



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

SAYONARA RAISSA VICENTE ALVES

**COMPUTAÇÃO EM NUVEM E A LEI GERAL DE PROTEÇÃO DE DADOS: uma
revisão da literatura**

PEDRO II, PI

2025

SAYONARA RAISSA VICENTE ALVES

COMPUTAÇÃO EM NUVEM E A LEI GERAL DE PROTEÇÃO DE DADOS: uma
revisão da literatura

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Prof. Esp. Willyams Moreira Saraiva.

PEDRO II, PI

2025

COMPUTAÇÃO EM NUVEM E A LEI GERAL DE PROTEÇÃO DE DADOS: uma revisão da literatura

Sayonara Raissa Vicente Alves¹
Willyams Moreira Saraiva²

RESUMO

A crescente adoção da computação em nuvem por organizações brasileiras tem intensificado os debates sobre os desafios de conformidade com a Lei Geral de Proteção de Dados (LGPD). Neste contexto, este trabalho realiza uma revisão da literatura com o objetivo de investigar as principais barreiras e estratégias propostas para a adequação da computação em nuvem às exigências legais. A partir de critérios metodológicos definidos, foram selecionados 10 artigos publicados entre 2020 e 2025, extraídos das bases IEEE Xplore e Scopus, que discutem aspectos como segurança da informação, privacidade desde o design, governança organizacional e mecanismos de conformidade. Os resultados trazem que a conformidade com a LGPD em ambientes de nuvem envolve obstáculos técnicos, jurídicos e institucionais, relacionados à localização de dados, contratos com provedores e cultura organizacional. Portanto, esta revisão pretende contribuir ao organizar e sintetizar os conhecimentos sobre o tema, evidenciando lacunas e pretendendo subsidiar futuras pesquisas.

Palavras-chave: Computação em Nuvem; LGPD; Proteção de Dados; Segurança.

ABSTRACT

The growing adoption of cloud computing by Brazilian organizations has intensified debates about the challenges of compliance with the General Data Protection Law (LGPD). In this context, this paper conducts a literature review to investigate the main barriers and proposed strategies for adapting cloud computing to legal issues. Based on defined methodological criteria, 10 articles published between 2020 and 2025 were selected, extracted from the IEEE Xplore and Scopus databases, which discuss aspects such as information security, privacy by design, organizational governance, and compliance mechanisms. The results show that compliance with the LGPD in cloud environments involves technical, legal, and institutional obstacles related to data location, contracts with providers, and organizational culture. Therefore, this review aims to contribute by organizing and synthesizing knowledge on the topic, highlighting gaps and aiming to inform future research.

Keywords: Cloud Computing; LGPD; Data Protection; Security.

Data de aprovação: 22/07/2025 (data de apresentação do TCC)

¹ Graduação em Análise e Desenvolvimento de Sistemas. IFPI. Sayonararaissa95@gmail.com

² Especialização em Governança de TI. IFPI. Willyams.saraiva@ifpi.edu.br

1 INTRODUÇÃO

No cenário atual, a transformação digital tem impulsionado empresas e startups a evoluírem com o mercado tecnológico, promovendo mais eficiência, escalabilidade e alinhamento às novas demandas do consumidor (Silva, 2019). Entende-se por *startups* negócios inovadores em estágio inicial, geralmente voltados à criação com alto potencial de crescimento e uso intensivo de tecnologia (Lee *et al.*, 2025).

Computação em nuvem é um modelo de processamento no qual recursos como armazenamento, servidores e *softwares* são gerenciados de maneira centralizada e disponibilizados aos usuários conforme a necessidade, como um serviço sob demanda (Chee; Franklin Junior, 2010). Nesse contexto, a computação em nuvem surge como uma aliada estratégica, ao permitir a redução de custos com infraestrutura física, o redirecionamento de recursos para o desenvolvimento de produtos e a ampliação da escalabilidade e mobilidade organizacional (Silva, 2019).

De acordo com Mell e Grance (2011), esse modelo tecnológico reduz a dependência de recursos locais, ao transferir o processamento de dados para servidores remotos. Isso elimina a necessidade de instalação de sistemas no ambiente do usuário, tornando o acesso mais simples e prático por meio de navegadores *web*.

Apesar desses benefícios, parte do setor corporativo ainda demonstra resistência quanto à adoção de soluções em nuvem. Uma pesquisa realizada em 2024 (Paloalto Networks, 2024) revelou que, embora mais de 60% das organizações brasileiras tenham investido em computação em nuvem, 44% delas ainda têm receios em relação à segurança da informação.

Como reforçam István, Ponnappalli e Chidambaram (2020), a adequação jurídica em ambientes de nuvem demanda soluções técnicas que integrem os princípios legais às camadas operacionais da infraestrutura. A ausência de mecanismos nativos de conformidade configura um obstáculo relevante, indicando a necessidade de abordagens que aliem tecnologia e legislação de forma mais direta, acessível e eficaz.

Essa preocupação torna-se ainda mais relevante com a vigência da Lei Geral de Proteção de Dados nº 13.709/2018, que estabelece regras rigorosas para o tratamento e a proteção de dados pessoais (Brasil, 2018). Em especial, ambientes

digitais e transnacionais, como os serviços de computação em nuvem, que exigem atenção redobrada quanto ao cumprimento dessas exigências legais.

Nesse contexto, este trabalho propõe uma revisão da literatura com o objetivo de investigar a relação entre a computação em nuvem e a Lei Geral de Proteção de Dados (2018). A proposta é compreender, a partir de diferentes perspectivas, como essa tecnologia tem sido abordada no contexto da legislação brasileira.

A seleção dos trabalhos seguiu critérios metodológicos bem definidos, priorizando fontes científicas confiáveis e atualizadas. A importância deste estudo está na necessidade de apoiar organizações que adotam soluções em nuvem, para que essa transição ocorra de forma consciente, segura e em conformidade com a LGPD (Brasil, 2018). Ao reunir e organizar os principais achados sobre o tema, esta pesquisa oferece uma base informativa que pode contribuir para decisões mais responsáveis no uso da computação em nuvem no Brasil.

1.1 Objetivo geral

Avaliar, por meio de uma revisão da literatura, a relação entre a computação em nuvem e os princípios e exigências estabelecidos pela LGPD (2018).

1.2 Objetivos específicos

- Compreender os principais aspectos da computação em nuvem.
- Avaliar exigências da LGPD (2018) aplicáveis à computação em nuvem.
- Verificar a relação da computação em nuvem com a LGPD (2018).
- Apontar desafios e limitações na aplicação da LGPD (2018) na computação em nuvem.
- Sugerir possibilidades de adequação e estudos futuros.

Organização do trabalho: A Seção 1 - Introdução, A Seção 2 - Fundamentação teórica. A Seção 3 - Metodologia , Seção 4 - Resultados e discussões, Seção 5 - Conclusão e trabalhos futuros.

2 REFERENCIAL TEÓRICO

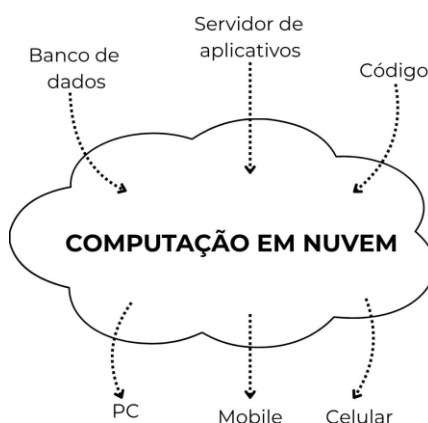
Esta seção contempla os principais conceitos acerca do referencial teórico, necessários para o entendimento e desenvolvimentos de tópicos importantes abordados no trabalho.

2.1 Computação em nuvem

De acordo com a definição apresentada pela *Amazon Web Services (AWS)*, empresa líder mundial em serviços de computação em nuvem, a computação em nuvem pode ser compreendida como a oferta, sob demanda, de recursos de tecnologia da informação por meio da internet, incluindo capacidade de processamento, armazenamento de dados, aplicações e outros serviços correlatos. Essa oferta é disponibilizada conforme a necessidade do usuário, em um modelo de precificação baseado no consumo efetivo dos recursos utilizados (AWS, 2019).

Complementando essa concepção, o *National Institute of Standards and Technology (NIST)*, instituição norte-americana de referência internacional na formulação de padrões e diretrizes técnicas, caracteriza a computação em nuvem como um modelo que permite acesso ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos computacionais configuráveis. Como redes, servidores, armazenamento, aplicações e serviços, que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor (Mell; Grance, 2011).

Figura 1: Estrutura básica da computação em nuvem.



Fonte: Elaborado pelo autor.

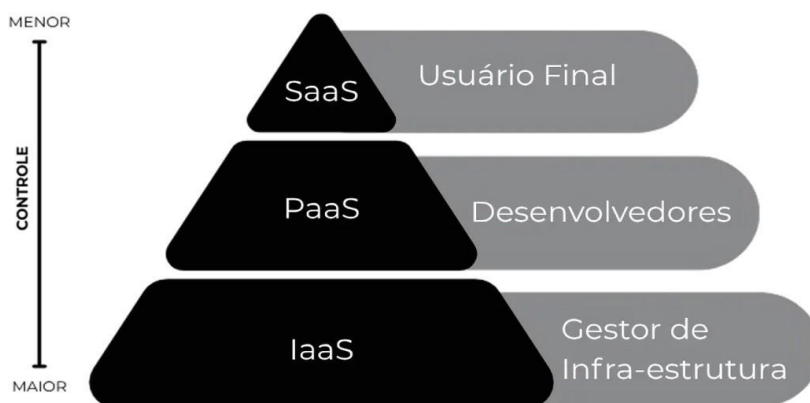
Diante desse contexto, a computação em nuvem configura-se como uma alternativa eficiente para otimizar e flexibilizar o uso de recursos computacionais, em virtude da diversidade de serviços oferecidos pelos provedores. De acordo com Buyya, Yeo e Venugopal (2008), tais serviços incluem, por exemplo, o armazenamento de dados, o desenvolvimento de aplicações personalizadas e a gestão de infraestrutura. Além disso, conforme os autores, cada elemento dessa infraestrutura é disponibilizado como um serviço, sendo usualmente hospedado em centros de dados que utilizam *hardware* compartilhado tanto para operações de computação quanto para armazenamento.

2.1.1 Modelos de serviços

Os autores Sousa, Moreira e Machado (2009) explicam que, para utilizar os serviços disponibilizados pela computação em nuvem, é necessário que o usuário disponha apenas de um sistema operacional, um navegador e acesso à internet, não sendo imprescindível que seu dispositivo possua elevado poder de processamento. Essa característica, como destacam, elimina a necessidade de investimentos em equipamentos robustos, uma vez que todos os recursos computacionais estão centralizados na nuvem.

Complementando essa perspectiva, Nogueira *et al.* (2016) definem a computação em nuvem como um modelo que se estrutura em três principais modalidades de serviço: *Software* como Serviço (SaaS), Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS).

Figura 2: Visão geral dos três modelos de serviço em nuvem.



Fonte: Elaborado pelo autor.

Esses modelos formam a base conceitual que permite compreender as diferentes formas de utilização da nuvem, conforme a seguir Nogueira *et al.* (2016):

Software como Serviço (SaaS): O consumidor utiliza aplicações fornecidas pelo provedor, que estão hospedadas na nuvem e acessadas via dispositivos clientes, geralmente por navegador *web* ou interface específica. O consumidor não controla nem gerencia a infraestrutura subjacente, como rede, servidores, sistemas operacionais ou armazenamento, podendo apenas ajustar configurações restritas às aplicações.

Plataforma como Serviço (PaaS): O consumidor implanta suas próprias aplicações na infraestrutura do provedor, utilizando linguagens, bibliotecas e ferramentas oferecidas. Não há controle sobre a infraestrutura física ou virtual, mas o consumidor administra as aplicações implantadas e configurações do ambiente de hospedagem.

Infraestrutura como Serviço (IaaS): O consumidor provisiona recursos básicos de computação, armazenamento e rede para implantar sistemas operacionais e aplicações à sua escolha. O provedor gerencia a infraestrutura física, enquanto o consumidor controla o sistema operacional, armazenamento, aplicações e, em alguns casos, aspectos limitados da rede, como *firewalls*.

2.2 Riscos e proteção de dados em ambientes digitais

Mesmo sem acessar ou utilizar diretamente dispositivos e plataformas tecnológicas, é praticamente inevitável que informações pessoais estejam inseridas nesse ambiente, devido à crescente informatização social e à formação de amplas redes de dados (Hermes, 2023). A partir dessa perspectiva, o autor destaca dois elementos centrais: os dados pessoais que são constantemente incorporados ao espaço digital e as implicações que esse processo acarreta sobre as liberdades individuais, tanto no meio virtual quanto na vida cotidiana.

Diante da presença cada vez mais intensa de informações pessoais no ambiente digital, é fundamental compreender o que se considera dado pessoal e por que sua proteção é tão relevante (Cabral; Rangel, 2020). Toda ação realizada na internet, por mais simples que seja, deixa vestígios que podem ser utilizados para identificar um indivíduo, ainda que de forma indireta (Alves; Souza, 2021).

Nesse sentido, os dados pessoais abrangem informações, que vão desde

elementos básicos como nome, e-mail e endereço, até dados sensíveis, como características físicas, origem racial, informações sobre saúde e até registros eletrônicos como o endereço IP, número que identifica de forma única um dispositivo conectado a uma rede, possibilitando sua localização e rastreamento em conexões digitais (Lima, 2014).

No Brasil, a criação do Marco Civil da Internet e da LGPD (2018) representa um avanço para regular e proteger as atividades digitais citadas. Contudo, ainda são comuns os vazamentos, a exposição inadequada e o uso indevido de dados pessoais, o que compromete a segurança dos cidadãos, conforme (Carvalho Júnior; Rezende, 2024).

A LGPD estabelece fundamentos essenciais para o tratamento responsável das informações pessoais, enfatizando a necessidade de transparência, segurança e igualdade no uso dos dados (Bueno; Sampaio Neto, 2024). Embora tenha representado um avanço no cenário jurídico brasileiro, especialistas ressaltam que ainda existem lacunas que limitam sua efetividade em certas áreas críticas.

2.3 Lei geral de proteção de dados

A privacidade está diretamente ligada ao direito que cada indivíduo possui de controlar suas próprias informações e decidir quando, como e por quem elas podem ser acessadas. Essa proteção influencia diretamente a qualidade dos dados compartilhados, já que há um equilíbrio delicado entre manter a privacidade e garantir a utilidade dessas informações (Brito; Machado, 2017).

No Brasil, a preocupação com a proteção de dados pessoais resultou na criação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 14 de agosto de 2018 (Brasil, 2018). Seu principal objetivo é regulamentar o tratamento de dados pessoais, abrangendo práticas como coleta, armazenamento, compartilhamento e proteção dessas informações, tanto no setor público quanto no privado.

O autor Burkart (2021) destaca, que a lei estabelece dez princípios que devem ser seguidos no tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilidade e prestação de contas.

Tais princípios estão formalmente dispostos no artigo 6º da Lei nº 13.709/2018,

a qual estabelece que as atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes fundamentos:

I – Finalidade: o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado o tratamento posterior de forma incompatível com essas finalidades;

II – Adequação: o tratamento deve ser compatível com as finalidades informadas ao titular, respeitando o contexto no qual os dados foram coletados;

III – Necessidade: deve haver limitação do tratamento ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os dados pertinentes, proporcionais e não excessivos;

IV – Livre acesso: é garantido ao titular dos dados o direito de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de suas informações;

V – Qualidade dos dados: assegura ao titular a exatidão, clareza, relevância e atualização dos dados, conforme a necessidade e para o cumprimento da finalidade do tratamento;

VI – Transparência: garante ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes, respeitados os segredos comercial e industrial;

VII – Segurança: exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou difusão;

VIII – Prevenção: determina a adoção de medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – Não discriminação: veda a realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – Responsabilização e prestação de contas: impõe ao agente de tratamento o dever de demonstrar a adoção de medidas eficazes que comprovem o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas ações.

No entanto, ainda conforme Burkart (2021), embora haja uma estrutura legal que busca assegurar a proteção dos dados pessoais, é perceptível que o exercício do direito individual de acesso às próprias informações ocorre, muitas vezes, sem que o titular compreenda plenamente o real propósito dessa disponibilização.

Evidenciando que, apesar dos avanços legislativos, ainda é essencial o aprofundamento do conhecimento acerca da LGPD (2018) e dos direitos que ela assegura, de modo a fortalecer a autonomia dos indivíduos no controle de suas informações e promover uma cultura mais consciente e responsável no uso de dados pessoais.

3 METODOLOGIA

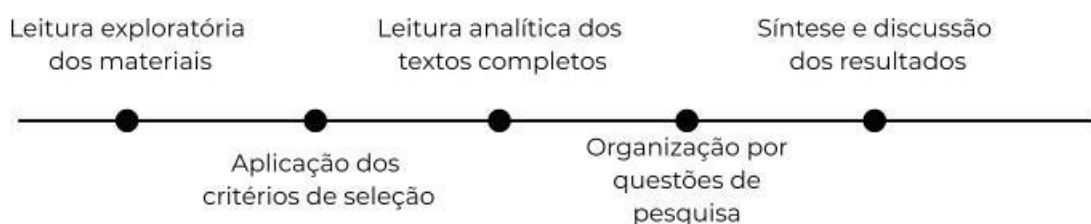
Nesta seção são apresentados os métodos utilizados para a realização desta pesquisa. Este estudo constitui uma revisão da literatura, de natureza exploratória e descritiva, com o objetivo de compreender a relação entre a computação em nuvem e a LGPD (2018).

3.1 Etapas da revisão

A revisão da literatura realizada neste estudo seguiu um conjunto de etapas, com base na análise de conteúdo temática proposta por Bardin (2009) e adaptada por Cunha e Gomes (2015). A Figura 3 apresenta o fluxo metodológico adotado para a identificação, seleção, categorização e interpretação dos estudos analisados.

A seguir, apresenta-se a descrição de cada etapa:

Figura 3: Fluxo metodológico.



Fonte: Elaborado pelo autor.

A primeira etapa consiste na leitura exploratória dos materiais coletados nas bases selecionadas, com o objetivo de identificar estudos potencialmente pertinentes. Na segunda etapa, realiza-se a filtragem e organização inicial dos conteúdos, com base em critérios como ano de publicação, 2020 a 2025 e aderência ao tema. A terceira etapa corresponde à leitura analítica dos textos, visando à extração de categorias centrais relacionadas à relação entre LGPD (2018) e computação em

nuvem. Em seguida, na quarta etapa os estudos são organizados com base nas questões de pesquisas, facilitando a organização dos achados. Por fim, a quinta etapa envolve o tratamento e a interpretação dos dados, alinhando os resultados aos objetivos e questões da pesquisa.

3.2 Objetivos e questões de pesquisa

Para direcionar a seleção e análise dos artigos, foram definidas duas questões norteadoras, conforme demonstrado na Tabela 1.

Tabela 1 – Objetivos e questões de pesquisa.

ID	Questão de pesquisa	Motivação
QP1	Quais os principais desafios da conformidade da computação em nuvem com a LGPD (2018)?	Identificar os principais obstáculos técnicos e jurídicos enfrentados.
QP2	Quais estratégias e abordagens têm sido propostas na literatura para adequar serviços em nuvem à LGPD (2018)?	Levantar práticas, soluções e estratégias discutidas nos estudos a fim de promover a conformidade com a LGPD (2018).

Fonte: Elaborado pelo autor.

3.3 Estratégia de busca

A estratégia de busca adotada foi estruturada com base nas diretrizes de Booth, Sutton e Papaioannou (2021), que recomendam uma abordagem para identificação e seleção de literatura, mesmo em revisões de escopo tradicional. Com base nas questões de pesquisa (QP), refinou-se a estratégia de busca utilizada nas bases de dados digitais, garantindo alinhamento com os objetivos da revisão. Modelos semelhantes de estruturação metodológica foram utilizados com êxito por Ribeiro e Silva Neto (2024), servindo como referência complementar para a delimitação e aplicação das etapas desta revisão.

Foram selecionados termos de busca nos idiomas português e inglês, aplicados principalmente nos títulos e resumos das publicações.

- Português: "computação em nuvem", "proteção de dados", "LGPD"
- Inglês: "cloud computing", "data protection", "LGPD"

Para ampliar o alcance das buscas, os descritores foram combinados por meio dos operadores booleanos *AND* e *OR*, integrando termos essenciais, sinônimos e variações, conforme recomendado por (Silva Neto; Gomes; Soares, 2019). Essa estratégia visou maximizar a recuperação de estudos relevantes nas bases de dados selecionadas. A Tabela 2 apresenta as bases utilizadas no processo de busca.

Tabela 2 – Bases de dados utilizadas na busca.

Base de dados	URL
IEEE XPLORE	https://ieeexplore.ieee.org
SCOPUS (Elsevier)	https://www.scopus.com/home.uri .

Fonte: Elaborado pelo autor.

Para assegurar a qualidade e pertinência dos estudos, foram definidos critérios de inclusão e exclusão que guiaram a seleção dos artigos encontrados. Os critérios de inclusão abrangeram publicações em texto completo, disponíveis em português ou inglês, e com foco direto na relação entre computação em nuvem e LGPD (2018). Já os critérios de exclusão consideraram artigos duplicados, trabalhos sem relação direta ao tema e publicações em línguas que não sejam Inglês ou Português.

Para assegurar a adequação dos materiais analisados, foram definidos critérios de inclusão e exclusão conforme a Tabela 3.

Tabela 3 – Critérios de inclusão e exclusão.

Tipo	Critério
Inclusão (CI)	CI1 – Publicações entre 2020 e 2025 CI2 – Artigos disponíveis em texto completo CI3 – Trabalhos em português ou inglês CI4 – Foco na computação em nuvem, privacidade de dados ou LGPD (2018).
Exclusão (CE)	CE1 – Artigos duplicados CE2 – Estudos não relacionados às questões de pesquisa CE3 – Estudos publicados em línguas que não sejam Inglês ou Português

Fonte: Elaborado pelo autor.

Esta revisão sistemática da literatura destaca tópicos importantes presentes em artigos científicos sobre a temática do *smart campus* e sua relação com a gestão de informações. Neste trabalho, o autor relata entre outros tópicos o papel inerente à informação, e como a organização e tratamento adequados possibilitam obter distintas visões sobre uma série de dados, assim como dar significado àquele conjunto, é dito que dados só se tornam utilizáveis se transformados em conhecimento.

Aplicação desses critérios permitiu a seleção de estudos alinhados aos objetivos da revisão, assegurando a qualidade da análise subsequente.

4 RESULTADOS

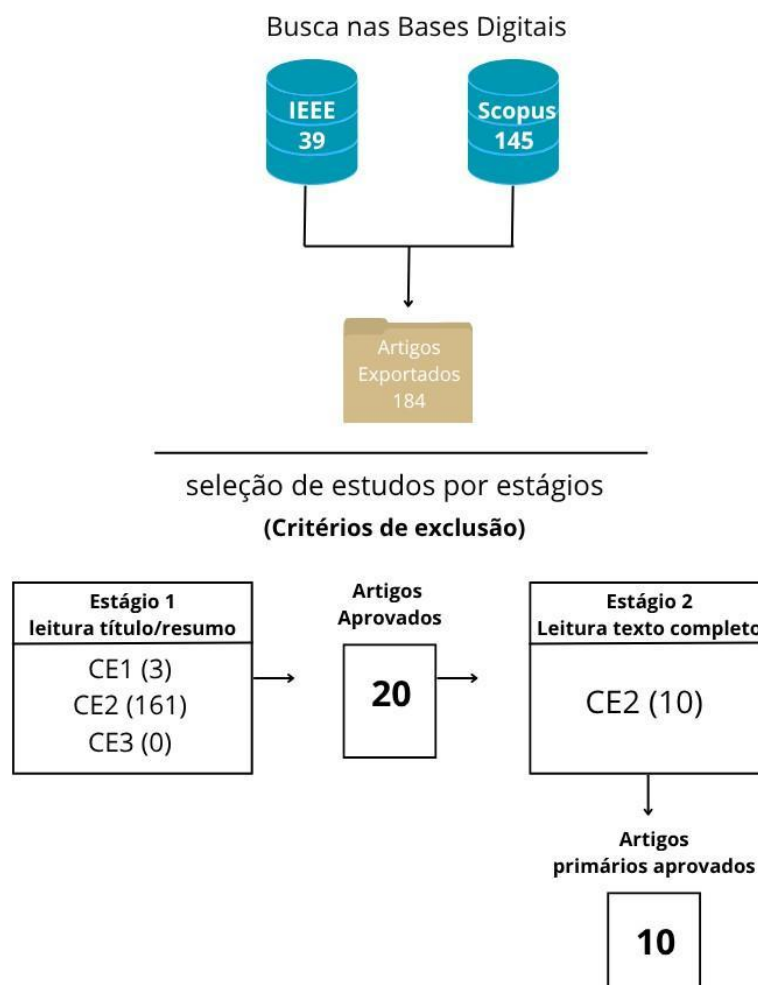
O processo de busca e seleção permitiu reunir artigos que contribuem para compreender a relação entre a computação em nuvem e a LGPD (2018). A triagem dos artigos foi conduzida em etapas, conforme detalhado na Figura 4, que ilustra visualmente o fluxo desde a exportação inicial até a filtragem final.

Inicialmente, foram recuperados 184 (cento e oitenta e quatro) artigos publicados entre 2020 e 2025 nas bases de dados selecionadas. Após a aplicação dos critérios de exclusão na primeira etapa, que envolveu a análise de títulos e resumos, 20 (vinte) estudos foram selecionados e avançaram para leitura completa. Na etapa final, com a avaliação detalhada do conteúdo, apenas 10 (dez) artigos apresentaram aderência direta aos objetivos da pesquisa, compondo o corpus final da revisão.

Os artigos incluídos nesta revisão da literatura, assim como seus critérios de categorização, estão detalhados na Tabela 4. Para maior transparência, todo o material relacionado ao processo de seleção, incluindo artigos analisados e excluídos, está disponível no repositório³ de dados deste estudo.

³ https://drive.google.com/drive/folders/19hg_KLRWfsXycXI3WZGA7BexuuVFD5ke?usp=sharing

Figura 4 – Processo de seleção dos artigos primários.



Fonte: Elaborado pelo autor.

Para uma análise detalhada dessas publicações, a Tabela 4 sintetiza as principais características dos estudos, incluindo artigo, tema central, base de dados e motivação, permitindo uma visão comparativa do corpus final.

Tabela 4 – Artigos selecionados na revisão.

Artigo	Tema Central	Base de Dados	Motivação
(Canedo <i>et al.</i> , 2020)	Visões de TI sobre privacidade	Scopus	Mapear opinião técnica sobre desafios da LGPD (2018) em desenvolvimento de software.
(Beppu;Maciel; Viterbo, 2021)	Tratamento de dados legados e LGPD (2018)	Scopus	Analisar orientações legais sobre dados existentes antes da LGPD (2018).

(Fernandes <i>et al.</i> , 2021)	Estratégias de segurança de dados em nuvem	Scopus	Avaliar métodos técnicos que suportem a LGPD (2018) em ambientes de nuvem.
(Ferrão <i>et al.</i> , 2024)	Conformidade processual com a LGPD (2018)	Scopus	Propor uma taxonomia abrangente de requisitos de privacidade.
(Canedo <i>et al.</i> , 2021)	Privacidade em equipes ágeis	IEEE Xplore	Entender como equipes ágeis incorporam LGPD (2018) no desenvolvimento.
(Farias; Barros, 2022)	Aplicação prática da LGPD (2018)	IEEE Xplore	Identificar recomendações operacionais para conformidade baseada em casos reais.
(Ferreira <i>et al.</i> , 2022)	Panorama da implementação da LGPD (2018) no Brasil	IEEE Xplore	Investigar nível de maturidade da implementação da LGPD (2018) em iniciativas brasileiras.
(Almeida; Soares, 2022)	Impactos da LGPD (2018) no cenário digital	Scopus	Compreender mudanças regulatórias e seus impactos na nuvem.
(Andrade <i>et al.</i> , 2023)	Perspectiva técnica sobre privacidade	IEEE Xplore	Mapear desafios técnicos durante o ciclo de desenvolvimento.
(Choudhary; Vyas; Li- Lhore, 2023)	Estratégias de segurança em nuvem	IEEE Xplore	Identificar lacunas de segurança e práticas recomendadas no contexto LGPD (2018).

Fonte: Elaborado pelo autor.

Os resultados desta revisão da literatura foram estruturados com base nas duas questões de pesquisa definidas inicialmente: Os principais desafios da conformidade da computação em nuvem com a LGPD (2018) e quais estratégias e abordagens têm sido propostas na literatura para adequar serviços em nuvem à LGPD (2018). Para cada uma delas, os artigos selecionados passaram por uma análise qualitativa, considerando seus objetivos principais, contribuições e limitações. A categorização dos dados revelou padrões, pontos em comum e lacunas nos estudos sobre a

computação em nuvem e a LGPD (2018). As próximas subseções detalham as discussões referentes a cada questão investigada.

4.1 Resultados e discussões

Os artigos foram categorizados conforme suas contribuições às questões de pesquisa, revelando os temas predominantes sobre o assunto.

4.1.1 QP1 – Quais os principais desafios da conformidade da computação em nuvem com a LGPD (2018)?

Essa questão de pesquisa investiga a conformidade da computação em nuvem com a LGPD (2018). Os artigos avaliados apresentaram desafios como aspectos técnicos, jurídicos, organizacionais e culturais, conforme apresentado na figura 5.

Figura 5 – Representação dos desafios encontrados.



Fonte: Elaborado pelo autor.

4.1.1 Desafios técnicos e operacionais

E entre os principais entraves técnicos, destaca-se a dificuldade de garantir a

segurança e a privacidade dos dados em ambientes virtualizados, sobretudo devido à suscetibilidade a ataques como *ransomware*, vazamento de dados, port scanning, acesso indevido e outras ameaças cibernéticas (Fernandes *et al.*, 2021; Choudhary; Vyas; Lilhore, 2023). O modelo de computação em nuvem, ao transferir o controle da infraestrutura para terceiros, compromete a visibilidade e a rastreabilidade dos dados, dificultando auditorias e o cumprimento de exigências legais como a identificação da localização exata do armazenamento (Ferreira *et al.*, 2022).

Além disso, a gestão de identidade e acesso, a distribuição de responsabilidades entre controlador e operador, e a ausência de padrões claros para *backup*, criptografia e monitoramento contínuo dificultam a implantação de medidas técnicas compatíveis com os princípios da LGPD (Almeida; Soares, 2022; Fernandes *et al.*, 2021). A literatura também aponta obstáculos relacionados à integração entre serviços em nuvem e sistemas locais, comprometendo a interoperabilidade e a governança dos dados.

4.1.2 Barreiras organizacionais e culturais

Outro eixo recorrente nos estudos diz respeito à baixa maturidade organizacional para lidar com os requisitos da LGPD (2018). Muitas organizações ainda se encontram em estágios iniciais de conformidade, com políticas internas incipientes ou inexistentes (Ferreira *et al.*, 2022). A falta de cultura institucional voltada à proteção de dados, somada à escassez de treinamentos específicos, compromete a conscientização dos colaboradores e gera riscos operacionais significativos (Farias; Barros, 2022)

A estruturação deficiente de comitês de privacidade, a ausência de responsáveis formais pelo tratamento de dados, e a dificuldade em atender aos direitos dos titulares, como o fornecimento de informações, a exclusão de dados e a revogação do consentimento, figuram como lacunas críticas, sobretudo em ambientes altamente dependentes de tecnologias de nuvem (Fernandes *et al.*, 2021).

4.1.3 Falhas na integração da privacidade ao desenvolvimento

Em ambientes de desenvolvimento de *software*, observa-se a integração tardia de requisitos de privacidade no ciclo de vida dos sistemas. Muitas organizações tratam a privacidade de forma reativa, abordando-a apenas nas etapas finais de entrega do

produto, em desacordo com o princípio do *privacy by design*. Esse princípio defende que a proteção de dados pessoais deve ser considerada desde o início do desenvolvimento dos sistemas, sendo incorporada de forma proativa em todas as fases do projeto (Canedo *et al.*, 2021; Andrade *et al.*, 2023).

As dificuldades são ampliadas pela falta de processos sistemáticos para eliciação de requisitos de privacidade, pela ausência de ferramentas específicas, e pela confusão entre os conceitos de segurança e privacidade, frequentemente tratados como equivalentes (Ferrão *et al.*, 2024).

A carência de profissionais com conhecimento jurídico adequado para interpretar os fundamentos da LGPD (2018), aliada à complexidade dos requisitos não funcionais, compromete a implementação efetiva da conformidade, especialmente quando sistemas em nuvem são desenvolvidos sob metodologias ágeis, que priorizam a entrega rápida em detrimento da robustez jurídica (Canedo *et al.*, 2020).

4.1.4 Lacunas legais e contratuais

Do ponto de vista jurídico, a literatura aponta a ausência de uma retaguarda legal específica para algumas situações comuns em ambientes de nuvem, como o tratamento de dados transnacionais ou o gerenciamento de legados digitais (Beppu; Maciel; Viterbo, 2021). A falta de contratos claros entre empresas e provedores de serviços de nuvem, que estabeleçam responsabilidades, escopo do tratamento e formas de consentimento, compromete a responsabilização prevista nos Art. 37 a 42 da LGPD (Brasil, 2018).

Questões como a falta de regulamentação sobre o legado digital pós-morte, o uso de dados por terceiros sem consentimento explícito, e a insuficiência de políticas de transparência e portabilidade evidenciam que o arcabouço normativo atual ainda é insuficiente frente aos desafios impostos pela arquitetura da nuvem (Beppu; Maciel; Viterbo, 2021; Almeida; Soares, 2022).

4.1.5 QP2 – Quais estratégias e abordagens têm sido propostas na literatura para adequar serviços em nuvem à LGPD (2018)?

A literatura analisada apresenta um conjunto diverso de estratégias e abordagens para a adequação de serviços em nuvem à LGPD (2018). Essas propostas podem ser organizadas em quatro eixos:

- (i) Abordagens técnicas de segurança e controle.
- (ii) Princípios de privacidade desde o design.
- (iii) Governança organizacional e processos de conformidade.
- (iv) Ferramentas e práticas de apoio à implementação da lei.

No eixo técnico, destacam-se medidas como a criptografia de dados em repouso e em trânsito, a autenticação multifator, a definição de políticas de controle de acesso, e o uso de ferramentas de monitoramento contínuo para detectar e responder a incidentes de segurança (Choudhary; Vyas; Lilhore, 2023). Essas estratégias buscam garantir a confidencialidade, integridade e disponibilidade dos dados pessoais em ambientes de nuvem, além de mitigar riscos associados à distribuição geográfica e ao compartilhamento com múltiplos agentes.

Complementando essas soluções, distintas abordagens propõem a adoção dos princípios de *Privacy by Design* e *Privacy by Default* no desenvolvimento de sistemas e serviços. Enquanto o *Privacy by Design* recomenda que a proteção de dados deve ser incorporada desde a concepção dos sistemas, o *Privacy by Default* assegura que, por padrão, apenas os dados estritamente necessários sejam coletados e utilizados, garantindo o nível máximo de privacidade sem exigir configurações adicionais por parte do usuário (Carvalho; Nobre; Marques-Neto, 2022).

A integração da privacidade desde as fases iniciais do ciclo de vida do *software* permite antecipar riscos regulatórios e alinhar requisitos técnicos aos direitos dos titulares de dados. Essa perspectiva está presente em estudos que discutem a importância da engenharia de requisitos de privacidade, sobretudo no contexto ágil (Canedo *et al.*, 2021; Andrade *et al.*, 2023).

Outro pilar é o da governança organizacional e da estruturação de processos internos, que envolve ações como a criação de comitês de privacidade, a designação do encarregado, *Data Protection Officer* (DPO), profissional que atua como elo entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados, o estabelecimento de programas de conformidade, e a promoção de treinamento e capacitação contínua para colaboradores. A literatura aponta que a conformidade em nuvem exige uma atuação coordenada entre áreas técnicas, jurídicas e administrativas, sendo fundamental o engajamento de todas as partes interessadas (Farias; Barros, 2022).

Além disso, abordagens baseadas em ferramentas de apoio à implementação têm ganhado espaço, com destaque para o uso do LGPD *Model Canvas*, ferramenta visual para mapear a conformidade com a LGPD (2018) e o *Design Thinking*, metodologia colaborativa para resolver problemas focando no usuário (Ferreira *et al.*, 2022). Essas ferramentas se mostram úteis especialmente em ambientes de nuvem, onde os fluxos de dados são dinâmicos e complexos.

O estudo de (Ferrão *et al.*, 2024) traz a taxonomia de requisitos de privacidade baseada na LGPD (2018) e na norma ISO/IEC 29100, que define princípios e diretrizes para a proteção de dados pessoais em sistemas de informação, permitindo uma sistematização dos aspectos que devem ser considerados durante o desenvolvimento de sistemas (ISO, 2024). Essa proposta contribui diretamente para a formalização de critérios de conformidade em soluções baseadas na nuvem, ao facilitar a tradução da LGPD (2018) em requisitos técnicos acionáveis.

Já o trabalho de Fernandes *et al.* reforça a importância de estratégias jurídicas e contratuais específicas para o contexto da computação em nuvem, evidenciando desafios como a insegurança jurídica em relação à localização dos dados, a falta de padronização nos contratos com provedores e a dificuldade de garantir a rastreabilidade dos dados pessoais. Esses aspectos destacam a necessidade de abordagens integradas, que combinem soluções técnicas, revisão contratual e políticas organizacionais.

Em síntese, a conformidade da computação em nuvem com a LGPD (2018) não depende de soluções isoladas, mas de conjuntos articulados de estratégias, que abrangem desde tecnologias de segurança e engenharia de privacidade, até modelos de governança, metodologias de gestão e fundamentos legais claros. A integração desses pilares permite que organizações lidem com os desafios complexos impostos pela lei, garantindo a proteção de dados pessoais de forma efetiva, mesmo em ambientes distribuídos e dinâmicos como os serviços em nuvem.

5 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou uma revisão da literatura sobre a relação entre a computação em nuvem e a LGPD (2018), com o objetivo de identificar os principais desafios e estratégias propostas para a adequação dos ambientes de nuvem às exigências da legislação brasileira. Para isso, foi aplicada uma metodologia de revisão

sistemática inspirada no modelo de mapeamento da literatura, com procedimentos definidos para busca, seleção e análise de artigos científicos publicados entre 2020 e 2025, extraídos das bases IEEE Xplore e Scopus.

Após o processo de triagem e aplicação dos critérios de inclusão e exclusão, 10 (dez) artigos foram selecionados para compor a base da análise. Os resultados permitiram responder às duas questões de pesquisa e mostraram que a conformidade com a LGPD (2018) em ambientes de nuvem envolve barreiras como, técnicas, jurídicas e organizacionais. Entre os principais desafios estão a falta de controle sobre o ciclo de vida dos dados, a complexidade contratual com provedores de nuvem e a baixa maturidade institucional em termos de governança da privacidade.

Em resposta a esses desafios, a literatura aponta estratégias agrupadas, como:

- (i) abordagens técnicas de segurança e controle, como criptografia e autenticação forte.
- (ii) princípios de privacidade incorporados desde o design dos sistemas.
- (iii) ações de governança organizacional, como políticas internas, treinamentos e nomeação de DPOs.
- (iv) o uso de ferramentas e métodos de apoio, como taxonomias de requisitos e modelos visuais de adequação.

Como pontos positivos, este trabalho reuniu, organizou e apresentou de forma clara abordagens sobre a relação entre nuvem e LGPD (2018), oferecendo uma visão que pode facilitar a compreensão do tema por estudantes, profissionais e pesquisadores. A utilização de uma metodologia estruturada deu consistência à revisão e possibilitou comparações entre diferentes enfoques presentes nos artigos analisados.

Entre as contribuições do estudo, destacam-se: o mapeamento de práticas e soluções já discutidas na literatura, a identificação de lacunas pouco exploradas, como a falta de diretrizes específicas para contratos com provedores e a proposta de uma organização temática dos desafios e estratégias, o que pode ajudar futuras pesquisas a se aprofundarem em aspectos específicos, como capacitação profissional ou ferramentas de auditoria de conformidade.

Assim, além de cumprir os objetivos propostos, este trabalho pode contribuir ao oferecer uma síntese atualizada das principais discussões acadêmicas sobre o tema, podendo servir como referência para pesquisadores, profissionais da área de tecnologia e gestores que atuam com a proteção de dados em ambientes de nuvem.

Diante da crescente digitalização das atividades corporativas e do rigor da legislação vigente, a discussão sobre a proteção de dados na computação em nuvem tende a se intensificar nos próximos anos, o que torna fundamental o aprofundamento contínuo sobre o tema, especialmente no que tange à identificação de boas práticas, ao estudo de casos reais e à articulação entre aspectos jurídicos e tecnológicos na construção de soluções efetivas de conformidade.

5.1 Trabalhos futuros

Como desdobramentos desta pesquisa, sugerem-se os seguintes caminhos:

- Realizar estudos práticos com empresas que utilizam serviços de computação em nuvem, a fim de entender, na prática, como essas organizações têm buscado se adequar à LGPD (2018) e quais dificuldades mais frequentemente enfrentam.
- Avaliar a conformidade de serviços de nuvem utilizados no Brasil, com foco em critérios como segurança da informação, exclusão e portabilidade de dados, permitindo identificar lacunas ainda presentes no mercado.
- Desenvolver materiais de orientação acessíveis, voltados especialmente a pequenas e médias empresas, que ainda enfrentam barreiras técnicas ou jurídicas para adotar a computação em nuvem de forma segura e em conformidade com a legislação.

REFERÊNCIAS

ALMEIDA, S. D. C. D. de.; SOARES, T. A. Os impactos da lei geral de proteção de dados – LGPD no cenário digital. **Perspectivas em Ciencia da Informacao**, v. 27, n. 3, p. 26-45, 2022. Disponível em: <https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/abstract/?lang=pt>. Acesso em: 3 fev. 2025.

ALVES, G. B.; SOUZA, R. T. de. Comércio digital e proteção de dados: a era do big data. **Revista da Defensoria Pública do Distrito Federal**, Distrito Federal, Brasília, v. 3, n. 1, p. 99–122, 2021. Disponível em: <https://revista.defensoria.df.gov.br/index.php/revista/article/view/116>. Acesso em: 3 fev. 2025.

AMAZON WEB SERVICES (AWS). O que é a computação em nuvem? **Amazon Web Services**, 2019. Disponível em: <https://aws.amazon.com/pt/what-is-cloud-computing/>. Acesso em: 25 maio 2025.

ANDRADE, V. C. et al. Personal data privacy in software development processes: a practitioner's point of view. In: **IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)**, 22., 2023, Exeter. Anais [...]. Exeter: IEEE, 2023. p. 2727-2734. Disponível em: <https://ieeexplore.ieee.org/document/10538505/>. Acesso em: 25 maio 2025.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2009.

BEPPU, F. R.; MACIEL, C.; VITERBO, J. Contributions of the Brazilian Act for the Protection of Personal Data for treating Digital Legacy. **Journal on Interactive Systems**, Porto Alegre, RS, v. 12, n. 1, p. 112 – 124, 2021. Disponível em: <https://journals-sol.sbc.org.br/index.php/jis/article/view/1654>. Acesso em: 3 fev. 2025.

BOOTH, A.; SUTTON, A.; PAPAIOANNOU, D. **Systematic approaches to a successful literature review**. London: SAGE Publications Ltd, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 maio 2025.

BRITO, F. T.; MACHADO, J. C. Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. In: SOCIEDADE BRASILEIRA DE COMPUTAÇÃO (SBC) (org.). **Jornadas de Atualização em Informática 2017**. Porto Alegre: SBC, 2017. cap. 3, p. 91–130.

BUENO, M. E. B.; SAMPAIO NETO, W. F. Direito digital: A ética e a privacidade no contexto digital. **Revista Unifev: Ciência & Tecnologia**, v. 4, n. 2, 2024. Disponível em: <https://periodicos.unifev.edu.br/index.php/revistaunifev/article/view/2028/1801>. Acesso em: 25 maio 2025.

BURKART, D. V. V. **Proteção de dados e o estudo da LGPD**. Orientador: Prof. Dr. Francisco Machado Filho. 2021. 141 f. Dissertação (Mestrado em Mídia e Tecnologia) — Faculdade de Artes, Arquitetura e Comunicação, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Bauru, 2021. Disponível em: <http://hdl.handle.net/11449/204091>. Acesso em: 25 maio 2025.

BUYA, R.; YEO, C. S.; VENUGOPAL, S. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In: **IEEE International Conference on High Performance Computing and Communications**, 10., 2008, Dalian. Anais [...]. Dalian: IEEE, 2008. p. 5-13. Disponível em: <https://ieeexplore.ieee.org/document/4637675>. Acesso em: 25 maio 2025.

2025.

CABRAL, C. P.; RANGEL, T. L. V. A lei geral de proteção de dados em um cenário de reconhecimento de dados: a tutela dos direitos fundamentais no ambiente digital. **Múltiplos Acessos**, v. 5, n. 2, p. 31–51, 2020. Disponível em: <http://www.multiplosacessos.com/multaccess/index.php/multaccess/article/view/157>. Acesso em: 25 maio 2025.

CANEDO, E. D. et al. Agile teams' perception in privacy requirements elicitation: LGPD's compliance in brazil. In: **IEEE International Requirements Engineering Conference (RE)**, 29., 2021, Notre Dame. Anais [...]. Notre Dame: IEEE, 2021. p. 58–69. Disponível em: <https://ieeexplore.ieee.org/document/9604706>. Acesso em: 25 maio 2025.

CANEDO, E. D. et al. Perceptions of ict practitioners regarding software privacy. **Entropy**, v. 22, n. 4, p. 429, 2020. Disponível em: <https://www.mdpi.com/1099-4300/22/4/429>. Acesso em: 25 maio 2025.

CARVALHO, D. F. F. B. de; NOBRE, C. N.; MARQUES-NETO, H. T. Evaluating cognitive privacy heuristics that influence facebook users data disclosure. **Journal of Internet Services and Applications**, v. 13, n. 1, p. 66–81, 2022. Disponível em: <https://journals-sol.sbc.org.br/index.php/jisa/article/view/2550>. Acesso em: 25 maio 2025.

CARVALHO JÚNIOR, P. C. de; REZENDE, P. I. da S. Direito digital e suas aplicações: A violação de privacidade, a proteção de dados e medidas de solução. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 11, p. 3720–3733, 2024. Disponível em: <https://periodicorease.pro.br/rease/article/view/16960>. Acesso em: 11 jun. 2025.

CHEE, B. J. S.; FRANKLIN JUNIOR, C. **Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center**, Boca Raton: CRC Press, 2010.

CHOUDHARY, C.; VYAS, N.; LILHORE, U. K. Cloud security: Challenges and strategies for ensuring data protection. In: **International Conference on Technological Advancements in Computational Sciences (ICTACS)**, 3., 2023, Tashkent. Anais [...]. Tashkent: IEEE, 2023. p. 669–673. Disponível em: <https://ieeexplore.ieee.org/document/10390302>. Acesso em: 31 maio 2025.

CUNHA, R. B. B.; GOMES, R. Young male homosexuals and their health: a systematic review. **Interface-Comunicação, Saúde, Educação**, v. 19, n. 52, p. 57–70, 2015. Disponível em: <https://www.scielo.br/j/icse/a/wZJ5cYchyLrgvmptgKMWKcP/abstract/?lang=en>. Acesso em: 31 maio 2025.

FERRÃO, S. É. R. et al. Towards a taxonomy of privacy requirements based on the LGPD and iso/iec 29100. **Information and Software Technology**, v. 168, 2024. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85182267044&doi=10.10162fj.infsof.2024.107396&partnerID=40&md5=2b16717984b70bb5a5c8db2b1c4ce958>. Acesso em: 2 jun. 2025.

FERREIRA, L. et al. A panorama of the implementation of the general law for the protection of personal data (LGPD) in brazil: an exploratory survey. In: **IEEE Annual Computing and Communication Workshop and Conference (CCWC)**, 12., 2022, Las Vegas. Anais [...]. Las Vegas, NV: IEEE, 2022. p. 723–729. Disponível em: <https://ieeexplore.ieee.org/document/9720879>. Acesso em: 2 jun. 2025.

HERMES, P. H. **Proteção de dados pessoais na sociedade de risco: limites e possibilidades à liberdade no ambiente digital**. 2023. Dissertação (Mestrado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2023. Disponível em: <https://repositorio.unisc.br/jspui/handle/11624/3559>. Disponível em: <https://repositorio.unisc.br/jspui/handle/11624/3559>. Acesso em: 2 jun. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 29100:2024 — Information technology — Security techniques — Privacy framework**. Genebra: ISO, 2024. Disponível em: <https://www.iso.org/standard/85938.html>. Acesso em: 19 jul. 2025.

ISTVÁN, Z.; PONNAPALLI, S.; CHIDAMBARAM, V. Towards software-defined data protection: GDPR compliance at the storage layer is within reach. **arXiv:2008.04936 [cs.CR]**, v. 1, 2020. Disponível em: <https://arxiv.org/abs/2008.04936>. Acesso em: 5 jun. 2025.

LEE, K. et al. Unpacking sustainability in start-ups: a systematic review and research agenda. **Discover Sustainability**, v. 6, p. 218, 2025. Disponível em: <https://link.springer.com/article/10.1007/s43621-025-01070-7>. Acesso em: 11 jun. 2025.

LIMA, C. C. C. **Marco civil da internet: Garantia da privacidade e dados pessoais à luz do marco civil da internet**. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MELL, P.; GRANCE, T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Gaithersburg: **National Institute of Standards and Technology, U.S. Department of Commerce**, 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 19 jun. 2025.

NOGUEIRA, E. et al. Issues on developing interoperable cloud applications: definitions, concepts, approaches, requirements, characteristics and evaluation models. **Journal of Software Engineering Research and Development**, v. 4, p. 7:1 – 7:23, 2016. Disponível em: <https://journals-sol.sbc.org.br/index.php/jserd/article/view/423>. Acesso em: 27 maio 2025.

PALOALTO NETWORKS. State of Cloud-Native Security Report 2024. **Paloalto Networks**, 07 abr. 2024. Disponível em: <https://www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2024>. Acesso em: 25 maio 2025.

RIBEIRO, P. V. de. S.; SILVA NETO, M. G. da. Tecnologias computacionais no auxílio ao aprendizado de indivíduos com tdah: Um mapeamento sistemático da literatura. **Revista Brasileira de Informática na Educação**, v. 32, p. 765–806, 2024. Disponível em: <https://journals-sol.sbc.org.br/index.php/rbie/article/view/4005>.

Acesso em: 25 maio 2025.

SILVA, E. V. F. G. da. **Os desafios e oportunidades da integração e migração de empresas com Cloud Computing**. Orientador: José Carlos Cavalcanti. 2019. 48 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) — Universidade Federal de Pernambuco, Recife, 2019. Disponível em: https://www.cin.ufpe.br/~tg/2019-2/TG_CC/tg_evfgs.pdf. Acesso em: 25 maio 2025.

SILVA NETO, M. G. da.; GOMES, D. G.; SOARES, J. M. Credibility on crowdsensing data acquisition: a systematic mapping study. **Journal of Communication and Information Systems**, v. 34, n. 1, p. 248–269, 2019. Disponível em: <https://jcis.sbrc.org.br/jcis/article/view/673>. Acesso em: 19 jun. 2025.

SOUSA, F. R. C.; MOREIRA, L. O.; MACHADO, J. C. **Computação em nuvem: Conceitos, Tecnologias, Aplicações e Desafios**. Fortaleza: Universidade Federal do Ceará, 2009. Disponível em: <https://www.researchgate.net/publication/237644729>. Acesso em: 26 maio 2025.