Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Uma Abordagem Arquitetural para Consentimentos, Rastreabilidade e Controle de Versões de Políticas de Privacidade

Claudio Henrique Pereira de Castro

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

Orientadora
Prof.a Dr.a Edna Dias Canedo

Brasília
2026

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Uma Abordagem Arquitetural para Consentimentos, Rastreabilidade e Controle de Versões de Políticas de Privacidade

Claudio Henrique Pereira de Castro

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

Prof.a Dr.a Edna Dias Canedo (Orientadora)
Universidade de Brasília (UnB)

Prof. Dr. Geraldo Pereira Rocha Filho
Universidade Estadual do Sudoeste da Bahia, UESB

Prof. Dr. Fernando Antônio Mota Trinta
Universidade Federal do Ceará, UFCE

Prof.a Dr.a Cláudia Nalon
Coordenadora do Programa de Pós-graduação em Informática

Brasília, 21 de Maio de 2026

Dedicatória

Dedico esta dissertação a Alethele Santos, cujo incentivo para que eu ingressasse no mestrado foi determinante para que este trabalho se tornasse realidade. Sem o seu encorajamento, esta conquista não teria sido possível.

Agradecimentos

Expresso meus sinceros agradecimentos à minha orientadora, Prof.ª Dr.ª Edna Dias Canedo, pela paciência, pela valiosa ajuda e pela dedicação que tornaram possível a realização desta pesquisa. Agradeço igualmente ao meu amigo, professor Prof. Dr. Fernando Trinta, cujo incentivo e apoio foram fundamentais.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Contexto: A evolução da internet ocorreu sem mecanismos robustos de proteção à privacidade, o que possibilitou a coleta indiscriminada de dados pessoais e sua exploração econômica sem salvaguardas adequadas. Esse cenário resultou em incidentes de vazamento, roubo de identidade e manipulação algorítmica, fortalecendo a percepção pública sobre a importância da privacidade e da proteção de dados. A crescente adoção de legislações como o GDPR e a LGPD trouxe à tona a necessidade de soluções técnicas que assegurem transparência, rastreabilidade e conformidade regulatória. Objetivo: Desenvolver uma arquitetura para registro, versionamento de políticas de privacidade, controle e auditoria de consentimentos de usuários, garantindo integridade, imutabilidade e alinhamento com legislações de privacidade e normas internacionais. Método: A pesquisa adota uma abordagem de engenharia de software orientada à conformidade regulatória. O trabalho envolve levantamento de requisitos legais e técnicos, modelagem de dados relacionais, gestão de consentimentos e políticas de privacidade, além da avaliação da solução quanto à segurança, escalabilidade e aderência a padrões internacionais (ISO/IEC 29184, ISO/IEC TS 27560, ISO/IEC 29100). Resultados: A proposta prevê um conjunto de serviços que possibilita o cadastro e versionamento de políticas de privacidade, bem como o registro, a rastreabilidade e a auditoria de consentimentos. O modelo de dados assegura a vinculação imutável entre consentimentos e versões específicas de políticas, permitindo consultas eficientes para fins de auditoria e governança. Conclusão: Espera-se que a solução contribua para a literatura acadêmica, ao preencher lacunas práticas sobre implementação de sistemas de gestão de consentimento, e para a aplicação real em organizações que precisam alinhar tecnologia, governança e conformidade regulatória. A abordagem oferece um modelo de referência para promover transparência, prestação de contas e segurança no tratamento de dados pessoais.

Palavras-chave: LGPD, GDPR, Gestão de Consentimento, Privacidade de Dados, Política de privacidade

Abstract

Context: The evolution of the internet occurred without robust privacy protection mechanisms, enabling indiscriminate collection of personal data and its economic exploitation without adequate safeguards. This scenario resulted in data breaches, identity theft, and algorithmic manipulation, strengthening public awareness of the importance of privacy and data protection. The growing adoption of regulations such as the GDPR and LGPD has highlighted the need for technical solutions that ensure transparency, traceability, and regulatory compliance. **Goal:** To develop an architecture for the registration and versioning of privacy policies, and for the control, management, and auditing of user consents, ensuring integrity, immutability, and alignment with privacy legislation and international standards. **Method:** The research adopts a software engineering approach oriented toward regulatory compliance. The work includes the identification of legal and technical requirements, data modeling, privacy policy management, and the evaluation of the solution regarding security, scalability, and adherence to international standards (ISO/IEC 29184, ISO/IEC TS 27560, ISO/IEC 29100). **Results:** The proposed solution offers a set of services enabling the registration and versioning of privacy policies, as well as the recording, traceability, and auditing of user consents. The relational data model ensures immutable linkage between consents and specific policy versions, allowing efficient queries for auditing and governance. **Conclusion:** The solution is expected to contribute to academic literature by addressing practical gaps in the implementation of consent management systems, and to support real-world adoption in organizations that need to align technology, governance, and regulatory compliance. The approach provides a reference model that promotes transparency, accountability, and security in personal data processing.

Keywords: LGPD, GDPR, Consent Management, Data Privacy

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Esse capítulo apresenta uma contextualização para o conteúdo deste estudo, juntamente com o problema de pesquisa que motivou a realização deste trabalho. Adicionalmente, o capítulo apresenta a metodologia utilizada para alcançar os resultados esperados e os apresenta, respectivamente. Por fim, o capítulo apresenta a organização do manuscrito como um todo.

1.1 Contextualização

Nas últimas décadas, a sociedade testemunhou uma transformação digital marcada pela coleta massiva e pelo uso intensivo de dados pessoais. Inicialmente, a ausência de mecanismos regulatórios e de tecnologias de proteção robustas favoreceu práticas de coleta indiscriminada, que se consolidaram como modelo de negócio predominante em diversos setores econômicos [2]. A crescente percepção de que os dados constituem um ativo estratégico, uma verdadeira *commodity* digital, trouxe à tona preocupações éticas, sociais e legais relacionadas à privacidade e ao uso justo da informação [3]. Incidentes recorrentes de vazamentos, roubo de identidade e manipulação algorítmica reforçaram a noção de que a privacidade deve ser compreendida como um direito fundamental, cuja garantia requer tanto salvaguardas normativas quanto soluções tecnológicas eficazes [4].

Nesse contexto, legislações como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[5] e a Lei Geral de Proteção de Dados do Brasil (LGPD)[6] estabeleceram marcos regulatórios que impõem obrigações rigorosas a organizações que coletam e processam dados pessoais. Entre os fundamentos legais de tratamento, o **consentimento** assume papel central, devendo ser coletado de forma livre, informada, específica e inequívoca, além de registrado de maneira transparente, versionada e auditável. Tais exigências tornam a gestão de consentimento não apenas uma questão de conformidade legal, mas

também um elemento estratégico para a construção de confiança entre organizações e titulares de dados [2].

A implementação prática desses requisitos, entretanto, permanece desafiadora. A partir da entrada em vigor do GDPR, houve um crescimento expressivo das chamadas *Consent Management Platforms* (CMPs), soluções responsáveis por operacionalizar banners e formulários de privacidade em websites. Estudos indicam que a adoção dessas plataformas passou de menos de 5% dos sites antes de 2018 para mais de 40% em 2023 no contexto europeu [2]. No Brasil, a vigência da LGPD em 2020 também impulsionou o uso dessas ferramentas. Apesar disso, análises empíricas revelam falhas significativas: mais de 60% dos sites que utilizam CMPs ainda instalam cookies de rastreamento antes da manifestação do usuário, comprometendo a conformidade regulatória [2]. Além disso, a forma como os banners são desenhados exerce influência direta sobre o comportamento dos usuários: quando a opção "rejeitar tudo" é acessível em um clique, cerca de 60% recusam os cookies; quando exige múltiplos passos, aproximadamente 90% acabam aceitando, ilustrando o chamado *paradoxo da privacidade*, em que decisões reais se distanciam das preocupações declaradas.

Outro problema estrutural diz respeito à qualidade e clareza das próprias políticas de privacidade. Pesquisas recentes evidenciam que esses documentos são frequentemente extensos, vagos e inconsistentes, o que dificulta a compreensão dos usuários e compromete o valor legal do consentimento associado [4]. A ausência de padronização para descrever riscos e práticas de tratamento resulta em lacunas que aumentam a assimetria de informação entre controladores e titulares, enfraquecendo o princípio da transparência e dificultando a responsabilização das organizações.

Paralelamente, estudos anteriores têm chamado atenção para o uso de *dark patterns* na coleta de consentimento, ou seja, práticas de design persuasivo que induzem os usuários a aceitar opções mais invasivas de privacidade [7, 3, 8]. Tais práticas não apenas colocam em dúvida a legitimidade do consentimento, mas também reforçam a necessidade de soluções técnicas que priorizem a autonomia e a autodeterminação informativa dos indivíduos.

Diante dessas limitações, a literatura recente tem explorado arquiteturas descentralizadas como alternativa às soluções tradicionais. Modelos de *dynamic consent*, implementados com o apoio de tecnologias como *blockchain* e *smart contracts*, têm buscado oferecer maior transparência, imutabilidade e rastreabilidade no gerenciamento de consentimentos [9]. Esses sistemas permitem que os titulares não apenas expressem consentimento, mas também deleguem direitos, acompanhem históricos de uso, recebam notificações de violações e revoguem permissões a qualquer momento. Ainda que promissores, tais modelos enfrentam barreiras práticas relacionadas à complexidade de gerenciamento de chaves, desempenho, escalabilidade e à tensão existente entre o direito ao esquecimento previsto

no GDPR e a imutabilidade inerente ao *blockchain*.

Esse panorama revela que, embora tenham ocorrido avanços significativos após a adoção de legislações de proteção de dados, persistem lacunas técnicas e conceituais que limitam a eficácia da gestão de consentimento. Assim, emerge a necessidade de arquiteturas mais flexíveis, modulares e interoperáveis, capazes de assegurar rastreabilidade, integridade e transparência, ao mesmo tempo em que se alinham a requisitos legais [10] e aos requisitos de privacidade [11, 12] e boas práticas de engenharia de software. É nesse espaço que se insere a presente dissertação, cujo objetivo é propor uma solução para registro, versionamento e auditoria de consentimentos, preservando o vínculo histórico entre consentimentos e versões específicas de políticas de privacidade.

1.2 Problema de Pesquisa

Embora legislações como a GDPR e a LGPD tenham estabelecido requisitos claros para a coleta, registro e auditoria do consentimento, a implementação prática desse processo continua repleta de desafios [13]. As CMPs amplamente utilizadas ainda apresentam falhas técnicas, como a instalação de cookies antes da manifestação do usuário, e problemas de usabilidade, como o uso de *dark patterns* que comprometem a legitimidade do consentimento [2, 3, 4, 13]. Além disso, políticas de privacidade extensas, vagas e inconsistentes enfraquecem o princípio da transparência e dificultam a responsabilização das organizações [13].

Outro desafio relevante refere-se às próprias limitações cognitivas dos usuários no processo de decisão. Diversos estudos demonstram que, mesmo quando as políticas de privacidade são disponibilizadas, fatores como a racionalidade limitada (*bounded rationality*) e o viés de desconto hiperbólico levam os titulares a supervalorizar consequências imediatas e subestimar riscos futuros, dificultando decisões de consentimento realmente informadas [13]. Nesse sentido, a literatura tem sugerido a adoção de mecanismos de **comunicação de riscos** para complementar avisos de privacidade, permitindo que os indivíduos compreendam melhor os potenciais efeitos adversos do processamento de seus dados e possam exercer seus direitos de maneira mais consciente.

Modelos descentralizados baseados em *blockchain* e *smart contracts* surgiram como alternativas, oferecendo imutabilidade e rastreabilidade [9]. Entretanto, tais soluções enfrentam barreiras práticas, incluindo complexidade de gerenciamento de chaves, escalabilidade limitada e tensões entre o direito ao esquecimento e a natureza imutável do registro distribuído. Assim, mesmo com os avanços acadêmicos e tecnológicos recentes, ainda não há consenso sobre arquiteturas que equilibrem, de forma prática e eficiente, requisitos de

conformidade regulatória, clareza na comunicação de riscos, segurança, escalabilidade e aplicabilidade organizacional.

Diante desse cenário, emerge a questão central que orienta esta pesquisa:

> *Como projetar e implementar uma arquitetura escalável e interoperável que permita o registro, o versionamento e a auditoria de consentimentos de usuários, assegurando rastreabilidade, integridade, comunicação transparente de riscos e conformidade com legislações de privacidade, preservando o vínculo histórico entre consentimentos e versões específicas das políticas de privacidade vigentes?*

1.3 Justificativa

O consentimento é um dos principais fundamentos legais para o tratamento de dados pessoais estabelecidos tanto pela LGPD [6] quanto pelo GDPR [5]. Sua gestão adequada é importante não apenas para evitar sanções regulatórias, mas também para construir confiança junto aos titulares de dados. No entanto, a literatura acadêmica e a prática organizacional ainda carecem de soluções concretas que conciliem conformidade legal, rastreabilidade técnica e boas práticas de engenharia de software.

As soluções atualmente predominantes, como as CMPs, apresentam limitações significativas, incluindo falhas técnicas, uso de *dark patterns* e políticas de privacidade extensas e vagas, que comprometem a transparência e a legitimidade do consentimento. Além disso, pesquisas recentes evidenciam que os titulares de dados enfrentam barreiras cognitivas no processo de decisão, como racionalidade limitada e viés de desconto hiperbólico, o que dificulta a compreensão plena das consequências de suas escolhas. Assim, mesmo quando formalmente obtido, o consentimento frequentemente não é genuinamente informado, reduzindo sua eficácia como mecanismo de proteção [13].

Nesse cenário, torna-se necessário investigar abordagens arquiteturais que aliem **conformidade regulatória, clareza na comunicação de riscos e rastreabilidade técnica**. Modelos descentralizados baseados em *blockchain* oferecem avanços em imutabilidade e auditoria, mas enfrentam desafios de aplicabilidade prática, como complexidade de gerenciamento de chaves e incompatibilidades com o direito ao esquecimento. Isso reforça a necessidade de alternativas que sejam mais flexíveis, escaláveis e aderentes ao contexto organizacional.

Dessa forma, o desenvolvimento de uma arquitetura de microsserviços para a gestão de consentimento apresenta-se como uma contribuição relevante tanto do ponto de vista científico quanto prático. Cientificamente, a proposta avança a discussão ao integrar requisitos técnicos de privacidade, segurança e rastreabilidade com preocupações regulatórias e cognitivas dos usuários. Do ponto de vista prático, oferece um modelo de referência para organizações que necessitam alinhar tecnologia, governança e requisitos regulatórios,

promovendo maior transparência, integridade e confiança nos processos de tratamento de dados pessoais.

1.4 Objetivo Geral

Avaliar, comparar arquiteturas existentes, bem como meios de persistencias, e propor uma arquitetura de software para o registro, controle e auditoria de consentimentos de usuários, assegurando integridade dos dados, rastreabilidade das operações e conformidade com legislações de privacidade.

1.5 Objetivos Específicos

Analisar e comparar arquiteturas monolíticas e baseadas em microserviços, considerando requisitos de registro, controle e auditoria de consentimentos de usuários, abordagens de persistência de dados, utilizando bancos de dados relacionais e NoSQL, quanto à capacidade de garantir integridade, rastreabilidade e versionamento das informações.

Projetar uma arquitetura de software para o registro, controle e auditoria de consentimentos de usuários, alinhada aos estilos arquiteturais e modelos de persistência avaliados. Definindo mecanismos de versionamento de políticas de privacidade, de vinculação entre políticas e registros de consentimento e de execução do direito ao esquecimento que atendam as diretrizes da LGPD.

Avaliar a arquitetura proposta quanto a desempenho, escalabilidade, segurança e conformidade com legislações de privacidade, considerando sua aplicabilidade prática.

1.6 Resultados Esperados

Espera-se, como resultado deste trabalho, a concepção e implementação de um protótipo funcional de arquitetura de software capaz de oferecer suporte à gestão de consentimentos de usuários de forma confiável e auditável. Em particular, espera-se que a solução desenvolvida seja capaz de:

1. possibilitar o cadastro, o versionamento e a consulta de políticas de privacidade;
2. registrar e auditar consentimentos de usuários de forma rastreável, preservando o vínculo histórico com as versões das políticas vigentes;
3. demonstrar a integridade dos dados por meio do uso de mecanismos de verificação, como funções de hash criptográfico;

4. apresentar características de escalabilidade, segurança e desempenho compatíveis com ambientes organizacionais e corporativos.

1.7 Contribuições do Trabalho

As principais contribuições deste trabalho podem ser sintetizadas na contribuição científica para a área de engenharia de software aplicada à privacidade e à proteção de dados, ao investigar e comparar diferentes estilos arquiteturais e abordagens de persistência. Na proposição de uma arquitetura de referência para gestão de consentimentos, alinhada a requisitos técnicos de rastreabilidade, integridade e auditoria. No apoio prático a organizações que buscam adequação às legislações de privacidade, como a LGPD e o GDPR, bem como a padrões internacionais relacionados à gestão de consentimento. E no fornecimento de uma base metodológica e arquitetural que pode ser utilizada e estendida em pesquisas futuras sobre gestão, auditoria e governança de consentimentos.

1.8 Lacunas Abordadas e Stakeholders

Apesar da existência de soluções amplamente utilizadas para gestão de consentimentos, como as *Consent Management Platforms* (CMPs), a literatura e a prática organizacional ainda apresentam lacunas relevantes no que se refere à integração entre conformidade regulatória, rastreabilidade técnica e boas práticas de arquitetura de software [2, 3, 4, 10].

Em particular, observa-se a ausência de abordagens arquiteturais que tratem de forma explícita e integrada: (i) o versionamento de políticas de privacidade; (ii) a preservação do vínculo histórico entre consentimentos e versões específicas dessas políticas; e (iii) a auditabilidade técnica dos registros de consentimento ao longo do tempo. Muitas soluções existentes priorizam aspectos funcionais ou legais, mas carecem de mecanismos arquiteturais que assegurem integridade, rastreabilidade e transparência de forma sistemática.

Além disso, a literatura aponta limitações na discussão sobre o impacto das escolhas arquiteturais, como estilos monolíticos ou baseados em microserviços e diferentes estratégias de persistência de dados, no contexto específico da gestão de consentimentos [14, 15, 16]. Este trabalho busca contribuir para esse debate ao analisar essas escolhas sob a perspectiva de requisitos regulatórios e de engenharia de software.

A proposta apresentada beneficia diferentes grupos de *stakeholders*. Do ponto de vista organizacional, gestores e responsáveis por governança de dados podem utilizar a arquitetura proposta como referência para apoiar iniciativas de conformidade com legislações de privacidade, como a LGPD e o GDPR. Para equipes técnicas, incluindo arquitetos de

software e desenvolvedores, o trabalho oferece subsídios conceituais e arquiteturais para a implementação de soluções auditáveis e escaláveis de gestão de consentimentos.

Do ponto de vista regulatório e jurídico, a proposta contribui ao oferecer mecanismos técnicos que facilitam a demonstração de conformidade e a realização de auditorias. Por fim, os titulares de dados são beneficiados indiretamente, na medida em que a arquitetura favorece maior transparência, rastreabilidade e controle sobre o uso de seus dados pessoais.

1.9 Metodologia de Pesquisa

Esta pesquisa adota a abordagem de Design Science Research (DSR), fundamentada na criação e avaliação de artefatos tecnológicos para a resolução de problemas práticos. O ciclo metodológico é estruturado em quatro etapas macro: (i) levantamento de requisitos legais e normativos (LGPD/GDPR/ISO); (ii) modelagem e especificação de uma arquitetura de microsserviços; (iii) implementação de uma prova de conceito (PoC); e (iv) avaliação técnica de segurança e conformidade. O detalhamento de cada fase, bem como a justificativa para a escolha da DSR como framework de condução, é apresentado no Capítulo 3.

1.10 Estrutura do Trabalho

Este trabalho está organizado em sete capítulos, além desta introdução, conforme descrito a seguir:

- **Capítulo 2** apresenta a fundamentação teórica que sustenta a pesquisa. São discutidos os conceitos de privacidade e proteção de dados pessoais, sua evolução no contexto digital contemporâneo e as principais regulamentações aplicáveis, com destaque para o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a Lei Geral de Proteção de Dados brasileira (LGPD) e normas internacionais relacionadas à privacidade da informação. O capítulo também aborda aspectos de consentimento e conceitos de arquitetura de software relevantes ao domínio do estudo.
- **Capítulo 3** descreve a metodologia de pesquisa adotada, fundamentada na abordagem de Design Science Research. São apresentadas as etapas do processo metodológico, incluindo o levantamento de requisitos, a modelagem e especificação arquitetural, a implementação do protótipo e os procedimentos de avaliação, detalhando como as decisões da pesquisa foram conduzidas de forma sistemática.

- **Capítulo 4** detalha a fase de engenharia de requisitos voltada à privacidade e conformidade regulatória. A investigação é fundamentada em uma Revisão Sistemática da Literatura (SLR) para identificação de técnicas e uma Revisão de Literatura Cinzenta (GLR) para mapeamento de práticas de mercado em Políticas de Privacidade. O capítulo consolida um conjunto de requisitos funcionais e não funcionais. O resultado é uma especificação técnica que alinha os princípios da ISO/IEC 29100 com as imposições legais da LGPD e do GDPR.
- **Capítulo 5** apresenta e justifica as decisões arquiteturais e de persistência de dados adotadas na solução proposta. Neste capítulo são discutidas as alternativas avaliadas, os critérios técnicos e regulatórios considerados e os trade-offs envolvidos, consolidando a arquitetura definida a partir do processo metodológico descrito no capítulo anterior.
- **Capítulo 6** descreve a concepção do artefato proposto, detalhando a arquitetura lógica e os mecanismos de proteção de dados *by design*, detalhando o desenvolvimento da Prova de Conceito (PoC), com foco na garantia de integridade documental e na implementação de estratégias de persistência que visam resolver a dicotomia entre a auditabilidade histórica e o direito ao esquecimento.
- **Capítulo 7** apresenta a avaliação da solução desenvolvida, considerando aspectos como segurança, desempenho, escalabilidade e conformidade regulatória.
- **Capítulo 8** apresenta as conclusões do trabalho, destacando as contribuições da pesquisa, suas limitações e sugestões para trabalhos futuros.

Capítulo 2

Embasamento Teórico

Este capítulo apresenta a fundamentação teórica que sustenta o desenvolvimento desta dissertação, situando o problema de pesquisa no contexto da privacidade, da proteção de dados pessoais e das soluções técnicas necessárias para sua efetiva implementação em sistemas de informação.

Inicialmente, são discutidos os conceitos de privacidade e proteção de dados, destacando sua evolução histórica e sua crescente relevância no contexto digital contemporâneo, marcado pela intensificação da coleta, processamento e compartilhamento de dados pessoais. Em seguida, são analisadas as principais legislações e normas que regulam o tratamento de dados pessoais, com ênfase no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) [5], na Lei Geral de Proteção de Dados do Brasil (LGPD) [17] e em padrões internacionais, como a ISO/IEC 29100, a ISO/IEC 29184 e a ISO/IEC TS 27560, que estabelecem princípios, requisitos e diretrizes para a gestão de privacidade e consentimento.

O capítulo também examina o consentimento como uma das bases legais centrais para o tratamento de dados pessoais, discutindo seus requisitos normativos, suas características essenciais e os desafios práticos associados à sua obtenção, manutenção, versionamento e auditoria ao longo do tempo. Nesse contexto, evidencia-se que a conformidade legal não depende apenas de aspectos jurídicos, mas exige suporte técnico adequado para garantir integridade, rastreabilidade e transparência dos registros de consentimento.

Na sequência, são discutidas abordagens de engenharia de software voltadas à conformidade regulatória, com foco em estilos arquiteturais, estratégias de persistência de dados e mecanismos de comunicação entre sistemas. São analisados aspectos relacionados ao uso de arquiteturas monolíticas e baseadas em microserviços, ao emprego de APIs como meio de integração e às boas práticas de segurança, escalabilidade e interoperabilidade necessárias para o suporte a soluções de gestão de consentimento em ambientes organizacionais.

Por fim, são apresentados e analisados trabalhos relacionados, abrangendo tanto pesquisas acadêmicas quanto sistemas e plataformas existentes de gestão de consentimentos. Essa análise permite identificar limitações e lacunas nas abordagens atuais, especialmente no que se refere à integração entre requisitos regulatórios, decisões arquiteturais e mecanismos técnicos de auditabilidade, motivando a proposta arquitetural desenvolvida nesta dissertação.

2.1 Privacidade de Dados

A privacidade configura-se como um conceito complexo e em constante transformação, que vai além da simples noção de controle sobre dados pessoais. Trata-se de um direito fundamental relacionado à autonomia dos indivíduos de gerenciar suas próprias informações, decidindo de que forma, em que momento e com quais atores esses dados podem ser compartilhados [18]. No cenário atual, o debate sobre privacidade não se restringe à proteção contra práticas de vigilância governamental ou corporativa, mas incorpora a noção de autodeterminação informacional, segundo a qual o titular deve ser capaz de exercer poder decisório efetivo sobre o ciclo de vida de seus dados [19].

Veseli *et al.* [20] discutem esse tema a partir de três esferas de atuação nas quais profissionais de engenharia de software desempenham papel essencial: (i) *user sphere*, relacionada ao ambiente do próprio usuário e aos dispositivos que utiliza, assegurando que ele mantenha controle pleno sobre suas informações; (ii) *recipient sphere*, vinculada ao contexto organizacional, na qual cabe aos engenheiros implementar práticas que reduzam riscos de exposição indevida de dados e violações de privacidade; e (iii) *joint sphere*, referente às organizações que armazenam dados pessoais em larga escala, demandando medidas mais amplas para prevenir vazamentos, bem como o uso de técnicas e ferramentas que aliem proteção de dados e segurança da informação.

Mesmo antes da consolidação do debate atual, Kalloniatis *et al.* [21] já destacavam, em 2005, que a privacidade individual estava ameaçada globalmente em virtude da intensificação do uso da internet. Os autores defendiam a criação de metodologias capazes de apoiar a especificação de requisitos de privacidade e chamavam atenção para a necessidade de harmonização internacional das legislações sobre o tema. Entretanto, reconheciam que diferenças culturais, políticas e econômicas representavam barreiras significativas a esse processo. De fato, observa-se hoje que, embora existam pontos de convergência entre legislações de diferentes países, a diversidade de contextos impede a consolidação de um marco legal único e universal sobre privacidade de dados.

2.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) [6], representa um marco regulatório para o tratamento de dados no Brasil. Inspirada em legislações internacionais, como o Regulamento Europeu (GDPR)[5], a LGPD busca harmonizar a proteção de dados com o desenvolvimento tecnológico e econômico, estabelecendo regras aplicáveis tanto ao setor público quanto ao setor privado. Seu objetivo central é assegurar os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural [6].

A LGPD estabelece como fundamentos a autodeterminação informativa, a inviolabilidade da intimidade, o respeito aos direitos humanos e a dignidade, bem como a defesa do consumidor e o incentivo à inovação. A disciplina do tratamento de dados deve observar dez princípios centrais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (*accountability*). Esses princípios orientam todo o ciclo de vida do tratamento de dados pessoais e visam garantir equilíbrio entre interesses econômicos, inovação tecnológica e proteção do indivíduo [6].

O âmbito da LGPD é amplo, abrangendo qualquer operação de tratamento realizada no território nacional, independentemente do meio ou da sede do controlador, desde que os dados pertençam a indivíduos localizados no Brasil no momento da coleta. A lei também se aplica quando a finalidade do tratamento é a oferta de bens ou serviços a pessoas situadas no Brasil. Existem, contudo, exceções expressas, como tratamentos realizados para fins exclusivamente pessoais, acadêmicos, artísticos, jornalísticos, de segurança pública ou defesa nacional [6].

O tratamento de dados pessoais somente é legítimo quando fundamentado em uma das hipóteses previstas no Art. 7º da LGPD. Entre elas, destacam-se: o consentimento do titular, o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, a realização de pesquisas, a execução de contratos, o exercício regular de direitos, a proteção da vida ou da saúde, a tutela do crédito e o legítimo interesse do controlador. Para dados sensíveis, o Art. 11 impõe requisitos mais rigorosos, como a exigência de consentimento específico e destacado ou hipóteses restritivas ligadas a interesses vitais, sanitários ou de pesquisa [6].

A LGPD reforça a posição central do titular, garantindo-lhe uma série de direitos previstos no Art. 18. Esses incluem: confirmação da existência de tratamento, acesso aos dados, correção, anonimização, bloqueio ou eliminação, portabilidade, informação sobre compartilhamento, possibilidade de negar consentimento e revogação a qualquer tempo. Além disso, a lei assegura o direito de revisão de decisões automatizadas (Art.

20), permitindo que o titular solicite avaliação por pessoa natural em casos que afetem diretamente seus interesses [6].

A lei define os papéis de controlador e operador, bem como a obrigatoriedade de indicação de um encarregado pelo tratamento de dados (DPO). Estabelece ainda deveres de registro das operações, de elaboração de relatórios de impacto à proteção de dados (DPIA) e de adoção de medidas técnicas e administrativas de segurança desde a fase de concepção (*privacy by design*). A Autoridade Nacional de Proteção de Dados (ANPD) foi criada para fiscalizar, orientar e regulamentar a aplicação da lei [6].

O regime sancionatório da LGPD prevê medidas administrativas que vão desde advertências até multas de até 2% do faturamento da pessoa jurídica no Brasil, limitadas a R$ 50 milhões por infração, além de medidas como bloqueio ou exclusão de dados pessoais. A aplicação das sanções observa critérios de proporcionalidade, reincidência e cooperação do agente, reforçando o princípio da responsabilização [6].

A LGPD, portanto, estabelece um arcabouço normativo abrangente para o tratamento de dados pessoais no Brasil. Ao equilibrar princípios de proteção com a necessidade de inovação e desenvolvimento econômico, a lei busca não apenas resguardar direitos individuais, mas também fornecer segurança jurídica às organizações. Sua implementação prática, contudo, impõe desafios técnicos, organizacionais e culturais, que exigem soluções arquiteturais capazes de garantir conformidade, rastreabilidade e efetiva proteção da privacidade.

2.3 General Data Protection Regulation (GDPR)

O Regulamento (UE) 2016/679, conhecido como General Data Protection Regulation (GDPR), foi aprovado em abril de 2016 e entrou em vigor em maio de 2018, substituindo a Diretiva 95/46/CE. Diferentemente das diretivas, que necessitam ser internalizadas pelas legislações nacionais, o GDPR possui efeito direto e uniforme em todos os Estados-Membros da União Europeia. Seu objetivo é harmonizar a proteção de dados pessoais na Europa, reforçar os direitos fundamentais dos cidadãos e estabelecer regras claras para organizações que processam dados dentro e fora do território europeu [5].

A GDPR fundamenta-se na proteção de dados como um direito fundamental previsto na Carta de Direitos Fundamentais da União Europeia (Art. 8). O regulamento adota sete princípios que norteiam todo tratamento de dados: (i) licitude, lealdade e transparência; (ii) limitação da finalidade; (iii) minimização dos dados; (iv) exatidão; (v) limitação da conservação; (vi) integridade e confidencialidade; e (vii) responsabilização (*accountability*). Tais princípios orientam controladores e operadores em todas as etapas do ciclo de vida dos dados [5].

A GDPR possui escopo territorial amplo, aplicando-se não apenas às operações realizadas na União Europeia, mas também a organizações fora da UE que ofereçam bens ou serviços a titulares localizados em seu território ou que monitorem seu comportamento online. O regulamento cobre qualquer operação de tratamento de dados pessoais, seja automatizada ou manual, quando integrados a um sistema estruturado de arquivos [5].

O Art. 6º do GDPR prevê seis bases legais para o tratamento de dados: consentimento; execução de contrato; cumprimento de obrigação legal; proteção de interesses vitais; exercício de funções de interesse público ou autoridade oficial; e interesses legítimos do controlador ou de terceiros, desde que não se sobreponham aos direitos fundamentais do titular. Para o tratamento de dados sensíveis (Art. 9º), o regulamento é mais restritivo, exigindo consentimento explícito ou hipóteses excepcionais, como interesse público relevante, medicina preventiva ou pesquisa científica [5].

O regulamento fortalece os direitos dos titulares de dados, ampliando-os em relação à diretiva anterior. Além dos direitos de acesso, retificação, apagamento e oposição, o GDPR introduz inovações relevantes: o **direito ao esquecimento** (Art. 17), permitindo ao titular solicitar a exclusão de seus dados em determinadas circunstâncias; o **direito à portabilidade** (Art. 20), que assegura a transferência de dados a outro fornecedor de serviços; e o direito de não se submeter a decisões automatizadas com efeitos jurídicos significativos (Art. 22), reforçando a necessidade de intervenção humana em sistemas de perfis e algoritmos [5].

A GDPR estabelece deveres rigorosos para controladores e operadores. Entre eles destacam-se: a obrigação de manter registros detalhados de operações (Art. 30); a realização de avaliações de impacto à proteção de dados (DPIA – Art. 35) para operações de alto risco; e a designação de um Encarregado de Proteção de Dados (DPO) em determinadas circunstâncias (Art. 37). O regulamento também introduz o princípio do *privacy by design and by default*, exigindo que medidas de proteção sejam incorporadas desde a concepção de sistemas e serviços [5].

A GDPR regula de forma detalhada a transferência de dados para fora da União Europeia (Arts. 44–50). Essas só são permitidas para países com decisão de adequação emitida pela Comissão Europeia, ou mediante garantias adequadas, como cláusulas contratuais padrão, regras corporativas globais (*binding corporate rules*) ou mecanismos de certificação reconhecidos. A lógica é assegurar que o nível de proteção não seja enfraquecido quando os dados circulam além das fronteiras europeias [5].

A aplicação do GDPR é descentralizada, realizada por autoridades nacionais de proteção de dados, sob coordenação do Comitê Europeu de Proteção de Dados (EDPB). O regulamento prevê sanções severas em caso de infrações: multas administrativas que podem atingir até €20 milhões ou 4% do faturamento anual global da organização, preva-

lecendo o maior valor. A severidade do regime sancionatório reforça o caráter vinculante e a seriedade do cumprimento da norma [5].

A GDPR consolidou-se como referência global em proteção de dados pessoais, influenciando legislações em diversos países, incluindo a LGPD no Brasil. Ao conjugar princípios robustos, direitos ampliados aos titulares e um regime de sanções rigoroso, o regulamento busca criar um ambiente digital mais seguro e transparente, ao mesmo tempo em que promove a confiança entre cidadãos, empresas e autoridades públicas.

Embora a LGPD tenha sido fortemente inspirada na GDPR, as duas legislações apresentam diferenças relevantes em termos de escopo, princípios, bases legais e mecanismos de aplicação. A Tabela 2.1 sintetiza as principais convergências e divergências, com destaque para o tratamento do **consentimento**, aspecto central desta dissertação.

Tabela 2.1: Comparação entre GDPR e LGPD

Categoria	GDPR	LGPD
Escopo territorial	Aplicável a operações de tratamento realizadas na UE e a organizações fora da UE que ofereçam bens/serviços ou monitorem indivíduos na UE.	Aplicável a operações realizadas no Brasil ou relativas a titulares localizados no Brasil no momento da coleta.
Princípios	7 princípios: licitude, lealdade, transparência; limitação da finalidade; minimização; exatidão; limitação da conservação; integridade/confidencialidade; responsabilização.	10 princípios: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização.
Bases legais	6 bases (consentimento, contrato, obrigação legal, interesses vitais, interesse público/autoridade oficial, legítimo interesse).	10 bases, incluindo as do GDPR e outras específicas, como proteção ao crédito e pesquisas por órgãos de pesquisa.
Consentimento	Deve ser **livre, específico, informado e inequívoco**. Para dados sensíveis, exige-se consentimento **explícito**. Revogação deve ser tão fácil quanto a concessão (Art. 7º e 9º).	Deve ser **livre, informado e inequívoco**, com destaque para cláusulas contratuais. Para dados sensíveis, requer consentimento **específico e destacado** (Art. 7º, 8º e 11). Pode ser revogado a qualquer tempo, de forma gratuita e facilitada.
Direitos dos titulares	Acesso, retificação, apagamento, oposição, portabilidade, restrição do tratamento, direito ao esquecimento, revisão de decisões automatizadas.	Confirmação, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, informação sobre compartilhamento, revogação de consentimento, revisão de decisões automatizadas.
Agentes de tratamento	Controlador, processador e Data Protection Officer (DPO) quando aplicável.	Controlador, operador e Encarregado (DPO). Obrigatoriedade mais ampla, podendo ser flexibilizada pela ANPD.
Transferência internacional	Permitida apenas para países com nível adequado de proteção ou com garantias adequadas (Cláusulas Padrão, Regras Corporativas Vinculantes (BCRs) – regras internas aprovadas por autoridade europeia para transferências intragrupo), Certificações).	Permitida em hipóteses semelhantes, mas depende de regulamentação da ANPD sobre critérios de adequação e mecanismos de transferência.
Sanções	Multas de até €20 milhões ou 4% do faturamento global, além de restrições e suspensão do tratamento.	Multas de até R$ 50 milhões por infração, além de bloqueio e eliminação de dados.

As convergências e diferenças entre GDPR e LGPD evidenciam a necessidade de diretrizes técnicas que operacionalizem requisitos jurídicos de consentimento, transparência e responsabilização. É nesse ponto que ganham relevância as normas ISO/IEC, que traduzem princípios em controles e estruturas implementáveis no ciclo de vida de sistemas.

2.4 ISO/IEC 29100 – Estrutura de Privacidade

A norma ISO/IEC 29100, adotada no Brasil como ABNT NBR ISO/IEC 29100:2020, estabelece uma estrutura de alto nível para a proteção de dados pessoais em sistemas de tecnologia da informação e comunicação (TIC). Diferentemente das legislações nacionais, a norma não cria obrigações legais, mas fornece um *framework* técnico e organizacional para orientar o tratamento responsável de dados pessoais, complementando as exigências regulatórias existentes [22].

A norma tem como objetivos principais: (i) especificar uma terminologia comum para privacidade; (ii) definir os atores envolvidos no tratamento de dados pessoais e seus papéis; (iii) descrever requisitos de salvaguarda da privacidade; e (iv) referenciar princípios internacionalmente reconhecidos de proteção de dados. É aplicável a organizações e indivíduos envolvidos em especificação, aquisição, concepção, desenvolvimento, manutenção e operação de sistemas de TIC que tratam dados pessoais [22].

O documento identifica quatro atores principais: (i) **titulares de dados pessoais**, que fornecem informações e determinam suas preferências de privacidade; (ii) **controladores**, responsáveis por definir as finalidades e os meios de tratamento; (iii) **operadores**, que processam os dados em nome do controlador; e (iv) **terceiros**, que recebem dados mas não atuam em nome do controlador [22]. Essa taxonomia é consistente com legislações como a LGPD e o GDPR, permitindo interoperabilidade conceitual.

A norma descreve fatores que influenciam a definição de requisitos de salvaguarda, incluindo exigências legais e regulatórias, obrigações contratuais, fatores de negócio e preferências individuais dos titulares. Esses requisitos devem ser tratados no contexto de uma gestão de riscos de privacidade, que envolve identificação, avaliação, tratamento, comunicação e monitoramento de riscos. Um elemento central é a realização de Avaliações de Impacto de Privacidade (Privacy Impact Assessments – PIA), para antecipar implicações antes da implementação de novos sistemas ou serviços [22].

A ISO/IEC 29100 sistematiza 11 princípios fundamentais que devem nortear projetos e operações envolvendo dados pessoais [22]: 1. Consentimento e escolha; 2. Especificação e legitimidade de objetivo; 3. Limitação de coleta; 4. Minimização de dados; 5. Limitação de uso, retenção e divulgação; 6. Precisão e qualidade; 7. Abertura, transparência e notificação; 8. Acesso e participação individual; 9. Responsabilização; 10. Segurança da informação; e 11. Conformidade com a privacidade.

Entre esses princípios, destaca-se o de **consentimento e escolha**, que exige que os titulares tenham mecanismos claros, acessíveis e compreensíveis para decidir sobre o tratamento de seus dados, incluindo a possibilidade de retirar o consentimento de maneira facilitada. Esse princípio conecta-se diretamente ao problema de pesquisa desta disser-

tação, pois reforça a necessidade de arquiteturas que permitam o registro inequívoco, a rastreabilidade e a revogação transparente do consentimento [22].

A ISO/IEC 29100 fornece, portanto, um arcabouço de referência para integrar princípios de privacidade em sistemas de TIC desde a concepção (*privacy by design*) até a operação. Ao alinhar práticas organizacionais, técnicas e regulatórias, a norma busca apoiar organizações na criação de ambientes confiáveis, capazes de atender a diferentes legislações e expectativas sociais quanto à proteção de dados pessoais [22].

2.5 ISO/IEC 29184 – Avisos de Privacidade Online e Consentimento

A norma ISO/IEC 29184:2020 [23] estabelece diretrizes para a elaboração de avisos de privacidade online e para a obtenção de consentimento dos titulares de dados pessoais de maneira justa, transparente, inequívoca e revogável. Diferente da ISO/IEC 29100, que apresenta um framework de princípios, a ISO/IEC 29184 foca na implementação prática de dois deles: **consentimento e escolha**, e **abertura, transparência e notificação** [23].

O objetivo central da norma é assegurar que os titulares compreendam como seus dados são coletados e tratados, e que possam exercer escolhas de maneira consciente. Para isso, define controles que moldam tanto o conteúdo e a forma dos avisos quanto o processo de solicitação de consentimento. A norma é aplicável a qualquer contexto online no qual haja coleta de dados pessoais, como websites, aplicativos móveis ou serviços digitais [23].

A ISO/IEC 29184 estabelece requisitos para a apresentação de avisos de privacidade, os quais devem ser [23]: a) **Claros e compreensíveis**: redigidos em linguagem simples e acessível, sem jargões técnicos; b) **Disponibilizados no momento e local apropriados**: preferencialmente antes da coleta dos dados; c) **Acessíveis**: em formatos compatíveis com diferentes dispositivos e tecnologias assistivas; e d) **Versionados**: permitindo que titulares consultem tanto a versão em vigor quanto aquelas vinculadas a consentimentos anteriores.

O conteúdo mínimo de um aviso deve incluir: finalidades da coleta, identificação do controlador, métodos de coleta e uso, transferências para terceiros, período de retenção dos dados, riscos associados, direitos dos titulares e canais para consulta ou reclamação. No que se refere ao consentimento, a norma detalha critérios fundamentais [23]: 1. **Validade**: deve ser obtido de forma livre, informada, inequívoca e específica; 2. **Ação afirmativa**: requer um ato claro do titular, como clicar em uma caixa de seleção ou botão; 3. **Separação**: deve ser distinto de outros termos contratuais ou condições de uso; 4. **Granularidade**: titulares devem poder consentir separadamente em relação a elementos

necessários e opcionais de dados; e 5. **Revogabilidade**: a retirada do consentimento deve ser tão fácil quanto sua concessão. A norma também recomenda que o consentimento seja renovado em caso de mudanças substanciais nas condições de tratamento, como alteração de finalidade, transferência para novos terceiros ou extensão do período de retenção.

Um elemento inovador da norma é a ênfase na geração de **recibos de consentimento**, que funcionam como comprovantes digitais do ato de consentir. Esses recibos devem registrar informações essenciais como identidade do controlador, finalidades aprovadas, base legal utilizada, elementos de dados coletados, bem como data, hora e método da coleta. Essa prática fortalece a auditabilidade e a responsabilização das organizações [23].

A ISO/IEC 29184 fornece um guia operacional para transformar princípios de privacidade em práticas concretas em ambientes online. Ao padronizar avisos de privacidade e processos de coleta de consentimento, contribui para maior transparência e confiança, além de alinhar sistemas técnicos aos requisitos de legislações como a GDPR e a LGPD. Para esta dissertação, a norma é particularmente relevante por destacar mecanismos que garantem rastreabilidade, clareza e revogabilidade do consentimento, pilares centrais da arquitetura proposta [23].

2.6 ISO/IEC TS 27560 – Estrutura de informações do registro de consentimento

A ISO/IEC TS 27560:2023, intitulada *Privacy Technologies — Consent record information structure* [24], estabelece uma estrutura padronizada para o registro de consentimentos relacionados ao tratamento de dados pessoais em sistemas de tecnologia da informação. Trata-se de uma especificação técnica desenvolvida no âmbito do subcomitê ISO/IEC JTC 1/SC 27, que tem como objetivo harmonizar e uniformizar a forma como consentimentos são documentados, armazenados e auditados em diferentes contextos organizacionais [24].

O documento define requisitos técnicos para a representação estruturada de informações associadas ao consentimento, de forma a garantir interoperabilidade entre sistemas distintos e a permitir que o consentimento seja registrado, gerenciado e auditado ao longo do tempo. Seu escopo abrange tanto o tratamento de dados pessoais comuns quanto dados sensíveis, fornecendo orientações aplicáveis a organizações de diversos portes e setores [24].

A ISO/IEC TS 27560 especifica um conjunto mínimo de elementos que devem compor um registro de consentimento, incluindo [24]: 1. **Identificação do titular**: informações que permitem vincular o consentimento a um indivíduo específico; 2. **Identificação do controlador**: entidade responsável pelo tratamento de dados; 3. **Descrição da política ou aviso de privacidade**: referência à versão da política vigente no momento

do consentimento; 4. **Finalidades do tratamento**: objetivos específicos para os quais os dados foram coletados e autorizados; 5. **Condições de validade**: período de validade ou condições para revogação do consentimento; e 6. **Metadados do consentimento**: data, hora, canal de coleta, meio de autenticação e prova criptográfica.

A estrutura definida pela norma visa assegurar que o consentimento seja: **Rastreável**: cada consentimento deve ser vinculado a uma versão específica da política de privacidade aceita; **Auditável**: o registro deve permitir comprovar, perante autoridades ou terceiros, que o consentimento foi obtido de forma válida; **Imutável**: alterações posteriores devem ser registradas como novos eventos, sem sobrescrever o histórico; e **Interoperável**: a estrutura deve permitir troca de informações entre diferentes sistemas de forma padronizada.

A norma contribui para a efetiva implementação de requisitos previstos em legislações como o GDPR [5] e a LGPD[6], que exigem consentimento inequívoco, informado e revogável a qualquer tempo. Ao padronizar a forma como consentimentos são registrados e preservados, a ISO/IEC TS 27560 fornece subsídios técnicos para operacionalizar princípios de transparência, responsabilização (*accountability*) e autodeterminação informacional [24].

A ISO/IEC TS 27560 representa um passo importante para a consolidação de práticas técnicas que assegurem a confiabilidade da gestão de consentimentos. Sua adoção facilita a criação de sistemas interoperáveis, robustos e auditáveis, sendo diretamente aplicável ao objetivo desta dissertação, que propõe uma arquitetura de microsserviços orientada ao registro, versionamento e auditoria de consentimentos [24].

2.7 Consentimento como base legal de tratamento de dados

O consentimento ocupa posição central no debate sobre privacidade e proteção de dados, sendo reconhecido como uma das principais bases legais tanto no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) [5] quanto na Lei Geral de Proteção de Dados brasileira (LGPD) [6]. Em ambos os regulamentos, ele deve ser obtido de forma **livre, informada, específica e inequívoca**, representando um ato afirmativo do titular que autoriza o tratamento de seus dados pessoais [5, 6]. Para dados sensíveis, ambos os regimes exigem consentimento **explícito**, o que reforça a necessidade de clareza e de mecanismos de prova associados ao processo de coleta.

No contexto regulatório, a GDPR estabelece que a revogação do consentimento deve ser tão simples quanto a sua concessão (Art. 7º) [5], enquanto a LGPD assegura que essa revogação deve ser gratuita e facilitada (Art. 8º) [6]. Essa simetria normativa

reflete o princípio da *autodeterminação informacional*, pelo qual o indivíduo mantém controle contínuo sobre suas escolhas. Contudo, a prática organizacional revela desafios significativos, como o uso de *dark patterns* em banners de consentimento e a dificuldade dos usuários em compreender políticas extensas e pouco transparentes [2, 3, 4].

As normas internacionais complementam o arcabouço jurídico ao oferecer diretrizes técnicas para a implementação do consentimento. A ISO/IEC 29100 [22] inclui o princípio de **consentimento e escolha** como fundamento essencial da proteção de dados, reforçando a necessidade de mecanismos claros e acessíveis para o titular [22]. A ISO/IEC 29184 [23], por sua vez, detalha requisitos para a apresentação de avisos de privacidade online e para a coleta justa e transparente do consentimento, incluindo granularidade, revogabilidade e emissão de recibos [23]. Já a ISO/IEC TS 27560 [24] estabelece uma estrutura padronizada para registros de consentimento, contemplando metadados como finalidade, controlador, versão da política de privacidade e prova criptográfica, garantindo rastreabilidade e auditabilidade [24].

A literatura também destaca a complexidade do ecossistema técnico-jurídico associado ao consentimento. Estudos sobre *Consent Management Platforms* (CMPs) [2, 25, 26] demonstram que, embora projetadas para operacionalizar o consentimento de forma padronizada, muitas vezes essas plataformas assumem papéis ambíguos entre *processadores* e *controladores*, o que gera incertezas sobre suas obrigações legais e responsabilidades [27]. Além disso, análises empíricas apontam violações frequentes, como o pré-carregamento de cookies antes da manifestação do usuário ou a apresentação enviesada de opções, comprometendo a validade do consentimento coletado.

Em áreas sensíveis, como a saúde, o consentimento digital (*e-consent*) tem sido explorado como forma de conciliar exigências regulatórias com a necessidade de dinamismo e continuidade em pesquisas biomédicas. No entanto, modelos baseados apenas em consentimento amplo ou opt-out revelam fragilidades éticas e legais, especialmente diante das exigências de granularidade, renovação e revogabilidade previstas pelo GDPR [28]. Tais experiências evidenciam a importância de sistemas que permitam engajamento contínuo e transparente dos titulares, aproximando-se do conceito de *dynamic consent*.

Diante desse panorama, torna-se evidente que o consentimento, embora essencial, não é trivial em sua operacionalização. Para ser juridicamente válido e tecnicamente confiável, requer arquiteturas que integrem aspectos legais, normativos e de usabilidade, assegurando tanto a conformidade regulatória quanto a efetividade prática da autodeterminação informacional [29]. É nesse contexto que se insere esta dissertação, ao propor uma arquitetura de microsserviços orientada à rastreabilidade, versionamento e auditoria de consentimentos, alinhada às legislações vigentes e às melhores práticas internacionais.

2.7.1 Consentimento na LGPD, GDPR e Normas ISO/IEC

O consentimento, embora seja reconhecido tanto pela LGPD quanto pelo GDPR como uma das principais bases legais para o tratamento de dados pessoais, apresenta diferenças quanto à forma de obtenção, revogação e registro. As normas ISO/IEC complementam esses marcos legais ao fornecer diretrizes técnicas que operacionalizam princípios de privacidade, traduzindo exigências jurídicas em práticas de engenharia de software. A Tabela 2.2 sintetiza os principais aspectos relacionados ao consentimento, destacando como cada legislação e norma internacional o trata. Essa visão comparativa é fundamental para fundamentar a proposta desta dissertação, que busca alinhar conformidade regulatória, boas práticas técnicas e mecanismos de rastreabilidade e auditoria.

Tabela 2.2: Comparação do tratamento do consentimento na LGPD, GDPR e normas ISO/IEC

Aspecto	**LGPD**	**GDPR**	**ISO/IEC 29100**	**ISO/IEC 29184**	**ISO/IEC TS 27560**
Definição	Livre, informado, inequívoco; sensíveis: específico e destacado.	Livre, específico, informado, inequívoco; sensíveis: explícito.	Princípio de consentimento e escolha.	Consentimento como ato afirmativo claro, granular e separado.	Estrutura de registro vinculada a política e finalidade.
Forma de obtenção	Escrito ou outro meio que demonstre vontade.	Exige opt-in; caixas pré-marcadas inválidas.	Ênfase em escolha clara pelo titular.	Granularidade, separação e recibo digital de consentimento.	Define metadados obrigatórios de coleta (método, canal, data).
Revogação	Gratuita e facilitada a qualquer tempo.	Tão simples quanto a concessão.	Escolha contínua garantida ao titular.	Retirada tão simples quanto concessão; renovação em mudanças.	Registro deve conter condições de validade e revogação.
Prova / registro	Ônus do controlador.	Controlador deve demonstrar validade.	Responsabilização (*accountability*).	Exige recibo como evidência de coleta.	Estrutura padronizada com identificação, finalidade, versão e prova criptográfica.
Vínculo com políticas	Associado a cláusulas ou políticas transparentes.	Deve estar acompanhado de aviso claro.	Relacionado a princípios de abertura e transparência.	Define requisitos mínimos para avisos de privacidade.	Registro deve vincular-se à versão específica da política aceita.

2.8 Arquitetura de software para conformidade regulatória

O cumprimento de legislações como a LGPD e o GDPR demanda que sistemas de software incorporem requisitos regulatórios desde a concepção, em consonância com os princípios de *privacy by design* e *privacy by default* [30]. Nesse cenário, a arquitetura de software assume papel central, pois deve conciliar flexibilidade, escalabilidade e segurança com a necessidade de garantir rastreabilidade e auditabilidade no tratamento de dados pessoais.

Em especial, a gestão de consentimento exige soluções arquiteturais capazes de lidar com versionamento, revogação e vinculação inequívoca a políticas de privacidade vigentes.

A segurança constitui dimensão fundamental para a validade do consentimento, visto que apenas registros íntegros, protegidos contra manipulação e acessos não autorizados, podem ser considerados juridicamente válidos. Entre as práticas recomendadas destacam-se: autenticação robusta por meio de *tokens* (e.g., JWT), controle de acesso baseado em papéis (RBAC) ou atributos (ABAC), criptografia ponta a ponta (AES-256, RSA/ECC), pseudonimização, anonimização e monitoramento contínuo de incidentes [31]. Esses mecanismos podem ser incorporados em diferentes estilos arquiteturais, ainda que com distintas estratégias de implementação e níveis de granularidade no controle das interações entre componentes.

Além disso, a rastreabilidade é reforçada pelo uso de registros imutáveis de consentimento, associados a provas criptográficas e *logging* distribuído, o que facilita a prestação de contas perante autoridades regulatórias. Nesse sentido, a literatura sobre modelos formais em saúde destaca que técnicas de verificação podem garantir a consistência lógica de políticas de consentimento e reduzir ambiguidades em sua aplicação [32]. Tais requisitos podem ser contemplados tanto em arquiteturas monolíticas quanto em arquiteturas de microsserviços, embora cada abordagem apresente vantagens e limitações específicas em termos de modularidade, governança e auditabilidade.

A escalabilidade é igualmente crítica, sobretudo em plataformas globais que lidam com altos volumes de usuários e solicitações simultâneas. O uso de orquestração de contêineres (como Kubernetes), arquiteturas orientadas a eventos e *service mesh* (como Istio) possibilita balanceamento dinâmico de carga, implantação multi-região e monitoramento distribuído de desempenho [29]. Por outro lado, arquiteturas monolíticas podem oferecer benefícios em cenários de menor complexidade operacional, com maior simplicidade de implantação, integração e gestão centralizada dos componentes.

Antunes e Guimarães [33] reforçam que a implementação de privacidade em microsserviços deve adotar múltiplas linhas defensivas, com níveis variados de granularidade e versatilidade. O uso combinado de padrões como *gatekeeper*, *service*, *enclave*, *endpoint* e *sidecar* permite maior resiliência e adaptabilidade diante de requisitos regulatórios dinâmicos e ameaças emergentes. Ainda assim, a adoção desses padrões deve ser analisada em função do estilo arquitetural escolhido e dos objetivos específicos do sistema.

De modo geral, a literatura demonstra que diferentes arquiteturas de software podem servir de base para o desenvolvimento de sistemas em conformidade regulatória, desde que aliadas a boas práticas de segurança, rastreabilidade e escalabilidade. Nesse sentido, a presente dissertação não parte da premissa de uma arquitetura previamente definida, mas realiza uma avaliação comparativa entre abordagens monolíticas e baseadas

em microsserviços, a fim de identificar aquela mais adequada para sustentar requisitos como granularidade, rastreabilidade, revogabilidade do consentimento, auditoria contínua e vínculo inequívoco com versões específicas de políticas de privacidade.

2.9 Trabalhos relacionados

Diversos trabalhos na literatura abordam o gerenciamento de consentimento sob perspectivas técnicas, formais e regulatórias, buscando alinhar sistemas de software às exigências de legislações como o GDPR e a LGPD. Marillonnet et al. [34] propuseram um modelo de gerenciamento de consentimento centrado no usuário para plataformas de múltiplos serviços. O estudo utiliza uma arquitetura modular que combina políticas de privacidade com preferências declaradas pelos titulares, permitindo uma personalização mais granular do consentimento. O método inclui o design de um sistema baseado em regras e simulações em cenários multisserviços. Os resultados mostram que abordagens centradas no usuário aumentam a transparência e reduzem riscos de consentimentos inválidos, embora ainda enfrentem limitações de escalabilidade em contextos de grande volume de dados.

Santos et al. [27] analisaram o papel das *Consent Management Platforms* (CMPs) no contexto do GDPR, com foco na ambiguidade entre sua atuação como processadores ou controladores. O estudo combina análise legal e experimentação técnica em plataformas amplamente utilizadas (Quantcast e OneTrust), investigando como os CMPs coletam, processam e transmitem sinais de consentimento. Os resultados indicam que, embora formalmente classificados como processadores no âmbito do *Transparency and Consent Framework* (TCF), os CMPs em muitos casos exercem funções típicas de controladores, como a varredura e categorização de cookies ou a implementação de interfaces enviesadas para maximizar a aceitação. Essa dualidade de papéis levanta questões de responsabilização legal e reforça a necessidade de maior clareza regulatória sobre a atribuição de responsabilidades nesse ecossistema.

Chhetri et al. [29] apresentaram uma ferramenta para gerenciamento de consentimento e verificação automatizada de conformidade com o GDPR. O trabalho adota uma arquitetura baseada em microsserviços e APIs RESTful, utilizando autenticação via *JWT*, registros imutáveis e provas criptográficas. O método envolve o desenvolvimento de um protótipo validado em cenários de cidades inteligentes e seguros de veículos. Os resultados indicam que o sistema suporta mais de 200.000 usuários ativos com 241 requisições por segundo, demonstrando viabilidade em ambientes de larga escala.

Em um estudo voltado a aplicações móveis globais, Erigha et al. [31] propuseram uma arquitetura de gerenciamento de consentimento compatível com o GDPR, baseada em microsserviços em nuvem. O método adotado envolve o design modular com orquestração

em Kubernetes e integração com *service mesh* para comunicação segura. O sistema inclui serviços de logging imutável, orquestração de preferências e relatórios de conformidade. Os principais achados reforçam que arquiteturas modulares e orientadas a eventos são mais adaptáveis a requisitos regulatórios dinâmicos e facilitam auditorias distribuídas.

Antunes e Guimarães [33] propuseram um guia para implementação de privacidade em arquiteturas de microsserviços. O trabalho utiliza um método de revisão sistemática e modelagem arquitetural, identificando sete padrões de proteção de privacidade: *gatekeeper*, *service*, *enclave*, *endpoint*, *mesh*, *federation* e *sidecar*. O estudo conclui que a combinação de múltiplas linhas defensivas, com diferentes níveis de granularidade, aumenta a resiliência e a conformidade regulatória. Esse framework é especialmente relevante para a integração de mecanismos de consentimento em ambientes distribuídos.

Peyrone [32] explorou o uso de modelos formais para a gestão de consentimento. O método adotado inclui a aplicação de lógica temporal e ontologias para especificar políticas de privacidade e verificar sua conformidade. Os resultados evidenciam que abordagens formais permitem detectar inconsistências e garantir a aplicação correta das regras de consentimento em ambientes críticos, como sistemas hospitalares, onde dados sensíveis exigem níveis elevados de proteção.

Novikova et al. [4] propõem uma metodologia baseada em ontologias para análise de políticas de privacidade e cálculo de índices de risco associados ao tratamento de dados. O método envolve mineração de textos de políticas e classificação semântica em categorias de risco. Os resultados mostram que políticas vagas ou genéricas aumentam substancialmente o risco percebido e reduzem a legitimidade do consentimento obtido. O estudo destaca a importância de alinhar gestão de consentimento a políticas de privacidade claras e consistentes.

Bax e Barbosa [35] abordaram o consentimento sob a perspectiva de modelagem ontológica, buscando representar de forma estruturada os conceitos e relações envolvidos no tratamento de dados pessoais. O método adotado envolve a construção de uma ontologia de consentimento baseada em princípios legais e normativos, de modo a padronizar terminologias e reduzir ambiguidades presentes em políticas de privacidade. Os principais achados indicam que a adoção de ontologias pode favorecer a interoperabilidade entre sistemas, a clareza na comunicação com os titulares e a rastreabilidade de decisões relacionadas ao consentimento. Embora não apresente uma arquitetura técnica para implementação prática, o estudo oferece uma contribuição conceitual importante que complementa iniciativas normativas, como a ISO/IEC TS 27560, ao propor um modelo formal para representação do consentimento.

Os estudos demonstram diferentes perspectivas para a gestão de consentimento: desde abordagens centradas no usuário [34], análises críticas de plataformas [27], até arquiteturas

baseadas em microsserviços [29, 31], modelos formais [32] e frameworks arquiteturais [33]. Em comum, todos reconhecem que o consentimento é peça-chave para a conformidade regulatória, mas apontam lacunas técnicas, organizacionais e de usabilidade que ainda comprometem sua efetividade. Essa diversidade de abordagens evidencia a relevância da proposta desta dissertação, que busca integrar princípios legais e normativos a uma arquitetura técnica baseada em microsserviços, voltada para rastreabilidade, versionamento e auditoria de consentimentos.

Capítulo 3

Metodologia

Este capítulo apresenta a metodologia de pesquisa adotada, fundamentada na abordagem de *Design Science Research* (DSR). A DSR é amplamente reconhecida na área de Sistemas de Informação e Ciência da Computação como uma estratégia para a criação e avaliação de artefatos tecnológicos inovadores, destinados à solução de problemas práticos e relevantes [1].

O ciclo metodológico da DSR é estruturado em fases iterativas que envolvem: (i) identificação do problema; (ii) definição dos objetivos da solução; (iii) construção do artefato; (iv) demonstração; (v) avaliação; e (vi) comunicação. Além disso, a DSR admite a retroalimentação entre etapas, de modo que novos insights ou falhas detectadas em fases posteriores possam levar ao refinamento das fases anteriores. A Figura 3.1 ilustra o processo metodológico adotado nesta dissertação.

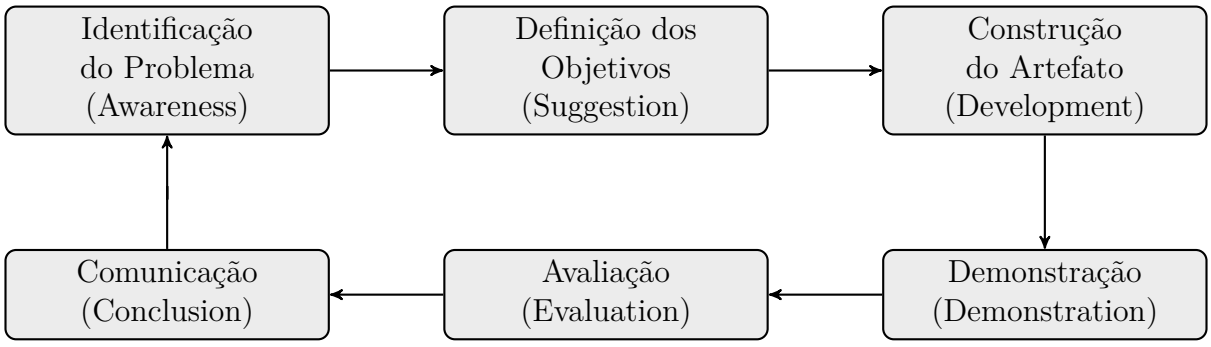

Figura 3.1: Ciclo da Design Science Research (adaptado de Vaishnavi & Kuechler [1]).

3.1 Estratégia de Pesquisa

A DSR busca resolver problemas práticos por meio do desenvolvimento de artefatos inovadores, como modelos, métodos, arquiteturas e sistemas. A abordagem é particularmente

adequada quando a pesquisa envolve a conciliação de requisitos normativos, técnicos e organizacionais, como é o caso da conformidade regulatória em proteção de dados pessoais.

Neste trabalho, a DSR foi aplicada de forma cíclica, partindo da análise do problema da gestão de consentimento, avançando pela construção e demonstração de uma arquitetura baseada em microsserviços, até sua avaliação e comunicação dos resultados à comunidade acadêmica e ao setor organizacional.

3.1.1 Identificação do Problema

Esta etapa corresponde à fase de *awareness of problem*, em que o pesquisador toma consciência do problema a ser resolvido. No contexto desta dissertação, o problema foi evidenciado por limitações das legislações (LGPD e GDPR) em termos de operacionalização prática dos requisitos de consentimento, exigências estabelecidas por normas internacionais (ISO/IEC 29100, ISO/IEC 29184, ISO/IEC TS 27560) sobre registro, versionamento e auditabilidade e deficiências de soluções existentes, como *Consent Management Platforms*, que frequentemente apresentam falhas de conformidade, uso de *dark patterns* e registros pouco transparentes.

A combinação desses fatores configura um cenário onde ainda não existem arquiteturas consolidadas que garantam, simultaneamente, rastreabilidade, auditabilidade, escalabilidade e usabilidade na gestão de consentimento.

3.1.2 Definição dos Objetivos da Solução

Corresponde à fase de *suggestion*, na qual foi estabelecido os objetivos do artefato desenvolvido. O objetivo principal foi projetar uma arquitetura modular, escalável e auditável que permitiu o registro inequívoco de consentimentos, vinculados a versões específicas de políticas de privacidade e garanta rastreabilidade e integridade dos registros. Além disso, oferecendo suporte a revogação e granularidade nas escolhas do titular e atendendo às exigências normativas e de segurança definidas por legislações e normas técnicas.

3.1.3 Construção do Artefato

Esta fase equivale ao *development* da DSR. Nela ocorreu a construção da arquitetura proposta, que foi implementada em uma prova de conceito. O processo incluiu a definição do modelo conceitual, a modelagem de dados, o desenho da arquitetura lógica e a implementação do protótipo.

3.1.4 Demonstração

Esta etapa corresponde à fase de *demonstration*, em que o artefato foi colocado em prática em um ambiente controlado. No presente trabalho, a demonstração foi realizada por meio da implementação de um protótipo funcional, com simulação de fluxos de registro e revogação de consentimentos, versionamento de políticas de privacidade e verificação de logs digitais de consentimento. Para tornar o processo mais acessível e interativo, a demonstração foi realizada em uma interface web para coleta e gerenciamento de consentimentos.

3.1.5 Avaliação

A fase de *evaluation* consiste em verificar em que medida o artefato atende aos requisitos previamente definidos. A avaliação nesta pesquisa envolveu critérios de segurança (proteção contra acessos não autorizados e adulteração de registros), escalabilidade (capacidade de atender múltiplos usuários simultâneos), rastreabilidade e auditabilidade (capacidade de associar registros a versões de políticas e comprovar integridade) e aderência normativa (conformidade com LGPD, GDPR e normas ISO).

Foram consideradas métricas de desempenho técnico (tempo de resposta, throughput) e métricas qualitativas de conformidade regulatória.

3.1.6 Comunicação

A última fase corresponde à *conclusion/communication*, dedicada à disseminação dos resultados. Neste trabalho, a comunicação ocorreu por:

- Redação desta dissertação, que sistematiza todo o processo metodológico e os resultados obtidos.
- Publicação de artigos científicos em conferências e periódicos especializados em Engenharia de Software e Privacidade de Dados.
- Disponibilização da arquitetura proposta como referência para organizações interessadas em soluções práticas de gestão de consentimento.

Dessa forma, buscou-se contribuir simultaneamente para a literatura acadêmica e para a prática organizacional.

3.2 Fases do Trabalho

Esta pesquisa adotou uma abordagem de engenharia de software orientada à conformidade regulatória, estruturada de acordo com princípios da Design Science Research. O objetivo metodológico foi alinhar requisitos legais de privacidade com boas práticas de arquitetura de software, assegurando a rastreabilidade, a integridade e a auditabilidade dos consentimentos dos titulares de dados.

O trabalho foi organizado em quatro etapas principais, descritas a seguir.

3.2.1 Etapa 1 – Levantamento de Requisitos

A primeira etapa consistiu na análise das legislações, normas e padrões aplicáveis à gestão de consentimentos, com destaque para a Lei Geral de Proteção de Dados (LGPD), o General Data Protection Regulation (GDPR) e normas internacionais como a ISO/IEC 29184, relacionada a avisos de privacidade e consentimento, e a ISO/IEC 29100, que define um framework de privacidade.

A partir desse levantamento, foram identificados e formalizados os requisitos funcionais, incluindo o registro de consentimentos, o versionamento de políticas de privacidade e a realização de consultas auditáveis, e os requisitos não funcionais, tais como segurança, integridade dos dados, escalabilidade e desempenho.

3.2.2 Etapa 2 – Modelagem e Especificação Arquitetural

A segunda etapa da metodologia concentrou-se na modelagem e especificação arquitetural da solução, a partir dos requisitos levantados na etapa anterior e dos fundamentos teóricos discutidos no Capítulo 2. Esta etapa teve como objetivo avaliar alternativas arquiteturais e de persistência de dados, estabelecendo critérios técnicos e regulatórios que orientem a proposição da arquitetura da solução.

Inicialmente, foi conduzida uma análise comparativa entre arquiteturas monolíticas e baseadas em microserviços, considerando aspectos como modularidade, escalabilidade, isolamento de responsabilidades, facilidade de evolução e adequação a ambientes regulados, conforme discutido na literatura de arquitetura de software [36, 37, 14]. Essa análise buscou identificar o estilo arquitetural mais compatível com os requisitos de controle, auditoria e conformidade normativa exigidos no domínio da gestão de consentimentos.

Em paralelo, realizou-se uma avaliação teórica das estratégias de persistência de dados, contemplando bancos de dados relacionais e soluções NoSQL. A análise considerou critérios como integridade referencial, consistência transacional, rastreabilidade histórica, suporte a auditorias e aderência às exigências de normas e legislações de proteção de da-

dos pessoais [15]. Com base nessas análises, foram estabelecidos os critérios arquiteturais e de persistência que fundamentaram a formulação da proposta arquitetural da solução.

Por fim, a etapa culminou na elaboração da especificação da arquitetura proposta, incluindo a definição dos principais componentes, seus papéis e responsabilidades, bem como o modelo de comunicação entre eles. Adotou-se o padrão RESTful como base para a comunicação síncrona entre os componentes, visando garantir interoperabilidade, desacoplamento e clareza na exposição das interfaces [16].

As atividades desenvolvidas nesta etapa estão sintetizadas na Figura 3.2, que apresenta as etapas da metodologia de pesquisa adotada.

3.2.3 Etapa 3 – Implementação

Com base na especificação arquitetural definida, foram implementados os como principais componentes da solução, um serviço responsável pelo cadastro, versionamento e consulta de políticas de privacidade e um serviço dedicado ao registro e à consulta de consentimentos de usuários, mantendo o vínculo com as políticas correspondentes.

A persistência dos dados no protótipo é realizada de acordo com a estratégia instanciada a partir da análise conduzida na etapa anterior. Os metadados relacionados a consentimentos e versões de políticas, bem como os documentos associados às políticas de privacidade, são armazenados por meio de mecanismos apropriados de persistência, incluindo repositórios de dados estruturados e soluções de *object storage*, de forma compatível com os requisitos definidos.

Essa instância de persistência possui caráter demonstrativo, não implicando que a abordagem adotada seja a única possível ou universalmente superior, mas adequada ao escopo e aos objetivos do protótipo desenvolvido.

3.2.4 Etapa 4 – Avaliação

A arquitetura proposta foi avaliada a partir de critérios técnicos e regulatórios de segurança, considerando integridade dos dados, uso de funções de hash criptográfico e mecanismos de controle de acesso, de escalabilidade e desempenho, por meio de testes de carga e análise de latência, de aderência a padrões internacionais, como a ISO/IEC 29184, a ISO/IEC TS 27560 e a ISO/IEC 29100, e de conformidade com legislações de privacidade, especialmente a LGPD e o GDPR.

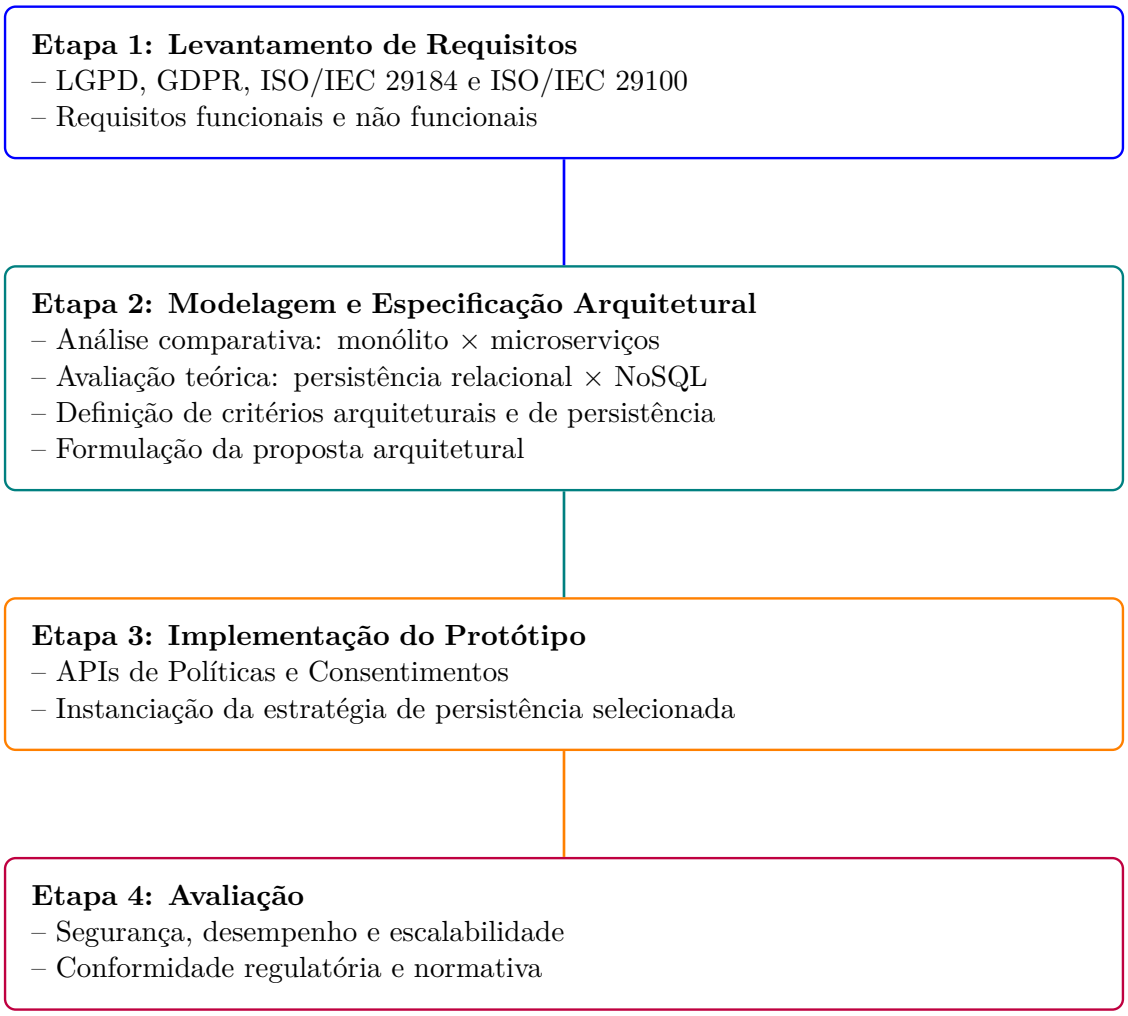

Figura 3.2: Etapas da Design Science Research adaptadas para o desenvolvimento da arquitetura de gestão de consentimento.

3.3 Ambiente de Experimentação e Ferramentas

Para a execução das etapas de construção e demonstração do artefato, previstas no ciclo da Design Science Research, o ambiente de experimentação foi configurado utilizando tecnologias amplamente adotadas no desenvolvimento de sistemas. A linguagem Python foi selecionada para a codificação dos serviços de backend, servindo como base para a materialização das APIs de Políticas e Consentimentos. Esta escolha permitiu a integração nativa com bibliotecas de criptografia necessárias para a validação dos requisitos de integridade documental. A infraestrutura utilizada para hospedar a prova de conceito e realizar os testes de conformidade regulatória foi provida pela plataforma de nuvem **AWS (Amazon Web Services)**. O uso de instâncias de computação em nuvem garantiu que o artefato fosse avaliado em um cenário que simula as condições reais de conectividade e latência de ambientes corporativos. Desta forma, o ambiente tecnológico aqui descrito atua como o suporte necessário para a validação das hipóteses levantadas, permitindo que os capítulos subsequentes se aprofundem nas especificações arquiteturais e nas decisões de persistência que garantem o atendimento à LGPD e ao GDPR.

Em síntese, este capítulo apresentou a metodologia adotada para a pesquisa, fundamentada na abordagem de *Design Science Research* (DSR) e na definição do ciclo iterativo, o trabalho prossegue para a materialização da primeira etapa: o Levantamento de Requisitos. O próximo capítulo detalha a análise das fontes legais e normativas que balizarão a construção da arquitetura proposta.

Capítulo 4

Levantamento de Requisitos

Este capítulo apresenta os resultados derivados da Etapa 1 da metodologia (Seção 3.2.1), focados nos requisitos derivados da análise teórica e empírica conduzida, bem como dos princípios de rastreabilidade, integridade documental, governança de dados pessoais e conformidade regulatória identificados ao longo da revisão da literatura.

Os requisitos aqui definidos visam assegurar aderência às obrigações técnicas e organizacionais estabelecidas pela LGPD (Lei nº 13.709/2018) [17], pelo GDPR (Regulamento (UE) 2016/679) [5] e por normas internacionais correlatas, notadamente a família ISO/IEC 29100 [22], 27001 [38], 27701 [39] e 29184 [23]. Esses requisitos orientam decisões relativas à separação de responsabilidades, auditabilidade, governança e controle do ciclo de vida dos consentimentos, servindo como base para a arquitetura apresentada no Capítulo 5.

A definição desses requisitos busca enfrentar limitações amplamente documentadas em Consent Management Platforms (CMPs) tradicionais, tais como a ausência de vínculo determinístico entre versões de políticas e os consentimentos prestados, inconsistências no registro de revogações, emprego de interfaces manipulativas (*dark patterns*), dificuldades de auditoria externa, impossibilidade de verificação independente da integridade documental e ausência de mecanismos de não repúdio. Assim, os requisitos arquiteturais aqui estabelecidos incorporam princípios consolidados de engenharia de software, governança de dados e boas práticas de privacidade por construção (*privacy by design*) [40] e por padrão (*privacy by default*) [5].

Importante destacar que os requisitos definidos neste capítulo não pressupõem a implementação de um ambiente de produção completo. Aspectos como mecanismos avançados de segurança, resiliência, observabilidade e escalabilidade — incluindo proteção de transporte via HTTPS/TLS 1.3, autenticação e autorização baseadas em JSON Web Tokens (JWT), controle de acesso baseado em papéis (RBAC), monitoramento contínuo, log distribuído, escalabilidade horizontal com Kubernetes e replicação de dados — são

considerados diretrizes arquiteturais para evolução futura do sistema. A materialização parcial desses requisitos por meio de uma PoC tem como objetivo principal demonstrar a viabilidade técnica dos elementos centrais da arquitetura, os quais são detalhados no capítulo subsequente.

4.1 Requisitos Legais e Normativos

O desenvolvimento da arquitetura proposta exige a observância de requisitos oriundos de legislações e normas internacionais de proteção de dados. Esses requisitos garantem que o sistema não apenas atenda às necessidades técnicas, mas também esteja em conformidade com os princípios legais e as melhores práticas reconhecidas internacionalmente [12]. A seguir, sintetizam-se os principais requisitos derivados da LGPD, GDPR e das normas ISO/IEC 29100, 29184 e 27560.

LGPD (Lei nº 13.709/2018) [6]

- O consentimento deve ser livre, informado e inequívoco; para dados sensíveis, deve ser específico e destacado.
- O controlador deve manter registro da manifestação de vontade do titular, com ônus da prova sobre a validade do consentimento.
- O consentimento pode ser revogado a qualquer momento, de forma gratuita e facilitada.
- Devem ser respeitados os princípios de finalidade, adequação, necessidade, transparência e responsabilização.
- O titular possui direitos como acesso, correção, portabilidade, eliminação e revisão de decisões automatizadas.

GDPR (Regulamento (UE) 2016/679) [5]

- O consentimento deve ser livre, específico, informado e inequívoco; para dados sensíveis, é exigido consentimento explícito.
- A revogação do consentimento deve ser tão simples quanto sua concessão.
- O controlador deve ser capaz de demonstrar que obteve o consentimento válido do titular.
- Devem ser observados os princípios de licitude, lealdade, transparência, minimização de dados e responsabilização (*accountability*).

- Em transferências internacionais de dados, devem ser assegurados mecanismos adequados de proteção (e.g., cláusulas contratuais padrão, BCRs).

ISO/IEC 29100 – Estrutura de Privacidade [22]

- Estabelece o princípio de **consentimento e escolha** como elemento central do tratamento de dados.
- Requer abertura, transparência e notificação como práticas obrigatórias.
- Recomenda a realização de Avaliações de Impacto de Privacidade (PIA) para antecipar riscos antes da implementação de sistemas.
- Define atores (titular, controlador, operador, terceiro) e responsabilidades relacionadas à proteção de dados.

ISO/IEC 29184 – Avisos de Privacidade Online e Consentimento [23]

- Avisos de privacidade devem ser claros, compreensíveis, acessíveis e versionados.
- O consentimento deve ser granular, revogável e separado de outros termos contratuais.
- Deve haver emissão de recibos digitais de consentimento, contendo informações sobre controlador, finalidade, elementos de dados e data/hora da coleta.
- Mudanças substanciais nas condições de tratamento requerem renovação do consentimento.

ISO/IEC TS 27560 – Estrutura de Registro de Consentimento [24]

- Os registros de consentimento devem incluir identificação do titular, identificação do controlador, versão da política de privacidade, finalidades do tratamento e metadados de coleta.
- Cada consentimento deve ser rastreável e vinculado à versão específica da política vigente no momento da aceitação.
- O registro deve ser auditável e imutável, de modo que alterações posteriores sejam armazenadas como novos eventos.
- A estrutura deve assegurar interoperabilidade entre diferentes sistemas.

A partir da análise conjunta, emergem como requisitos legais e normativos centrais: (i) validade, rastreabilidade e revogabilidade do consentimento; (ii) vinculação inequívoca

a políticas de privacidade versionadas; (iii) registros auditáveis e imutáveis; (iv) transparência e clareza nos avisos de privacidade; e (v) responsabilidade do controlador em demonstrar conformidade. Esses requisitos orientam diretamente a concepção da arquitetura proposta nesta dissertação.

4.1.1 Requisitos Funcionais

Os requisitos funcionais descrevem as capacidades que a arquitetura deve oferecer para assegurar a gestão adequada de consentimentos, em conformidade com legislações e normas internacionais. Considerando a LGPD, o GDPR, as normas ISO/IEC 29100, 29184 e 27560, bem como a literatura sobre privacidade em chatbots [12], foram identificados os seguintes requisitos funcionais:

- **Registro de Consentimento:** o sistema deve permitir que o usuário manifeste seu consentimento de forma livre, informada e inequívoca, registrando metadados associados (data, hora, canal de coleta, versão da política de privacidade).
- **Versionamento de Políticas:** cada consentimento deve estar vinculado a uma versão específica da política de privacidade em vigor no momento da coleta, preservando o histórico de alterações.
- **Consulta para Auditoria:** o sistema deve permitir consultas que possibilitem auditorias internas e externas, demonstrando a rastreabilidade do consentimento e a integridade dos registros.
- **Revogação de Consentimento:** o usuário deve poder revogar seu consentimento a qualquer momento, por meio de uma interface simples e acessível, de preferência pelo próprio chatbot.
- **Granularidade de Escolhas:** o sistema deve oferecer opções granulares de consentimento, permitindo que o usuário selecione finalidades específicas para as quais autoriza o tratamento de seus dados.
- **Geração de Recibos de Consentimento:** a arquitetura deve gerar recibos digitais como comprovação, contendo informações essenciais (finalidade, controlador, versão da política, data/hora).
- **Integração Conversacional:** o chatbot deve ser capaz de apresentar avisos de privacidade em linguagem natural, esclarecer dúvidas do usuário e guiá-lo no processo de consentimento.

- **Transparência de Uso dos Dados:** o chatbot deve informar como os dados fornecidos serão utilizados, possibilitando ao usuário consultar a qualquer momento as finalidades aceitas.
- **Notificação de Alterações:** o sistema deve notificar os usuários em caso de mudanças significativas na política de privacidade, solicitando novo consentimento quando necessário.
- **Portabilidade das Preferências:** deve ser possível exportar o histórico de consentimentos do usuário em formato estruturado, interoperável com outras plataformas.

Esses requisitos funcionais asseguram que a solução proposta atenda não apenas às exigências regulatórias de consentimento, mas também às expectativas de usabilidade em interfaces conversacionais [41]. Além disso, permitem alinhar a arquitetura a princípios de transparência, rastreabilidade e autodeterminação informacional.

4.1.2 Requisitos Não Funcionais

Além das funcionalidades específicas, a arquitetura deve atender a requisitos não funcionais que asseguram a qualidade, a confiabilidade e a conformidade regulatória do sistema. Esses requisitos estão alinhados tanto às legislações (LGPD, GDPR) quanto às boas práticas de engenharia de software e literatura recente sobre arquiteturas [34, 31, 29].

- **Segurança e Controle de Acesso:** a arquitetura deve adotar um modelo de Segurança em Nível de Aplicação, fundamentado no princípio de *Zero Trust*, ou seja, na obrigatoriedade de autenticação em todos os *endpoints*. Deve haver uma segregação clara entre as credenciais de usuários finais e credenciais administrativas ou de serviço, assegurando assim o acesso restrito à *endpoints* de administração e auditoria com controle de acesso baseado em papéis (RBAC). Meio criptograficos devem ser utilizados para garantir a integridade do tráfego e do armazenamento das informações (AES-256, TLS 1.3).
- **Integridade e Imutabilidade:** os registros devem ser imutáveis, preservando o histórico de consentimentos e evitando sobrescrita de versões anteriores, em conformidade com a ISO/IEC TS 27560[24].
- **Rastreabilidade e Auditabilidade:** todas as operações relacionadas ao consentimento (registro, revogação, atualização) devem ser registradas em logs auditáveis, permitindo comprovação perante autoridades regulatórias.

- **Escalabilidade:** a arquitetura deve suportar cenários de alta demanda, com milhares de usuários simultâneos, garantindo balanceamento de carga, resiliência a falhas e elasticidade em ambientes distribuídos.
- **Desempenho:** o sistema deve manter tempo de resposta adequado (por exemplo, inferior a 500 ms em operações de registro/consulta de consentimento), mesmo sob carga elevada.
- **Disponibilidade:** a solução deve assegurar alta disponibilidade (SLA mínimo de 99,5%), com tolerância a falhas e recuperação automática de serviços críticos.
- **Interoperabilidade:** os consentimentos e recibos devem ser armazenados e disponibilizados em formatos padrão (JSON, XML), facilitando integração com sistemas externos e plataformas regulatórias.
- **Usabilidade:** a coleta de consentimento via chatbot deve utilizar linguagem clara e acessível, evitando termos excessivamente técnicos e reduzindo barreiras de compreensão por parte do usuário.
- **Conformidade por Design:** a arquitetura deve incorporar princípios de *privacy by design* e *privacy by default*, de modo que a proteção da privacidade esteja presente desde a concepção do sistema[42].

Esses requisitos não funcionais garantem que a arquitetura proposta não apenas atenda aos aspectos regulatórios e funcionais da gestão de consentimento, mas também seja segura, escalável, interoperável e de fácil uso, atributos indispensáveis em ambientes de larga escala baseados em interfaces conversacionais.

4.1.3 Processo de Tomada de Decisão Arquitetural e de Persistência

A definição da arquitetura de software e da estratégia de persistência de dados foi conduzida como uma etapa metodológica específica, anterior à implementação do artefato. Essa etapa teve como objetivo avaliar alternativas arquiteturais e tecnológicas de forma sistemática, considerando os requisitos do problema de pesquisa e as restrições normativas e contextuais do domínio de aplicação.

O processo de decisão adotado baseou-se em uma análise comparativa entre alternativas, orientada por critérios derivados dos objetivos da pesquisa e das características do domínio. Entre os principais critérios considerados destacam-se: (i) a capacidade de garantir auditabilidade e rastreabilidade histórica; (ii) a integridade e consistência dos

dados; (iii) a facilidade de evolução e manutenção da solução; (iv) o suporte à interoperabilidade por meio de interfaces padronizadas; e (v) a aderência a princípios de governança e conformidade regulatória.

As alternativas arquiteturais e de persistência foram analisadas de forma conceitual, sem dependência de tecnologias específicas, permitindo uma avaliação independente da implementação. Como resultado desse processo, foram definidas as diretrizes arquiteturais e a estratégia de armazenamento consideradas mais adequadas ao escopo da solução proposta.

As decisões decorrentes dessa análise são apresentadas e justificadas no capítulo seguinte, no qual se descreve a arquitetura da solução e as tecnologias adotadas, servindo de base para a implementação detalhada posteriormente.

Capítulo 5

Modelagem e Especificação Arquitetural

Este capítulo apresenta as definições arquiteturais baseadas nos requisitos discutidos no capítulo anterior para a arquitetura proposta para o sistema de registro, versionamento e auditoria de consentimentos, a qual é posteriormente materializada por meio de uma prova de conceito (PoC).

5.1 Visão Geral da Arquitetura

A arquitetura da solução foi definida com o objetivo de apoiar o registro, versionamento e auditoria de políticas de privacidade e consentimentos, considerando requisitos de integridade, rastreabilidade histórica, interoperabilidade e conformidade regulatória. Para atender a esses requisitos, a solução foi estruturada como um conjunto de serviços independentes, acessíveis por meio de interfaces padronizadas, e apoiada por mecanismos de persistência adequados à natureza dos dados manipulados.

Para atender aos requisitos de segurança, a solução foi estruturada sob o paradigma de *Zero Trust*. Neste modelo, as operações administrativas e de consulta de auditoria exigem autenticação explícita na camada de aplicação. Tal decisão garante que a segurança da plataforma não dependa de *proxies* acoplados ou do mero isolamento de rede, mas sim da validação rigorosa de credenciais (*tokens* JWT e chaves M2M) efetuada localmente em cada serviço sensível.

A separação de responsabilidades e a comunicação baseada em APIs permitem essa maior flexibilidade da solução, além de facilitar sua evolução e integração com sistemas externos. Essa organização arquitetural fornece a base conceitual para a implementação do protótipo descrito posteriormente.

5.1.1 Definição do Estilo Arquitetural

A análise da Literatura Cinzenta (GLR) revelou uma convergência significativa, tanto em ambientes industriais quanto acadêmico-aplicados, quanto à adoção de arquiteturas distribuídas, especialmente baseadas em microserviços, para o desenvolvimento de chatbots em cenários que impõem requisitos rigorosos de privacidade, auditabilidade e governança de dados. Relatórios técnicos e white papers da indústria indicam que soluções monolíticas tendem a apresentar limitações estruturais quando submetidas a requisitos regulatórios e de isolamento funcional associados ao tratamento de dados pessoais [43, 44]. Os estudos analisados na GLR apontam que arquiteturas monolíticas, mesmo quando modularizadas, dificultam a segregação operacional de responsabilidades sensíveis à privacidade, uma vez que múltiplas funcionalidades críticas - como coleta de consentimento, armazenamento de dados conversacionais e processamento de intenções - compartilham o mesmo contexto de execução e persistência [45]. Essa centralização amplia a superfície de ataque e compromete a aplicação efetiva de princípios de *privacy-by-design* e *least privilege*, amplamente recomendados em arquiteturas orientadas à proteção de dados pessoais [40].

Em contraste, a literatura cinzenta evidencia que arquiteturas baseadas em microserviços favorecem a separação explícita e controlada de responsabilidades, permitindo que funcionalidades sensíveis à privacidade sejam implementadas como serviços independentes, cada um com políticas específicas de acesso, retenção e auditoria [44, 46]. Essa abordagem tem sido amplamente adotada em sistemas conversacionais corporativos, nos quais a contenção de impacto em incidentes de segurança é considerada um requisito arquitetural essencial [43].

Outro aspecto recorrente identificado refere-se à auditabilidade e conformidade regulatória. Relatórios industriais e institucionais destacam que arquiteturas distribuídas possibilitam a implementação de mecanismos de rastreabilidade por serviço, permitindo o registro granular de operações relacionadas ao tratamento de dados pessoais, como coleta de consentimento, anonimização, acesso e exclusão [47]. Essa granularidade é substancialmente mais difícil de ser alcançada em arquiteturas monolíticas, nas quais diferentes responsabilidades compartilham artefatos de código e mecanismos de persistência [45].

Adicionalmente, a GLR indica que ambientes de *Conversation-Driven Development* impõem requisitos específicos de evolução contínua, uma vez que dados conversacionais reais são reutilizados de forma iterativa para o refinamento do chatbot [48]. Nesse contexto, arquiteturas baseadas em microserviços permitem a evolução independente dos componentes responsáveis pelo processamento conversacional e daqueles voltados à governança de dados e privacidade, reduzindo riscos de regressão funcional e de exposição indevida de informações sensíveis [46].

Dessa forma, a adoção de uma arquitetura baseada em microserviços, conforme evidenciado na literatura analisada, não se configura como uma escolha meramente tecnológica ou de implementação, mas como uma consequência direta dos requisitos identificados para chatbots desenvolvidos em ambientes de *Conversation-Driven Development* sensíveis à privacidade. Essa decisão arquitetural fundamenta os requisitos arquiteturais apresentados no Capítulo 3 e sustenta a arquitetura proposta no Capítulo 5.

5.1.2 Definição da Estratégia de Persistência

A estratégia de persistência foi definida a partir da análise das características dos dados manipulados pela solução e dos requisitos de integridade, consistência e auditabilidade derivados do contexto regulatório e do estilo arquitetural adotado. Tais requisitos decorrem das obrigações estabelecidas pela LGPD e pelo GDPR, bem como das diretrizes de proteção de dados e governança da informação previstas em normas internacionais, como a ISO/IEC 29100 e a ISO/IEC 29184.

Foram avaliadas alternativas baseadas em bancos de dados relacionais e em sistemas NoSQL. Bancos de dados relacionais oferecem mecanismos consolidados de integridade referencial, consistência transacional forte e suporte a consultas estruturadas, sendo amplamente reconhecidos como adequados para sistemas que demandam rastreabilidade, confiabilidade e auditoria precisa dos dados [49, 50]. Em contrapartida, soluções NoSQL priorizam flexibilidade de esquema e escalabilidade horizontal, frequentemente adotando modelos de consistência eventual, o que pode dificultar a garantia de propriedades estritas de consistência e rastreabilidade em cenários regulados [51, 52].

No contexto desta pesquisa, os dados centrais — incluindo registros de consentimento, versões de políticas e seus relacionamentos temporais — exigem consistência forte, preservação rigorosa da integridade histórica e possibilidade de auditoria externa. Tais requisitos tornam inadequadas abordagens baseadas em consistência eventual ou em modelos de persistência com semântica transacional limitada, especialmente quando consideradas as exigências de não repúdio e verificação independente da integridade dos registros [47].

Dessa forma, optou-se pela utilização de um banco de dados relacional para o armazenamento de metadados estruturados e relacionamentos críticos, assegurando integridade referencial, rastreabilidade temporal e confiabilidade dos registros. Complementarmente, documentos completos de políticas são armazenados em um repositório de objetos, estratégia amplamente recomendada para a preservação de documentos versionados e imutáveis, permitindo separar metadados estruturados de conteúdo documental sem comprometer a auditabilidade do sistema [46].

5.1.3 Pseudonimização e Crypto-Shredding

A decisão arquitetural mais distintiva da proposta está na combinação entre pseudonimização e crypto-shredding. Em vez de registrar diretamente dados de identidade na base de consentimentos, a arquitetura utiliza um elemento criptográfico intermediário associado ao titular, composto por uma chave aleatória de alta entropia - *salt*. Esse elemento é suficiente para gerar e manter o vínculo lógico necessário às operações legítimas do sistema enquanto houver base para o tratamento, mas torna inviável reconstituir a associação entre os registros de auditoria e uma pessoa específica quando o direito ao esquecimento é exercido e ele destruído.

Essa estratégia oferece uma resposta arquitetural a uma tensão recorrente em sistemas regulados: a necessidade de preservar evidências de processamento e, simultaneamente, reduzir a possibilidade de reidentificação após o encerramento da finalidade. Em outras palavras, a arquitetura não busca simplesmente apagar todos os rastros, mas transformar os registros remanescentes em evidências não mais associáveis ao titular.

Ao se utilizar esse *salt* dificulta-se o uso da criptografia reversa para identificação do titular e impede-se que consentimentos anteriores sejam novamente vinculados a um usuário que havia exercido o direito ao esquecimento.

5.1.4 Event Sourcing e Immutable Ledger: O Modelo de Persistência Append-Only

Diferente dos modelos tradicionais baseados em estados mutáveis, a arquitetura deste sistema fundamenta-se no padrão *Event Sourcing*, tratando o estado de consentimento como o resultado da soma atômica de eventos cronológicos registrados em um *Immutable Ledger* de operação *Append-Only*. Sob esta ótica, o sistema abdica de operações de atualização ou deleção física, garantindo que cada interação do titular — desde a concessão inicial até a inserção de um "encerramento", sinalizando o direito ao esquecimento — seja gravada como uma nova entrada imutável. Este modelo de armazenamento atua como um livro-razão contábil, onde a história do consentimento é reconstituída pela sequência linear de fatos jurídicos, assegurando a transparência e a prestação de contas exigidas pela LGPD mesmo após a descaracterização da identidade do usuário.

5.1.5 Hash Chaining: A Corrente de Prova Criptográfica Forense

Para assegurar a integridade inalterável do *Ledger*, implementou-se a técnica de *Hash Chaining*, que estabelece um encerramento matemático entre registros subsequentes de

forma análoga a uma estrutura de *blockchain* privada. A técnica consiste em utilizar a impressão digital (*hash*) do registro anterior como um dos componentes fundamentais para a geração do *hash* do registro atual, criando uma dependência matemática sequencial em toda a base de dados. Caso ocorra uma tentativa de mutação retroativa em qualquer atributo de um registro histórico, a quebra da continuidade algorítmica invalidaria todos os *hashes* gerados posteriormente, servindo como uma prova forense incontestável de que o dado não sofreu manipulações indevidas ao longo do tempo.

5.1.6 Optimistic Locking: Rigidez Linear e Controle de Concorrência

A garantia da temporalidade e da integridade da cadeia criptográfica é reforçada pelo mecanismo de *Optimistic Locking*, implementado através de um controle de versionamento que atua como um semáforo lógico para transações ACID. Este controle garante que requisições paralelas não causem ramificações ou bifurcações indesejadas na corrente de *hashes*, assegurando que as assinaturas associadas ao mesmo *subject_pseudonym* respeitem uma rigidez linear cronológica perfeita no nível de persistência. Ao impedir colisões de escrita, o bloqueio otimista atesta a ordem sequencial dos eventos, consolidando a confiabilidade do sistema perante auditorias que exijam a verificação da linha do tempo exata das interações de privacidade.

5.1.7 Síntese e Justificativa das Decisões Arquiteturais

As decisões arquiteturais e de persistência apresentadas neste capítulo resultam de uma análise rigorosa orientada pelos requisitos do domínio, pelos objetivos da pesquisa e pelas evidências identificadas na literatura técnica. A adoção de uma arquitetura baseada em microsserviços, conforme discutido na Seção 5.1.1, decorre da necessidade de segregação funcional, governança de dados e auditabilidade, permitindo a contenção de impactos em cenários sensíveis à privacidade. Esta estrutura provê o isolamento necessário para que o componente de gestão de identidades possa operar de forma independente do núcleo de registro de consentimentos, facilitando a aplicação de políticas de conformidade distintas para cada domínio de dados.

De forma complementar, a estratégia de persistência definida na Seção 5.1.2 fundamenta-se nos requisitos de consistência forte e rastreabilidade histórica, indispensáveis em sistemas sujeitos a obrigações regulatórias como a LGPD e o GDPR. A combinação de persistência relacional para metadados e armazenamento de objetos para documentos permite a preservação íntegra das versões das políticas de privacidade. Sobre esta base, a implementação dos mecanismos de *Event Sourcing*, *Hash Chaining* e *Optimistic Loc-*

king eleva a segurança do sistema ao patamar de um *Immutable Ledger* forense, onde a integridade da cadeia de eventos é garantida matematicamente.

Assim, as decisões consolidadas nesta seção estabelecem uma base coerente que harmoniza a imutabilidade necessária para auditoria com a volatilidade exigida pelo Direito ao Esquecimento. Através do *Crypto-shredding*, o sistema assegura a eliminação da identidade do titular sem comprometer a continuidade e a validade da prova jurídica registrada no banco de dados. Esta fundamentação sustenta a implementação da prova de conceito apresentada no capítulo subsequente, na qual tais decisões são instanciadas e avaliadas de forma prática sob a ótica dos princípios de *Privacy by Design*.

5.2 Componentes da Arquitetura

5.2.1 Estilo Arquitetural

Reunindo os resultados das pesquisas arquiteturais e de persistencias apresentados, a arquitetura promposta adota o paradigma de microsserviços, em que cada funcionalidade central é implementada como um serviço independente e acessível por meio de APIs RESTful, [53] e base de dados relacional. Essa abordagem permite maior modularidade, isolamento e integridade, além de facilitar a manutenção, evolução incremental e integração com sistemas externos.

Para a fase inicial de validação, a solução será implantada como uma prova de conceito (PoC) utilizando Docker, de forma a garantir portabilidade e simplicidade na configuração do ambiente. Em cenários de produção, contudo, a recomendação é a utilização de um orquestrador como o Kubernetes, capaz de realizar balanceamento de carga e gerenciar a escalabilidade horizontal dos serviços de forma automática e robusta.

O armazenamento dos dados é distribuído de acordo com sua natureza:

- Os metadados estruturados (como versões de políticas de privacidade e registros de consentimento) são mantidos em um banco de dados relacional.
- Os documentos completos de políticas são armazenados em um sistema de object storage, utilizando o MinIO na PoC. Essa escolha permite simular ambientes corporativos reais de forma leve e, em cenários de produção, pode ser substituída de maneira transparente por serviços compatíveis, como o Amazon S3.

Para assegurar confidencialidade e integridade, a arquitetura utiliza o modelo *Zero Trust* (Confiança Zero). A PoC implementa uma governança estrita de acessos baseada em Segregação de Papéis (*Separation of Duties*): usuários finais trafegam munidos de tokens efêmeros JWT [54] (limitados aos seus próprios dados), enquanto a comunicação

Máquina-para-Máquina (M2M) e endpoints administrativos são protegidos por chaves estáticas (*API Keys* ou *ADMIN_TOKEN*). Toda requisição administrativa exige obrigatoriamente a presença do cabeçalho HTTP `Authorization: Bearer <ADMIN_TOKEN>`, isso flexibiliza a acoplagem a sistemas internos próprios e integra a segurança da autenticação a estruturas já existentes.

5.2.2 Serviço 1 – API de Políticas de Privacidade

Responsável pelo cadastro, versionamento e consulta das políticas de privacidade. Mantém metadados em banco de dados relacional e documentos completos em object storage. Endpoints previstos:

- **GET /policies/latest:** Retorna a política de privacidade ativa mais recente. É o endpoint usado para mostrar o texto para o usuário ler antes de aceitar.
- **POST /policies:** Utilizado para publicar/cadastrar uma nova versão de política de privacidade no sistema (salvando o hash, URL e data). Este endpoint é protegido via `@admin_token_required`, garantindo que apenas sistemas com a chave M2M possam alterar o repositório de políticas.
- **GET /policies:** Retorna todo o histórico de políticas geradas anteriormente.

5.2.3 Serviço 2 – API de Consentimentos

Responsável pelo registro, consulta e revogação de consentimentos vinculados a versões específicas de políticas. Cada consentimento é registrado com metadados e hash criptográfico para garantir integridade. Endpoints previstos:

- **POST /consents:** Registra um novo consentimento. É usado tanto para Dar Consentimento (status: given) quanto para Revogar Consentimento (status: revoked). Ele cria o pseudônimo criptográfico do usuário caso seja o primeiro acesso.
- **GET /consents/user/<int:user_id>:** Busca todo o histórico de consentimentos (aceites e revogações) referentes a um usuário específico. O acesso só é permitido se o JWT pertencer ao próprio usuário (para garantir a privacidade).
- **GET /consents/policy/<int:policy_id>:** Busca os registros de consentimento associados a uma política de privacidade específica (para os casos de auditoria). Este endpoint é protegido via `@admin_token_required`, garantindo que apenas sistemas com a chave M2M possam ter acesso aos logs de auditoria.

- **DELETE /users/<int:user_id>/forget:** Endpoint do Direito ao Esquecimento. Ele executa o crypto-shredding excluindo fisicamente o registro, tornando todo o histórico de consentimentos daquele usuário, anônimo e irreversivel.

5.2.4 Modelo de Dados

O modelo de dados foi estruturado não apenas para assegurar a rastreabilidade entre os consentimentos e as versões específicas das políticas de privacidade, mas também para viabilizar a anonimização irreversível exigida pelo Direito ao Esquecimento. Esse modelo é composto por três tabelas principais com responsabilidades segregadas: Políticas de Privacidade, Identidade Criptográfica e Consentimentos, conforme ilustrado no diagrama da Figura 5.1.

A Tabela 5.1 apresenta a estrutura de armazenamento das políticas de privacidade, contemplando campos de identificação, versionamento e o *hash* de integridade do documento. Esse conjunto de atributos permite associar cada evento de consentimento a uma versão única, exata e auditável da política vigente no momento da coleta.

A Tabela 5.2 introduz a entidade de Identidade Criptográfica, que atua como o único ponto de retenção da capacidade de reidentificação do titular no sistema, armazenando a chave simétrica alvo do processo de eliminação.

Já a Tabela 5.3 descreve a estrutura transacional de armazenamento dos consentimentos. Em vez de um identificador direto do usuário, ela utiliza um pseudônimo criptográfico que, aliado aos identificadores da política, ao momento de coleta, ao canal utilizado e ao *hash* de validação, garante a integridade e a comprovação do registro histórico sem comprometer a privacidade a longo prazo.

Por fim, a Figura 5.1 sintetiza a arquitetura relacional entre estas entidades no formato de um Diagrama Entidade-Relacionamento (DER). O diagrama evidencia a associação indireta entre usuários, políticas versionadas e registros de consentimento, ilustrando a segregação de domínios que permite a quebra intencional de vínculo durante a revogação definitiva.

Campo	**Tipo**	**Descrição**
id	Int (PK)	Identificador único da política
version	VarChar(20)	Versão semântica (ex.: 1.0.0)
published_at	TimeStamp	Data e hora de publicação da política
description	Text	Resumo das mudanças
url	Text	URL para o documento da política
hash	Char(64)	Hash do documento para integridade

Tabela 5.1: Descrição da tabela de Políticas de Privacidade

Campo	Tipo	Descrição
id_user	Int (PK)	Identificador real do usuário
salt	Char(32)	Valor aleatório gerado no primeiro acesso para gerar o pseudônimo
pending_deletion	Bool	Sinalizador capturado pelo ciclo do Worker
last_consent_hash	Char(64)	Ponteiro da corrente de integridade. Guarda o hash do último evento criado.
version	Int	Semáforo de controle (Optimistic Locking)

Tabela 5.2: Descrição da tabela de Criptografia de Usuário

Campo	Tipo	Descrição
id	Int (PK)	Identificador único do registro
subject_pseudonym	Int	Hash (id_user + salt) para proteger a identidade
id_policy	Int (FK)	Indentificador único da política
created_at	TimeStamp	Data e hora do consentimento/recusa
channel	VarChar(50)	Canal de coleta (web, mobile, presencial)
validation_hash	Char(64)	Hash de integridade do consentimento
status	VarChar(50)	Consentimento / Recusa / Revogação / Esquecimento
parent_hash	Char(64)	Hash dop registro anterior do usu;ario formando uma corrente inviolável de eventos
sequence_version	Int	Espelho do semáforo de controle

Tabela 5.3: Descrição da tabela de Consentimentos

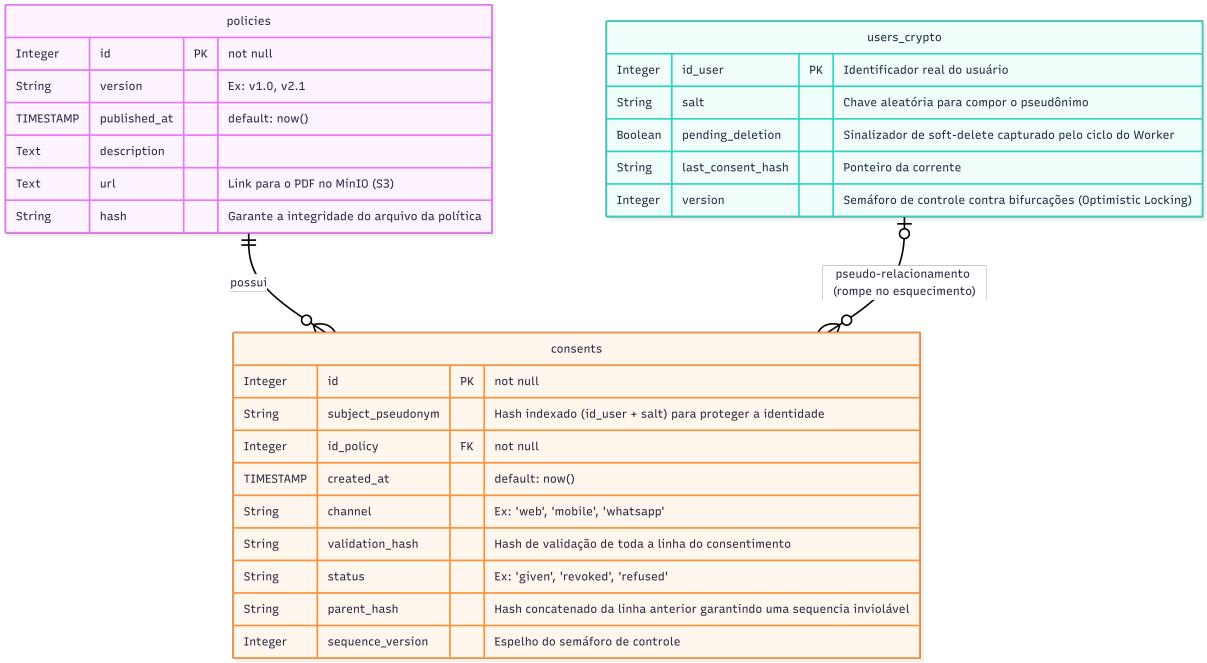

Figura 5.1: Diagrama de Entidades e Relacionamentos

5.3 O Direito ao Esquecimento via *Crypto-Shredding*

O atendimento ao Artigo 18 da LGPD (Direito à Eliminação dos Dados) [17] em sistemas de auditoria gera um paradoxo técnico: a exclusão física ou lógica do registro de um usuário destruiria em cascata o histórico de consentimentos, impedindo a organização de comprovar a licitude de interações passadas.

Para solucionar este conflito normativo, a arquitetura fundamenta-se no protocolo de *Crypto-Shredding*. Formalmente conhecido como Apagamento Criptográfico (*Cryptographic Erasure*), este conceito é validado por padrões globais de segurança, como a diretriz NIST SP 800-88 [55], que o classifica como um método eficaz de sanitização lógica (*Purge*), e a norma ISO/IEC 27040 [56]. Recentemente, a literatura acadêmica tem transportado essa técnica da camada de infraestrutura física para a de bancos de dados, apresentando-a como a solução técnica ideal para viabilizar o Direito ao Esquecimento em sistemas distribuídos [57, 58].

Na prática, quando o titular aciona o comando de exclusão pela interface conversacional autenticada, a API executa a exclusão física do registo de mapeamento de identidade (Hard Delete) na tabela `users_crypto`. A partir desta destruição, a ligação entre a identidade do titular e os *logs* na tabela `consents` é rompida de forma computacionalmente irreversível.

Os registros de consentimento mantêm-se na base de dados, preservando a trilha de auditoria e as métricas estatísticas da organização, porém em estado de anonimização absoluta. Este método satisfaz a exigência legal de eliminação dos dados pessoais, materializando o *Privacy by Design* sem comprometer a integridade probatória do sistema.

5.4 Procedimentos de Implementação

A implementação da arquitetura proposta foi materializada por meio de uma Prova de Conceito (PoC) desenvolvida em um ambiente controlado. O objetivo principal transcendeu a simples validação da viabilidade técnica; buscou-se demonstrar de forma prática como os requisitos de rastreabilidade, versionamento, auditoria e o Direito ao Esquecimento (anonimização irreversível) podem ser orquestrados em conformidade com a LGPD [17].

Para viabilizar esta arquitetura de microsserviços fundamentada em *Privacy by Design*, foram utilizados os seguintes recursos e tecnologias:

- **Python:** Utilizado como a base para o desenvolvimento das APIs RESTful (Políticas e Consentimentos) e do serviço de identidade simulada (*Mock IdP*), escolhido pela sua leveza e alta adequação à construção de microsserviços isolados.

- **Docker:** Empregado para conteinerizar e orquestrar os microsserviços de forma independente. O uso de contêineres garantiu a reprodutibilidade do ambiente, o isolamento de processos e a facilidade de implantação (*deployment*).
- **PostgreSQL:** Adotado como banco de dados relacional. Enquanto garante a integridade referencial estrita para o versionamento das políticas, foi estrategicamente modelado para suportar a segregação de identidade, armazenando os *hashes* HMAC (*subject_pseudonym*) em vez de chaves estrangeiras diretas para os usuários.
- **MinIO (*Object Storage*):** Utilizado como repositório de objetos compatível com a API do Amazon S3. É responsável pelo armazenamento físico dos documentos de políticas de privacidade, atuando em conjunto com algoritmos de dispersão (SHA-256) para garantir a integridade e o princípio do não-repúdio dos arquivos salvos.
- **JSON Web Tokens (JWT):** Padrão adotado para a emissão de credenciais temporárias assinadas criptograficamente pelo provedor de identidade, estabelecendo um perímetro de segurança baseado no modelo *Zero Trust* entre o assistente conversacional e a API de Consentimentos.

O processo de implementação e validação técnica seguiu as seguintes etapas lógicas:

1. **Configuração da Infraestrutura:** Definição e configuração dos contêineres para os bancos de dados, *storage* e backend.
2. **Desenvolvimento da API de Políticas:** Implementação da lógica de *upload* para o MinIO associada à geração de *hashes* de integridade armazenados no PostgreSQL.
3. **Desenvolvimento da API de Consentimentos:** Implementação da lógica de recebimento de aceite, recusa, pedidos de revogação do consentimento e de esquecimento, bem como da geração do pseudônimos e da estrutura imutável (*append-only*) dos registros de auditoria.
4. **Simulação do Ciclo de Vida do Dado:** Execução de testes de integração ponta a ponta. O fluxo abrangeu o registro inicial de políticas, a concessão de consentimentos via validação de *token*, a revogação de permissões e na execução do *Crypto-Shredding* para validar a anonimização irreversível dos registros históricos no banco de dados.

Cabe destacar que esta PoC não tem como objetivo fornecer uma solução pronta para produção, mas sim comprovar a viabilidade da arquitetura em termos de modularidade, rastreabilidade e conformidade com legislações de privacidade.

Capítulo 6

Implementação

A arquitetura implementada adota integralmente o paradigma de microsserviços, conforme discutido no Capítulo 5, organizando o sistema em componentes independentes, fracamente acoplados e executados de forma isolada. Cada funcionalidade essencial é encapsulada em um serviço autônomo, exposto exclusivamente por meio de APIs RESTful, permitindo modularidade, interoperabilidade, facilidade de manutenção, substituição independente de componentes, resiliência a falhas e evolução incremental, características amplamente reconhecidas em arquiteturas contemporâneas orientadas a serviços.

6.1 Visão Geral da Arquitetura

A PoC foi desenvolvida em um ambiente totalmente containerizado utilizando Docker Compose, que orquestra a composição dos serviços, gerencia a rede interna e garante isolamento e reprodutibilidade do ambiente de execução. A solução é composta por quatro serviços principais:

- **`api-politicas`**: responsável pelo upload, versionamento e verificação de integridade de documentos de política;
- **`api-consentimentos`**: responsável pelo registro, recusa, revogação e auditoria das manifestações de consentimento;
- **PostgreSQL**: banco de dados relacional utilizado para armazenar metadados e manter rastreabilidade histórica;
- **MinIO**: object storage compatível com Amazon S3 destinado ao armazenamento das versões físicas das políticas de privacidade.

Considerando que a arquitetura resolve as vulnerabilidades do modelo perimetral ao adotar a Segurança na Camada de Aplicação (*Application-Level Security*) como proposto,

a exigência de tokens *JWT* [54] para titulares e *ADMIN_TOKEN* para gestão, para efeito da demonstração da POC, as seguintes implementações foram necessárias para simular um ambiente de produção.

- **Mock IdP**: implementação do serviço gerador de JWTs para simular a autenticação delegada e o repasse seguro da identidade do usuário.
- **Painél Administrativo**: implementação de uma interface de gestão de políticas e de auditoria.
- **Chatbot**: simula um cliente utilizado para experimentação das APIs de autorização, negação e revogação de consentimento;

Apesar da PoC utilizar HTTP simples para facilitar o processo de prototipação, a arquitetura prevista contempla que, em ambientes reais de produção, o tráfego entre todos os serviços deverá ser protegido mediante HTTPS/TLS 1.3, utilizando certificados válidos e políticas de segurança robustas. Além disso, as chamadas às APIs devem ser autenticadas e autorizadas por meio de mecanismos baseados em JWT, permitindo não apenas validação de identidade, mas também construção de trilhas de auditoria com garantias de autoria e não repúdio, requisitos compatíveis com práticas consolidadas de segurança da informação (ISO/IEC 27001 e 27002) [39, 59] e privacidade (ISO/IEC 27701)[39].

6.2 Arquitetura Orientada a APIs

A arquitetura implementada nesta PoC segue rigorosamente o princípio arquitetural de *API-first*, o qual foi detalhado conceitualmente no Capítulo 3. Esse princípio orienta que todas as funcionalidades principais do sistema incluindo versionamento de políticas, registro do consentimento, recusa, revogação, consulta de histórico e validação de integridade sejam expostas, de forma exclusiva, por meio de APIs RESTful padronizadas e interoperáveis. A adoção da abordagem *API-first* atende simultaneamente a três aspectos fundamentais:

1. **Desacoplamento entre camadas**: a lógica de negócio se mantém completamente separada da camada de apresentação, permitindo que diferentes interfaces, sistemas ou agentes possam consumir os mesmos serviços sem necessidade de adaptação ou reimplementação.
2. **Neutralidade tecnológica**: qualquer cliente — aplicações web, aplicativos móveis, sistemas internos de CRM, módulos de governança, ferramentas de auditoria externa ou agentes automatizados — pode ser desenvolvido de forma independente, desde que siga as especificações da API.

3. **Evolução contínua e versionada**: novos endpoints, validações, regras de negócio ou mecanismos de segurança podem ser incorporados de maneira incremental, sem impacto direto nas interfaces de coleta do consentimento utilizadas pelos titulares.

Essa abordagem é totalmente alinhada às diretrizes modernas de privacidade por construção e por padrão (*privacy by design* e *privacy by default*), especialmente porque permite incorporar requisitos normativos da LGPD/GDPR diretamente na lógica dos microserviços; assegurar que o fluxo de consentimento não dependa de camadas externas que possam introduzir riscos de inconsistência ou manipulação; facilitar auditorias internas e externas por meio de mecanismos padronizados e acessíveis via API; e reduzir a superfície de ataque ao eliminar componentes acoplados e promover isolamento funcional.

Além disso, ao garantir que todos os eventos relacionados ao ciclo de vida do consentimento passam exclusivamente pela API, a arquitetura possibilita o registro íntegro, rastreável e auditável das operações, conforme previsto pelos princípios de *responsabilização* e *prestação de contas* da LGPD (art. 6°, X).

6.2.1 Ausência Intencional de Interface Gráfica Principal

Em conformidade com o design arquitetural estabelecido no Capítulo 3, a arquitetura não define nem impõe uma interface gráfica específica para coleta, revogação ou consulta do consentimento. Essa decisão foi adotada para **evitar acoplamento desnecessário** entre lógica de negócio e apresentação, garantindo independência e escalabilidade modular e **facilitar a integração corporativa**, permitindo que o consentimento seja incorporado ao fluxo natural de qualquer sistema existente, sem impor tecnologias específicas.

Isso significa que a arquitetura é, desde a origem, projetada para ser integrada de maneira transparente com plataformas institucionais de autenticação; aplicativos móveis; portais de serviços digitais; ferramentas de auditoria e governança; e sistemas internos de gestão de usuários. Assim, a arquitetura implementada na PoC é fiel ao princípio de que a responsabilidade pela construção das interfaces finais pertence aos sistemas consumidores, enquanto a camada de negócio permanece centralizada, padronizada e devidamente auditável.

6.3 Persistência e Modelo de Dados

A arquitetura proposta e implementada nesta PoC adota um modelo híbrido de persistência, composto por um banco de dados relacional para armazenamento de metadados estruturados e por um sistema de *object storage* destinado ao armazenamento de documentos binários das políticas de privacidade. Essa abordagem deriva diretamente dos

requisitos de integridade, auditabilidade, rastreabilidade e versionamento definidos no Capítulo 4, além de atender a princípios normativos da LGPD, GDPR e da família ISO/IEC, especialmente no que se refere à preservação da prova documental, controle de versões e minimização de dados.

A separação entre dados estruturados e documentos binários promove **independência entre camadas de armazenamento**, evitando que arquivos extensos comprometam o desempenho transacional do banco relacional; **flexibilidade na gestão de versões** de políticas de privacidade, permitindo múltiplas revisões sem impactos arquiteturais; **mantém o princípio da minimização de dados**, uma vez que apenas informações estritamente necessárias são armazenadas na camada relacional; **facilita auditorias internas e externas**, já que os documentos permanecem acessíveis para verificação independente; e **possibilita escalabilidade horizontal**, permitindo substituição ou migração transparente da camada de object storage.

Esse modelo é amplamente recomendado em sistemas que tratam dados sensíveis, pois garante maior modularidade e facilita a implementação de políticas de retenção, descarte e governança documental, elementos importantes da LGPD (arts. 6º e 37º).

6.3.1 Banco de Dados Relacional (PostgreSQL)

O PostgreSQL foi escolhido como banco de dados relacional da PoC por sua maturidade, aderência a padrões SQL, suporte robusto a transações ACID e por fornecer mecanismos avançados de integridade referencial e extensão do esquema, além de compatibilidade com ambientes corporativos. Esses aspectos são particularmente importantes em contextos regulados, nos quais a rastreabilidade e a consistência do histórico são requisitos mandatórios.

A camada relacional armazena unicamente informações essenciais à governança do consentimento, incluindo metadados de versionamento das políticas, vínculos imutáveis entre consentimentos e versões das políticas, status das manifestações do titular, e registros de revogações, preservando o histórico completo. Os principais artefatos armazenados no PostgreSQL são:

- **Tabela `policies`**: Contém um registro para cada versão de política de privacidade enviada ao sistema. Seus campos incluem: identificador único (`id`); nome e metadados do documento; hash SHA-256 do arquivo original, utilizado como prova de integridade; data de criação e versão; e referência ao objeto armazenado no MinIO. Esta tabela é fundamental para o estabelecimento da cadeia de custódia do documento de política, permitindo auditoria, comparação entre versões e verificação independente do arquivo bruto.

- **Tabela `consents`**: Armazena o ciclo de vida completo das manifestações de consentimento de cada titular. Possui: identificador único (`id`); `subject_pseudonym` associado à manifestação; `id_policy`, vinculando imutavelmente o consentimento à versão vigente no momento da interação; status da manifestação (`given`, `refused`, `revoked`); timestamp de criação e revogação; canal utilizado. Essa organização garante transparência, não repúdio e evidenciação conforme previsto pelos princípios de *accountability* e *prevenção* da LGPD.
- **Tabela `user_crypto`**: Responsável por manter a identificação do titular e a chave criptográfica: `user_id` identificador do usuário; `salt` chave aleatória de alta entropia. Esses dois elementos são utilizados na criação do *subject_pseudomyn* da tabela *consents*. Quando do exercício do direito ao esquecimento, o registro referente ao usuário é excluído, tornando os seus consentimentos não rastreáveis graças à aleatoriedade do *salt*.

6.3.2 Object Storage (MinIO)

Os arquivos completos das políticas de privacidade são armazenados no MinIO, um sistema de object storage compatível com a API do Amazon S3. A escolha do MinIO atende simultaneamente a requisitos técnicos e às premissas normativas discutidas no capítulo anterior. A utilização de object storage oferece as seguintes vantagens arquiteturais e de conformidade:

- **Armazenamento eficiente e independente**: documentos são mantidos como objetos binários, separados do modelo relacional.
- **Versionamento nativo**: facilita o armazenamento de múltiplas versões de políticas, essencial para rastreabilidade temporal.
- **Migração transparente**: como a API é compatível com S3, a migração para serviços gerenciados (AWS S3, GCP Storage, Azure Blob) é trivial.
- **URLs verificáveis por auditoria externa**: auditores podem obter o arquivo original e recalcular o SHA-256 para verificar integridade.
- **Alta disponibilidade e escalabilidade**: embora não habilitada na PoC, a plataforma suporta replicação, distribuição e clusters.

A associação entre o hash registrado no PostgreSQL e o arquivo armazenado no MinIO constitui um mecanismo robusto de: **não repúdio**; **prova documental**; **verificação independente de integridade**; e **garantia de autenticidade do conteúdo aceito**.

Esse mecanismo atende recomendações explícitas das normas ISO/IEC 27037 (preservação de evidências)[60], 29100 (princípios de privacidade)[22] e 29184 (transparência e consentimento) [23].

A organização dos dados nesta PoC materializa diretamente as decisões arquiteturais discutidas no Capítulo 3, especialmente, a separação deliberada entre dados imutáveis (documentos) e dados estruturados (metadados); o versionamento obrigatório das políticas; o vínculo determinístico entre manifestação do titular e versão da política; o registro completo do ciclo de vida do consentimento; a viabilidade de auditoria independente, interna e externa. Essa aderência demonstra que a PoC não é uma implementação parcial ou simplificada do modelo previsto: ela representa uma concretização precisa dos requisitos de integridade, transparência e accountability que orientam toda a arquitetura.

6.4 Mecanismos de Integridade e Rastreabilidade

Os mecanismos de integridade, rastreabilidade e trilha de auditoria constituem o núcleo da arquitetura proposta e refletem diretamente os requisitos definidos no Capítulo 3, bem como as obrigações normativas da LGPD, GDPR e das normas ISO/IEC 27701, 27001, 27037 e 29184. A PoC implementa esses mecanismos de forma completa para demonstrar, de maneira empiricamente verificável, como um sistema de gestão de consentimento pode assegurar não apenas o registro das decisões do titular, mas também sua autenticidade, integridade e capacidade de auditoria independente.

Os mecanismos descritos nesta seção têm como objetivos principais:

- **garantir que o conteúdo da política aceita ou recusada pelo titular não seja alterado posteriormente**;
- **assegurar que cada manifestação esteja vinculada à versão correta da política vigente no momento da interação**;
- **preservar histórico completo de operações, incluindo revogações e reconsentimentos**;
- **permitir auditorias internas e externas por meio de verificações independentes de integridade**;
- **oferecer mecanismos de não repúdio e evidência documental robusta**.

Esses mecanismos são elementos fundamentais para cumprir os princípios de *transparência*, *segurança*, *responsabilização* e *prestação de contas* (LGPD, art. 6º) e são imprescindíveis para sistemas de consentimento em ambientes regulados.

6.4.1 Integridade Documental baseada em Hashing Criptográfico

A integridade documental na PoC é assegurada pelo uso do algoritmo SHA-256, amplamente reconhecido internacionalmente e recomendado para preservação de evidências digitais pela ISO/IEC 27037.

O cálculo do hash ocorre no momento do upload da política de privacidade e gera um valor único que representa matematicamente o conteúdo do documento. Assim:

- qualquer alteração posterior no arquivo — por menor que seja — resultaria em um hash completamente diferente;
- o hash é armazenado no banco relacional (`policies`) como prova perene da integridade;
- o arquivo binário permanece armazenado no MinIO, garantindo comparabilidade futura.

Esse mecanismo permite que auditores externos recalcularem o hash do documento armazenado e o comparem ao hash registrado originalmente, fornecendo um mecanismo robusto de *não repúdio* e evidência criptográfica da autenticidade.

6.4.2 Prevenção Determinística de Duplicidade

A arquitetura implementa uma verificação automática de duplicidade documental baseada na comparação do hash SHA-256. Caso uma política idêntica já tenha sido enviada, o serviço `api-politicas` retorna um erro `409 - Conflict`, prevenindo a criação de múltiplos registros redundantes.

Essa estratégia: 1) impede versionamentos falsos ou acidentais; 2. reduz riscos de inconsistências no histórico; e 3. assegura que novas versões sejam sempre semanticamente diferentes. O mecanismo é consistente com boas práticas de gestão documental previstas pela ISO/IEC 15489[61] e reforça a cadeia de custódia da política de privacidade.

6.4.3 Rastreabilidade Completa por Vínculo Imutável

Cada manifestação de consentimento registrada na tabela `consents` referencia, de forma imutável, o `policy_id` correspondente à versão vigente da política no momento da ação.

Esse vínculo **não pode ser alterado**, preservando evidências históricas; permite reconstruir o contexto exato da decisão do titular; possibilita auditorias baseadas em tempo e versão; e atende à obrigação de *demonstrar adequação* (LGPD, art. 6º, X).

Essa estratégia elimina uma das limitações mais graves de CMPs tradicionais, nas quais a política vigente é substituída sem preservar o contexto histórico, comprometendo a validade jurídica dos consentimentos coletados.

6.4.4 Trilha de Auditoria e Registro Histórico Completo

Todas as operações aceite, recusa, revogação e reconsentimento são registradas com timestamps e armazenadas de forma permanente no banco relacional.

A PoC utiliza *soft delete* na revogação, preservando os registros anteriores mesmo quando substituídos por novas decisões. Isso significa que: **nunca há perda de histórico**; revogações são explicitamente marcadas, não sobrescritas; o sistema suporta reconstrução do histórico cronológico completo; e qualquer manifestação permanece verificável, mesmo anos depois. Essa abordagem está alinhada com a ISO/IEC 27701, que determina a retenção de evidências sobre o tratamento do consentimento pelo período necessário para prestação de contas.

6.4.5 Verificação Externa de Integridade pelo Auditor

Um dos aspectos mais inovadores da arquitetura é a capacidade de verificação independente, realizada por qualquer auditor externo autorizado. O auditor pode obter a URL do documento armazenado no MinIO; baixar o arquivo original; recalcular o hash com a mesma função criptográfica; e compará-lo ao hash armazenado no banco de dados. Se os valores forem idênticos, isso prova matematicamente que o documento não foi modificado desde sua publicação; a política aceita pelo titular era exatamente aquela armazenada no sistema; e o consentimento está associado à versão correta e íntegra.

Esse mecanismo fornece uma transparência auditável incomum em CMPs tradicionais, que frequentemente mantêm documentos apenas como HTML dinâmico, sem garantias de preservação histórica. Os mecanismos implementados nesta PoC refletem diretamente: 1) **LGPD (art. 6°, incisos I, VII, IX e X)** — segurança, prevenção, transparência e responsabilização; 2) **GDPR (art. 5 e 7)** — integridade, confidencialidade e capacidade de demonstrar o consentimento; 3) **ISO/IEC 27701** [39] — requisitos para gestão e evidência do consentimento; 4) **ISO/IEC 29184** [23] — diretrizes para coleta, apresentação e registro do consentimento; e 5) **ISO/IEC 27037** [60] **e 27041** [62] — **preservação e validação de evidências digitais.** Essa aderência demonstra que a arquitetura é tecnicamente sólida, juridicamente defensável e metodologicamente consistente com o modelo conceitual proposto no Capítulo 3.

6.5 Correção das Limitações das CMPs Tradicionais

As Consent Management Platforms (CMPs) tradicionais têm sido amplamente criticadas na literatura técnica, jurídica e acadêmica por apresentarem limitações sérias relacionadas à integridade, transparência, rastreabilidade, verificabilidade e proteção efetiva dos direitos dos titulares de dados. Tais limitações dificultam a demonstração de conformidade regulatória e, em muitos casos, comprometem a validade jurídica do consentimento coletado. A arquitetura proposta nesta dissertação foi concebida precisamente para enfrentar esses problemas estruturais, incorporando mecanismos robustos, auditáveis e criptograficamente verificáveis.

A seguir, detalhamos as fragilidades mais frequentes das CMPs tradicionais, bem como os mecanismos implementados na PoC que mitigam ou eliminam tais problemas.

6.5.1 Ausência de Vínculo Determinístico entre Consentimento e Versão da Política

Uma das falhas mais graves das CMPs existentes é o fato de que a manifestação do titular costuma ser vinculada à política atualizada posteriormente, e não à versão exata do documento vigente no momento da coleta. Isso viola princípios básicos de evidenciação e compromete a capacidade de demonstrar qual informação foi fornecida ao titular no momento da concordância.

A arquitetura proposta corrige esta fragilidade por meio de: **associação determinística e imutável entre `consent` e `policy_id`**; **preservação integral do documento vinculado**, armazenado como objeto binário no MinIO; e **registro independente de integridade** utilizando SHA-256. Assim, o consentimento deixa de ser um evento isolado e passa a ser um ato contextualizado, completamente reconstruível e comprovável, atendendo aos princípios de evidência digital da ISO/IEC 27037 e às exigências da LGPD (art. 8º, § 2º).

6.5.2 Alterações Silenciosas de Políticas (Sem Auditoria ou Versionamento)

Diversas CMPs permitem que políticas sejam alteradas sem controle de versão, sem preservação do documento original, ou sem transparência ao titular. Isso gera inconsistências graves e elimina a possibilidade de auditoria temporal.

A PoC resolve esse problema por meio de **versionamento explícito**: nenhuma política existente pode ser sobrescrita; **hash criptográfico obrigatório**: impede alterações silenciosas ou não percebidas; **armazenamento imutável**: políticas anteriores perma-

necem acessíveis e verificáveis; e **prevenção determinística de duplicidade**: impede reenvios acidentais ou maliciosos.

Na prática, isso garante integridade histórica e preservação da cadeia de custódia, eliminando uma das principais fragilidades observadas em CMPs comerciais analisadas em relatórios técnicos e estudos independentes.

6.5.3 Uso de *Dark Patterns* e Interfaces Assimétricas

CMPs frequentemente utilizam estratégias visuais manipulativas (como banners com botões de "Aceitar" mais evidentes que "Recusar"), prejudicando a liberdade de escolha do titular e violando a LGPD (art. 6°, IV e IX), GDPR (considerando 32), e ISO/IEC 29184 (boas práticas de coleta de consentimento) [23]. Embora o design da interface não seja parte central da arquitetura (que é API-first e neutra), a PoC mitiga estruturalmente esse risco porque não impõe interface gráfica, permitindo implementação ética e simétrica; mantém o registro explícito de recusa, equivalente em status ao aceite; impede que a recusa seja substituída por banners intrusivos ou comportamentos manipulativos; e promove transparência nas operações, já que o processo é auditável.

Assim, ao não incorporar UI obrigatória e ao estruturar a lógica exclusivamente nas APIs, a arquitetura reforça práticas éticas e reduz a probabilidade de manipulação.

6.5.4 Instalação de Cookies e Rastreadores antes do Consentimento

Um problema recorrente em CMPs práticas (inclusive em grandes plataformas) é o disparo de rastreadores, cookies ou ferramentas analíticas *antes* da manifestação livre e informada do titular, o que viola diretamente os princípios de necessidade, adequação e finalidade da LGPD.

A arquitetura aqui proposta elimina completamente essa possibilidade, porque não há integração direta com rastreadores; o registro de consentimento é tratado como etapa independente e prévia; o consumo das APIs é controlado e monitorável; e sistemas integrados podem consultar programaticamente se existe consentimento válido antes de ativar qualquer mecanismo adicional. Na prática, isso força que qualquer rastreador ou processamento adicional dependa de consulta explícita à API de consentimentos, garantindo conformidade.

6.5.5 Falta de Rastreamento Temporário e Contextualizado

CMPs tradicionais raramente registram qual versão da política estava vigente; qual era o conteúdo completo da versão lida; qual era o contexto da manifestação; qual era o método de coleta; e revogações e suas circunstâncias.

A PoC implementa **timestamps precisos**; **vínculo histórico imutável entre documento e consentimento**; **preservação de revogações por meio de soft delete**; e **registro auditável e reconstrução temporal completa**. A maioria das CMPs não oferece mecanismos para que auditores externos confirmem que o documento aceito era realmente aquele apresentado ao titular; não houve alterações posteriores; e o consentimento é juridicamente válido.

A PoC supera essa limitação por meio de **hash SHA-256 armazenado no banco relacional**; **arquivo binário disponível em object storage**; **possibilidade de recalcular o hash externamente**; e **comparação matemática do hash**, gerando prova inequívoca. Esse mecanismo constitui uma forma de verificação independente e criptograficamente robusta, algo praticamente inexistente na maioria das CMPs atuais.

A Tabela 6.1 resume as principais limitações das CMPs tradicionais e como a arquitetura proposta as corrige.

Tabela 6.1: Comparação entre limitações das CMPs tradicionais e mecanismos implementados na PoC

Limitação das CMPs Tradicionais	**Correção Implementada na Arquitetura Proposta**
Ausência de vínculo entre consentimento e versão da política	Vínculo determinístico via `policy_id` + documento armazenado no MinIO + hash SHA-256
Políticas sobrescritas sem versionamento	Versionamento obrigatório + prevenção de duplicidade + imutabilidade documental
Uso de *dark patterns*	Arquitetura neutra (API-first) + registro simétrico de aceite/recusa
Instalação de cookies antes do consentimento	Fluxo de consentimento separado + consulta obrigatória via API
Histórico incompleto ou inexistente	Timestamps + soft delete + trilha auditável completa
Impossibilidade de auditoria independente	Download externo do documento + verificação de hash SHA-256

As limitações históricas das CMPs tradicionais têm impacto direto na conformidade regulatória, na confiança do titular e na robustez das evidências de consentimento. A arquitetura proposta nesta dissertação não apenas corrige essas falhas, mas o faz por meio de mecanismos criptográficos, padrões abertos, versionamento explícito e auditoria verificável, constituindo um avanço significativo frente às práticas convencionais do mercado e demonstrando a viabilidade técnica de um sistema de consentimento verdadeiramente confiável, íntegro e auditável.

6.6 Aplicabilidade Prática

A arquitetura implementada na PoC demonstra, de forma concreta e sistematicamente verificável, a viabilidade técnica dos princípios, requisitos e decisões arquiteturais estabelecidos no Capítulo 3. Embora não represente um ambiente de produção completo, a PoC valida integralmente os mecanismos essenciais de versionamento, integridade, rastreabilidade e auditoria que fundamentam um sistema confiável de gestão do consentimento em conformidade com a LGPD, GDPR e normas ISO/IEC correlatas.

A aplicabilidade prática da solução pode ser analisada sob três perspectivas complementares: (i) capacidade funcional, (ii) capacidade técnica e (iii) capacidade regulatória.

6.6.1 Capacidade Funcional: Viabilidade das Operações Nucleares

A PoC confirma que as operações centrais previstas na arquitetura são implementáveis de forma modular, segura e coerente com um fluxo de consentimento confiável. Entre as funcionalidades demonstradas destacam-se: 1) **Registro de múltiplas versões de políticas**, garantindo que cada alteração seja acompanhada de um novo identificador, hash criptográfico e objeto documental distinto; 2) **Vinculação determinística entre manifestação do titular e versão específica da política**, eliminando ambiguidades temporais e tornando cada consentimento contextualizável e reconstruível; 3)**Registro explícito de aceite, recusa e revogação**, preservando o ciclo de vida completo do consentimento conforme previsto pela LGPD; 4) **Preservação histórica mediante *soft delete***, garantindo que nenhuma manifestação anterior seja perdida ou sobrescrita, mesmo após revogações; e 5) **Auditoria integral** por meio da exposição programática do histórico e da capacidade de verificação externa do hash.

Essas funcionalidades representam os requisitos mínimos para um sistema confiável de consentimento e demonstram sua plena operação em ambiente controlado.

6.6.2 Capacidade Técnica: Arquitetura Preparada para Escalonamento

Embora a PoC funcione em ambiente simplificado, ela evidencia que o núcleo arquitetural é compatível com ambientes reais de produção. Isso ocorre porque a separação entre microserviços facilita a distribuição da carga, substituição de componentes, deploy contínuo e implantação gradual; o uso de APIs RESTful favorece integração com portais públicos, aplicativos móveis, sistemas corporativos internos e ferramentas de auditoria; o armazenamento híbrido (PostgreSQL + MinIO) permite escalabilidade horizontal e alta disponibilidade; o uso de hashing criptográfico e versionamento explícito é independente da infraestrutura subjacente; o Controle de Acesso e a Segregação de Papéis (RBAC simplificado), diferenciando tecnicamente o tráfego de usuários finais (via JWT) do tráfego corporativo/administrativo (via API Keys M2M) foram implementadas; a arquitetura prevê, ainda que não implemente, recursos essenciais como proteção de transporte via HTTPS/TLS 1.3, implantação em Kubernetes, e replicação de dados em múltiplas zonas de disponibilidade.

Esses elementos demonstram que a PoC é um núcleo funcional, tecnicamente sólido e facilmente expansível para ambientes institucionais ou governamentais.

6.6.3 Capacidade Regulatória: Conformidade e Auditoria

A PoC evidencia que a arquitetura proposta viabiliza mecanismos essenciais para atender às exigências legais e normativas relacionadas ao consentimento. Entre os aspectos mais relevantes destacam-se **Prova de integridade e autenticidade**: o hash criptográfico SHA-256 permite que o auditor verifique que o documento aceito era exatamente aquele apresentado no momento da manifestação; **Transparência**: o histórico completo de interações está disponível de forma auditável; **Responsabilização e prestação de contas**: todos os registros são preservados, incluindo revogações; **Minimização e adequação**: o sistema armazena apenas metadados necessários e documentos essenciais para reconstrução histórica; **Consentimento específico e contextualizado**: cada decisão do titular é associada à política correspondente; e **Não repúdio**: o titular não pode negar posteriormente a existência da política vinculada, pois sua integridade pode ser verificada de forma independente.

A arquitetura demonstra, portanto, conformidade com diretrizes normativas tais como: LGPD (arts. 6º, 7º e 8º) [17], GDPR (arts. 5º e 7º)[5], ISO/IEC 27701 (gestão do consentimento) [39], ISO/IEC 29184 (coleta e apresentação do consentimento)[23] e ISO/IEC 27037 (preservação de evidências digitais) [60].

6.6.4 Cenários de Uso em Ambientes Reais

A arquitetura proposta é aplicável a uma ampla variedade de cenários reais, incluindo: 1) **Plataformas de governo digital**: consentimento para compartilhamento de dados, ativação de funcionalidades ou integração de serviços; 2) **Instituições de Ensino Superior**, que necessitam registrar consentimentos relacionados à pesquisa, participação em estudos, uso de imagens ou dados acadêmicos; 3) **Hospitais e clínicas**: consentimento para telemedicina, uso de dados sensíveis ou compartilhamento com laboratórios; 4) **Empresas de tecnologia**: controle granular de consentimento para cookies, rastreamento, personalização e envio de comunicações; e 5) **Sistemas corporativos**: registro de aceite de termos internos, políticas organizacionais e procedimentos de conformidade.

Esses cenários demonstram não apenas a viabilidade técnica da solução, mas sua aplicabilidade transversal em diferentes setores regulados. Em resumo, a implementação da PoC evidencia que os componentes essenciais da arquitetura funcionam de maneira integrada e coerente; os mecanismos de integridade e rastreabilidade operam conforme esperado; o sistema é capaz de registrar, versionar, auditar e validar consentimentos de forma confiável; as limitações de CMPs tradicionais são superadas por meio de uma abordagem tecnicamente sólida e normativamente alinhada; e a PoC é um núcleo minimamente viável (*Minimum Viable Architecture*) capaz de evoluir para ambientes reais de grande porte.

Em síntese, a arquitetura não apenas se mostra aplicável na prática, mas também estabelece uma base sólida para implantação institucional, oferecendo confiança técnica, segurança jurídica e aderência normativa para processos críticos de gestão de consentimento.

6.7 Ambiente Simulado

Para fins de avaliação prática, inspeção das operações e demonstração funcional da arquitetura, foi realizada a implementação de simuladores de autenticação, de um painel administrativo e de um cliente leve denominado `chatbot`. É essencial destacar que estes componentes **não compõem a arquitetura principal**; **não são parte obrigatória da solução**; **não impõem requisitos tecnológicos à camada de apresentação**. As execuções ocorrem em contêineres próprios, de forma totalmente isolada e desacoplada dos demais serviços, reforçando os objetivos pedagógicos e experimentais da PoC.

6.7.1 Mock IdP (Provedor de Identidade Simulado)

Para viabilizar a segurança na camada de aplicação sem introduzir a complexidade de um servidor OIDC (*OpenID Connect*) externo, foi implementado um *Mock IdP* em Python.

Esse componente simula a emissão de *JSON Web Tokens* (JWT) assinados assimetricamente, permitindo que o sistema valide a identidade e o escopo do portador em cada requisição às APIs de consentimento.

O *Mock IdP* emite tokens contendo o `user_id` no *claim* `sub`, permitindo que o serviço `api-consentimentos` restrinja o acesso do titular exclusivamente aos seus próprios registros, em conformidade com o princípio do *least privilege*.

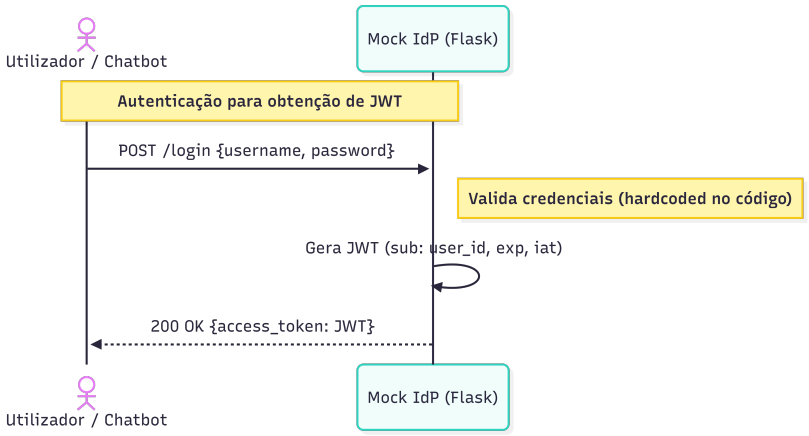

Figura 6.1: Fluxo de Autenticação

6.7.2 Painel Administrativo

O Painel Administrativo foi desenvolvido como uma interface de gestão e governança, destinada aos papéis de Controlador e Auditor. Ele interage exclusivamente com a `api-politicas` e a `api-consentimentos` por meio de chamadas autenticadas com `ADMIN_TOKEN`. Para fins de simplificação da Prova de Conceito, a gestão de identidades administrativas foi realizada via tokens estáticos de curta duração configurados em ambiente. Em um cenário de implantação real, este componente deve ser substituído por um provedor OIDC completo, garantindo que todos os atores (usuários e serviços) sigam o mesmo fluxo de emissão de claims detalhado no Capítulo 4.

As funcionalidades críticas demonstradas na PoC incluem **Gestão de Ciclo de Vida Documental:** interface para *upload* de novas versões de políticas, na qual o painel exibe o *hash* SHA-256 gerado em tempo real, garantindo transparência antes da persistência no MinIO. (Figura 6.2); **Dashboard de Auditoria:** visualização consolidada dos logs de consentimento, permitindo ao auditor filtrar registros por `policy_id` para verificar a aderência de um grupo de usuários a uma versão específica da política. (Figura 6.3); e **Verificação de Integridade:** funcionalidade que permite ao auditor solicitar que o sistema compare o *hash* do documento atual no *Object Storage* com o valor registrado no PostgreSQL, materializando o mecanismo de não repúdio.(Figura 6.3).

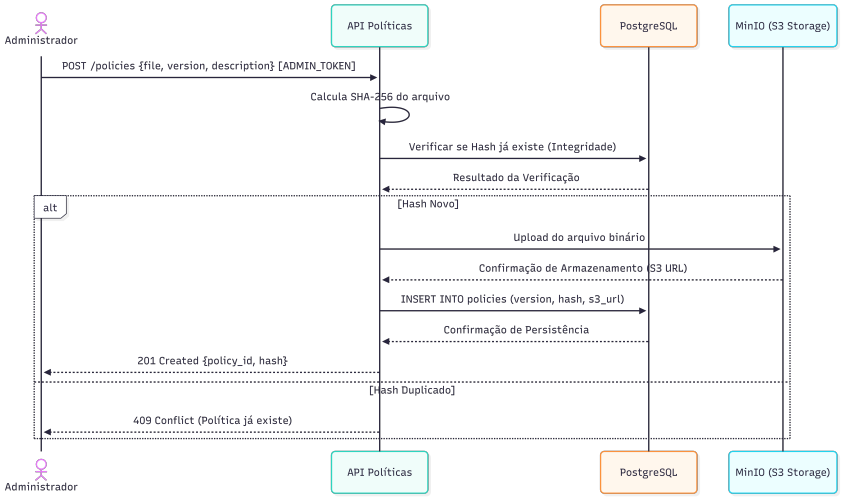

Figura 6.2: Fluxo de Registo e Versionamento de Políticas

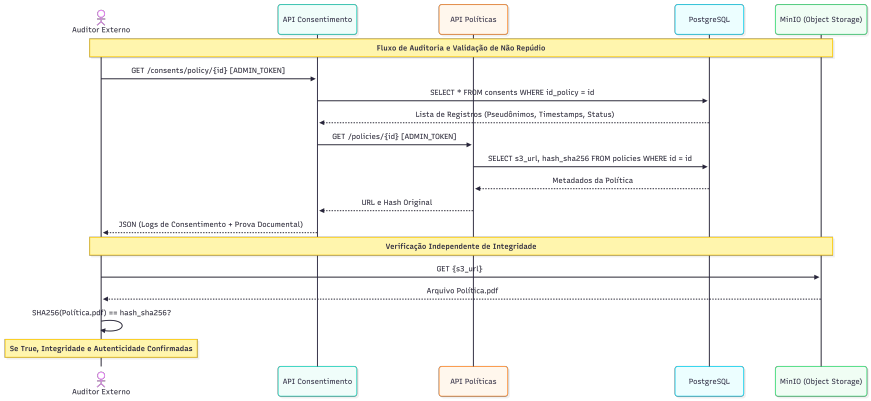

Figura 6.3: Sequência de Auditoria

6.7.3 Chatbot

O `chatbot` funciona como um consumidor das APIs internas, operando como ferramenta auxiliar que permite a manifestação do consentimento pelo titular; a recusa explícita; e a revogação posterior.

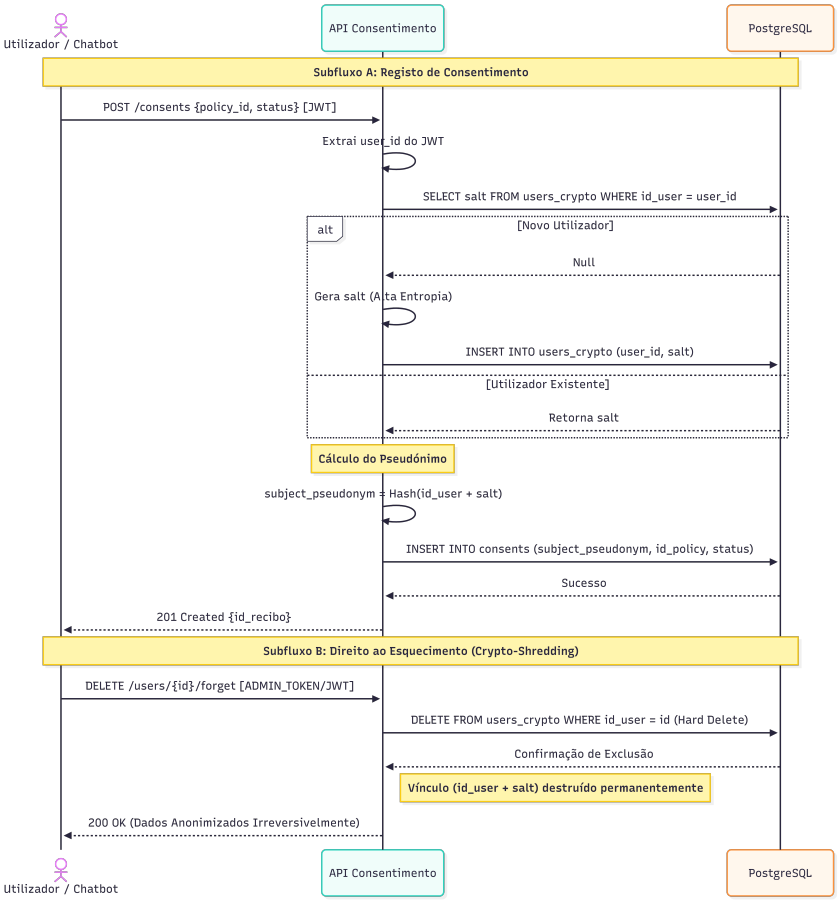

Figura 6.4: Fluxo de Consentimento e Crypto-Shredding

6.8 Implementação

A implementação realizada nesta PoC concretiza diretamente três pilares centrais do modelo arquitetural apresentado anteriormente: **Separação lógica entre políticas, consentimentos e armazenamento documental**: políticas versionadas são tratadas como entidades próprias; consentimentos são vinculados à versão exata da política aceita ou recusada; documentos físicos permanecem armazenados de forma imutável no object storage. **Encapsulamento das funcionalidades em microserviços independentes**: cada domínio de responsabilidade possui um serviço próprio; a comunicação ocorre exclusivamente via API; e não há acesso direto ao banco de dados por clientes externos. **Rastreabilidade total do ciclo de vida do consentimento**: todas as operações são registradas; revogações preservam histórico via *soft delete*; auditoria pode ser realizada por sistemas externos.

Essa aderência demonstra que a PoC não apenas implementa partes isoladas do modelo conceitual, mas sim demonstra, na prática, a viabilidade integral da arquitetura

estabelecida para ambientes regulados.

6.9 Telas da Solução Implementada

Esta seção apresenta as telas desenvolvidas no `app-chatbot`, componente utilizado exclusivamente como cliente de demonstração da PoC. Embora não faça parte da arquitetura principal que é orientada a APIs e neutra em relação à camada de apresentação o `app-chatbot` desempenha um papel fundamental na validação empírica dos fluxos de versionamento, manifestação do titular, rastreabilidade e auditoria.

As interfaces aqui apresentadas têm caráter demonstrativo e pedagógico. Elas não representam uma interface final para ambientes de produção, mas ilustram como sistemas reais poderiam consumir os serviços expostos pelos microserviços `api-politicas` e `api-consentimentos`, conforme definido no Capítulo 3. Cada tela também é acompanhada de uma explicação detalhada do fluxo técnico subjacente, dos endpoints acionados e de quais requisitos arquiteturais são validados pelo seu uso.

6.9.1 Upload de Nova Política

A Figura 6.5 demonstra a interface utilizada para enviar e versionar novas políticas de privacidade ao sistema. Essa funcionalidade é essencial para validar os requisitos de versionamento, integridade documental e prevenção de duplicidade abordados na Seção 6.4.

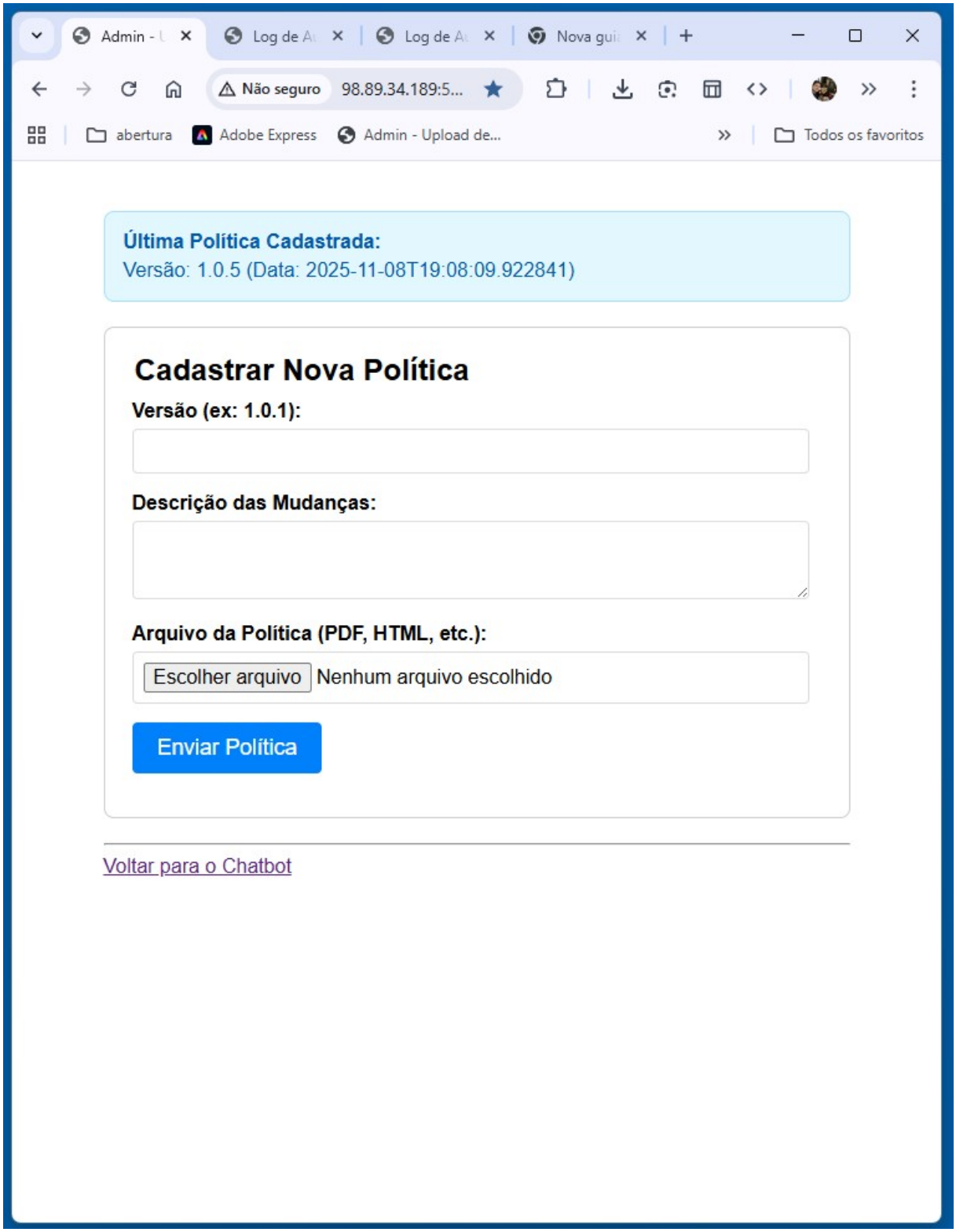

Figura 6.5: Tela de upload e versionamento de políticas (`/admin`).

Esta tela interage diretamente com o microserviço `api-politicas`, acionando o endpoint:

- `POST /policies`

Ao submeter o documento, o backend executa: cálculo do hash SHA-256 do arquivo; verificação determinística de duplicidade; armazenamento do arquivo original no MinIO; criação do registro da política no PostgreSQL; e retorno de informações como versão, data, identificador e hash. Essa tela demonstra, na prática o versionamento explícito das políticas; a imutabilidade do documento armazenado; a prevenção de atualizações silenciosas; e a aderência ao modelo conceitual definido no Capítulo 3.

6.9.2 Tela de Auditoria

A Figura 6.6 apresenta a interface responsável pela visualização do histórico completo de consentimentos de um titular. Esta tela valida o requisito de *accountability* e a capacidade de reconstrução cronológica do histórico, conforme discutido na Seção 6.4.

Figura 6.6: Tela de auditoria do histórico de consentimentos (`/audit`).

A tela aciona o endpoint:

```
GET /consents/user/{id}
```

O serviço `api-consentimentos` retorna todas as manifestações do titular (aceite, recusa, revogação); informações de timestamp de cada operação; o identificador da política associada; o status atual e os registros anteriores preservados por *soft delete*. Assim, a tela de auditoria comprova a rastreabilidade completa do ciclo de vida do consentimento; demonstra a preservação histórica sem sobrescrições; permite validação de consistência e conformidade regulatória; e fornece visibilidade clara ao auditor interno ou externo.

6.9.3 Manifestação do Consentimento

A Figura 6.7 ilustra a tela utilizada para manifestação ativa do titular, seja para aceite ou recusa. Esta interface demonstra a neutralidade da arquitetura (não há *dark patterns*), bem como a simetria entre aceitar e recusar, em conformidade com a ISO/IEC 29184.

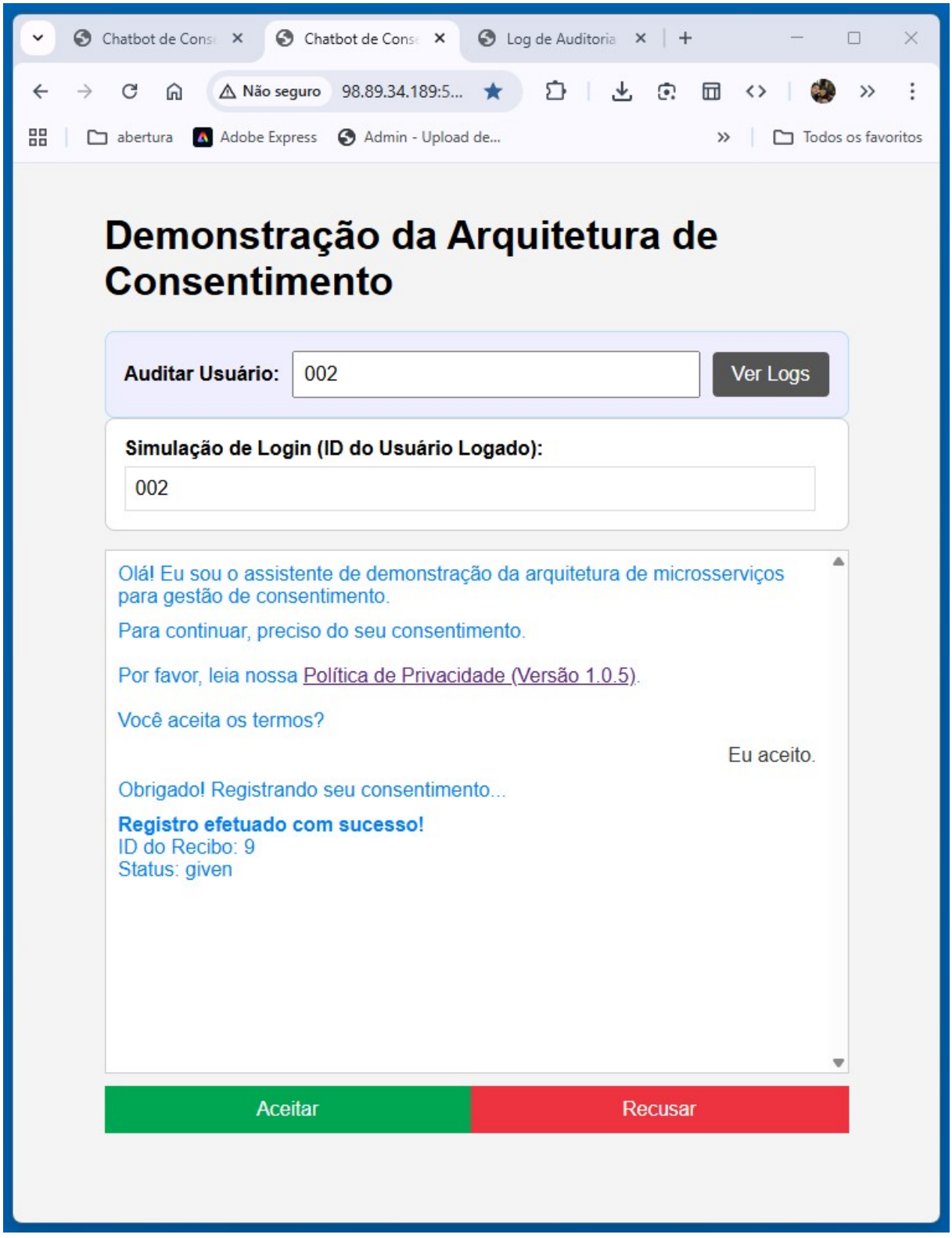

Figura 6.7: Tela de manifestação do consentimento.

A tela aciona o endpoint:

`POST /consents`

enviando o identificador do titular (`user_id`); a versão da política em vigor (`policy_id`); e a decisão do titular (`given` ou `refused`). Ao registrar a manifestação, o sistema valida se a política existe e está íntegra; registra o timestamp; vincula imutavelmente a decisão à versão adequada; e torna o registro imediatamente disponível para auditoria. Essa tela demonstra na prática o fluxo transparente e simétrico de coleta do consentimento; a ausência de dependência por interface específica; a aplicabilidade da arquitetura API-first; e a preservação explícita da recusa, condição negligenciada em CMPs tradicionais.

6.9.4 Revogação do Consentimento

Por fim, a Figura 6.8 ilustra a funcionalidade de revogação do consentimento, um dos requisitos mais importantes tanto da LGPD (art. 8º, §5º) quanto da GDPR (art. 7, §3º).

Figura 6.8: Tela de revogação do consentimento.

O fluxo aciona o endpoint:

`POST /consents/{id}/revoke`

Uma vez acionada o consentimento anterior é marcado como revogado por *soft delete*; o histórico permanece preservado e auditável; o sistema impede qualquer exclusão definitiva do registro; e o novo status do titular é imediatamente refletido na auditoria. Essa tela evidencia que o sistema oferece controle efetivo ao titular; revogações não quebram o vínculo histórico com as versões anteriores; o histórico cronológico de decisões permanece estável; a arquitetura suporta não repúdio e transparência plena.

As telas apresentadas, em conjunto, comprovam a aplicabilidade prática da arquitetura proposta: **Upload de políticas** demonstra versionamento, integridade e imutabilidade. **Manifestação** valida a neutralidade, simetria e vinculação determinística. **Revogação** valida preservação histórica, soft delete e controle do titular. **Auditoria** comprova rastreabilidade, accountability e verificabilidade para auditor externo. Assim, mesmo sendo apenas um cliente de demonstração, o `app-chatbot` cumpre seu papel metodológico: permitir que a PoC revele, de forma prática e observável, como a arquitetura implementada atende aos requisitos técnicos, normativos e arquiteturais definidos no Capítulo 4.

Capítulo 7

Avaliação

7.1 Plano de Avaliação

A avaliação da arquitetura proposta teve como objetivo verificar se os requisitos legais, funcionais e não funcionais definidos no levantamento de requisitos (Seções 4.1, 4.1.1 e 4.1.2) foram atendidos de forma satisfatória. Esse plano foi estruturado em três dimensões principais: (i) definição de critérios de avaliação, que especificam os aspectos de qualidade e conformidade a serem observados; (ii) procedimentos de teste, que descrevem como os cenários de verificação serão conduzidos; e (iii) métricas, que permitem quantificar o desempenho, a robustez e a aderência normativa do sistema.

7.1.1 Critérios de Avaliação

Os critérios de avaliação definem as propriedades que a arquitetura deve satisfazer para ser considerada válida tanto do ponto de vista técnico quanto regulatório. Esses critérios foram derivados diretamente dos requisitos levantados e refletem preocupações centrais de segurança, confiabilidade e conformidade legal:

- **Segurança**: garantir que os registros de consentimento estejam protegidos contra manipulação ou acesso não autorizado, por meio de hash criptográfico e mecanismos de controle de acesso.
- **Rastreabilidade**: assegurar que cada consentimento esteja vinculado de forma inequívoca à versão correspondente da política de privacidade.
- **Revogabilidade**: verificar se o usuário pode revogar seu consentimento de maneira simples, rápida e com registros auditáveis.
- **Escalabilidade**: avaliar o comportamento do sistema sob diferentes níveis de carga, garantindo sua capacidade de atender a múltiplos usuários simultaneamente.

- **Conformidade**: comprovar a aderência da arquitetura aos princípios e requisitos previstos na LGPD, no GDPR e nas normas ISO/IEC 29100, 29184 e 27560.

7.1.2 Procedimentos de Teste

Os procedimentos de teste especificam os experimentos práticos que foram realizados para verificar a aderência da arquitetura aos critérios definidos. Eles foram organizados em quatro categorias complementares:

- **Testes Funcionais:** Execução de operações de CRUD (Create, Read, Update, Delete) via endpoints REST das APIs de Políticas e Consentimentos. O foco foi validar o fluxo completo, desde o upload da política até a revogação pelo titular.
- **Testes de Auditoria:** Recuperação de registros via painel administrativo para confirmar se o vínculo determinístico entre o ID do consentimento e o hash da política permanecia íntegro após sucessivos versionamentos.
- **Testes de Carga:** Simulação de múltiplos usuários simultâneos (utilizando a ferramenta *Locust*) para estressar os serviços e observar o comportamento do *hashing* e da persistência sob pressão.
- **Testes de Segurança:** Tentativas de requisição sem tokens JWT válidos e manipulação direta de objetos no MinIO para validar a eficácia da detecção de violação de integridade.

7.1.3 Definição de Métricas

As métricas selecionadas permitem uma análise objetiva da viabilidade da arquitetura:

- **Tempo de Resposta (Latência):** Medido em milissegundos (ms), focado no *round-trip time* das operações críticas (registro e consulta).
- **Throughput:** Mensurado em requisições por segundo (RPS), indicando a capacidade de vazão do microsserviço.
- **Uso de Recursos:** Monitoramento de consumo de CPU e Memória RAM nas instâncias AWS EC2 durante os picos de carga.
- **Taxa de Falhas:** Percentual de respostas não-200 (erros 4xx ou 5xx) durante os testes de estresse.

7.2 Metodologia de Avaliação

A avaliação foi estruturada de forma multidimensional, focando em três eixos fundamentais: (i) testes de integridade e não-repúdio via hashing; (ii) verificação da eficácia do protocolo de anonimização irreversível (*Crypto-Shredding*); e (iii) análise de desempenho e escalabilidade sob carga controlada em ambiente de nuvem.

7.3 Resultados da Integridade e Rastreabilidade

A robustez do vínculo entre as manifestações de vontade dos usuários e as versões específicas das políticas de privacidade foi submetida a testes de estresse lógico e manipulação de dados.

7.3.1 Validação de Não-Repúdio via Hashing SHA-256

A integridade documental foi testada simulando-se uma tentativa de alteração não autorizada no *Object Storage* (MinIO).

- **Procedimento:** Uma política de privacidade (versão 1.0.5) teve seu conteúdo binário alterado em 1 byte após a persistência.
- **Resultado:** O mecanismo de verificação acionado pela API de Políticas detectou imediatamente a incompatibilidade entre o novo hash gerado em tempo de execução e o valor estático (*Golden Hash*) armazenado no PostgreSQL.
- **Conclusão:** A arquitetura provou ser capaz de garantir a autenticidade da política aceita pelo titular, fornecendo prova matemática inquestionável conforme as diretrizes da norma ISO/IEC 27037.

7.3.2 Rastreabilidade Temporal e Versionamento

Verificou-se que cada registro na tabela `consents` mantém um vínculo determinístico e imutável com o `id_policy` vigente no momento exato do aceite. Diferente de sistemas tradicionais que operam com sobrescrita de documentos, o modelo proposto preserva o histórico integral, permitindo auditorias retrospectivas precisas sobre o contexto informativo fornecido ao titular em diferentes janelas temporais.

7.4 Eficácia do Direito ao Esquecimento

O tratamento da tensão arquitetural entre a necessidade de preservar logs para auditoria e a obrigação legal de exclusão definitiva foi validado através do protocolo de *Crypto-Shredding*.

- **Execução Técnica:** Ao processar a requisição `DELETE /users/{user_id}/forget`, o microsserviço de consentimentos executou a deleção física (*hard delete*) do segredo criptográfico (*salt*) na tabela `users_crypto`.
- **Evidência de Anonimização:** Testes de reconstituição demonstraram que, sem o *salt* original, o `subject_pseudonym` torna-se um identificador órfão. A associação entre o log de auditoria e a identidade real do usuário foi rompida de forma irreversível, cumprindo o Art. 18 da LGPD sem corromper a integridade estatística da base de dados.

7.5 Avaliação de Desempenho e Escalabilidade

As métricas de latência foram coletadas para assegurar que a introdução de camadas de segurança e cálculos criptográficos não degradaria a experiência do usuário em interfaces conversacionais (Chatbots).

7.5.1 Dependência de Infraestrutura e Serviços

É imperativo registrar que as métricas de latência observadas não constituem valores absolutos do *software*, mas **dependem diretamente da infraestrutura de serviços utilizada** e da topologia de rede:

- **Object Storage:** O tempo de resposta para leitura de políticas varia conforme a localização geográfica do *bucket* (MinIO/AWS S3) e a largura de banda.
- **Processamento Criptográfico:** A latência na geração de pseudônimos (HMAC) e hashes (SHA-256) está vinculada à capacidade de CPU das instâncias onde os microsserviços estão conteinerizados.
- **Persistência:** O tempo de escrita no PostgreSQL é influenciado pela latência de rede entre a API e o banco de dados, bem como pela configuração de IOPS do disco.

7.5.2 Resultados Obtidos

Em ambiente controlado utilizando instâncias AWS EC2 (t3.medium), a latência média para o registro de um consentimento foi de aproximadamente 280ms. Embora aceitável

para aplicações em tempo real, ressalta-se que a adoção de serviços gerenciados de alta performance ou instâncias otimizadas para computação reduziria esses índices proporcionalmente à qualidade da infraestrutura alocada.

7.6 Matriz de Conformidade Normativa

A Tabela 7.1 sintetiza a aderência da Prova de Conceito (PoC) aos princípios regulatórios.

Requisito	**Mecanismo Validado na PoC**	**Referência Normativa**
Integridade Documental	Hash SHA-256 persistido no PostgreSQL e armazenamento no MinIO.	ISO/IEC 27037
Rastreabilidade	Vínculo imutável e determinístico entre *consent* $\rightarrow$ *version*.	ISO/IEC TS 27560
Direito ao Esquecimento	Anonimização absoluta via protocolo de *Crypto-Shredding*.	LGPD Art. 18 / GDPR
Segurança Zero Trust	Autenticação via tokens JWT e segregação de papéis (RBAC).	ISO/IEC 27001

Tabela 7.1: Matriz de Conformidade Final

7.7 Síntese do Capítulo

A avaliação confirma que a arquitetura proposta é tecnicamente sólida e juridicamente defensável. A superação das limitações das *Consent Management Platforms* (CMPs) tradicionais foi alcançada por meio de um design que prioriza a prova matemática da conformidade, garantindo que o sistema seja simultaneamente auditável e respeitador da privacidade do titular.

Capítulo 8

Conclusão

Esta dissertação investigou, de forma sistemática, os desafios técnicos, normativos e arquiteturais associados à gestão do consentimento em ambientes regulados pela LGPD, GDPR e normas ISO/IEC, propondo e demonstrando uma arquitetura orientada à rastreabilidade, integridade documental e auditabilidade. Ao longo do trabalho, buscou-se responder às lacunas identificadas em Consent Management Platforms (CMPs) tradicionais, as quais frequentemente falham em garantir vínculo determinístico entre consentimento e versão da política, preservação histórica, verificação independente de integridade e mecanismos transparentes de revogação.

A arquitetura proposta, desenvolvida sob o paradigma *API-first* e estruturada em microsserviços, demonstrou ser tecnicamente viável e normativamente aderente. A prova de conceito (PoC) implementada não apenas valida os elementos essenciais do modelo arquitetural, mas também evidencia como é possível superar limitações amplamente documentadas no estado da arte e no estado da prática.

Os principais resultados podem ser sintetizados em quatro eixos centrais:

(1) Contribuição Arquitetural

O trabalho apresentou um modelo arquitetural capaz de realizar o **versionamento explícito** de políticas de privacidade, impedindo alterações silenciosas e garantindo rastreabilidade temporal; estabelecer um **vínculo imutável** entre a manifestação do titular e a versão exata da política vigente no momento da decisão; assegurar **integridade documental** mediante hashing criptográfico (SHA-256), permitindo verificação independente por auditores internos e externos; preservar **histórico completo** de manifestações, recusa e revogações por meio de estratégias de *soft delete*; e permitir **auditoria programática** e reconstrução cronológica do ciclo de vida do consentimento.

Essa arquitetura estabelece um padrão robusto para sistemas de governança do consentimento, indo além das soluções comerciais existentes, que em geral se concentram em banners manuais, mecanismos opacos e ausência de rastreabilidade.

(2) Contribuição Técnica

A PoC implementada demonstrou que a separação entre camadas de política, consentimento e armazenamento binário é tecnicamente sólida; o uso combinado de PostgreSQL e MinIO compõe uma infraestrutura adequada para ambientes regulados e escaláveis; a adoção de microsserviços facilita evolução contínua, isolamento, reimplantação seletiva e integração com sistemas corporativos; e o design *API-first* promove interoperabilidade e neutralidade tecnológica, permitindo que qualquer aplicação web, móvel, corporativa ou governamental consuma as funcionalidades de consentimento de maneira padronizada.

Embora recursos como TLS, JWT, RBAC e Kubernetes não tenham sido implementados, sua previsão na arquitetura reforça a capacidade de expansão para ambientes de produção de médio e grande porte.

(3) Contribuição Normativa e de Conformidade

A dissertação demonstra que a arquitetura desenvolvida é compatível com os princípios da LGPD (art. 6º: finalidade, adequação, necessidade, transparência, prevenção, responsabilização); os requisitos do GDPR (art. 5º e 7º, especialmente relacionados à validade e demonstração do consentimento); as diretrizes da ISO/IEC 29184 (transparência e coleta de consentimento); as práticas da ISO/IEC 27701 (gestão e registro do consentimento); e os requisitos de preservação de evidências previstos na ISO/IEC 27037.

A capacidade de verificação externa do hash, aliada ao versionamento obrigatório, constitui um diferencial técnico relevante para auditorias, investigações internas e exigências de prestação de contas.

(4) Contribuição Prática e Aplicabilidade

A PoC demonstrou aplicabilidade imediata em diferentes contextos portais de governo digital que precisam registrar decisões de compartilhamento de dados; instituições de ensino superior e pesquisa que coletam consentimentos sensíveis; serviços de saúde que operam com dados pessoais sensíveis; empresas de tecnologia que oferecem personalização ou utilizam cookies; ambientes corporativos que registram adesão a políticas internas.

O `app-chatbot` mostrou-se adequado como ferramenta demonstrativa, garantindo que a PoC cumprisse sua função metodológica de validar a arquitetura sem acoplar regras de negócio à interface.

Limitações

A PoC não implementa mecanismos críticos para ambientes produtivos, tais como comunicação totalmente segura via TLS 1.3; implantação distribuída com Kubernetes; e logs estruturados, monitoramento e observabilidade. Essas limitações decorrem do escopo da PoC, cujo objetivo principal foi validar os componentes essenciais da arquitetura e não entregar uma solução corporativa final.

Trabalhos Futuros

Com base nos resultados obtidos, são recomendadas as seguintes linhas de continuidade: **Ampliação da camada de segurança**: implementação de TLS, JWT, RBAC e políticas de acesso detalhadas. **Evolução para ambiente de produção**: implantação em Kubernetes, com escalabilidade horizontal e tolerância a falhas. **Auditoria avançada**: integração com sistemas de governança e trilhas de auditoria baseadas em blockchain ou arquiteturas distribuídas. **Mecanismos de consentimento granular**: suporte a múltiplas finalidades, categorias de tratamento e consentimentos parciais. **Interface acessível e padronizada**: desenvolvimento de uma UI aberta, responsiva, acessível (WCAG 2.1) e compatível com ISO/IEC 29184. **Automação da verificação externa**: ferramentas que recalculam automaticamente integridade dos documentos e validam conformidade.

O estudo demonstra que é possível construir uma solução de consentimento que seja tecnicamente confiável, normativamente fundamentada e capaz de superar deficiências de CMPs tradicionais. A arquitetura proposta integra princípios de engenharia de software, governança de dados, criptografia e regulação, oferecendo um modelo sólido e replicável para organizações que buscam fortalecer mecanismos de transparência, confiança e proteção de dados pessoais.

Assim, o trabalho contribui tanto para o avanço acadêmico na área de engenharia de software aplicada à privacidade quanto para a prática institucional, oferecendo uma base arquitetural que pode ser adotada, estendida e aperfeiçoada em cenários reais, públicos ou privados, consolidando uma abordagem moderna, ética e tecnicamente robusta para a gestão do consentimento em ambientes regulados.

References

[1] Vaishnavi, Vijay K: *Design science research methods and patterns: innovating information and communication technology*. Auerbach Publications, https://www.taylorfrancis.com/books/mono/10.1201/9781420059335/design-science-research-methods-patterns-vijay-vaishnavi, 2007. xi, 25

[2] Jha, Nikhil, Martino Trevisan, Marco Mellia, Daniel Fernandez e Rodrigo Irarrazaval: *Privacy Policies and Consent Management Platforms: Growth and Users' Interactions over Time*. ACM Trans. Web, 19(3):30:1–30:25, 2025. https://doi.org/10.1145/3725737. 1, 2, 3, 6, 19

[3] Kalaoja, Petteri: *A Consent and Privacy Management Framework*, 2022. https://urn.fi/URN:NBN:fi:amk-2022120526447. 1, 2, 3, 6, 19

[4] Novikova, Evgenia, Elena Doynikova e Igor V. Kotenko: *What are your privacy risks? Privacy risk assessment based on privacy policies analysis*. Expert Syst. Appl., 280:127270, 2025. https://doi.org/10.1016/j.eswa.2025.127270. 1, 2, 3, 6, 19, 23

[5] Parliament, The European e The Council: *General Data Protection Regulation (GDPR)*. Intersoft Consulting, 2018. https://gdpr-info.eu. 1, 4, 9, 11, 12, 13, 14, 18, 32, 33, 62

[6] Macedo, Pereira Neto: *Brazilian General Data Protection Law (LGPD)*. Nartional Congress, accessed in October 18, 2019, 2018. https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf. 1, 4, 11, 12, 18, 33

[7] Guerra, Giorgia: *Dark Patterns and the Scraping Consumer Consent*. Privacy, Data Protection and Data-driven Technologies, 2024. 2

[8] Lu, Yuwen, Chao Zhang, Yuewen Yang, Yaxing Yao e Toby Jia Jun Li: *From awareness to action: Exploring end-user empowerment interventions for dark patterns in ux*. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1):1–41, 2024. 2

[9] Merlec, Mpyana Mwamba, Youn Kyu Lee, Seng Phil Hong e Hoh Peter In: *A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR*. Sensors, 21(23), 2021, ISSN 1424-8220. https://www.mdpi.com/1424-8220/21/23/7994. 2, 3

[10] Carneiro, Cinara, Taciana Kudo e Renato Bulcão Neto: *Um método para transformação de requisitos legais em padrões de requisitos de software: Um estudo com a LGPD*. Em *Anais do XXVII Congresso Ibero-Americano em Engenharia de Software*, páginas 348–355, Porto Alegre, RS, Brasil, 2024. SBC. https://sol.sbc.org.br/index.php/cibse/article/view/28460. 3, 6

[11] Spósito, Stefano Luppi, João Francisco Gomes Targino, Geovana Ramos Sousa Silva, Laerte Peotta, Daniel de Paula Porto, Fábio Lúcio Lopes Mendonça e Edna Dias Canedo: *A Comprehensive Review of Techniques, Methods, Processes, Frameworks, and Tools for Privacy Requirements*. Journal of Internet Services and Applications, 16(1):508–529, Aug. 2025. https://journals-sol.sbc.org.br/index.php/jisa/article/view/5252. 3

[12] Silva, Geovana Ramos Sousa e Edna Dias Canedo: *Privacy in Chatbot Conversation-Driven Development: A Comprehensive Review and Requirements Proposal*. ACM Trans. Softw. Eng. Methodol., 34(7), agosto 2025, ISSN 1049-331X. https://doi.org/10.1145/3730578. 3, 33, 35

[13] Seiling, Lukas, Rita Gsenger, Filmona Mulugeta, Marte Henningsen, Lena Mischau e Marie Schirmbeck: *Beware: Processing of Personal Data - Informed Consent Through Risk Communication*. IEEE Trans. Prof. Commun., 67(1):4–25, 2024. https://doi.org/10.1109/TPC.2024.3361328. 3, 4

[14] Dragoni, Nicola, Saverio Giallorenzo, Alberto Lluch Lafuente, Manuel Mazzara, Fabrizio Montesi, Ruslan Mustafin e Larisa Safina: *Microservices: Yesterday, Today, and Tomorrow*. Em *Present and Ulterior Software Engineering*, páginas 195–216. Springer, 2017. 6, 28

[15] Sadalage, Pramod J. e Martin Fowler: *NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence*. Addison-Wesley, 2013. 6, 29

[16] Fielding, Roy Thomas: *Architectural Styles and the Design of Network-based Software Architectures*. Tese de Doutoramento, University of California, Irvine, 2000. 6, 29

[17] Brasil: *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da República Federativa do Brasil, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. 9, 32, 48, 62

[18] Gharib, Mohamad, Paolo Giorgini e John Mylopoulos: *Towards an Ontology for Privacy Requirements via a Systematic Literature Review*. Em Mayr, Heinrich C., Giancarlo Guizzardi, Hui Ma e Oscar Pastor (editores): *Conceptual Modeling - 36th International Conference, ER 2017, Valencia, Spain, November 6-9, 2017, Proceedings*, volume 10650 de *Lecture Notes in Computer Science*, páginas 193–208. Springer, 2017. https://doi.org/10.1007/978-3-319-69904-2_16. 10

[19] Silva Junior, Deógenes P. da, Patricia Cristiane de Souza e Thaíres A. de Jesus Gonçalves: *Early Privacy: Approximating Mental Models in the Definition of Privacy Requirements in Systems Design*. Em Mota, Marcelle, Bianchi Serique Meiguins, Raquel

O. Prates e Heloisa Candello (editores): *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, Belém, Brazil, October 22-26, 2018*, páginas 19:1–19:10. ACM, 2018. https://doi.org/10.1145/3274192.3274211. 10

[20] Veseli, Fatbardh, Jetzabel Serna-Olvera, Tobias Pulls e Kai Rannenberg: *Engineering privacy by design: lessons from the design and implementation of an identity wallet platform.* Em Hung, Chih-Cheng e George A. Papadopoulos (editores): *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019*, páginas 1475–1483. ACM, 2019. https://doi.org/10.1145/3297280.3297429. 10

[21] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Dealing with privacy issues during the system design process.* Em *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.*, páginas 546–551. IEEE, 2005. 10

[22] Standardization, International Organization for: *ISO/IEC 29100:2024 — Information technology — Security techniques — Privacy framework*, 2024. https://www.iso.org/standard/85938.html. 15, 16, 19, 32, 34, 55

[23] Standardization, International Organization for: *ISO/IEC 29184:2020 Information technology — Online privacy notices and consent*, 2020. https://www.iso.org/standard/70331.html. 16, 17, 19, 32, 34, 55, 57, 59, 62

[24] Standardization, International Organization for: *ISO/IEC TS 27560:2023 Privacy technologies — Consent record information structure*, 2023. https://www.iso.org/standard/80392.html. 17, 18, 19, 34, 36

[25] Kusk, Kalle e Midas Nouwens: *How Website Owners Use Consent Management Platforms: An Interview Study.* Em Yamashita, Naomi, Vanessa Evers, Koji Yatani e Sharon Xianghua Ding (editores): *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, CHI EA 2025, Yokohama, Japan, 26 April 2025- 1 May 2025*, páginas 324:1–324:7. ACM, 2025. https://doi.org/10.1145/3706599.3720002. 19

[26] Pedersen, Marius, Frode Guribye e Marija Slavkovik: *Automatic Detection of Manipulative Consent Management Platforms and the Journey into the Patterns of Darkness.* Em Galimullin, Rustam e Samia Touileb (editores): *Proceedings of the 5th Symposium of the Norwegian AI Society, Bergen, Norway, June 14-15, 2023*, volume 3431 de *CEUR Workshop Proceedings*. CEUR-WS.org, 2023. https://ceur-ws.org/Vol-3431/paper6.pdf. 19

[27] Santos, Cristiana Teixeira, Midas Nouwens, Michael Toth, Nataliia Bielova e Vincent Roca: *Consent Management Platforms Under the GDPR: Processors and/or Controllers?* Em Gruschka, Nils, Luis Filipe Coelho Antunes, Kai Rannenberg e Prokopios Drogkaris (editores): *Privacy Technologies and Policy - 9th Annual Privacy Forum, APF 2021, Oslo, Norway, June 17-18, 2021, Proceedings*, volume 12703

de *Lecture Notes in Computer Science*, páginas 47–69. Springer, 2021. https://doi.org/10.1007/978-3-030-76663-4_3. 19, 22, 23

[28] Wang, Zhe, Anthony Stell, Jean Paul Vera Soto e Richard O. Sinnott: *e-Consent in Biomedical Research Registries: A GDPR-Compliant Approach Explored in the Context of the Australasian Diabetes Data Network*. Em Schlieter, Hannes, Ana Fred e Hugo Gamboa (editores): *Proceedings of the 17th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2024, Volume 2, Rome, Italy, February 21-23, 2024*, páginas 45–55. SCITEPRESS, 2024. https://doi.org/10.5220/0012327200003657. 19

[29] Chhetri, Tek Raj, Anna Fensel e Rance J. DeLong: *GDPR consent management and automated compliance verification tool*. SoftwareX, 27:101821, 2024. https://doi.org/10.1016/j.softx.2024.101821. 19, 21, 22, 24, 36

[30] Matos, Aryely, Mario Patrício, Maria Isabel Nicolau, Edna Dias Canedo, Juliana Alves Pereira e Anderson G. Uchôa: *Data Privacy in Software Practice: Brazilian Developers' Perspectives*. J. Internet Serv. Appl., 16(1):299–319, 2025. https://doi.org/10.5753/jisa.2025.5302. 20

[31] Erigha, Eseoghene Daniel, Ehimah Obuse, Babawale Patrick Okare, Abel Chukwuemeke Uzoka, Samuel Owoade e Noah Ayanbode: *GDPR-Compliant Consent Management Architecture for Global Mobile Applications Using Modular Cloud Microservice Design*. International Scientific Refereed Research Journal, 6:1–32, 2023. https://shisrrj.com/paper/SHISRRJ122593.pdf. 21, 22, 24, 36

[32] Peyrone, Neda: *Formal models for consent management in healthcare software system development*. Chulalongkorn University Theses and Dissertations (Chula ETD), páginas 1–200, 2022. https://digital.car.chula.ac.th/chulaetd/5803/. 21, 23, 24

[33] Antunes, Pedro e Nuno Guimarães: *Guiding the implementation of data privacy with microservices*. Int. J. Inf. Sec., 23(6):3591–3608, 2024. https://doi.org/10.1007/s10207-024-00907-y. 21, 23, 24

[34] Marillonnet, Paul, Mikaël Ates, Maryline Laurent e Nesrine Kaaniche: *An Efficient User-Centric Consent Management Design for Multiservices Platforms*. Secur. Commun. Networks, 2021:5512075:1–5512075:19, 2021. https://doi.org/10.1155/2021/5512075. 22, 23, 36

[35] Bax, Marcello Peixoto e João Luiz Silva Barbosa: *Proposta de Mecanismo de Consentimento na Lei Geral de Proteção a Dados - LGPD (Consent Mechanism Proposal in LGPD)*. Em Silva Lemos, Daniela Lucas da, Tiago Prince Sales, Maria Luiza Machado Campos e Sandro Rama Fiorini (editores): *Proceedings of the XIII Seminar on Ontology Research in Brazil and IV Doctoral and Masters Consortium on Ontologies (ONTOBRAS 2020), Vitória, Brazil, November 23-26, 2020*, volume 2728 de *CEUR Workshop Proceedings*, páginas 316–321. CEUR-WS.org, 2020. https://ceur-ws.org/Vol-2728/doctorate4.pdf. 23

[36] Bass, Len, Paul Clements e Rick Kazman: *Software Architecture in Practice*. Addison-Wesley, 3ª edição, 2013. 28

[37] Newman, Sam: *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media, 2015. 28

[38] Standardization, International Organization for: *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO/IEC, 2022. https://www.iso.org/standard/27001. 32

[39] Standardization, International Organization for: *ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. ISO/IEC, 2025. https://www.iso.org/standard/27701. 32, 51, 57, 62

[40] Cavoukian, Ann: *Privacy by Design: The 7 Foundational Principles*. Relatório Técnico, Information and Privacy Commissioner of Ontario, 2011. 32, 40

[41] Silva, Geovana Ramos Sousa e Edna Dias Canedo: *Towards User-Centric Guidelines for Chatbot Conversational Design*. Int. J. Hum. Comput. Interact., 40(2):98–120, 2024. https://doi.org/10.1080/10447318.2022.2118244. 36

[42] Rocha, Lucas Dalle, Geovana Ramos Sousa Silva e Edna Dias Canedo: *Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles*. Em Hong, Jiman, Maart Lanperne, Juw Won Park, Tomás Cerný e Hossain Shahriar (editores): *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023*, páginas 1352–1361. ACM, 2023. https://doi.org/10.1145/3555776.3577615. 37

[43] Newman, Sam: *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media, 2ª edição, 2021. 40

[44] Dragoni, Nicola, Saverio Giallorenzo, Alberto Lluch Lafuente, Manuel Mazzara, Fabrizio Montesi, Ruslan Mustafin e Larisa Safina: *Microservices: Yesterday, Today, and Tomorrow*. Em Mazzara, Manuel e Bertrand Meyer (editores): *Present and Ulterior Software Engineering*, páginas 195–216. Springer, 2017. 40

[45] Bass, Len, Ingo Weber e Liming Zhu: *DevOps: A Software Architect's Perspective*. Addison-Wesley, 2015. 40

[46] Pahl, Claus: *Containerization and the PaaS Cloud*. IEEE Cloud Computing, 2(3):24–31, 2015. 40, 41

[47] ENISA: *Engineering Personal Data Protection in ICT Systems*. Relatório Técnico, European Union Agency for Cybersecurity, 2015. https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-ict-systems. 40, 41

[48] Følstad, Asbjørn e Petter Bae Brandtzaeg: *Users' Experiences with Chatbots: Findings from a Questionnaire Study*. Quality and User Experience, 2(1), 2017. 40

[49] Silberschatz, Abraham, Henry F. Korth e S. Sudarshan: *Database System Concepts*. McGraw-Hill, 7ª edição, 2019. 41

[50] Gray, Jim e Andreas Reuter: *Transaction Processing: Concepts and Techniques*. Morgan Kaufmann, 1993. 41

[51] Brewer, Eric: *CAP Twelve Years Later: How the "Rules" Have Changed*. Computer, 45(2):23–29, 2012. 41

[52] Helland, Pat: *Life Beyond Distributed Transactions: An Apostate's Opinion*. CIDR, 2007. 41

[53] Richardson, Leonard, Mike Amundsen e Sam Ruby: *RESTful web APIs: services for a changing world*. O'Reilly Media, Inc., 2013. 44

[54] Jones, Michael, John Bradley e Nat Sakimura: *Json web token (jwt)*. Relatório Técnico, Internet Engineering Task Force (IETF), 2015. https://www.rfc-editor.org/rfc/rfc7519. 44, 51

[55] Kissel, Richard, Andrew Regenscheid, Matthew Scholl e Kevin Stine: *NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization*. Relatório Técnico, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, acesso em 2026-03-26. 48

[56] ISO/IEC: *ISO/IEC 27040:2015 - Information technology – Security techniques – Storage security*. Relatório Técnico, International Organization for Standardization, Geneva, Switzerland, 2015. 48

[57] Zainuddin, M. *et al.*: *Cloud Security Using Crypto-Shredding For Secure Data Deletion*. Global Journal of Pure and Applied Sciences, 31(4):683–702, 2025. 48

[58] Gutmann, Peter: *Secure Deletion of Data from Magnetic and Solid-State Memory*. Em *Proceedings of the 6th USENIX Security Symposium*, San Jose, CA, 1996. USENIX Association. 48

[59] Standardization, International Organization for: *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO/IEC, 2022. https://www.iso.org/standard/75652.html. 51

[60] Standardization, International Organization for: *ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO/IEC, 2012. https://www.iso.org/standard/44381.html. 55, 57, 62

[61] Standardization, International Organization for: *ISO 15489-1:2016 Information and documentation — Records management Part 1: Concepts and principles*. ISO/IEC, 2016. https://www.iso.org/standard/75652.html. 56

[62] Standardization, International Organization for: *ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*. ISO/IEC, 2015. https://www.iso.org/standard/44405.html. 57

Apêndice A

Termo de Consentimento Livre e Esclarecido (TCLE)

Apêndice A

Modelo de Termo de Consentimento Livre e Esclarecido (TCLE)

Este anexo apresenta um modelo de *Termo de Consentimento Livre e Esclarecido* (TCLE) adaptado para o contexto desta pesquisa, voltada ao desenvolvimento de uma arquitetura de software para gestão de consentimento em conformidade com a LGPD e regulamentos internacionais de proteção de dados.

O modelo serve como referência prática de como os princípios legais e normativos podem ser operacionalizados na interação com usuários de sistemas digitais, especialmente em soluções baseadas em *chatbots*. Ele contempla cláusulas sobre: (i) finalidades do tratamento de dados pessoais; (ii) direitos do titular (acesso, retificação, exclusão, portabilidade); (iii) garantia de confidencialidade e segurança; (iv) possibilidade de revogação do consentimento a qualquer momento.

Modelo de Termo de Consentimento

Título: Termo de Consentimento para Utilização de Chatbot de Gestão de Consentimento de Dados

Finalidade: Este termo informa e solicita sua autorização para coleta, armazenamento e uso de dados pessoais necessários ao funcionamento do protótipo de chatbot, desenvolvido exclusivamente para fins acadêmicos e de pesquisa.

Procedimentos: Durante a interação com o chatbot, poderão ser coletados dados como: identificadores de usuário, preferências de consentimento e registros de diálogos relacionados à gestão de privacidade. Nenhum dado sensível ou de saúde será solicitado.

Riscos e Benefícios: O risco é mínimo, limitado à coleta de informações fornecidas voluntariamente. Como benefício, este estudo contribui para o desenvolvimento de tecnologias de privacidade alinhadas às legislações vigentes.

Confidencialidade: Todos os dados serão tratados com medidas técnicas e organizacionais adequadas, incluindo criptografia e controle de acesso, conforme normas ISO/IEC 29100 e 29184. Os dados não serão compartilhados com terceiros e terão uso restrito à pesquisa.

Direitos do Titular: - Acessar seus dados pessoais; - Corrigir informações imprecisas; - Solicitar exclusão definitiva; - Revogar este consentimento a qualquer momento, sem prejuízo.

Contato: Para dúvidas ou solicitações sobre seus dados, entre em contato com a equipe de pesquisa pelo e-mail: `[inserir e-mail institucional]`.

Declaro que li e compreendi as informações acima e, de forma livre e esclarecida, consinto com a participação no presente estudo.

Nome do Participante: _____

Assinatura: _____ **Data:** _____