problemas difíceis no contexto de confiança, como transparência de segurança, medição de níveis de serviço e processos de interpretação para tomada de decisão na perspectiva do consumidor de serviços de Nuvem. Um aprofundamento da pesquisa deve levar ao desenvolvimento de indicadores que melhor representem a qualidade dos CSPs. O FTACSP é destinado para os usuários de serviços de computação em nuvem que exigem alto nível de qualidade em seus sistemas e infraestruturas.

Também será importante incorporar outros recursos para automatizar a avaliação, incluindo a coleta automática de dados de segurança e privacidade dos CSPs.

7.1 Limitações e Trabalhos Futuros

Com respeito às limitações, como foram avaliados apenas três serviços, identificou se a dificuldade para extrapolar os dados obtidos para outros provedores. Essa limitação também não nos permitiu tirar algumas conclusões, pois os avaliadores são diferentes entre si e para cada CSP avaliado.

Ademais, o protótipo de software carece de aprimoramento de algumas características atuais (e.g., desenvolver a capacidade de coleta automática de dados dos CSPs), além de ser necessário o desenvolvimento de novas características que lhe proporcionem maior proatividade (e.g., possibilidade de criação e configuração de

alertas).

Pesquisas futuras podem levar ao desenvolvimento de indicadores que melhor representem a qualidade dos CSPs. Para isso, como trabalhos futuros, espera-se:

a) Estender e aplicar o *framework* e o estudo de caso propostos a outros contextos, tais como *Edge* e *Fog Computing*;

b) Aprimorar o protótipo FTACSP, automatizando o processo de coleta de dados de CSPs;

c) Aprimorar o questionário de avaliação;

d) Gerar alertas aos consumidores de serviços de Nuvem quando algum parâmetro ou indicador estiver fora da faixa de controle.

7.2 Resultados Técnico-científicos da Tese

Como resultados técnico-científicos desta tese, foram publicados 3 artigos científicos com CAPES QUALIS[39], além do desenvolvimento e registro no INPI do protótipo de software. Uma síntese dos resultados obtidos é apresentada a seguir.

ARTIGO CIENTÍFICO 1 (QUALIS A4)

Objetivo Principal: Mapeamento Sistemático da Literatura

Conferência: 16th IEEE International Conference on Computer Systems and Applications (AICCSA 2019) - (https://doi.org/10.17485/ijst/2016/v9i47/108685)

Título: A study on Trust Models in Cloud Computing

Resumo traduzido: A Segurança da Informação é uma agregação de esforços de pessoas, processos e tecnologia para ajudar as organizações a fornecer confidencialidade, integridade e disponibilidade em seus ativos de informação. Hoje em dia quase todos os serviços de tecnologia são fortemente dependentes da computação em nuvem em suas várias formas de modelos de serviço. Percebemos

[39] Link para maiores informações sobre o CAPES QUALIS: https://pgcomp.ufba.br/qual-o-qualis-de-uma-conferencia-ou-um-periodico

que existem pontos fracos nos serviços de Nuvem em relação a questões de desempenho, confiabilidade, segurança e privacidade, entre outras questões. Os consumidores de serviços de Nuvem não têm informações suficientes sobre essas questões, nem sobre conformidade com leis e regulamentos. Neste artigo, apresentamos um mapeamento abrangente de trabalhos que lidam com aspectos de confiança na Nuvem do ponto de vista do usuário. Nosso objetivo é identificar como os usuários ou consumidores de serviços em Nuvem medem a confiança nos serviços de computação em nuvem. Nossas principais contribuições são:

a) um estudo atualizado sobre o estado da arte dos modelos de confiança na Nuvem;

b) uma ontologia de características e contribuições para a confiança na Nuvem;

c) uma discussão sobre trabalhos que apresentam problemas difíceis de pesquisa sobre modelos de confiança na Nuvem e lacunas de contribuições na literatura.

ARTIGO CIENTÍFICO 2 (QUALIS B2)

Objetivo Principal: Apresentação da Proposta Conceitual

Conferência: *17th International Conference on Information Technology--New Generations (ITNG 2020)* - (https://doi.org/10.1007/978-3-030-43020-7_14)

Título: *A Consumer-centric Conceptual Framework for Trust Assessment in Cloud Computing*

Resumo traduzido: Os consumidores dependem fortemente de serviços de computação em nuvem seguros e confiáveis. No entanto, existem várias deficiências nos serviços de Nuvem, como as relativas a desempenho, segurança, confiança e privacidade, entre outras. Os consumidores de serviços de Nuvem não têm informações suficientes sobre essas questões críticas nem sobre conformidade com leis e regulamentos. Apresentamos uma estrutura conceitual para avaliação de confiança de ambientes de computação em nuvem. Nossa proposta é baseada em uma abordagem centrada no consumidor, pois lida com aspectos de confiança na Nuvem sob a perspectiva dos usuários finais. Para tanto, são propostas métricas e indicadores para permitir que os consumidores avaliem a confiança dos provedores

de serviços de Nuvem. Nossas contribuições são:

a) uma estrutura conceitual com indicadores e processo para avaliação de confiança;
b) uma ontologia leve de conceitos-chave de avaliação de confiança;
c) um cenário de aplicação para ilustrar a adequação prática da estrutura conceitual.

ARTIGO CIENTÍFICO 3 (QUALIS A1)

Objetivo Principal: Aplicação para Validação da Proposta Conceitual

Revista: *IEEE Transactions on Services Computing* (2021)

Título: *Applying a Consumer-centric Framework for Trust Assessment of Cloud Computing Service Providers* - (https://doi.org/10.1109/TSC.2021.3134125)

Resumo traduzido: Os consumidores de serviços de computação em nuvem não possuem informações confiáveis suficientes sobre características críticas de seus provedores, como desempenho, segurança, confiança e privacidade, conformidade com leis e regulamentos, entre outros. Nossa proposta aborda esses problemas apresentando uma estrutura de avaliação de confiança que integra três domínios: Governança, Transparência e Informações sobre Segurança. Nossa abordagem é centrada no consumidor e lida com aspectos de confiança da perspectiva do usuário final. Utilizamos Indicadores para comunicar os resultados, que visam representar a expressão de ciber-segurança, gerenciabilidade e transparência dos serviços avaliados. Este artigo inclui uma proposta de implementação, protótipo e prova de conceito, em que o *framework* foi aplicado em um cenário real e executado em uma simulação de uso de longo prazo (18 meses) para verificar sua aplicabilidade, sensibilidade e robustez. Nosso estudo é destinado a consumidores de computação em nuvem que buscam conhecer e medir níveis de segurança cibernética, proteção de privacidade, transparência de segurança e altos níveis de qualidade em seus serviços e infraestrutura.

PROTÓTIPO DE SOFTWARE

Objetivo Principal: Aplicação para Validação da Proposta Conceitual

Instituição: *INPI*

Título: Framework for Trust Assessment of Cloud Computing Service Providers (FTACSP) *Número do Processo*: 512021003192-0 (em 20/11/2021)

Resumo da Tecnologia:

Linguagem: Python

Campo de Aplicação: IF07-Ciênc Info (Sistema de Informação, Rede de Informação, Teoria da Informação, Fluxo de Informação)

Tipo de Programa: TC01 – Aplicações Técnico-Científicas

Código fonte do FTACSP (Versão 1.0): https://github.com/FTACSP/prototype

REFERÊNCIAS

Alabool, H., Kamil, A., Arshad, N., & Alarabiat, D. (2018). Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review. *Journal of Systems and Software*, *139*, 161–188. https://doi.org/10.1016/j.jss.2018.01.038

Alhanahnah, M., Bertok, P., & Tari, Z. (2017). Trusting cloud service providers: Trust phases and a taxonomy of trust factors. *IEEE Cloud Computing*, *4*(1), 44–54. https://doi.org/10.1109/MCC.2017.20

Alhanahnah, M., Bertok, P., Tari, Z., & Alouneh, S. (2018). Context-Aware Multifaceted Trust Framework For Evaluating Trustworthiness of Cloud Providers. *Future Generation Computer Systems*, *79*, 488–499. https://doi.org/10.1016/j.future.2017.09.071

Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From Security to Assurance in the Cloud: A Survey. *ACM Computing Surveys*, *48*(1), 2:1–2:50. https://doi.org/10.1145/2767005

Ardagna, C. A., Damiani, E., Asal, R., & Vu, Q. H. (2014). On the Management of Cloud Non-Functional Properties: The Cloud Transparency Toolkit. *Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2014)*, 14–17. https://doi.org/10.1109/NTMS.2014.6814039

Asadullah, A., Oyebisi Oyefolahan, I., Bawazir, M. A., & Hosseini, S. E. (2015). Factors influencing users' willingness to use cloud computing services: An empirical study. *Advances in Intelligent Systems and Computing*, *361*, 227–236. https://doi.org/10.1007/978-3-319-19024-2_23

Balcão Filho, Amândio, de Franco Rosa, F., Ruiz, R., Bonacin, R., & Jino, M. (2020). A Consumer-Centric Conceptual Framework for Trust Assessment in Cloud Computing. *Advances in Intelligent Systems and Computing*, *1134*, 95–104. https://doi.org/10.1007/978-3-030-43020-7_14

Balcão Filho, Amandio, Rosa, F. de F., Ruiz, R. de S., Bonacin, R., & Jino, M. (2019). A study on Trust Models in Cloud Computing. *16th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA).*, *2019-Novem*, 8. https://doi.org/10.17485/ijst/2016/v9i47/108685

Balcão Filho, Amandio, Ruiz, N., Rosa, F. de F., Bonacin, R., & Jino, M. (2023). Applying a Consumer-Centric Framework for Trust Assessment of Cloud Computing Service Providers. *IEEE Transactions on Services Computing*, *16*(1), 95–107. https://doi.org/10.1109/TSC.2021.3134125

Barabanov, R., Kowalski, S., & Yngstrom, L. (2011). Information Security Metrics: Research Directions. *Journal of Information System Security*, *11*, 1–16. http://www.diva-portal.org/smash/get/diva2:469569/FULLTEXT01.pdf

Bayuk, J. (2011). Cloud Security Metrics. *System of Systems Engineering (SoSE), 6th International Conference On*, 341–345. https://doi.org/10.1109/SYSOSE.2011.5966621

Bayuk, J., & Mostashari, A. (2013). Measuring systems security. *Systems Engineering*, *16*(1), 1–14. https://doi.org/10.1002/sys.21211

Becker, J., Heddier, M., Öksüz, A., & Knackstedt, R. (2014). The effect of providing visualizations in privacy policies on trust in data privacy and security. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *Chapter 3*, 3224–3233. https://doi.org/10.1109/HICSS.2014.399

Bernabe, J. B., Perez, G. M., & Skarmeta Gomez, A. F. (2015). Intercloud Trust and

Security Decision Support System: an Ontology-based Approach. *Journal of Grid Computing*, *13*(3), 425–456. https://doi.org/10.1007/s10723-015-9346-7

Biolchini, J., Mian, P. G., Candida, A., & Natali, C. (2005). Systematic Review in Software Engineering. *Engineering*, *679*(May), 165–176. https://doi.org/10.1007/978-3-540-70621-2

Branco, T., & Santos, H. (2016). What is Missing for Trust in the Cloud Computing? In ACM (Ed.), *Proceedings of the 2016 ACM SIGMIS Conference on Computers and People Research* (pp. 27–28). ACM Press. https://doi.org/10.1145/2890602.2890605

Branco, T. T., & Santos, H. (2015). A trust model for cloud computing environment. *3rd International Conference on Cloud Security and Management (ICCSM)*, *Cc*, 1–15. http://repositorium.sdum.uminho.pt/bitstream/1822/39207/1/2015-ICCSM-TrustModel4CCEnv.pdf

Carr, N. G. (2005). The End of Corporate Computing. *MITSloan Management Review*, *46*(3), 62–73. https://doi.org/821058931

Chrysikos, A., & Mcguire, S. (2018). *A Predictive Model for Risk and Trust Assessment in Cloud Computing: Taxonomy and Analysis for Attack Pattern Detection*. Springer International Publishing. https://doi.org/10.1007/978-3-319-92624-7

Colombo, R. T., Pessôa, M. S., Guerra, A. C., Balcão Filho, A., & Gomes, C. C. (2012). Prioritization of software security intangible attributes. *ACM SIGSOFT Software Engineering Notes*, *37*(6), 1–7. https://doi.org/10.1145/2382756.2382781

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293–314.

Eftekhar, S. M., Suryn, W., Roy, J., & Roy, H. (2018). Towards the Development of a Widely Accepted Cloud Trust Model. *Computing and Quality: SQM XXVI*, 73–94.

Emeakaroha, V. C., Fatema, K., Van Der Werff, L., Healy, P., Lynn, T., & Morrison, J. P. (2017). A Trust Label System for Communicating Trust in Cloud Services. *IEEE Transactions on Services Computing*, *10*(5), 689–700. https://doi.org/10.1109/TSC.2016.2553036

Franek, J., & Kresta, A. (2014). Judgment Scales and Consistency Measure in AHP. *Procedia Economics and Finance*, *12*(March), 164–173. https://doi.org/10.1016/s2212-5671(14)00332-3

Giddens, A. (1991). *The Consequences of Modernity*. Stanford University Press, CA.

Gupta, P., & Gupta, P. K. (2020). Trust Modeling in Cloud. *Trust & Fault in Multi Layered Cloud Computing Architecture*, 77–93.

Gupta, S., & Saini, A. K. (2021). An artificial intelligence based approach for managing risk of IT systems in adopting cloud. *International Journal of Information Technology*, *13*, 2515–2523.

Habib, S. M., Ries, S., Muhlhauser, M., & Varikkattu, P. (2014). Towards a trust management system for cloud computing marketplaces: Using CAIQ as a trust information source. *Security and Communication Networks*, *7*(11). https://doi.org/10.1002/sec.748

Harker, P. T., & Vargas, L. G. (1987). The Theory of Ratio Scale Estimation: Saaty's Analytic Hierarchy Process. *Management Science*, *33*(11), 1383–1403. https://doi.org/10.1287/mnsc.33.11.1383

Hasan, M. Z., Hussain, M. Z., Mubarak, Z., Siddiqui, A. A., Qureshi, A. M., & Ismail, I. (2023). Data security and Integrity in Cloud Computing. *2023 International Conference for Advancement in Technology (ICONAT)*, 1–5.

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *2*(1), 9. https://doi.org/10.1186/2192-113X-2-9

Jansen, W. (2009). Directions in Security Metrics Research. *National Institute of Standards and Technology*, *April*, 1–26. https://doi.org/10.6028/NIST.IR.7564

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975

Junejo, A. K., Jokhio, I. A., & Jan, T. (2022). A Multi-Dimensional and Multi-Factor Trust Computation Framework for Cloud Services. *Electronics*, *11*(13), 1932.

Kanwal, A., Masood, R., Shibli, M. A., & Mumtaz, R. (2015). Taxonomy for trust models in cloud computing. *Computer Journal*, *58*(4), 601–626. https://doi.org/10.1093/comjnl/bxu138

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(TR/SE-0401), 28. https://doi.org/10.1.1.122.3308

Lim, S. Y., Musa, O. Bin, Al-Rimy, B. A. S., & Almasri, A. (2022). Trust models for blockchain-based self-sovereign identity management: A survey and research directions. *Advances in Blockchain Technology for Cyber Physical Systems*, 277–302.

Lins, S., Schneider, S., & Sunyaev, A. (2018). Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. *IEEE Transactions on Cloud Computing*, *6*(3), 890–903. https://doi.org/10.1109/TCC.2016.2522411

Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., McDermid, J., & Gollmann, D. (1993). Towards Operational Measures of Computer Security. *Journal of Computer Security*, *2*, 211–229. http://openaccess.city.ac.uk/1633/

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and. *NIST Special Publication 500-292*, *292*(9), 35. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: Solutions and future directions. *Journal of Computing Science and Engineering*, *9*(3), 119–133. https://doi.org/10.5626/JCSE.2015.9.3.119

Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. (2016). Development of a cloud trust label: A delphi approach. *Journal of Computer Information Systems*, *56*(3), 185–193. https://doi.org/10.1080/08874417.2016.1153887

Maher, D. (2018). On Software Standards and Solutions for a Trusted Internet of Things. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 5666–5675. https://doi.org/10.24251/hicss.2018.710

Martin, K. (2017). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, *82*(September 2017), 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Mehraj, S., & Banday, M. T. (2022). A Dynamic Weighted Averaging Technique for Trust Assessment in Cloud Computing. *International Journal of Cloud Applications and Computing (IJCAC)*, *12*(1), 1–21.

Meixner, F., & Buettner, R. (2012). Trust as an Integral Part for Success of Cloud Computing. *ICIW 2012, The Seventh International Conference on Internet and Web Applications and Services*, *c*, 207–214. http://thinkmind.org/download.php?articleid=iciw_2012_7_30_20174

Mell, P., & Grance, T. (2011). *NIST SP 800-145 - The NIST Definition of Cloud Computing.* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Minayo, M. C. D. S. (2009). Construção de indicadores qualitativos para avaliação de mudanças. *Revista Brasileira de Educação Médica*, *33*(1), 83–91. https://doi.org/10.1590/S0100-55022009000500009

Nahid, G. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–607. http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Nicol, D. M., Huang, J., & Nicol, D. M. (2010). A formal-semantics-based calculus of trust. *IEEE Internet Computing*, *14*(5), 38–46. https://doi.org/10.1109/MIC.2010.83

Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. *Computer*, *49*(2), 34–45. https://doi.org/10.1109/MC.2016.57

Noor, T. H., Sheng, Q. Z., Ngu, A. H. H. H., Alfazi, A., & Law, J. (2013). Cloud Armor: A Platform for Credibility-Based Trust Management of Cloud Services. *Proceedings of the 22nd ACM International Conference on Information Knowledge Management*, 2509–2512. https://doi.org/10.1145/2505515.2508204

Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., & Ngu, A. H. H. (2016). CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services. *IEEE Transactions on Parallel and Distributed Systems*, *27*(2), 367–380. https://doi.org/10.1109/TPDS.2015.2408613

Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys*, *46*(1), 1–30. https://doi.org/10.1145/2522968.2522980

Ollaik, L. G., & Ziller, H. M. (2012). Concepções de validade em pesquisas qualitativas. *Educação e Pesquisa*, *38*(1), 229–241. https://doi.org/10.1590/S1517-97022012005000002

Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing* (pp. 3–42). Springer-Verlag. https://doi.org/10.1007/978-1-4471-4189-1_1

Rizvi, S., Karpinski, K., Kelly, B., & Walker, T. (2015). Utilizing Third Party Auditing to Manage Trust in the Cloud. *Procedia Computer Science*, *61*(January), 191–197. https://doi.org/10.1016/j.procs.2015.09.192

Rizvi, S., Ryoo, J., Kissell, J., & Aiken, B. (2015). A stakeholder-oriented assessment index for cloud security auditing. *Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication - IMCOM '15*, 1–7. https://doi.org/10.1145/2701126.2701226

Romanosky, S., Sharp, R., & Acquisti, A. (2010). Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal? *Workshop on Economics of Information Security*, 1–34.

Roy, A., & Patil, K. (2023). Framework for Cloud Security Initiatives in Small and Medium-Sized Enterprises. *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 444–449. https://doi.org/10.1109/InCACCT57535.2023.10141743

Ruiz, N., Shukla, P., & Kazemian, H. (2020). Privacy in The First Line of the First Code. *Science Magazine Online*. https://science.sciencemag.org/content/317/5842/1178/tab-e-letters

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Science*, *1*(1), 83–98.

https://www.researchgate.net/profile/Thomas_Saaty/publication/228628807_Decision_making_with_the_analytic_hierarchy_process/links/54a44ff10cf257a63607248a.pdf

Saaty, T. L., & Ergu, D. (2015). When is a Decision-Making Method Trustworthy? Criteria for Evaluating Multi-Criteria Decision-Making Methods. *International Journal of Information Technology & Decision Making*, *14*(06), 1171–1187. https://doi.org/10.1142/s021962201550025x

Schneier, B. (2012). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Wiley.

Shaikh, R., & Sasikumar, M. (2015). Trust Model for Measuring Security Strength of Cloud Computing Service. *Procedia Computer Science*, *45*, 380–389. https://doi.org/10.1016/j.procs.2015.03.165

Singh, S., & Sidhu, J. (2017). Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. *Future Generation Computer Systems*, *67*, 109–132. https://doi.org/10.1016/j.future.2016.07.013

Sujana J., A. J., M., G., R., V. R., & Revathi T. (2019). *Trust Model Based Scheduling of Stochastic Workflows in Cloud and Fog Computing*. Springer International Publishing. https://doi.org/10.1007/978-3-030-03359-0_2

Sun Microsystems, I. (2009). Building Customer Trust in Cloud Computing with Transparent Security. *Sun Micro White Paper*, *November*. https://issuu.com/dragonjar/docs/sun_-_cloud_computing

Whaiduzzaman, M., & Gani, A. (2013). Measuring Security for Cloud Service Provider : A Third Party Approach. *Electrical Information and Communication Technology (EICT), 2013 International Conference On*. https://doi.org/10.1109/EICT.2014.6777855

Xu Wu. (2018). Study on Trust Model for Multi-users in Cloud Computing. *International Journal of Network Security*, *20*(4), 674–682. https://pdfs.semanticscholar.org/c69a/11d63645ee42a4cc7f71c1eee20638ec82fa.pdf

APÊNDICE I – LISTA DE NORMAS SOBRE COMPUTAÇÃO EM NUVEM

Tabela I. 1 – Compêndio de Normas ABNT sobre Segurança da Informação Aplicáveis ao Contexto da Computação em Nuvem

Número	Título	Objetivo
ISO/IEC 27000:2018 (Obs.: Não há correspondente norma editada pela ABNT)	*Information technology - Security techniques – Information security management systems - Overview and vocabulary*	*Overview and vocabulary (ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards.*
NBR ISO/IEC 27001:2013 (idêntica a ISO/IEC 27001:2013)	Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos	Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
NBR ISO/IEC 27002:2013 (idêntica a ISO/IEC 27002:2013)	Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação	Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
NBR ISO/IEC 27003:2020 (idêntica a ISO/IEC 27003:2017)	Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Orientações	Este documento fornece explicações e orientações sobre a ABNT NBR ISO/IEC 27001:2013.
NBRISO/IEC 27004:2017 (idêntica a ISO/IEC 27004:2016)	Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação	Este documento fornece orientações que têm como objetivo auxiliar as organizações a avaliarem o desempenho da segurança da informação e a eficácia do SGSI a fim de atender aos requisitos da ABNT NBR ISO/IEC 27001:2013.
NBR ISO/IEC 27005:2019 (idêntica a ISO/IEC 27005:2018)	Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação	Este documento fornece diretrizes para o processo de gestão de riscos de segurança da informação.
NBR ISO/IEC 27007:2021 (idêntica a ISO/IEC 27007:2020)	Segurança da informação, segurança cibernética e proteção da privacidade - Diretrizes para auditoria de sistemas de gestão da segurança da informação	Este documento fornece orientações sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI), como executar as auditorias e a competência dos auditores de SGSI, em complemento às orientações descritas na ABNT NBR ISO 19011.

NBR ISO/IEC 17788:2015 (idêntica a ISO/IEC 17788:2014)	Tecnologia da informação - Computação em nuvem - Visão geral e vocabulário	Esta Recomendação | Norma fornece uma visão geral de computação em nuvem, juntamente com um conjunto de termos e definições. É uma fundação de terminologia para normas de computação em nuvem.
NBR ISO/IEC 27014:2021 (idêntica a ISO/IEC 27014:2020)	Segurança da informação, segurança cibernética e proteção da privacidade - Governança da segurança da informação.	Este Documento fornece orientação sobre conceitos, objetivos e processos para a governança da segurança da informação pela qual as organizações podem avaliar, direcionar, monitorar e comunicar as atividades relacionadas à segurança da informação dentro da organização.
NBRISO/IEC 27017:2016 (idêntica a ISO/IEC 27017:2015)	Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem	Esta Recomendação | Norma fornece diretrizes para os controles de segurança da informação aplicáveis à prestação e utilização de serviços em nuvem, fornecendo o seguinte: diretrizes adicionais para implementação de controles relevantes especificados na ABNT NBR ISO/IEC 27002; controles adicionais com diretrizes de implementação que são relacionadas especificamente a serviços em nuvem.
NBR ISO/IEC 27032:2015 (idêntica a ISO/IEC 27032:2012)	Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética	Esta Norma fornece diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.
NBR 16167:2020	Segurança da informação – Diretrizes para classificação, rotulação, tratamento e gestão da informação	Esta Norma estabelece as diretrizes para classificação, rotulação, tratamento e gestão da informação, de acordo com a sua sensibilidade e criticidade para a organização, visando o estabelecimento de níveis adequados de proteção.
NBR ISO/IEC 27035-3:2021 (idêntica a ISO/IEC 27035-3:2020)	Tecnologia da informação - Gestão de incidentes de segurança da informação Parte 3: Diretrizes para operações de resposta a incidentes de TIC	Este documento fornece diretrizes para resposta a incidentes de segurança da informação em operações de TIC. Este documento faz isso abrangendo os aspectos operacionais da segurança de TIC em uma perspectiva de pessoas, processos e tecnologia. Em seguida, concentra-se na resposta incluindo detecção, relatórios, triagem, análise, resposta, contenção, erradicação, recuperação e conclusão.

Tabela I. 2 – Compêndio de Normas ABNT sobre Privacidade Aplicáveis ao Contexto da Computação em Nuvem

Número	Título	Objetivo
NBR ISO/IEC 27018:2021 (idêntica a ISO/IEC 27018:2019)	Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.	Este documento estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteção de dados pessoais (DP), de acordo com os princípios de privacidade descritos na NBR ISO/IEC 29100, para o ambiente de computação em nuvem pública.
NBR ISO/IEC 27701:2019 Versão Corrigida 2020 (idêntica a ISO/IEC 27701:2019)	Técnicas de segurança - Extensão da NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes	Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.
NBR ISO/IEC 29100:2020 (idêntica a ISO/IEC 29100:2011/Amd 1:2018)	Tecnologia da informação - Técnicas de segurança - Estrutura de Privacidade	Esta Norma fornece uma estrutura de privacidade que: especifica uma terminologia comum de privacidade; especifica os atores e os seus papéis no tratamento de dados pessoais (DP); descreve considerações de salvaguarda de privacidade; e fornece referências para princípios conhecidos de privacidade para tecnologia da informação.
NBR ISO/IEC 29151:2020 (idêntica a ISO/IEC 29151:2017)	Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais	Esta Recomendação/Norma estabelece objetivos de controle, controles e diretrizes para implementar controles, para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de dados pessoais (DP).
NBR ISO/IEC 29134:2020 (idêntica a ISO/IEC 29134:2017)	Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade - Diretrizes	Este documento fornece diretrizes para: processos de avaliação de impacto de privacidade, e estrutura e conteúdo de relatório de PIA

Tabela I. 3 – Compêndio de Normas ITU-T sobre Computação em Nuvem

Y.3500	*Information technology - Cloud computing - Overview and vocabulary*
Y.3501	*Cloud computing - Framework and high-level requirements*
Y.3502	*Information technology - Cloud computing - Reference architecture*
Y.3503	*Requirements for desktop as a service*
Y.3504	*Functional architecture for Desktop as a Service*
Y.3505	*Cloud computing - Overview and functional requirements for data storage federation*
Y.3506	*Cloud computing - Functional requirements for cloud service brokerage*
Y.3507	*Cloud computing - Functional requirements of physical machine*
Y.3508	*Cloud computing - Overview and high-level requirements of distributed cloud*
Y.3509	*Cloud computing - Functional architecture for data storage federation*
Y.3510	*Cloud computing infrastructure requirements*
Y.3511	*Framework of inter-cloud computing*
Y.3512	*Cloud computing - Functional requirements of Network as a Service*
Y.3513	*Cloud computing - Functional requirements of Infrastructure as a Service*
Y.3514	*Cloud computing - Trusted inter-cloud computing framework and requirements*
Y.3515	*Cloud computing - Functional architecture of Network as a Service*
Y.3516	*Cloud computing - Functional architecture of inter-cloud computing*
Y.3517	*Cloud computing - Overview of inter-cloud trust management*
Y.3518	*Cloud computing - functional requirements of inter-cloud data management*
Y.3519	*Cloud computing - Functional architecture of big data as a service*
Y.3520	*Cloud computing framework for end to end resource management*
Y.3521	*Overview of end-to-end cloud computing management*
Y.3522	*End-to-end cloud service lifecycle management requirements*
Y.3523	*Metadata framework for NaaS service lifecycle management*
Y.3524	*Cloud computing maturity requirements and framework*
Y.3525	*Cloud computing - Requirements for cloud service development and operation management*
Y.3526	*Cloud computing - Functional requirements of edge cloud management*
Y.3527	*Cloud computing - End-to-end fault and performance management framework of network services in inter-cloud*
Y.3528	*Cloud computing - Framework and requirements of container management in inter-cloud*
Y.3529	*Cloud computing - Data model framework for NaaS OSS virtualized network function*
Y.3530	*Cloud computing - Functional requirements for blockchain as a service*
Y.3531	*Cloud computing - Functional requirements for machine learning as a service*

Y.3535	*Cloud computing - Functional requirements for a container*
Y.3536	*Cloud computing - Functional architecture for cloud service brokerage*
Y.Sup46	*ITU-T Y.3500-series - Requirements and challenges regarding provision and consumption of cloud computing services in developing countries*
Y.Sup47	*Information-centric networking - Overview, standardization gaps and proof-of-concept*
Y.Sup48	*Proof-of-concept for data service using information centric networking in IMT-2020*
Y.Sup49	*ITU-T Y.3500-series - Cloud computing standardization roadmap (https://www.itu.int/rec/T-REC-Y.Sup49-201811-I/en)*

APÊNDICE II – QUESTÕES USADAS PARA A AVALIAÇÃO DA NUVEM

Neste Apêndice, constam dois Quadros com as questões que são usadas para fazer a avaliação de confiança do serviço de Nuvem. No Quadro 1, estão as questões que foram utilizadas para a realização da Prova de Conceito apresentada na Seção 6. No Quadro 2, estão as mesmas questões, mas corrigidos os erros e melhoradas as redações das questões. Portanto, deve-se usar para as próximas avaliações as questões do Quadro 2.

Quadro 1 – Questões originais usadas na PoC

GOVERNANÇA	
Q1	Infraestrutura de Segurança
Como você avalia a infraestrutura de segurança? Obs: Qual sua percepção sobre a infraestrutura de segurança do provedor.	
0 - Não há informações sobre a infraestrutura de segurança. 1 - As informações fornecidas são insuficientes para avaliar. 2 - A infraestrutura de segurança é deficiente. 3 - A infraestrutura de segurança é adequada. 4 - A infraestrutura de segurança é completa.	
Q2	Contramedidas instaladas
Quais são os controles ou contramedidas de segurança instalados? Obs: Qual sua percepção sobre as contramedidas instaladas pelo provedor.	
0 - Não há informações sobre os controles ou contramedidas de segurança instalados. 1 - As informações fornecidas são insuficientes para avaliar. 2 - Os controles ou contramedidas de segurança instalados são deficientes. 3 - Os controles ou contramedidas de segurança instalados são adequados. 4 - Os controles ou contramedidas de segurança instalados são completos.	
Q3	Auditoria de Terceiros (TPA)
O provedor possui auditorias de terceira parte?	
0 - Não há informações sobre auditorias de terceira parte. 1 - As informações fornecidas pelas auditorias são insuficientes para avaliar. 2 - As informações fornecidas pelas auditorias revelam muitas deficiências. 3 - As informações fornecidas pelas auditorias revelam poucas deficiências. 4 - As informações fornecidas pelas auditorias não revelam deficiências.	
Q4	Recomendação de especialistas
Existem recomendações dos serviços desse provedor, realizadas por especialistas?	

0 - Não há informações sobre recomendações de especialistas. 1 - As informações disponíveis sobre recomendações de especialistas não recomendam os serviços. 2 - As informações disponíveis sobre recomendações de especialistas são neutras na recomendação dos serviços. 3 - As informações disponíveis sobre recomendações de especialistas recomendam os serviços. 4 - As informações disponíveis sobre recomendações de especialistas recomendam fortemente os serviços.
Q5 Avaliação Média dos Usuários
Existem avaliações dos serviços desse provedor, realizadas por usuários desses serviços?
0 - Não há informações sobre avaliações por usuários. 1 - As informações disponíveis sobre avaliações por usuários são insuficientes para formar opinião. 2 - Os usuários estão insatisfeitos com os serviços. 3 - Os usuários estão satisfeitos com os serviços. 4 - Os usuários estão muito satisfeitos com os serviços.
Q6 Avaliação de impacto de privacidade
O provedor realiza avaliação de impacto de privacidade? Obs. Avalie as informações do impacto de privacidade dos serviços oferecidos.
0 - Não há informações sobre avaliações de impacto de privacidade. 1 - As informações disponíveis sobre avaliações de impacto de privacidade são insuficientes para formar opinião. 2 - As avaliações de impacto de privacidade apontam deficiências. 3 - As avaliações de impacto de privacidade são adequadas. 4 - As avaliações de impacto de privacidade são muito satisfatórias
Q7 *Técnicas de anonimização*
O provedor informa quais técnicas de anonimização são utilizadas?
0 - Não há informações sobre quais técnicas de anonimização são utilizadas. 1 - As informações disponíveis sobre as técnicas de anonimização utilizadas são insuficientes para formar opinião 2 - As técnicas de anonimização utilizadas são insuficientes. 3 - As técnicas de anonimização utilizadas são adequadas. 4 - As técnicas de anonimização utilizadas são bastante satisfatórias.
TRANSPARÊNCIA
Q8 Divulgação de informações de segurança
Como você avalia as informações sobre informações de segurança divulgadas pelo provedor? Obs. Como você avalia, de modo geral, a transparência da segurança da informação do provedor.
0 - Não há informações de segurança divulgadas pelo provedor. 1- As informações de segurança divulgadas pelo provedor são insuficientes para avaliar. 2. As informações de segurança divulgadas pelo provedor são bastante limitadas. 3 - As informações de segurança divulgadas pelo provedor são adequadas. 4 - As informações de segurança divulgadas pelo provedor são abrangentes
Q9 Divulgação Obrigatória
Como você avalia as políticas de divulgação obrigatória do provedor? Obs. Avalie a política de divulgação obrigatória sobre vazamento de dados e roubo de identidade.

0 - Não há informações sobre as políticas de divulgação obrigatória do provedor. 1 - As informações sobre as políticas de divulgação obrigatória do provedor são insuficientes para avaliar. 2 - As políticas de divulgação obrigatória do provedor são bastante limitadas. 3 - As políticas de divulgação obrigatória do provedor são adequadas. 4 - As políticas de divulgação obrigatória do provedor são abrangentes.
Q10 Requisitos regulamentares
Como você avalia o atendimento pelo provedor aos requisitos regulatórios? Obs. Avalie o atendimento aos requisitos regulatórios, como: aprovações, licenças, registros, autorizações e outros requisitos aplicáveis em relação aos serviços contratados.
0 - Não há informações sobre o atendimento pelo provedor aos requisitos regulatórios. 1 - As informações sobre o atendimento pelo provedor aos requisitos regulatórios são insuficientes para avaliar. 2 - O atendimento pelo provedor aos requisitos regulatórios é bastante limitado. 3 - O atendimento pelo provedor aos requisitos regulatórios é adequado. 4 - O atendimento pelo provedor aos requisitos regulatórios é abrangente
Q11 Incidentes de segurança
Como você avalia as informações sobre incidentes de segurança divulgadas pelo provedor? Obs. Avalie as informações sobre qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação, vinculados aos serviços contratados pelo consumidor.
0 - Não há informações sobre incidentes de segurança divulgadas pelo provedor. 1 - As informações sobre incidentes de segurança divulgadas pelo provedor são insuficientes para avaliar. 2 - As informações sobre incidentes de segurança divulgadas pelo provedor são bastante limitadas. 3 - As informações sobre incidentes de segurança divulgadas pelo provedor são adequadas. 4 - As informações sobre incidentes de segurança divulgadas pelo provedor são abrangentes.
Q12 Atendimento ao Cliente
Como você avalia o atendimento ao cliente prestado pelo provedor? Obs. Avalie o atendimento e a prestação de serviços aos clientes.
0 - Não há informações sobre o atendimento ao cliente prestado pelo provedor. 1 - O atendimento ao cliente é totalmente inadequado. 2 - O atendimento ao cliente é pouco eficiente. 3 - O atendimento ao cliente é adequado. 4 - O atendimento ao cliente supera as expectativas.
Q13 Relatórios
Como você avalia os relatórios de segurança emitidos pelo provedor? Obs. Os relatórios de segurança devem incluir análises das tendências das ameaças, quais são os elementos mais frágeis, previsões de ameaças à segurança, recomendações de como se proteger.
0 - Não há informações sobre relatórios de segurança emitidos pelos provedores. 1 - Os relatórios de segurança emitidos pelos provedores são insuficientes para avaliar. 2 - Os relatórios de segurança emitidos pelos provedores são bastante limitados. 3 - Os relatórios de segurança emitidos pelos provedores são adequados. 4 - Os relatórios de segurança emitidos pelos provedores são abrangentes.
Q14 Avisos
Como você avalia os avisos de segurança emitidos pelo provedor? Obs. Os avisos de segurança devem incluir alertas sobre ameaças aos serviços contratados, ataques em andamento e medidas emergenciais a serem tomadas pelo consumidor.

0 - Não há informações sobre avisos de segurança emitidos pelo provedor. 1 - Os avisos de segurança emitidos pelo provedor são proforma. 2 - Os avisos de segurança emitidos pelo provedor são limitados. 3 - Os avisos de segurança emitidos pelo provedor são adequados. 4 - Os avisos de segurança emitidos pelo provedor são abrangentes.
INFORMAÇÕES DE SEGURANÇA
Q15 Recursos Humanos
Como você avalia as informações sobre a experiência dos recursos humanos envolvidos na segurança da informação? Obs. Avalie quesitos como: os Recursos Humanos são qualificados, têm certificações, têm muitos anos de experiência na área de segurança?
0 - Não há informações sobre os recursos humanos envolvidos. 1 - As informações fornecidas são insuficientes para avaliar os recursos humanos envolvidos. 2 - Os recursos humanos envolvidos têm pouca experiência. 3 - Os recursos humanos envolvidos têm boa experiência. 4 - Os recursos humanos envolvidos têm bastante experiência.
Q16 Centro de operações de segurança (SOC)
Como você avalia a plataforma de prestação de serviços de prevenção, detecção e reação a incidentes de segurança?
0 - Não há informações sobre SOC. 1 - As informações fornecidas são insuficientes para avaliar SOC. 2 - O SOC presta serviços insuficientes. 3 - O SOC presta serviços - adequados. 4 - O SOC presta serviços completos.
Q17 Estrutura de Governança
Como você avalia a estrutura de governança de TI do provedor? Obs. Avalie quesitos como: existem políticas e procedimentos estabelecidas, gestor de segurança, existe plano de contingência e de recuperação de desastre?
0 - Não há informações sobre a estrutura de governança de TI. 1 - As informações fornecidas são insuficientes para avaliar. 2 - A estrutura de governança de TI é deficiente. 3 - A estrutura governança de TI é adequada. 4 - A estrutura governança de TI é completa.
Q18 Recursos tecnológicos
Como você avalia as informações sobre os recursos tecnológicos de segurança utilizados pelo provedor? Obs. Avalie quesitos como: *Firewall*, antivírus, varredura de vulnerabilidades, atualização dos sistemas, isolamento de clientes, SSO com vários fatores, ferramentas ante DOS?
0 - Não há informações sobre os recursos tecnológicos de segurança envolvidos. 1 - As informações fornecidas são insuficientes para avaliar os recursos de segurança envolvidos. 2 - Os recursos de segurança envolvidos são bastante limitados. 3 - Os recursos de segurança envolvidos são adequados. 4 - Os recursos de segurança envolvidos são abrangentes.
Q19 Normas Técnicas
Como você avalia as informações sobre as certificações do provedor? Obs. Avalie se o provedor possui certificações, p. ex: ISO-27001, GDPR, STAR-CSA, ISO-27018, ITIL.

0 - Não há informações sobre as certificações de segurança do provedor. 1 - As informações fornecidas são insuficientes para avaliar as certificações de segurança do provedor. 2 - As certificações de segurança do provedor são incompletas. 3 - As certificações de segurança do provedor são adequadas. 4 - As certificações de segurança do provedor são abrangentes.
Q20 Seguro
Como você avalia as cláusulas de seguro do contrato dos serviços? Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?
0 - Não há cláusulas de seguro estabelecida. 1 - O valor é irrisório. 2 - O valor é baixo. 3 - O valor é razoável. 4 - O valor é adequado.
Q21 Penalidade (SLA - *Service Level Agreement*)
Como você avalia as cláusulas de penalidades por descumprir parâmetros do SLA? Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?
0 - Não há cláusulas de penalidade estabelecida. 1 - Multa de >= a 5% e < 10% do valor do serviço. 2 - Multa de >= a 10% e < 15% do valor do serviço. 3 - Multa de >= a 15% e < 20% do valor do serviço. 4 - Multa >= a 20% do valor do serviço.
Q22 Reparação
Como você avalia as cláusulas de reparação aos incidentes que causaram prejuízo? Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?
0 - Não há cláusulas de reparação estabelecida. 1 - O valor é irrisório. 2 - O valor é baixo. 3 - O valor é razoável. 4 - O valor é adequado.
Q23 Desempenho (QoS, SLA)
Como você avalia o nível de serviço (disponibilidade/uptime) Obs. Avalie se o SLA/QoS são atendidos.
0 - Não há *uptime* estabelecido 1 - Cumpriu 70% com o *uptime* estabelecido 2 - Cumpriu 80% com o *uptime* estabelecido 3 - Cumpriu 90% com o *uptime* estabelecido 4 - Cumpriu 100% com o *uptime* estabelecido
Q24 Cláusulas Verde
Como você avalia as cláusulas de TI eficiente em energia do serviço contratado? Obs. Avalie se existe cláusula de TI eficiente em energia e como ela é atendida.
0 - Não há cláusula verde estabelecida 1 - A cláusula verde é proforma. 2 - A cláusula verde é limitada. 3 - A cláusula verde é adequada. 4 - A cláusula verde é abrangente.

Quadro 2 – Questões corrigidas e redação melhorada

GOVERNANÇA	
Q1	Infraestrutura de Segurança
Como você avalia a infraestrutura de segurança? Obs: Qual sua percepção sobre a infraestrutura de segurança do provedor.	
0 - Não há informações sobre a infraestrutura de segurança. 1 - As informações fornecidas são insuficientes para avaliar. 2 - A infraestrutura de segurança é deficiente. 3 - A infraestrutura de segurança é adequada. 4 - A infraestrutura de segurança é completa.	
Q2	Contramedidas instaladas
Controles ou contramedidas de segurança instalados? Obs: Qual sua percepção sobre as contramedidas instaladas pelo provedor.	
0 - Não há informações sobre os controles ou contramedidas de segurança instalados. 1 - As informações fornecidas são insuficientes para avaliar. 2 - Os controles ou contramedidas de segurança instalados são deficientes. 3 - Os controles ou contramedidas de segurança instalados são adequados. 4 - Os controles ou contramedidas de segurança instalados são completos.	
Q3	Auditoria de Terceiros (TPA)
O provedor possui auditorias de terceira parte?	
0 - Não há informações sobre auditorias de terceira parte. 1 - As informações fornecidas pelas auditorias são insuficientes para avaliar. 2 - As informações fornecidas pelas auditorias revelam muitas deficiências. 3 - As informações fornecidas pelas auditorias revelam poucas deficiências. 4 - As informações fornecidas pelas auditorias não revelam deficiências.	
Q4	Recomendação de especialistas
Existem recomendações dos serviços desse provedor, realizadas por especialistas?	
0 - Não há informações sobre recomendações de especialistas. 1 - As informações disponíveis sobre recomendações de especialistas não recomendam os serviços. 2 - As informações disponíveis sobre recomendações de especialistas são neutras na recomendação dos serviços. 3 - As informações disponíveis sobre recomendações de especialistas recomendam os serviços. 4 - As informações disponíveis sobre recomendações de especialistas recomendam fortemente os serviços.	
Q5	Avaliação Média dos Usuários
Existem avaliações dos serviços desse provedor, realizadas por usuários desses serviços?	
0 - Não há informações sobre avaliações por usuários. 1 - As informações disponíveis sobre avaliações por usuários são insuficientes para formar opinião. 2 - Os usuários estão insatisfeitos com os serviços. 3 - Os usuários estão satisfeitos com os serviços. 4 - Os usuários estão muito satisfeitos com os serviços.	
Q6	Avaliação de impacto de privacidade
O provedor realiza avaliação de impacto de privacidade? Obs. Avalie as informações do impacto de privacidade dos serviços oferecidos.	

0 - Não há informações sobre avaliações de impacto de privacidade. 1 - As informações disponíveis sobre avaliações de impacto de privacidade são insuficientes para formar opinião. 2 - As avaliações de impacto de privacidade apontam deficiências. 3 - As avaliações de impacto de privacidade são adequadas. 4 - As avaliações de impacto de privacidade são muito satisfatórias	
Q7	*Técnicas de anonimização*
O provedor informa quais técnicas de anonimização são utilizadas?	
0 - Não há informações sobre quais técnicas de anonimização são utilizadas. 1 - As informações disponíveis sobre as técnicas de anonimização utilizadas são insuficientes para formar opinião 2 - As técnicas de anonimização utilizadas são insuficientes. 3 - As técnicas de anonimização utilizadas são adequadas. 4 - As técnicas de anonimização utilizadas são bastante satisfatórias.	
TRANSPARÊNCIA	
Q8	Divulgação de informações de segurança
Como você avalia as informações sobre informações de segurança divulgadas pelo provedor? Obs. Como você avalia, de modo geral, a transparência da segurança da informação do provedor.	
0 - Não há informações de segurança divulgadas pelo provedor. 1- As informações de segurança divulgadas pelo provedor são insuficientes para avaliar. 2. As informações de segurança divulgadas pelo provedor são bastante limitadas. 3 - As informações de segurança divulgadas pelo provedor são adequadas. 4 - As informações de segurança divulgadas pelo provedor são abrangentes	
Q9	Divulgação Obrigatória
Como você avalia as políticas de divulgação obrigatória do provedor? Obs. Avalie a política de divulgação obrigatória sobre vazamento de dados e roubo de identidade.	
0 - Não há informações sobre as políticas de divulgação obrigatória do provedor. 1 - As informações sobre as políticas de divulgação obrigatória do provedor são insuficientes para avaliar. 2 - As políticas de divulgação obrigatória do provedor são bastante limitadas. 3 - As políticas de divulgação obrigatória do provedor são adequadas. 4 - As políticas de divulgação obrigatória do provedor são abrangentes.	
Q10	Requisitos regulamentares
Como você avalia o atendimento pelo provedor aos requisitos regulatórios? Obs. Avalie o atendimento aos requisitos regulatórios, como: aprovações, licenças, registros, autorizações e outros requisitos aplicáveis em relação aos serviços contratados.	
0 - Não há informações sobre o atendimento pelo provedor aos requisitos regulatórios. 1 - As informações sobre o atendimento pelo provedor aos requisitos regulatórios são insuficientes para avaliar. 2 - O atendimento pelo provedor aos requisitos regulatórios é bastante limitado. 3 - O atendimento pelo provedor aos requisitos regulatórios é adequado. 4 - O atendimento pelo provedor aos requisitos regulatórios é abrangente	
Q11	Incidentes de segurança
Como você avalia as informações sobre incidentes de segurança divulgadas pelo provedor? Obs. Avalie as informações sobre qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação, vinculados aos serviços contratados pelo consumidor.	

0 - Não há informações sobre incidentes de segurança divulgadas pelo provedor. 1 - As informações sobre incidentes de segurança divulgadas pelo provedor são insuficientes para avaliar. 2 - As informações sobre incidentes de segurança divulgadas pelo provedor são bastante limitadas. 3 - As informações sobre incidentes de segurança divulgadas pelo provedor são adequadas. 4 - As informações sobre incidentes de segurança divulgadas pelo provedor são abrangentes.	
Q12	Atendimento ao Cliente
Como você avalia o atendimento ao cliente prestado pelo provedor? Obs. Avalie o atendimento e a prestação de serviços aos clientes.	
0 - Não há informações sobre o atendimento ao cliente prestado pelo provedor. 1 - O atendimento ao cliente é totalmente inadequado. 2 - O atendimento ao cliente é pouco eficiente. 3 - O atendimento ao cliente é adequado. 4 - O atendimento ao cliente supera as expectativas.	
Q13	Relatórios
Como você avalia os relatórios de segurança emitidos pelo provedor? Obs. Os relatórios de segurança devem incluir análises das tendências das ameaças, quais são os elementos mais frágeis, previsões de ameaças à segurança, recomendações de como se proteger.	
0 - Não há informações sobre relatórios de segurança emitidos pelos provedores. 1 - Os relatórios de segurança emitidos pelos provedores são insuficientes para avaliar. 2 - Os relatórios de segurança emitidos pelos provedores são bastante limitados. 3 - Os relatórios de segurança emitidos pelos provedores são adequados. 4 - Os relatórios de segurança emitidos pelos provedores são abrangentes.	
Q14	Avisos
Como você avalia os avisos de segurança emitidos pelo provedor? Obs. Os avisos de segurança devem incluir alertas sobre ameaças aos serviços contratados, ataques em andamento e medidas emergenciais a serem tomadas pelo consumidor.	
0 - Não há informações sobre avisos de segurança emitidos pelo provedor. 1 - Os avisos de segurança emitidos pelo provedor são proforma. 2 - Os avisos de segurança emitidos pelo provedor são limitados. 3 - Os avisos de segurança emitidos pelo provedor são adequados. 4 - Os avisos de segurança emitidos pelo provedor são abrangentes.	
INFORMAÇÕES DE SEGURANÇA	
Q15	Recursos Humanos
Como você avalia as informações sobre a experiência dos recursos humanos envolvidos na segurança da informação? Obs. Avalie quesitos como: os Recursos Humanos são qualificados, têm certificações, têm muitos anos de experiência na área de segurança?	
0 - Não há informações sobre os recursos humanos envolvidos. 1 - As informações fornecidas são insuficientes para avaliar os recursos humanos envolvidos. 2 - Os recursos humanos envolvidos têm pouca experiência. 3 - Os recursos humanos envolvidos têm boa experiência. 4 - Os recursos humanos envolvidos têm bastante experiência.	
Q16	Centro de operações de segurança (SOC)
Como você avalia a plataforma de prestação de serviços de prevenção, detecção e reação a incidentes de segurança?	

0 - Não há informações sobre SOC. 1 - As informações fornecidas são insuficientes para avaliar SOC. 2 - O SOC presta serviços insuficientes. 3 - O SOC presta serviços - adequados. 4 - O SOC presta serviços completos.
Q17 Estrutura de Governança
Estrutura de governança de TI do provedor. Obs. Avalie quesitos como: existem políticas e procedimentos estabelecidas, gestor de segurança, existe plano de contingência e de recuperação de desastre?
0 - Não há informações sobre a estrutura de governança de TI. 1 - As informações fornecidas são insuficientes para avaliar. 2 - A estrutura de governança de TI é deficiente. 3 - A estrutura governança de TI é adequada. 4 - A estrutura governança de TI é completa.
Q18 Recursos tecnológicos
Informações sobre os recursos tecnológicos de segurança utilizados pelo provedor. Obs. Avalie quesitos como: *Firewall*, antivírus, varredura de vulnerabilidades, atualização dos sistemas, isolamento de clientes, SSO com vários fatores, ferramentas ante DOS?
0 - Não há informações sobre os recursos tecnológicos de segurança envolvidos. 1 - As informações fornecidas são insuficientes para avaliar os recursos de segurança envolvidos. 2 - Os recursos de segurança envolvidos são bastante limitados. 3 - Os recursos de segurança envolvidos são adequados. 4 - Os recursos de segurança envolvidos são abrangentes.
Q19 Normas Técnicas
Informações sobre as certificações do provedor. Obs. Avalie se o provedor possui certificações, p. ex: ISO-27001, GDPR, STAR-CSA, ISO-27018, ITIL.
0 - Não há informações sobre as certificações de segurança do provedor. 1 - As informações fornecidas são insuficientes para avaliar as certificações de segurança do provedor. 2 - As certificações de segurança do provedor são incompletas. 3 - As certificações de segurança do provedor são adequadas. 4 - As certificações de segurança do provedor são abrangentes.
Q20 Seguro
Cláusulas de seguro do contrato dos serviços. Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?
0 - Não há cláusulas de seguro estabelecida. 1 - O valor é irrisório. 2 - O valor é baixo. 3 - O valor é razoável. 4 - O valor é adequado.
Q21 Penalidades (SLA - *Service Level Agreement*)
Penalidades por descumprir parâmetros do SLA. Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?

0 - Não há cláusulas de penalidade estabelecida. 1 - Multa de >= a 5% e < 10% do valor do serviço. 2 - Multa de >= a 10% e < 15% do valor do serviço. 3 - Multa de >= a 15% e < 20% do valor do serviço. 4 - Multa >= a 20% do valor do serviço.
Q22 Reparação
Reparação aos incidentes que causaram prejuízo. Obs. Avalie quesitos como: o contrato especifica parâmetros e valores?
0 - Não há cláusulas de reparação estabelecida. 1 - O valor é irrisório. 2 - O valor é baixo. 3 - O valor é razoável. 4 - O valor é adequado.
Q23 Desempenho (QoS, SLA)
Nível de serviço (disponibilidade/uptime) Obs. Avalie se o SLA/QoS são atendidos.
0 - Não há *uptime* estabelecido 1 - Cumpriu 70% com o *uptime* estabelecido 2 - Cumpriu 80% com o *uptime* estabelecido 3 - Cumpriu 90% com o *uptime* estabelecido 4 - Cumpriu 100% com o *uptime* estabelecido
Q24 Cláusulas Verde
Como você avalia as cláusulas de TI eficiente em energia do serviço contratado? Obs. Avalie se existe cláusula de TI eficiente em energia e como ela é atendida.
0 - Não há cláusula verde estabelecida 1 - A cláusula verde é proforma. 2 - A cláusula verde é limitada. 3 - A cláusula verde é adequada. 4 - A cláusula verde é abrangente.

APÊNDICE III – TABELA DA AVALIAÇÃO SIMULADA DE 18 MESES

Abaixo estão os dados utilizados para simular uma avaliação de 18 meses, com e sem evento catastrófico - parâmetro “m”

Mês	Questões																							m
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	2	2	1	0	0	2	2	1	0	0	0	2	0	1	2	2	2	2	0	0	0	0	3	0	0
2	3	3	1	2	1	3	3	3	0	0	0	4	0	0	4	4	3	4	0	0	0	0	4	0	0
3	2	2	0	0	0	0	0	0	0	0	0	4	0	1	2	2	3	2	0	0	0	0	3	0	0
4	1	2	2	0	0	2	2	1	0	0	0	4	0	1	2	3	3	2	0	0	0	0	3	0	0
5	1	3	2	1	1	3	3	1	0	0	0	4	0	2	2	3	3	4	0	0	0	0	4	0	0
6	1	2	2	1	1	3	3	2	0	0	0	4	0	2	2	3	3	2	0	0	0	0	3	0	0
7	2	2	2	1	1	2	2	2	0	0	0	4	0	2	2	3	3	2	0	0	0	0	3	0	0
8	2	3	2	1	2	3	3	2	0	0	0	4	0	2	3	3	4	3	0	0	0	0	4	0	0
9	2	2	2	2	2	3	3	2	0	0	0	4	0	2	2	3	4	3	0	0	0	0	3	0	0
10	2	2	3	2	2	2	2	2	0	0	0	4	0	3	2	3	4	3	0	0	0	0	3	0	0
11	2	3	3	2	2	3	3	3	0	0	0	4	0	3	2	3	4	3	0	0	0	0	4	0	0
12	1	2	3	2	2	3	3	3	0	0	0	4	0	3	2	3	4	3	0	0	0	0	3	0	1
13	2	2	3	3	2	2	2	3	0	0	0	4	0	3	2	3	4	3	0	0	0	0	3	0	1/2
14	3	3	3	3	3	3	3	3	0	0	0	4	0	3	3	3	4	3	0	0	0	0	4	0	1/4
15	3	3	3	3	3	3	3	3	0	0	0	4	0	3	3	4	4	3	0	0	0	0	4	0	1/8
16	3	3	3	3	3	3	3	3	0	0	0	4	0	3	3	3	4	3	0	0	0	0	4	0	0
17	3	3	3	3	3	3	3	3	0	0	0	4	0	3	3	4	4	3	0	0	0	0	4	0	0
18	3	3	3	3	3	3	3	3	0	0	0	4	0	3	3	4	4	4	0	0	0	0	4	0	0