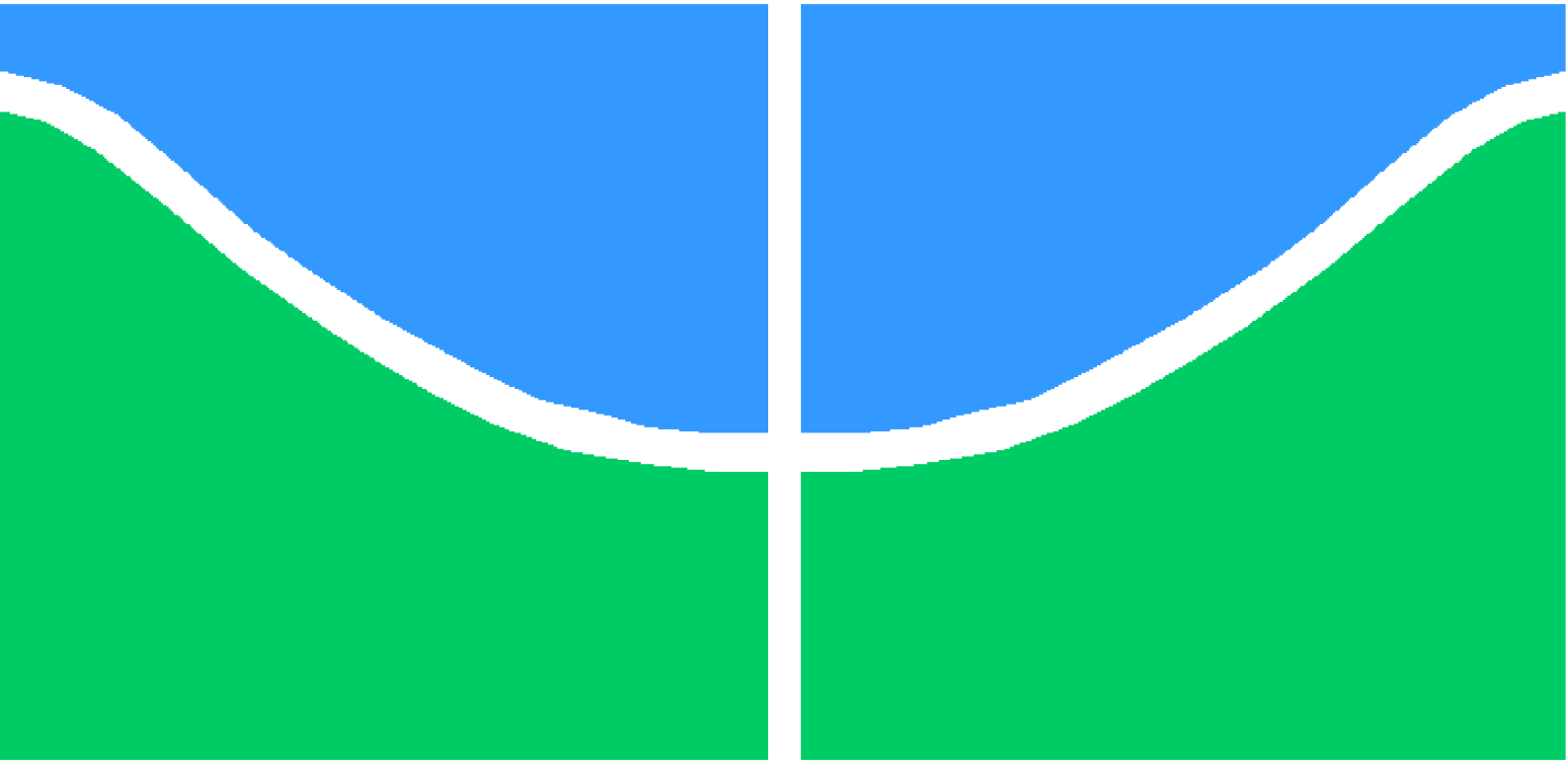

Universidade de Brasília - UnB

Faculdade UnB Gama - FGA

Engenharia de Software

Implementação de requisitos de privacidade da LGPD e ISO 29100 em aplicativos de saúde

Autor: Lucas Lopes Xavier

Orientador: Dra. Fabiana Freitas Mendes

Brasília, DF

2023

Lucas Lopes Xavier

Implementação de requisitos de privacidade da LGPD e ISO 29100 em aplicativos de saúde

Monografia submetida ao curso de graduação em (Engenharia de Software) da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em (Engenharia de Software).

Universidade de Brasília - UnB

Faculdade UnB Gama - FGA

Orientador: Dra. Fabiana Freitas Mendes

Brasília, DF

2023

Lucas Lopes Xavier
Implementação de requisitos de privacidade da LGPD e ISO 29100 em aplicativos de saúde/ Lucas Lopes Xavier. – Brasília, DF, 2023-
317 p. : il. (algumas color.) ; 30 cm.

Orientador: Dra. Fabiana Freitas Mendes

Trabalho de Conclusão de Curso – Universidade de Brasília - UnB
Faculdade UnB Gama - FGA , 2023.

1. Palavra-chave01. 2. Palavra-chave02. I. Dra. Fabiana Freitas Mendes. II. Universidade de Brasília. III. Faculdade UnB Gama. IV. Implementação de requisitos de privacidade da LGPD e ISO 29100 em aplicativos de saúde

CDU 02:141:005.6

Lucas Lopes Xavier

Implementação de requisitos de privacidade da LGPD e ISO 29100 em aplicativos de saúde

Monografia submetida ao curso de graduação em (Engenharia de Software) da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em (Engenharia de Software).

Trabalho aprovado. Brasília, DF, 25 de Julho de 2023:

Dra. Fabiana Freitas Mendes
Orientador

Dra. Edna Dias Canedo
Convidado 1

Msc. Sâmmara Éllen Renner Ferrão
Convidado 2

Brasília, DF
2023

Dedico este trabalho a Deus, que esteve ao meu lado do início ao fim, e aos meus pais, meu irmão, meus padrinhos e minha tia, que me ajudaram e apoiaram durante todo o percurso.

Agradecimentos

Agradeço primeiramente a Deus por me mostrar o caminho e estar ao meu lado do início ao fim. Agradeço também à minha família pelo apoio, principalmente nos momentos difíceis, e por me ajudarem a não desistir. Agradeço, ainda, aos amigos que fiz durante essa trajetória e que sempre me ajudaram. Por fim, gostaria de agradecer à minha orientadora, Fabiana Freitas Mendes, que me ajudou e aconselhou para que eu pudesse obter o melhor resultado possível neste trabalho.

"Esforçai-vos e animai-vos; não temais, nem vos espanteis diante deles;
porque o Senhor teu Deus é o que vai contigo;
a fim de distinguir qual é a vontade de Deus:
não te deixará nem te desamparará.
(Bíblia Sagrada, Deuteronômio 31,6)

Resumo

O crescente avanço das tecnologias da informação e comunicação na área da saúde tem possibilitado o desenvolvimento de aplicações de saúde que coletam e processam uma grande quantidade de dados pessoais sensíveis dos usuários. Consequentemente, a proteção da privacidade desses dados é uma preocupação crescente, especialmente com a entrada em vigor da Emenda Constitucional 115/22, na qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Além disso, também foi aprovada, em agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes e princípios para o tratamento adequado de dados pessoais. Nesse contexto, o objetivo deste trabalho é avaliar a implementação de requisitos de privacidade em aplicativos de saúde, a fim de avaliar a conformidade dessas aplicações em relação às normas de privacidade e proteção de dados pessoais. Para tanto, foi realizada uma revisão bibliográfica para entender os principais assuntos relacionados ao tema, seguida da seleção de aplicativos de saúde nos quais os requisitos seriam avaliados. Considerou-se como critérios de seleção a disponibilidade de documentos, bem como o acesso à aplicação. Em seguida, foi realizada a análise das aplicações, levando em consideração os requisitos de privacidade e proteção de dados estabelecidos pela taxonomia proposta por Ferrão (2022). As contribuições desse trabalho incluem a identificação do nível de conformidade das aplicações de saúde analisadas, destacando eventuais lacunas e oportunidades de melhoria. Além disso, contribui para o desenvolvimento de aplicações de saúde mais adequadas do ponto de vista da privacidade e proteção de dados, promovendo a conscientização sobre a importância desses aspectos na área da saúde e fornecendo diretrizes para aprimorar a conformidade das aplicações com as normas vigentes.

Palavras-chaves: Privacidade. Proteção de Dados. Aplicativos de Saúde.

Abstract

The growing advancement of information and communication technologies in the health area has enabled the development of health applications that collect and process a large amount of sensitive personal data from users. Consequently, the protection of the privacy of such data is a growing concern, especially with the entry into force of Constitutional Amendment 115/22, which guarantees, under the terms of the law, the right to protection of personal data, including in digital media. In addition, the General Data Protection Law (LGPD) was also approved in August 2018, which establishes guidelines and principles for the proper treatment of personal data. In this context, the objective of this work is to evaluate the implementation of privacy requirements in health applications, in order to assess the compliance of these applications in relation to privacy and personal data protection standards. To this end, a literature review was carried out to understand the main issues related to the topic, followed by the selection of health applications in which the requirements would be evaluated. The selection criteria were the availability of documents, as well as access to the application. Then, the applications were analyzed, taking into account the privacy and data protection requirements established by the taxonomy proposed by Ferrão (2022). The contributions of this work include identifying the compliance level of the analyzed health applications, highlighting any gaps and opportunities for improvement. In addition, it contributes to the development of health applications that are more adequate from the point of view of privacy and data protection, promoting awareness of the importance of these aspects in the health area and providing guidelines to improve application compliance with current regulations.

Key-words: Privacy. Data Protection. Health Apps.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ANPD	Autoridade Nacional de Proteção de Dados
ANVISA	Agência Nacional de Vigilância Sanitária
Art	Artigo
CadSuS	Cadastro Nacional de Usuários do SUS
CGU	Controladoria-Geral da União
CNS	Política Nacional de Informação e Informática em Saúde
CPF	Cadastro de Pessoa Física
CREA	Conselho Regional de Engenharia e Agronomia
CRM	Conselho Regional de Medicina
DATASUS	Departamento de Informática do SUS
EC	Emenda Constitucional
GDPR	Regulamento Geral sobre a Proteção de Dados
GSI/PR	Gabinete de Segurança da Informação da Presidência
ICN	Identificação Civil Nacional
IMC	Índice de Massa Corpórea
IP	Protocolo de Internet
LGPD	Lei Geral de Proteção de Dados Pessoais
OAB	Ordem dos Advogados do Brasil
PNIIS	Política Nacional de Informação e Informática em Saúde
RG	Registro Geral
RNDS	Rede Nacional de Dados em Saúde
SUS	Sistema Único de Saúde
TCC1	Trabalho de Conclusão de Curso 1

TCC2	Trabalho de Conclusão de Curso 2
TCU	Tribunal de Contas da União
UnB	Universidade de Brasília

Sumário

1 Introdução

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) entrou em vigor em setembro de 2020 e visa a regulamentação da utilização de dados pessoais no Brasil. Com isso, tornou-se necessária a adequação das empresas às novas diretrizes e regras de privacidade para evitar possíveis vazamentos e sanções e também garantir a segurança dos dados. No setor de saúde, em que há grande fluxo de informações, essa adequação se torna ainda mais relevante.

De acordo com os conceitos da LGPD (BRASIL, 2018), dados biométricos são considerados dados pessoais sensíveis, conforme previsto no artigo 11º. Isso significa que esses dados só podem ser compartilhados com o consentimento do titular ou de seu responsável legal e, segundo o inciso II, só podem ser utilizados para finalidades específicas previstas em lei. Os dados biométricos referem-se a características físicas, comportamentais ou fisiológicas únicas de um indivíduo. Esses dados são utilizados para identificar e autenticar uma pessoa com base em características distintivas do seu corpo ou comportamento. CEPETIC.BR (2021) mostrou que, entre as categorias pesquisadas, os dados biométricos ficaram entre os mais citados como informações que preocupam os usuários da Internet.

Essa preocupação demanda uma reflexão por parte de organizações públicas e privadas sobre a coleta, uso e compartilhamento de dados sensíveis, a fim de garantir a devida proteção e privacidade dos usuários. Nesse contexto, é fundamental que as empresas estabeleçam políticas e práticas sólidas de gerenciamento e privacidade de dados, incluindo a adoção de medidas técnicas e organizacionais para evitar o acesso não autorizado, a perda, a alteração ou a divulgação indevida de informações sensíveis.

Com o objetivo de auxiliar na identificação de requisitos de privacidade conforme a LGPD, que trata da regulação e do tratamento de dados pessoais no Brasil, Ferrão (2022) sugere a aplicação de uma taxonomia. Essa taxonomia deve estar em conformidade com as normas e padrões estabelecidos pela LGPD (BRASIL, 2018) e pela ISO/IEC 29100 (ISO/IEC, 2011), que é uma norma internacional para a gestão de privacidade e proteção de informações.

Com base no trabalho desenvolvido por Ferrão (2022), este trabalho visa analisar a implementação de requisitos de privacidade em aplicativos de saúde. Para isso, utilizou-se a taxonomia proposta por Ferrão (2022), que está em conformidade com a LGPD e a ISO/IEC 29100. A escolha dos aplicativos de saúde como objeto de estudo é justificada pela crescente popularidade desses aplicativos, que oferecem acesso rápido e fácil a informações sobre saúde e bem-estar. Neste cenário, a privacidade dos dados é de extrema importância, já que existe um grande volume de transações envolvendo dados sensíveis,

tornando-os vulneráveis a potenciais vazamentos.

Assim, por meio da taxonomia proposta por Ferrão (2022), foi possível identificar quais requisitos são atendidos pelo estudo de caso proposto. Dessa forma, este trabalho contribui para a discussão sobre a LGPD e a ISO/IEC 29100 no setor da saúde e para a avaliação de soluções que garantam a segurança e privacidade dos dados dos usuários nas aplicações de saúde.

1.1 Objetivos

O objetivo geral deste trabalho é **avaliar a implementação de requisitos de privacidade em sistemas de saúde**. Para tanto, foram propostos seguintes objetivos específicos (OE) os quais ajudam no alcance do objetivo geral.

(OE-1) Estudar e selecionar sistemas para avaliar a implementação de requisitos de privacidade, com base na taxonomia proposta por Ferrão (2022);

(OE-2) Entender os principais conceitos relacionados a privacidade de dados;

(OE-3) Avaliar a implementação dos requisitos de privacidade identificados nos sistemas selecionados;

(OE-4) Avaliar a eficácia da taxonomia adaptada para a proteção de dados em sistemas de saúde;

(OE-5) Propor recomendações para a implementação de medidas de proteção de dados nos sistemas selecionados e na taxonomia, com base nos resultados obtidos.

1.2 Cronograma de atividades

A seguir, na Figura 1, está o cronograma de atividades planejadas para a execução do TCC1. O cronograma apresenta as atividades planejadas e realizadas em cinco meses.

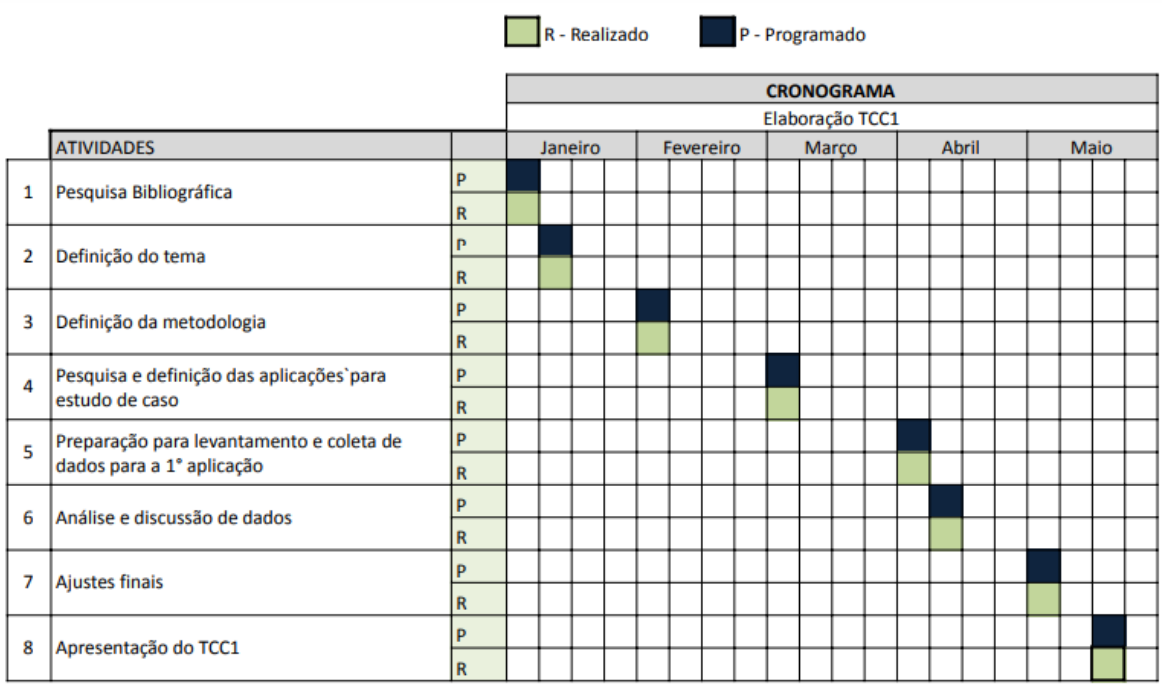

Figura 1 – Cronograma do TCC1. Fonte: Autor.

De acordo com o que é ilustrado na Figura 1, ao longo de um período de cinco meses, foi realizado um conjunto abrangente de atividades. Essas atividades incluíram pesquisa bibliográfica, definições do tema e metodologia, bem como o levantamento, coleta e análise de dados para uma aplicação.

Na Figura 2, está o cronograma de atividades planejadas e executadas durante o TCC2. O cronograma apresenta as atividades planejadas e realizadas em três meses.

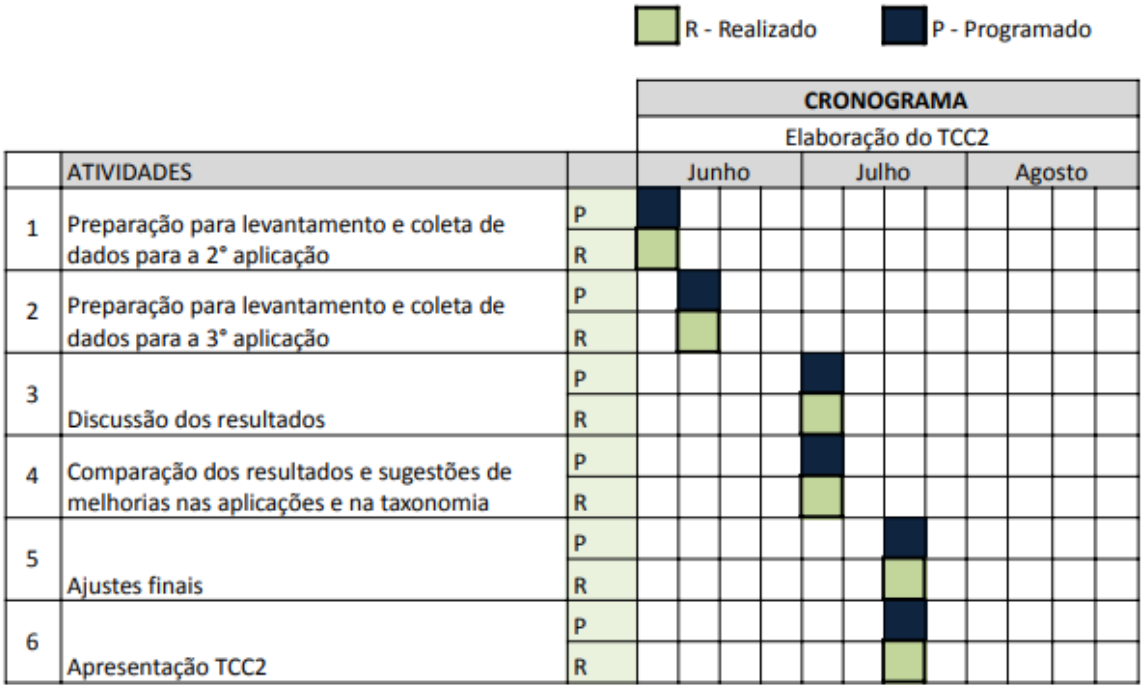

Figura 2 – Cronograma do TCC2. Fonte: Autor.

De acordo com o que é ilustrado na Figura 2, na segunda fase desse trabalho, procedeu-se à coleta de dados referente a mais duas aplicações, bem como à análise e discussão dos resultados obtidos com essas aplicações. No Capítulo 2, dedica-se a uma apresentação minuciosa do referencial teórico, abordando de maneira abrangente os principais conceitos que fundamentam e sustentam todo o desenvolvimento deste trabalho.

Já no Capítulo 3, realiza-se uma exposição da metodologia de pesquisa adotada neste trabalho. Através dessa metodologia, busca-se fornecer um suporte coerente ao processo de desenvolvimento deste trabalho e detalhando as etapas necessárias para a obtenção dos resultados que serão apresentados no capítulo subsequente.

É nos Capítulos 4, 5 e 6 que são apresentados, de forma detalhada, os resultados do estudo de caso realizado sobre os três aplicativos móveis selecionados como objetos de estudo. Por meio de uma análise cuidadosa, os resultados são dissecados e explorados em sua totalidade, visando oferecer uma compreensão abrangente dos aspectos abordados.

Por fim, reserva-se o Capítulo 7 para a discussão dos resultados obtidos e o Capítulo 8 para as considerações finais deste trabalho. Neste momento, são feitas reflexões conclusivas sobre os resultados obtidos, enfatizando as principais descobertas, limitações e possíveis direções futuras para pesquisas adicionais.

2 Referencial Teórico

Neste capítulo serão apresentado os principais conceitos e termos que são relevantes para o execução do trabalho e o referencial teórico utilizado para embasamento da pesquisa.

2.1 Legislações

A privacidade de dados é um conceito amplamente debatido e valorizado na sociedade atual, que lida com a proteção e o controle de informações pessoais de indivíduos. A definição de privacidade pode ser atribuída ao famoso jurista americano Louis Brandeis, que a definiu como "o direito de ser deixado em paz" (WARREN; BRANDEIS, 2013).

Neste contexto, a crescente preocupação com a proteção de dados pessoais ao redor do mundo tem se intensificado, sobretudo devido à pandemia da COVID-19, que impulsionou a utilização de sites e aplicativos voltados para a monitoração da saúde (FIOCRUZ, 2023). Essa rápida evolução gerou preocupações sobre a vulnerabilidade das informações pessoais, o que ocasionou grande destaque a leis e regulamentações específicas, como a Lei Geral de Proteção de Dados (BRASIL, 2018), o Regulamento Geral de Proteção de Dados (European Commission, 2016) e a norma internacional ISO 29100 (ISO/IEC, 2011). Nas próximas seções serão abordados cada uma dessas legislações e normas.

2.1.1 Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (GDPR) (European Commission, 2016) é um legislação que foi aprovada em 2016 e colocada em vigor desde 2018 na União Europeia. Essa legislação visa garantir a proteção dos indivíduos, estabelecendo diretrizes claras para a coleta, armazenamento e uso de dados pessoais (NEVES, 2021; European Commission, 2016).

Conforme destacado por Lorenzon (2021), o objetivo central da GDPR é a proteção dos dados pessoais, estabelecendo diretrizes claras para a coleta, armazenamento e o uso desses dados. Entretanto, algumas das restrições impostas pela GDPR podem gerar desafios para empresas que utilizam dados pessoais em seu escopo.

Caetano (2020) ressalta que a GDPR possui um escopo internacional, que pode impactar empresas e órgãos que utilizam dados pessoais de cidadãos da União Europeia, mesmo que seja fora da União Europeia. Diante desse cenário, é importante que as empresas e organizações estejam cientes das implicações da GDPR, a fim de garantir que ela esteja em conformidade com a regulamentação.

Além disso, a GDPR exerce um impacto significativo no desenvolvimento de tecnologias em escala global. Conforme destacam Li, Yu e He (2019), a regulamentação afeta empresas e organizações ao redor do mundo, trazendo implicações relevantes para a inovação e adoção de novas soluções tecnológicas. Isso ocorre porque a legislação impõe princípios e obrigações rigorosas relacionados à privacidade e à proteção dos dados pessoais dos usuários, obrigando as empresas a adaptarem suas práticas e sistemas para atenderem às normas estabelecidas.

Os princípios instituídos pela GDPR, listados na Tabela 1, servem para garantir a proteção e privacidade dos dados pessoais dos indivíduos da União Europeia. Eles foram criados para estabelecer um conjunto de padrões mínimos para a coleta, uso, processamento e armazenamento de dados pessoais pelas organizações.

Tabela 1 – Princípios instituídos pela GDPR

Princípio	**Descrição**
Licitude, Transparência e Lealdade	O processamento dos dados pessoais deve ser realizado de maneira legalizada, justa e transparente para o titular.
Limitação de Finalidade	Os dados pessoais só podem ser coletados para fins específicos, explícitos e legítimos.
Minimização de Dados	Os dados pessoais devem ser limitados ao mínimo necessário para os fins especificados
Exatidão	Os dados pessoais devem ser precisos e atualizados
Limitação de Armazenamento	Os dados pessoais só podem ser armazenados pelo tempo necessário para o tratamento e processamento
Integridade e Confiabilidade	Os dados pessoais devem ser processados de maneira segura e protegida contra perda, acesso ou divulgação não autorizados
Responsabilidade	Os agentes de tratamento devem ser responsáveis por garantir a conformidade com a GDPR e ser capaz de demonstrar.

Fonte: Adaptado de European Commission (2016).

Ao analisar os princípios apresentados na Tabela 1, pode-se observar que eles refletem e as principais ideias com foco na proteção, privacidade e tratamento de dados pessoais.

Os princípios de licitude, transparência e lealdade ressaltam a necessidade de tratar os dados pessoais de forma justa e transparente, garantido que o titular dos dados esteja ciente sobre o uso de suas informações. A limitação de finalidade e a minimização de dados, reforçam a ideia de que os dados pessoais são para fins específicos e legítimos, além de serem limitado ao mínimo necessário.

A exatidão e a limitação de armazenamento destacam a importância de manter os dados pessoais atualizados e armazená-los apenas pelo tempo necessário para cumprir a finalidade pretendida. Esses princípios, visam garantir que os dados sejam precisos e não fiquem armazenados indefinidamente, protegendo, assim, a privacidade do titular.

A integridade e a confiabilidade são princípios importantes pois tratam da segurança no processo de tratamento de dados pessoais. Esses princípios enfatizam a importância de implementar medidas de segurança adequadas para a proteção dos dados e do titular.

Por fim, a responsabilidade destaca os agentes de tratamento. Eles são responsáveis em garantir a conformidade com a GDPR e demonstrar essa conformidade quando necessário.

Os papéis também desempenham um papel fundamental na implementação da GDPR porque cada tipo de entidade tem responsabilidades específicas na gestão e proteção dos dados pessoais. Essas responsabilidades são estabelecidas para garantir a conformidade com os princípios da regulamentação. A GDPR atribui responsabilidades específicas a diferentes tipos de entidades, incluindo controladores, processadores e autoridades de proteção de dados. Os papéis são importantes para garantir a implementação adequada da GDPR e para assegurar que os direitos e privacidade dos indivíduos sejam protegidos de acordo com os princípios da regulamentação. A Tabela 2 mostra os papeis e a descrição estabelecidos pela GPDR.

Tabela 2 – Papéis instituídos pela GDPR

Papel	**Descrição**
Titular	Pessoa física identificável, a quem os dados pessoais se referem
Controlador	Pessoa jurídica ou física, de direito público ou privado, responsável por determinado os propósitos e os meios de processamento de dados
Encarregado	Indivíduo ou organização designado pelo controlador ou operador para monitorar a conformidade com a regulamentação
Autoridade	Entidade responsável por supervisionar a aplicação da regulamentação de proteção de dados na União Europeia
Terceiro	Pessoa física ou jurídica, de direito público ou privado, que não seja titulo, controlador, operador ou pessoa autorizada

Fonte: Adaptado de European Commission (2016).

Essa divisão de responsabilidades entre as entidades, conforme a Tabela 2, garante a implementação adequada da GDPR e facilita a cooperação entre os diversos atores envolvidos na proteção de dados. Além disso, contribui para assegurar que os direitos dos titulares sejam protegidos de acordo com os princípios da regulamentação.

2.1.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) é uma legislação brasileira, colocada em vigor em 2020, que visa regular o tratamento, coleta, armazenamento, processamento e o compartilhamento de dados. A LGPD tem como objetivo a proteção da privacidade e da liberdade individual e garantir o uso adequado e ético desses dados pelas empresas e órgãos públicos. Essa lei teve origem em um movimento internacional. Esse movimento, é caracterizado pela adoção de leis e regulamentações em todo o mundo, visando proteger a privacidade e os dados pessoais dos indivíduos, um exemplo disso é o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (European Commission, 2016).

O objetivo da LGPD é garantir que as empresas e órgãos que lidam com dados pessoais de usuários cumpram normas e diretrizes que garantam a proteção desses dados (BRASIL, 2018). Ela estabelece regras e princípios sobre como os dados devem ser tratados, com a finalidade de proteger a privacidade e os direitos dos titulares. Além disso, a importância da LGPD tem ganhado grande destaque devido à Emenda Constitucional 115/22 (Presidência da República Federativa do Brasil, 2022), que estabelece que o direito à proteção de dados pessoais tornou-se um direito individual assegurado pela Constituição Federal (Brasil, 1988).

Nos últimos anos, Diversas legislações têm se destacado ao tratar sobre a regulação de dados pessoais, incluindo o Marco Civil da Internet (BRASIL, 2014), a Regulação Geral de Proteção de Dados (GDPR) (European Commission, 2016) e a Constituição Federal de 1988 (Brasil, 1988). Além disso, pesquisadores como Silva (2020),Soares (2021) e outros têm se dedicado ao estudo da LGPD e suas implicações na área da saúde.

Atualmente, a LGPD determina papéis e atribui responsabilidades e deveres específicos a diferentes tipos de entidades que lidam com dados pessoais no Brasil, visando garantir a proteção dos direitos dos titulares dos dados e a segurança dos dados em geral. Os papéis da LGPD são importantes porque ajudam a garantir que os dados pessoais sejam tratados de forma adequada, respeitando os direitos dos titulares dos dados e seguindo as diretrizes estabelecidas na lei. A definição clara de papéis e responsabilidades também promove a transparência e a responsabilidade no tratamento de dados pessoais no Brasil (BRASIL, 2018). A Tabela 3 apresenta os papéis com a suas respectivas responsabilidades.

Tabela 3 – Papéis instituídos pela LPGD

Papel	**Descrição**
Titular	Pessoa natural, dono dos dados pessoais, responsável por acessar e conceder acesso
Controlador	Pessoa natural ou jurídica responsável pela tomada de decisões sobre o tratamento dos dados
Operador	Pessoa natural ou jurídica, responsável pelo tratamento de dados
Encarregado	Pessoa indicada pelo controlador e operador para receber demandas dos titulares e dos órgãos
Autoridade	Órgão público responsável por fiscalizar e aplicar sanções

Fonte: Adaptado de Brasil (2018).

Além dos papéis estabelecidos pela LGPD, há sanções que ocorrem em caso de descumprimento das diretrizes previstas na LGPD que incluem penalidades como multas, sanções administrativas e proibições de tratar dados pessoais (BRASIL, 2018). Essas sanções variam de acordo com a gravidade dos danos causados ao titular, podendo ser uma advertência que somente avisa a empresa sobre a infração e faça a exigência para que ela se adeque a lei ou uma multa diária de 0,5% do faturamento da empresa para infrações mais graves. Na Tabela 4, contém as principais punições de acordo com a LGPD e o estudo de Fretta (2021).

Tabela 4 – Punições de acordo com a LGPD

Advertência	**Descrição**
Advertência	Avisa a empresa sobre a infração e exigir que se adeque à lei
Multa simples	Multa de até 2 por cento do faturamento da empresa, limitada a 50 milhões
Multa diária	Multa de até 0,5 por cento do faturamento diário

Fonte: Adaptado de Brasil (2018).

Além disso, a LGPD possui princípios orientadores. Eles são fundamentais para a proteção dos dados pessoais e garantem que as empresas e órgãos públicos sigam normas éticas e adequadas no tratamento desses dados. De acordo com Brasil (2018), esses princípios incluem a finalidade específica, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas conforme a Tabela 5.

Tabela 5 – Princípios de acordo com a LGPD

Princípio	**Descrição**
Finalidade específica	Informar ao titular qual é a finalidade específica e o fim para qual os dados estão sendo coletados
Adequação	Garantir que os dados coletados sejam relevantes, adequados e limitados ao necessário
Necessidade	Coletar o mínimo de dados necessários
Livre acesso	Permitir que o titular tenha acesso aos seus dados pessoais e possa solicitar sua correção, exclusão ou portabilidade
Qualidade dos dados	Assegurar que os dados sejam precisos e atualizados
Transparência	Disponibilizar informações claras e acessíveis sobre os processos de tratamento de dados
Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
Prevenção	Adoção de medidas para evitar a ocorrência de danos ao titular dos dados
Não discriminação	Evitar que o tratamento dos dados seja utilizado para fins ilícitos ou abusivos;
Responsabilização e prestação de contas	Ser responsável pelo tratamento de dados pessoais e prestar contas aos titulares;

Fonte: Adaptado de Brasil (2018)

A Tabela 5 apresenta os princípios que norteiam a Lei Geral de Proteção de Dados no Brasil. Cada um desses princípios é fundamental para garantir que os dados pessoais sejam tratados de forma ética e adequada pelas empresas e órgãos públicos. A finalidade específica determina que o titular dos dados deve saber qual é o objetivo específico da coleta desses dados. Já o princípio da adequação garante que os dados coletados sejam relevantes, adequados e limitados ao necessário. O princípio do livre acesso permite que o titular dos dados tenha acesso a suas informações pessoais e possa solicitar correção, exclusão ou portabilidade desses dados. A qualidade dos dados é importante para garantir que as informações sejam precisas e atualizadas. A transparência assegura que informações claras e acessíveis sobre o processamento dos dados sejam disponibilizadas. A segurança, a prevenção e a não discriminação são princípios que visam proteger os dados pessoais de acessos não autorizados e evitar danos ao titular dos dados. Por fim, a responsabilização e prestação de contas determinam que as empresas e órgãos públicos são responsáveis pelo tratamento dos dados pessoais e devem prestar contas aos titulares desses dados.

Portanto, os princípios da LGPD são de extrema importância para garantir a privacidade e a liberdade individual dos cidadãos, bem como para promover um tratamento adequado e ético dos dados pessoais.

Outro ponto importante da LGPD é sobre o tratamento de dados sensíveis. Isso se torna ainda mais relevante quando se trata de dados sensíveis relacionados à saúde, uma vez que o vazamento dessas informações pode causar danos irreparáveis aos titulares. Segundo Martins e Teles (2021), a LGPD traz desafios para a implantação na área da saúde, especialmente devido à quantidade de abusos e vazamentos de dados que têm ocorrido nos últimos anos.

No artigo 5°, inciso II da LGPD (BRASIL, 2018), os dados sensíveis são classificados como "Dados pessoais sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde ou vida sexual, genética ou biometria, quando vinculados a uma pessoa natural."

Os dados de saúde são considerados dados sensíveis, pois podem ser usados para identificar pessoas e revelar informações íntimas (FRETTA, 2021; BRASIL, 2018). No entanto, de acordo com a LGPD, os dados podem ser anonimizados, ou seja, tratados de tal forma que não seja possível identificar um indivíduo. Isso permite que os dados de saúde sejam usados para fins de pesquisa e análise sem violar a privacidade dos pacientes (COSTA; ROSA, 2021).

Diante disso, o artigo 11 da LGPD traz as possibilidades de tratamento de dados sensíveis, como o consentimento específico do titular, o cumprimento de obrigação legal ou regulatória, a proteção da vida ou da incolumidade física do titular ou de terceiros, entre outras hipóteses. É importante que as empresas e organizações estejam cientes das obrigações impostas pela LGPD e implementem medidas de segurança adequadas para garantir a proteção desses dados (BRASIL, 2018).

A LGPD também exige que as entidades de saúde obtenham o consentimento dos usuários antes de coletar, armazenar ou compartilhar seus dados (COSTA, 2022). Isso significa que os usuários devem ser informados sobre como seus dados serão usados e devem conceder seu consentimento antes de qualquer dado ser coletado ou compartilhado.

Segundo um levantamento da Surfshark (DIGITAL, 2022), empresa que atua na área de ferramentas de privacidade e segurança online, o Brasil configura como o 6º país que mais sofre com vazamento de dados, ocasionados a partir de ataques ou brechas no sistema. Portanto, esses casos reforçam a importância de medidas de segurança adequadas para a proteção de dados sensíveis dos usuários e que contenham políticas transparentes sobre o tratamento dos dados, garantindo a privacidade e os direitos individuais dos usuários.

2.1.3 ISO/IEC 29100

A norma ISO/IEC 29100 (ISO/IEC, 2011) é uma norma internacional que estabelece princípios e requisitos para a privacidade de dados em sistemas de informação. Essa norma é importante porque a privacidade é um direito fundamental, estabelecido na constituição federal (Brasil, 1988). Por isso, as organizações e empresas que tratam informações pessoais precisam garantir a proteção dessas informações contra o uso indevido, acesso não autorizado e divulgação não autorizada. Além disso, a norma ISO/IEC 29100 serve como um guia para a implementação de boas práticas para a proteção da privacidade, fornecendo um guia estruturado para a gestão de privacidade da informação.

A ISO/IEC 29100 é importante porque ajuda as organizações a gerenciar riscos associados ao tratamento de informações pessoas e a proteger a privacidade dos usuários. A norma estabelece requisitos para a gestão da privacidade e a implementação de controles de segurança. Além disso, também estabelece a identificação e avaliação dos riscos de privacidade e a monitorização e revisão contínuas. Também, fornece um conjunto de princípios que orientam a gestão da privacidade da informação, incluindo: transparência, consentimento, minimização de dados, limitação de finalidade, precisão, segurança, retenção e destruição (ISO/IEC, 2011).

Os princípios estabelecidos na norma ISO/IEC 29100 são fundamentais para a gestão da privacidade da informação. A transparência é um princípio importante, pois os usuários têm o direito de saber quais informações estão sendo coletadas e como serão utilizadas. O consentimento é outro princípio importante, pois os indivíduos têm o direito de controlar o uso de suas informações pessoais. A precisão é importante porque as informações pessoais precisam ser precisas e atualizadas. A segurança é importante para proteger as informações pessoais contra acesso não autorizado e divulgação não autorizada. A retenção e destruição seguras são importantes para garantir que as informações pessoais sejam mantidas somente pelo tempo necessário e que sejam destruídas de forma segura quando não forem mais necessárias. Por fim, a minimização de dados e a limitação de finalidade são importantes porque ajudam a garantir que as informações coletadas sejam adequadas, relevantes e limitadas ao propósito específico para o qual foram coletadas.

Portanto, a norma é uma ferramenta importante para a gestão da privacidade, ela estabelece requisitos e princípios e auxilia a gerenciar os riscos associados ao tratamento de dados. As organizações e empresas que lidam com dados pessoais, devem considerar a implementação da norma como uma prática recomendada para garantir a proteção adequada dos dados, afim de proteger a privacidade dos usuários.

Em paralelo com a ISO/IEC 29100, há a Lei Geral de Proteção de dados no Brasil e o Regulamento Geral de Proteção de Dados na União Europeia. Ambos regulamentos reforçam os princípios contidos na ISO/IEC 29100, como transparência, consentimento,

minimização de dados, limitação de finalidade, precisão, segurança, e destruição de dados pessoais. Juntos, a ISO/IEC 29100, a LGPD e a GDPR representam um esforço conjunto para estabelecer um conjunto de normas, leis e regulamentos que garantam a privacidade e a proteção de dados pessoais em um mundo cada vez mais digital e globalizado.

2.2 Engenharia de Requisitos

A Engenharia de Requisitos é uma etapa fundamental no desenvolvimento de software que envolve a elicitação, análise, especificação, validação e gerenciamento de requisitos para desenvolvimento de software (SOMMERVILLE, 2011). É um processo para garantir que o software desenvolvido atenda as necessidades dos usuários e das partes interessadas.

De acordo com Pressman e Maxim (2016), a engenharia de requisitos é o processo de estabelecer os serviços que o cliente necessita e de garantir que esses serviços sejam entregues pelo sistema de software.

Castro (2015) destaca a importância da Engenharia de Requisitos para o sucesso de um projeto de software, além da necessidade de abordar o processo de forma sistemática, quantificável e estruturada. O autor também ressalta a importância da comunicação e colaboração entre desenvolvedores e stakeholders para garantir que as necessidades sejam perfeitamente atendidas. Assim, a identificação dos requisitos é essencial para o sucesso do projeto, pois se não forem identificados corretamente, podem ocorrer problemas como atrasos no desenvolvimento, aumento de custos e insatisfação do cliente.

2.2.1 Fases da Engenharia de Requisitos

As fases da engenharia de requisitos visam garantir a coleta adequada das necessidades dos usuários e stakeholders, além de especificar de forma clara e precisa os requisitos do sistema.

Pressman e Maxim (2016) apresentam as fases da engenharia de requisitos conforme ilustra a Figura 3.

Figura 3 – Fases da Engenharia de Requisitos. Fonte: Adaptado de Sommerville (2011).

Na fase de concepção é importante a comunicação da equipe de desenvolvimento com os clientes, para entender suas demandas e expectativas em relação ao software que será desenvolvido (CASTRO, 2015; SILVA, 2020).

Na fase de levantamento de requisitos, a equipe de desenvolvimento coleta as informações necessárias para entender quais são as necessidades dos usuários, para isso existem várias técnicas de elicitação de requisitos conforme a Tabela 6.

Durante a fase de análise, a equipe examina os requisitos previamente coletados, identificando possíveis conflitos e inconsistências. Nesta etapa, também ocorre a classificação dos requisitos, proporcionando maior organização e clareza. Na Seção 2.2.3 contém maiores detalhes sobre as classificações de requisitos.

Na fase de negociação ocorre discussão com os stakeholders sobre os requisitos, para que todos possam chegar a um consenso sobre o que é necessário para o software.

A fase de especificação é feita a documentação dos requisitos que servirá como base no desenvolvimento de software.

Por fim, a fase de gestão visa garantir que os requisitos do sistema sejam gerenciados de forma eficaz durante todo o ciclo de vida do software. Essa fase inclui atividades como a identificação, análise e validação dos requisitos,

Essas fases são consideras essenciais para garantir que os requisitos sejam coletados e especificados de forma adequada, garantido que as necessidades das partes interessadas (PRESSMAN; MAXIM, 2016).

2.2.2 Técnicas de elicitação de requisitos

As técnicas da engenharia de requisitos são importantes para a aplicação de uma taxonomia de requisitos de privacidade, pois elas fornecem meios para coletar e analisar as informações relacionadas à privacidade do usuário e ao tratamento de seus dados pessoais no software. Essas técnicas ajudam a equipe de desenvolvimento a entender as necessidades dos usuários e stakeholders em relação à privacidade, a identificar possíveis conflitos e inconsistências nos requisitos de privacidade coletados e a especificar claramente esses requisitos (SOMMERVILLE, 2011).

A elicitação de requisitos é uma das primeiras etapas do processo de desenvolvimento de software, que consiste na identificação, coleta e documentação dos requisitos. É uma fase crítica, pois se houver inconsistências e imprecisões podem ocasionar a insatisfação dos clientes (SOMMERVILLE, 2011; SILVA, 2020; JÚNIOR; VASCONCELOS; SILVA,).

Existem várias técnicas de elicitação de requisitos, e a escolha da técnica depende do contexto e características do projeto. Algumas das principais técnicas de elicitação são apresentadas na Tabela 6.

Tabela 6 – Técnicas de elicitação de requisitos

Técnica	**Descrição**
Observação	Observação dos processos, atividades e ambiente de trabalho dos usuários.
Análise de documentos	Analisa documentos existentes, como manuais, relatórios, contratos e normas
Entrevistas	Conversas estruturadas com usuários e stakeholders
Questionários	Elaboração de questionários para coletar informações dos usuários
Brainstorming	Geração livre de ideias para identificar possíveis requisitos
Grupos focais	Discussão em grupo com usuários e stakeholders para identificar requisitos em comuns e diferentes entre eles
Workshops	Reunião presenciais com usuários e desenvolvedores, para identificar e priorizar requisitos
Persona	Descrição fictícia de um usuário que representa as características e necessidades dos usuários reais
Casos de uso	Modela cenários que descrevem como os usuários interagem com o sistema
Storytelling	Conta histórias fictícias de como o sistema deveria funcionar
Prototipagem rápida	Criação de protótipos de software para obter feedback dos usuários. Pode ser descartável ou exploratório

Fonte: Adaptado de Sommerville (2011), Pressman e Maxim (2016).

Dentre as técnicas de engenharia de requisitos, algumas são especialmente relevantes para a aplicação de uma taxonomia de requisitos de privacidade. Por exemplo, as técnicas descritas por Pressman e Maxim (2016) como a técnica de entrevistas pode ser usada para coletar informações diretamente dos usuários e stakeholders sobre suas expectativas e preocupações em relação à privacidade. Já a técnica de análise de documentos permite a identificação de requisitos legais e regulatórios relacionados à privacidade, como a LPGD (BRASIL, 2018), a ISO 29100 (ISO/IEC, 2011) e a GDPR (European Commission, 2016).

2.2.3 Classificação de requisitos

A classificação de requisitos é uma ferramenta útil para a gestão de requisitos em projetos de software, ajudando a priorizar as diferentes fontes de requisitos com possíveis conflitos e desafios (CASTRO, 2015). Para isso, há diferentes formas de classificação conforme mostra a Figura 4.

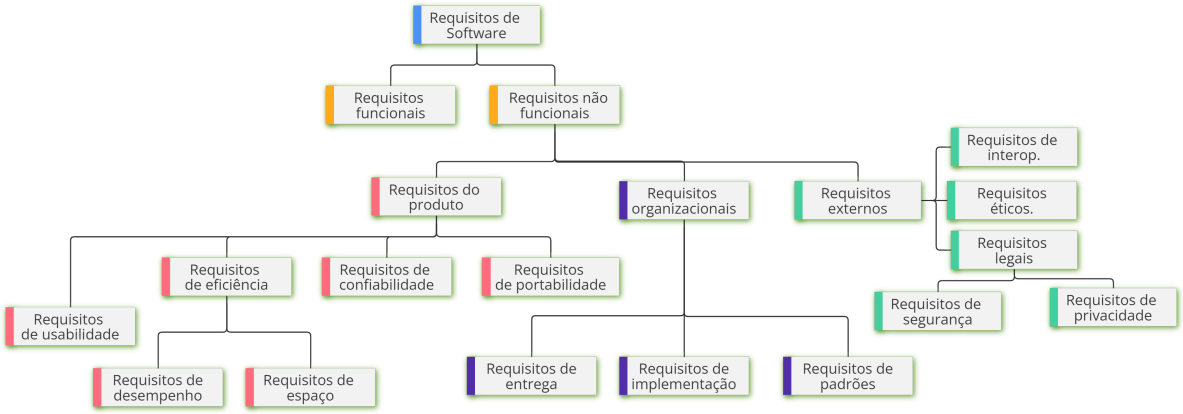

Figura 4 – Classificação de requisitos de software. Fonte: Adaptado de Sommerville (2011).

Uma das classificações existentes é aquela que considera o nível de abstração dos requisitos. Esse tipo de classificação permite uma melhor compreensão e organização dos requisitos do sistema em diferentes níveis de detalhamento. Segundo Sommerville (2011), essa classificação pode ser feita em três níveis: requisitos de usuários, requisitos do sistema e requisitos detalhados. Os requisitos do usuário são uma visão de alto nível dos objetivos e metas do cliente, enquanto os requisitos do sistema são uma descrição mais detalhada dos requisitos funcionais e não funcionais do sistema. Já os requisitos detalhados incluem especificação mais técnicas dos requisitos, e geralmente são utilizados na fase de desenvolvimento do software.

Por outro lado, Pressman e Maxim (2016), propõem uma classificação de requisitos em quatro níveis: requisitos do usuário, requisitos do sistema, requisitos de software e requisitos de interface. Os requisitos do usuário descrevem as necessidades e objetivos dos stakeholders do sistema, enquanto os requisitos do sistema descrevem as funcionalidades e características do sistema. Já os requisitos de software são a especificação precisa das funções e características do softwares e o requisitos de interface são as especificações de interface do usuário.

Outra classificação importante, é a classificação de requisitos em funcionais e não funcionais, que é amplamente discutida. Requisitos funcionais estão relacionados as funções que o sistema deve executar, ou seja, as suas características comportamentais, como por exemplo, processamento e saída de dados (SOMMERVILLE, 2011). Por outro lado,

requisitos não funcionais estão relacionados a atributos de qualidades do sistema, como desempenho, usabilidade, confiabilidade e segurança (PRESSMAN; MAXIM, 2016).

É importante destacar que a diferença entre requisitos funcionais e não funcionais não é tolamente clara e rígida. Muitas vezes não há distinção entre os dois tipos. (SOMMERVILLE, 2011)

Pressman e Maxim (2016) destacam que enquanto os requisitos funcionais definem o que o sistema deve fazer, os requisitos não funcionais definem como ele deve ser feito. Portanto, é fundamental identificar e especificar corretamente os requisitos desde o início do projeto, pois eles influenciam diretamente as decisões de implementação do orçamento.

Segundo Pressman e Maxim (2016) além das classificações citadas anteriormente, há também a classificação quanto a origem. De acordo com Sommerville (2011) existem três tipos principais de origens de requisitos: de produto, organizacionais e externos. Os requisitos de produto são aqueles que se referem diretamente ao produto de software. Se refere as funcionalidades, desempenho, usabilidade e entre outros. Já os requisitos organizacionais são aqueles que derivam das políticas, e diretrizes da organização. Os requisitos externos, por sua vez, são aqueles que estão relacionados a fontes externas a organização. Como requisitos legais, éticos e morais.

A proposta de taxonomia de Ferrão (2022) categoriza seus requisitos como funcionais e não funcionais, conforme descrito por Pressman e Maxim (2016), pois abrange tanto as funcionalidades que o sistema deve fazer quanto a forma como essas funcionalidades devem ser implementadas. Além disso, esses requisitos também são considerados legais. Sobre essa classificação há mais detalhes na Seção 2.3, uma vez que estão embasados na LGPD e na ISO 29100.

2.3 Requisitos de privacidade

Os requisitos de privacidade, podem ser classificados como requisitos legais, de acordo com a classificação tratada na Seção 2.2.3. Esses requisitos de privacidade são uma das principais preocupações atualmente quando se trata de sistema de tecnologia da informação. Eles visam garantir que as informações pessoais dos usuários desses sistemas sejam tratados de acordo com diretrizes e regras e que a privacidade do usuário seja preservada (BARNES, 2013).

De acordo com Solove (2006), a privacidade é um direito humano fundamental e deve ser protegida em todos os níveis. Portanto, é crucial que as empresas que lida com informações pessoais, principalmente dados sensíveis, tenham políticas e diretrizes de privacidades claras, bem definidas e eficazes. Esse objetivo, pode ser alcançado por meio da implementação de medidas de segurança, como criptografia e autenticação

A revisão feita por Mendes, Rosa e Bonacin (2019) destaca a importância do uso da semiótica na análise e especificação de requisitos de privacidade. A semiótica pode ser utilizada para identificar e analisar os requisitos envolvidos no processamento de dados, como os de privacidade e as políticas de privacidade, e para desenvolver soluções que garantam a privacidade dos usuários. Além disso, essa revisão destaca que os requisitos de privacidade devem ser estabelecidos com base na semiótica, considerando não apenas os aspectos técnicos, mas também as questões éticas e legais envolvidas no processamento de dados. É fundamental que os desenvolvedores de software adotem uma abordagem que considere a privacidade dos usuários desde a concepção do produto, seguindo os princípios de segurança por design (BARNES, 2013).

Com base nas análises dos autores Barnes (2013), Solove (2006), Mendes, Rosa e Bonacin (2019), pode-se concluir que os requisitos de privacidade devem ser estabelecidos com base na semiótica, considerando não apenas os aspectos técnicos, mas também as questões éticas e legais envolvidas no processamento de dados. É fundamental que os desenvolvedores de software adotem uma abordagem que considere a privacidade dos usuários desde a concepção do produto, seguindo os princípios de segurança por design.

2.4 Taxonomias de Requisitos de Privacidade

Uma taxonomia é uma técnica de classificação que visa organizar informações e conceitos em categorias hierárquicas, permitindo que as informações sejam identificados de forma clara e precisa (USMAN et al., 2017).

Segundo Pressman e Maxim (2016), a identificação correta dos requisitos é um dos principais desafios da engenharia de requisitos. A taxonomia pode ajudar a eliminar esse desafio, fornecendo uma estrutura clara e organizada para conceitos relacionados ao domínio da aplicação.

A taxonomia pode ser usado como uma ferramenta que visa auxiliar na elicitação, na validação e na verificação e na rastreabilidade dos requisitos ao longo do ciclo de vida do software (VEGAS; JURISTO; BASILI, 2009). Através de uma taxonomia, é possível identificar padrões, relações e dependências entre os requisitos, o que ajuda a entender melhor o domínio do problema e a tomar decisões em relação aos requisitos do software.

Segundo Vegas, Juristo e Basili (2009), a taxonomia pode ajudar a consolidar o conhecimento, fornecendo uma maneira de organizar e classificar as técnicas, metodologias e diferentes abordagens. Além disso, pode fornecer uma base para futuras pesquisas e consequentemente de um corpo de conhecimento mais estruturado.

O desenvolvimento de uma taxonomia pode ser estruturado através de uma metodologia em diversas fases, como propôs Usman et al. (2017), Bayona-Oré et al. (2014).

A metodologia consiste nas fases:

(F-1) Planejamento: Nessa fase, são estabelecidos planos para definir as atividades para o desenho e a construção da taxonomia.

(F-2) Identificação e extração: O plano de trabalho e as informações exigidas pela organização devem estar alinhados.

(F-3) Construção: É construído a taxonomia usando uma biblioteca de termos, a fim de determinar a estrutura final da taxonomia.

(F-4) Validação: Nessa fase, é verificado se a taxonomia está de acordo com o escopo proposto e se atende aos objetivos.

(F-5) Implantação: Por fim, a fase final, em que a taxonomia é implantada.

A metodologia proposta por (USMAN et al., 2017; BAYONA-ORÉ et al., 2014) pode ser adaptada para o contexto de engenharia de requisitos e a engenharia de software, permitindo a construção de uma taxonomia específica para o domínio de aplicação do software. Sendo assim, usada como uma ferramenta para auxiliar no processo de identificação, elicitação, validação e verificação de requisitos.

Pressman e Maxim (2016) aponta que requisitos mal-entendidos ou ambíguos é um dos principais problemas durante a elicitação de requisitos, com essa abordagem, é possível criar um vocabulário comum que facilita a comunicação entre diferentes stakeholders no processo de identificação e elicitação de requisitos. Outra característica importante da taxonomia, é sua flexibilidade e adaptabilidade (UNTERKALMSTEINER; FELDT; GORSCHEK, 2014).

2.4.1 Taxonomia escolhida

Ferrão (2022) propõe uma taxonomia de requisitos de privacidade com base na Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) e na norma ISO/IEC 29100 (ISO/IEC, 2011). O objetivo da taxonomia é fornecer uma estrutura sistemática para a identificação e classificação dos requisitos de privacidade em sistemas de informação, com foco na aplicação prática no setor de Open Banking no Brasil.

A taxonomia é importante porque fornece uma maneira estruturada de lidar com a complexidade dos requisitos de privacidade e ajuda a garantir que os sistemas de informação atendam aos requisitos regulatórios e de privacidade dos usuários. Ela pode ser usada por organizações para desenvolver e manter sistemas de informação que atendam aos requisitos de privacidade, para avaliar a conformidade dos sistemas de informação com os requisitos de privacidade. (FERRÃO, 2022)

Para desenvolver a taxonomia, a autora Ferrão (2022) realizou uma revisão sistemática da literatura sobre privacidade e regulamentações relevantes, como a LGPD (BRASIL, 2018) e a ISO/IEC 29100 (ISO/IEC, 2011). A revisão foi feita usando o protocolo de Kitchenham e Charters (KITCHENHAM; CHARTERS, 2007). Essa taxonomia é baseada em método de análise de requisitos com base em objetivos (ANTóN, 1996) que consiste em três passos principais.

(P-1) Identificação de requisitos: Nessa etapa, os objetivos do sistema são identificados, isso inclui a identificação das ações, determinação das partes envolvidas (FERRÃO, 2022).

(P-2) Classificação dos requisitos: Nessa etapa, os requisitos foram classificados em categorias com base em uma lista que possuem os mesmos objetivos. A ISO/IEC 29100 e a LGPD possuem bastante similaridade em alguns pontos, por isso, foram agrupados em um somente requisito, para evitar redundâncias desnecessárias (FERRÃO, 2022).

(P-3) Refinamento dos requisitos: Nessa etapa, foi verificado possíveis redundâncias e inconsistências (FERRÃO, 2022).

A figura 5, mostra o processo de construção de um requisito, elaborado por Ferrão (2022),

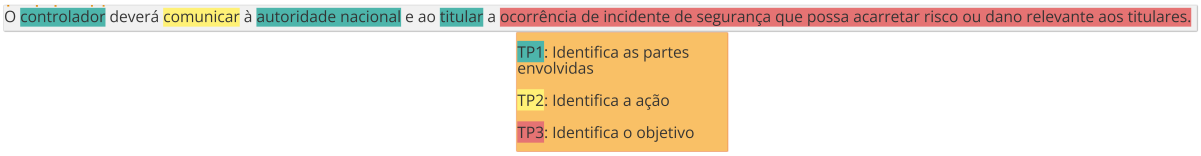

Figura 5 – Construção de requisito. Fonte: Adaptado de Ferrão (2022)

A construção dos requisitos foram divididos em 3 partes de acordo com Ferrão (2022). Em **TP1**, o objetivo é identifica as partes envolvidas no requisitos, em seguida, em **TP2**, o objetivo é identificar o que a parte envolvida realiza, a ação realizada pelas partes envolvidas. Por fim, em **TP3** é identificado o objetivo que os envolvidos estão participando.

Nas seções seguintes, estão detalhados a forma de divisão da taxonomia proposta por Ferrão (2022). A taxonomia é dívida em sete categorias e em cinco contextos que estão detalhados a seguir.

2.4.2 Categorias

A taxonomia proposta por Ferrão (2022) foi criada em sete categorias diferentes, baseada nos princípios da LGPD.

A **primeira categoria**, chamada de “finalidade”, determina que o uso e processamento dos dados deve se limitar a uma finalidade específica autorizada e preferencialmente de modo escrito pelo titular(FERRÃO, 2022).

A **segunda categoria**, chamada de “adequação”, garante que o tratamento deve ser compatível com a finalidade autorizada (FERRÃO, 2022)..

A **terceira categoria**, chamada de “necessidade” , estabelece que o tratamento deve se limitar à necessidade descrita previamente (FERRÃO, 2022).

A **quarta categoria**, denominada de “livre acesso”, garante ao titular dos dados, o direito de consulta gratuita sobre o tratamento de seus dados (FERRÃO, 2022).

A **quinta categoria**, chamado de “qualidade dos dados”, determina que os dados sejam exatos, claros, relevantes e atualizados (FERRÃO, 2022)..

A **sexta categoria**, chamado de “transparência”, garante que o titular tenha informações claras e precisas sobre o tratamento de seus dados (FERRÃO, 2022)..

A **sétima categoria**, chamado de “segurança”, promove medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados ou situações acidentais (FERRÃO, 2022).

A **oitava categoria**, chamado de “prevenção”, estabelece medidas para prevenir danos aos titulares e aos agentes de tratamento (FERRÃO, 2022).

A **nona categoria**, chamado de “não discriminação”, proíbe a utilização dos dados para fins discriminatórios ilícitos ou abusivos (FERRÃO, 2022).

Por fim, a **décima categoria**, chamado de “responsabilização e prestação de contas”, exige que os agentes de tratamento demonstrem a eficácia das medidas adotadas para cumprir as normas de proteção de dados pessoais (FERRÃO, 2022).

2.4.3 Contexto

Os contextos criados por Ferrão (2022) visam ajudar os analistas de sistemas a classificar as necessidades de privacidade em sua instituição para garantir a conformidade com a LGPD e a ISO/IEC 29100. Foram propostos cinco contextos conforme mostra a Figura 6.

Estudo e pesquisa, governança, gestão pública, software e infraestrutura foram os contextos propostos por Ferrão (2022). Eles visam auxiliar a equipe de desenvolvimento de software durante a elicitação de requisitos de privacidade.

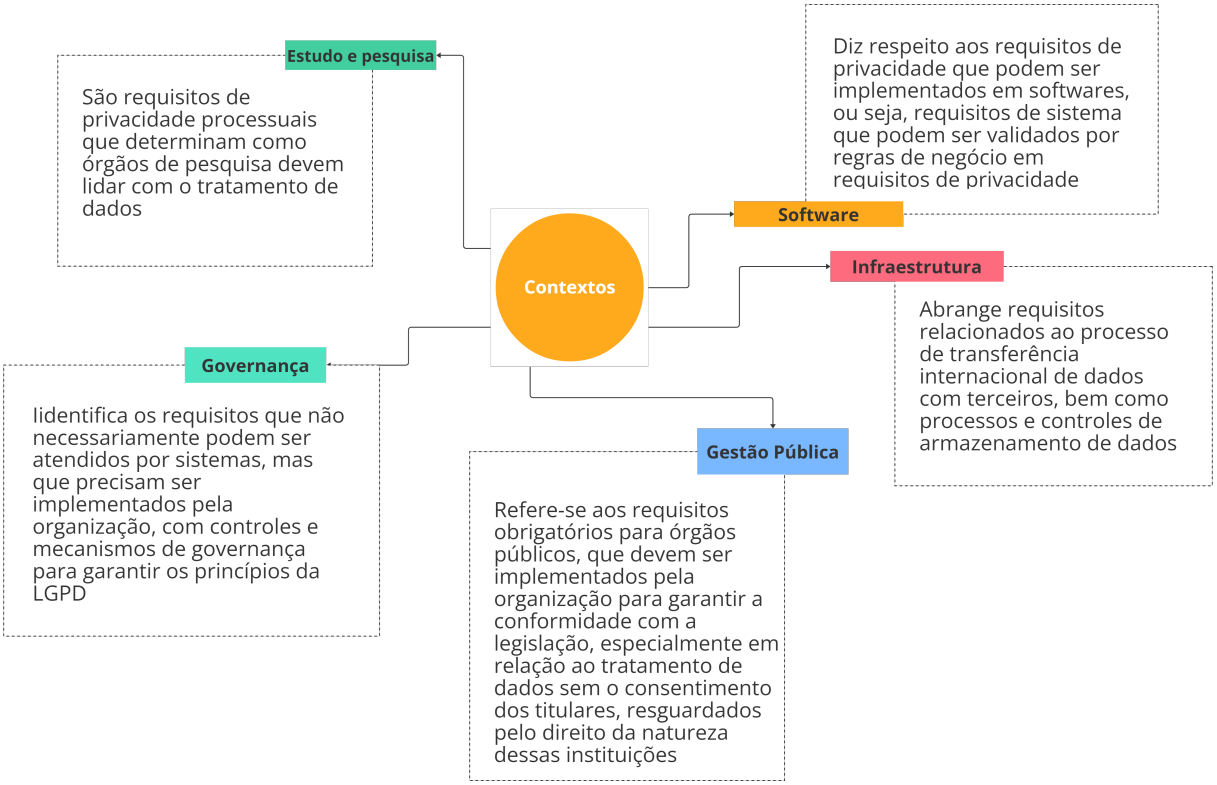

Figura 6 – Contextos. Fonte: Adaptado de Ferrão (2022)

2.4.4 Requisitos identificados

A taxonomia proposta por Ferrão (2022), identificou 129 requisitos, conforme a Figura 7 que mostra a classificação dos requisitos. A tabela presente no Anexo A apresenta todos os requisitos e a sua descrição.

A Figura 7, apresenta de forma estruturada a divisão da taxonomia proposta por (FERRÃO, 2022).

Figura 7 – Taxonomia. Fonte: Adaptado de Ferrão (2022)

De acordo com a Figura 7, a taxonomia se divide em dez categorias e cinco contextos. Na categoria de Finalidade, há 25 requisitos distribuídos em três contextos. Na categoria adequação, foram identificados cinco requisitos em 2 contextos distintos. Na categoria necessidade, há 18 requisitos em cinco diferentes contextos. Já na categoria de livre acesso, há apenas dois requisitos em um contexto. A categoria qualidade dos dados é dividida em três contextos, totalizando sete requisitos. A categoria transparência é composta por 13 requisitos distribuídos em dois contextos. Já a categoria segurança abrange 16 requisitos em quatro contextos diferentes. A categoria prevenção apresenta cinco requisitos divididos em três contextos. Por fim, a categoria responsabilidade e prestação de contas é composta por 36 requisitos distribuídos em três contextos diferentes. Todos esses requisitos foram avaliados por meio de um estudo de caso, e os resultados estão presentes nas Seções 4, 5 e 6.

3 Metodologia

Neste capítulo é apresentada a metodologia de pesquisa empregada neste trabalho. A metodologia de pesquisa é um aspecto fundamental em um Trabalho de Conclusão de Curso (TCC), pois define o processo que será utilizado para se chegar aos resultados. Segundo Gerhardt e Silveira (2009), ela pode ser definida como a maneira de conduzir a investigação, a fim de responder às questões de pesquisa ou hipóteses estabelecidas. De modo similar, Gil (2017) define metodologia como um conjunto de procedimentos, técnicas e instrumentos que serão utilizados para coletar e analisar os dados. As seções seguintes, descrevem a metodologia empregada neste trabalho. A Seção 3.1 é utilizada para descrever as fases principais na elaboração deste trabalho. Essa seção permite entender melhor como a metodologia será executada e como os dados serão coletados e analisados. A Seção 3.2 apresenta a abordagem metodológica escolhida, que consiste em analisar profundamente um caso específico. Já a Seção 3.3 é utilizada para justificar a escolha dos aplicativos de saúde avaliados e para descrever o objeto de estudo da pesquisa. Neste caso, o objetivo é avaliar o nível de conformidade dos aplicativos em relação aos requisitos de privacidade propostos por Ferrão (2022), contribuindo para a proteção dos dados pessoais e para o desenvolvimento de uma cultura de privacidade e proteção de dados no contexto da área da saúde.

3.1 Fluxo de atividades

As atividades realizadas neste trabalho consistem em quatro fases interligadas. Inicialmente, foi realizada uma revisão bibliográfica sobre a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) e da ISO/IEC 29100 (ISO/IEC, 2011). Essa etapa, exemplificada na Figura 8 como a fase **revisão bibliográfica**, tem como objetivo compreender a legislação que rege a privacidade de dados pessoais no Brasil, em especial no contexto da área da saúde, bem como entender as diretrizes éticas para a coleta de dados envolvendo dados pessoais.

Com base na revisão bibliográfica realizada, foi avaliada uma taxonomia de requisitos de privacidade e, em seguida, foi feito um mapeamento de requisitos que contemplou os aspectos mais relevantes da LGPD. Essas atividades foram feitas na fase **planejamento**, conforme o fluxograma presente na Figura 8. Com a taxonomia de requisitos de privacidade em mãos, foi elaborado um questionário, que está presente no Apêndice A, e serve para auxiliar na verificação da conformidade de sistemas de saúde em relação à legislação e diretrizes éticas. Esse questionário contempla perguntas objetivas sobre o tratamento dos dados pessoais, considerando os requisitos identificados na taxonomia proposta por

Ferrão (2022). As atividades realizadas nessa fase estão detalhadas de maneira visual no fluxograma, presente na Figura 8, na fase **execução**.

Para aplicar o questionário, foram escolhidos sistemas de saúde que são os casos aqui estudados. Esses sistemas serão avaliados por meio do preenchimento do questionário elaborado na etapa anterior, a fim de verificar a conformidade com a LGPD (BRASIL, 2018).

Após a aplicação do questionário, conforme o fluxograma, será realizada a fase de **resultados**, que consiste na realização de uma análise dos resultados obtidos, buscando identificar os pontos fortes e fracos do sistema avaliado em relação à privacidade de dados pessoais. A partir dessa análise, serão propostas medidas para a melhoria da conformidade com a legislação e diretrizes éticas.

Por fim, será elaborada uma conclusão sobre o trabalho, destacando os resultados obtidos e as medidas propostas para a melhoria da conformidade com a legislação e diretrizes éticas. A Figura 8 exemplifica as fases e atividades aplicadas nesse trabalho.

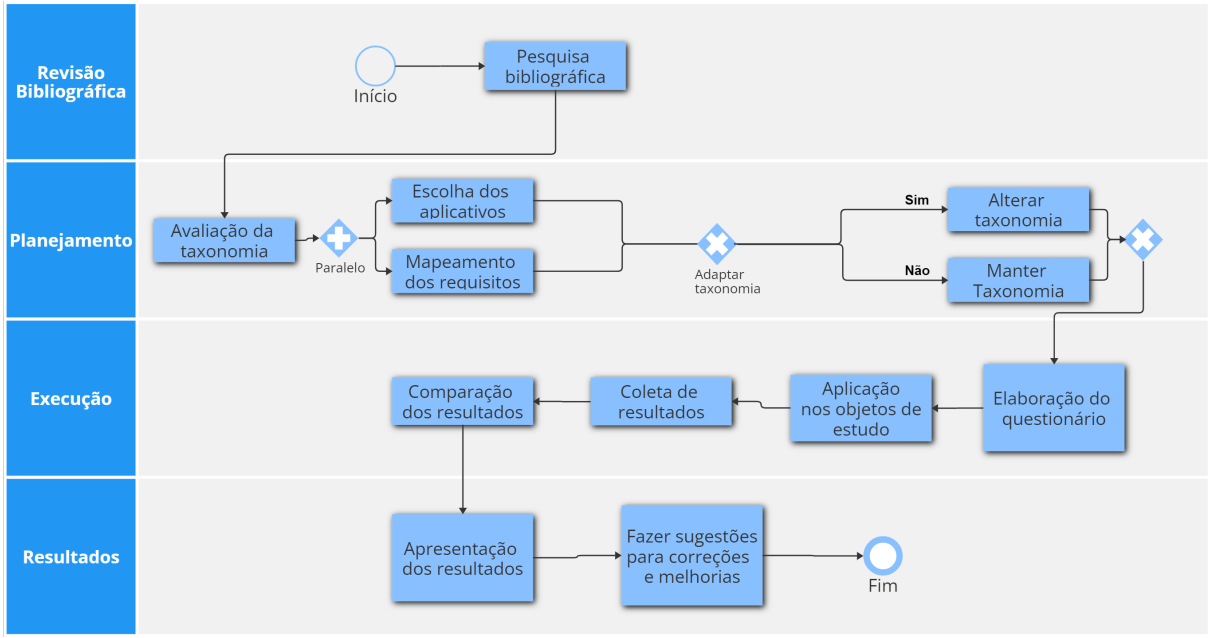

Figura 8 – Fluxograma. Fonte: Autor.

3.2 Estudo de caso

O Estudo de Caso é uma abordagem metodológica que consiste em analisar profundamente um caso específico. Já Gerhardt e Silveira (2009), de forma similar, afirmam que o estudo de caso é uma estratégia útil para investigar fenômenos complexos e pouco conhecidos. Dessa forma, é uma abordagem útil para o objeto de estudo apresentado na Seção 3.3.

Neste trabalho de conclusão de curso, a escolha da temática de saúde deu-se em virtude da importância dos dados de saúde no âmbito da segurança e da privacidade. Isso tornou-se especialmente relevante no contexto de pandemia, em que muitos usuários utilizaram aplicativos para monitorar e gerenciar seus dados de saúde (FIOCRUZ, 2023). Além disso, dados recentes apontam que o Brasil é o sexto país com mais vazamentos de dados no mundo, o que reforça a necessidade de avaliar a privacidade dos dados pessoais dos usuários de aplicativos de saúde (DIGITAL, 2022).

Nesse contexto, a taxonomia proposta por Ferrão (2022) foi desenvolvida com base na LGPD (BRASIL, 2018) e na ISO/IEC 29100 (ISO/IEC, 2011) e descreve 129 requisitos de privacidade, distribuídos em cinco contextos e de acordo com dez princípios. Dessa forma, o objeto de estudo desta pesquisa será a taxonomia citada anteriormente. Essa taxonomia está detalhada na Seção 2.4.1. Os casos estudados serão aplicações da área de saúde, conforme detalhado na Seção 3.3.

O objetivo, portanto, é avaliar o nível de conformidade dos aplicativos de saúde em relação aos requisitos de privacidade propostos por Ferrão (2022). Dessa forma, será possível avaliar se os aplicativos oferecem proteção de dados pessoais de seus usuários, em especial, os sensíveis. Ressalta-se que a avaliação de aplicativos de saúde quanto à conformidade com requisitos de privacidade é uma questão extremamente relevante e atual, especialmente no contexto de crescente digitalização dos serviços de saúde e dos dados dos pacientes. Ademais, a aplicação da taxonomia em diferentes aplicativos de saúde permitirá identificar pontos de melhoria e aprimoramento das políticas de privacidade desses aplicativos, contribuindo para a proteção dos dados pessoais e para o desenvolvimento de uma cultura de privacidade e proteção de dados no contexto da área da saúde.

Para a execução deste estudo, serão utilizadas as fases e atividades detalhadas na Seção 3.1. Além disso, a aplicação da taxonomia consiste em três fases principais na elaboração e aplicação do estudo de caso, sendo elas: Análise da taxonomia proposta, coleta de dados e análise dos resultados.

Na fase de **análise da taxonomia proposta**, foi realizada uma analise para determinar se a taxonomia atende aos requisitos demandados pela área de saúde, em especial aqueles relacionados à privacidade de dados sensíveis. Esta análise concluiu que a taxonomia proposta atende aos requisitos que são foco deste estudo, como, por exemplo, os requisitos RQ020, RQ031, RQ032, RQ035, RQ036, RQ037, RQ038 e RQ101. Além disso, foram analisados outros aspectos de privacidade que estão presentes na taxonomia proposta, como, por exemplo, em relação à transferência internacional de dados, o acesso fácil ao consentimento e outros aspectos que estão todos presentes no Anexo A.

Na fase de **coleta de dados**, foi criado um questionário, que está presente no Apêndice A. Esse questionário visa auxiliar a coleta de dados. Nesse questionário estão listados todos os 129 requisitos com opções para avaliar se o requisito é implementado

na aplicação avaliada. Há quatro tipos de respostas possíveis, de forma similar como propôs Ferrão (2022), ou seja: (1) Implementado - quando a aplicação cumpre o requisito avaliado; (2) Não implementado - quando a aplicação não cumpre o requisito avaliado; (3) Implementado de forma parcial - quando a aplicação cumpre o requisito de maneira parcial; e (4) Inválido - quando não é possível avaliar o requisito para a aplicação.

Na fase de **análise dos resultados**, avaliou-se a implementação dos requisitos por meio da análise dos termos de uso do usuário da aplicação, de documentos oficiais e de páginas públicas da empresa responsável pela aplicação. Vale ressaltar que a análise da implementação dos requisitos é feita considerando o ponto de vista do usuário, pois não houve a possibilidade da análise de código, estrutural e arquitetural da aplicação. Essa limitação também foi encontrada por Ferrão (2022), autora da taxonomia em questão.

3.3 Aplicativos do Estudo de Caso

Foram selecionadas três aplicações para serem utilizadas na aplicação do estudo de caso desta pesquisa de TCC. A escolha das aplicações foi embasada em um levantamento de informações preliminar, que teve como objetivo verificar a possibilidade de aplicar a taxonomia de acordo com o contexto da aplicação. Para isso, foi analisada a existência de documentos oficiais, termos de uso e políticas de privacidade das aplicações selecionadas. As aplicações que apresentaram maior compatibilidade com os objetivos citados anteriormente e maior potencial para serem estudadas são: ”SaúdeMoB“, ”Conecte SUS“ e ”Sabin“.

O **SaúdeMoB** é uma solução do grupo Pardini, uma empresa com mais de 60 anos de atuação que conta com cerca de 6 mil laboratórios parceiros. Essa aplicação é como um serviço de delivery, que coleta exames e aplica vacinas onde o usuário estiver. Além disso, o agendamento é todo realizado pelo WhatsApp, aplicativo amplamente utilizado para troca de mensagens. Com a utilização do SaúdeMoB, o usuário não precisa pegar fila e recebe atenção exclusiva por parte do prestador. (MOB, 2022).

O **Conecte SUS** é o aplicativo oficial do Ministério da Saúde, denominado Conecte SUS Cidadão. Ele é responsável por fornecer o acesso digital aos serviços do Sistema Único de Saúde (SUS). Por meio dele, é possível acompanhar o histórico clínico do cidadão de forma ágil e simples. O aplicativo exibe informações gerais sobre o usuário, incluindo a Carteira Nacional de Vacinação, Certificado Nacional de Covid-19, Cartão Nacional de Saúde, resultados de exames laboratoriais de Covid-19, medicamentos distribuídos pelo programa ”Farmácia Popular“, além dos registros de doações de sangue e acompanhamento da posição na lista de transplantes (Ministério da Saúde, 2023).

Sabin Medicina Diagnóstica: Há 39 anos atuando no Brasil, o Grupo Sabin é um dos maiores players no setor de medicina diagnóstica do país. Fundado em Brasília,

pelas bioquímicas Janete Vaz e Sandra Soares Costa, o grupo conta com mais de 7.000 colaboradores, que atendem mais de 7 milhões de clientes ao ano, com um amplo portfólio de serviços de análises clínicas, diagnósticos por imagem, vacinação e check-up executivo em 350 unidades de atendimento no Distrito Federal e nos estados de Amazonas, Bahia, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Piauí, Rio de Janeiro, Roraima, São Paulo, Tocantins e Santa Catarina. O Grupo também investe em empresas com atuação na área de atenção primária à saúde e gestão de saúde (Sabin, 2022).

4 Conecte SUS

A coleta de dados para o presente estudo foi realizada por meio de um questionário que está presente no Apêndice A.

No Conecte SUS realizou-se a avaliação da própria aplicação, bem como dos termos de uso, política de privacidade e nota informativa, conforme os Anexos C, D e E respectivamente, incluindo o mapeamento com notas para cada documento. Adicionalmente, também foi utilizada a aplicação presente no Anexo B.

No total foram avaliados 129 requisitos de privacidade, conforme a taxonomia proposta por Ferrão (2022). No entanto, como pode ser visto na Tabela 7, 70 desses requisitos foram classificados como inválidos. Em outras palavras, eles são incompatíveis com o contexto da aplicação ou não foi possível avaliá-los devido a limitações técnicas ou de acesso às informações necessárias.

Ainda na Tabela 7 pode ser visto que 36 requisitos foram avaliados como implementados, indicando que a aplicação possui medidas adequadas para garantir a privacidade dos dados dos usuários. Outros 14 requisitos foram considerados como implementados de forma parcial, sugerindo que ainda há margem para melhoria em algumas áreas específicas ou que precisam de mais detalhes para serem considerados totalmente implementados.

Por fim, nove requisitos foram considerados como não implementados, indicando áreas em que a aplicação precisa aprimorar suas medidas de privacidade.

Tabela 7 – Resultados da aplicação Conecte SUS.

Resultados da aplicação: Conecte SUS		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	129	100%
Requisitos implementados	36	28.0%
Requisitos implementados de forma parcial	14	11.0%
Requisitos inválidos	70	54.0%
Requisitos não implementados	9	7.0%

Fonte: Autor.

A Tabela 8 mostra os dados descartando-se os requisitos que foram considerados como inválidos. Observe que no Conecte SUS, 61.1% dos requisitos foram considerados como totalmente implementados. 23.7% foram considerados como implementados de forma parcial e 15.2% foram considerados como não implementados.

Tabela 8 – Resultados da aplicação Conecte SUS desconsiderando os dados inválidos

Resultados da aplicação Conecte SUS desconsiderando os dados inválidos		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	59	100%
Requisitos implementados	36	61.1%
Requisitos implementados de forma parcial	14	23.7%
Requisitos não implementados	9	15.2%

Fonte: Autor.

Nas seções seguintes,os resultados apresentados na Tabela 8 são detalhados, considerando as categorias definidas na taxonomia de Ferrão (2022). O questionário utilizado pode ser encontrado no Apêndice B.

4.1 Finalidade

Nessa categoria há três contextos: Software, Estudo e Pesquisa, e Gestão Pública. A Tabela 9 apresenta de forma resumida os resultados obtidos nessa categoria.

Dos 25 requisitos analisados, dez foram considerados inválidos por não ser possível avaliá-los na aplicação em questão. Entretanto, sete requisitos foram considerados como tolamente implementados e três foram implementados de forma parcial.

Tabela 9 – Resultados da categoria: Finalidade - Conecte SUS

Resultados da categoria Finalidade - Conecte SUS		
Requisito	**Situação**	**Justificativa**
RQ001	Implementado	De acordo com o consentimento presente no Anexo B, é possível recolher o consentimento do titular através do aplicativo.
RQ002	Implementado	Segundo o consentimento presente no Anexo B, a aplicação apresenta as finalidades ao mínimo exigido. Além disso, o usuário pode escolher entre consentimento geral e consentimento específico

RQ004	Implementado de forma parcial	Na Seção E.4 da nota informativa, há menção sobre o compartilhamento de dados com terceiros, porém não há forma de comprovação.
RQ006	Implementado	Sem consentimento presente no Anexo B, é possível revogar o consentimento a qualquer momento
RQ008	Implementado	De acordo com as Seções D.5 e D.11 da política de privacidade, ela garante o direito à limitação de tratamento dos dados, apresentando os dados possíveis de tratamento e o direito de não ser subordinado a decisões automatizadas, incluindo as decisões destinadas ao perfil de consumo e de crédito.
RQ009	Implementado de forma parcial	Há citação apenas do processo judicial que está presente na Seção E.6 da nota informativa.
RQ016	Implementado de forma parcial	Foi considerado como implementado de forma parcial, pois na Seção D.11 da política de privacidade há apenas citação de que o Conecte SUS se compromete a fornecer maior proteção aos dados de crianças e adolescentes, seguindo as legislações pertinentes, como o Estatuto da Criança e do Adolescente.
RQ021	Implementado	De acordo com a política de privacidade presente na Seção D.5, que garante o direito à limitação de tratamento dos dados, são apresentados os dados possíveis e o direito de não ser submetido a decisões automatizadas, incluindo aquelas destinadas ao perfil de consumo e de crédito.
RQ022	Implementado	Na nota informativa na Seção E.5, é apresentado o objetivo da RNDS, que é facilitar o acesso dos profissionais de saúde. Além disso, informa que as informações são precisas e atualizadas
RQ115	Implementado	Na Seção D.5 da política de privacidade, contém a relação de dados tratados.

Fonte: Autor.

Os requisitos RQ001, RQ002, RQ006, RQ008, RQ021, RQ022, e RQ115 estão implementados. Destes, destaca-se que o RQ002 permite ao usuário escolher entre consentimento geral e consentimento específico, e o RQ008 e RQ021 garantem o direito à limitação de tratamento dos dados. Também se nota que o RQ022 menciona que o objetivo da RNDS é facilitar o acesso dos profissionais de saúde.

Por outro lado, os requisitos RQ004, RQ009 e RQ016 estão implementados de forma parcial. No caso do RQ004, a nota informativa menciona o compartilhamento de dados com terceiros, mas não apresenta uma forma de comprovação. O RQ009 cita apenas o processo judicial, e o RQ016, apesar de se comprometer a fornecer maior proteção aos dados de crianças e adolescentes, a medida foi considerada apenas parcial.

4.2 Adequação

Nessa categoria, há cinco requisitos em dois contextos: Software e Estudo e Pesquisa, sendo que três dos cinco requisitos foram considerados inválidos por não ser possível avaliá-los para a aplicação em questão. A Tabela 10 mostra de forma resumida, os resultados obtidos. Nessa categoria, apenas dois requisitos foram considerados como implementados.

Tabela 10 – Resultados da categoria: Adequação - Conecte SUS

Resultados da categoria: Adequação - Conecte SUS		
Requisito	Situação	Justificativa
RQ027	Implementado	De acordo com a escolha do consentimento presente no Anexo B, é possível revogar o consentimento a qualquer momento.
RQ028	Implementado	De acordo com a escolha do consentimento presente no Anexo B, é possível revogar o consentimento a qualquer momento.

Fonte: Autor.

A Tabela 10 mostra os resultados da categoria “Adequação” relacionados a dois requisitos específicos identificados como RQ027 e RQ028. Ambos os requisitos foram implementados com sucesso, conforme indicado na coluna “Situação”. A justificativa para essa conclusão é baseada na escolha do consentimento presente no Anexo B, que permite a revogação do consentimento a qualquer momento. Esses resultados indicam que o sistema em análise atende às exigências de adequação em relação aos requisitos mencionados.

4.3 Necessidade

Para a categoria necessidade há 18 requisitos em cinco contextos: Software, Estudo e Pesquisa, Gestão Pública e Infra. A Tabela 11 mostra os resultados de forma resumida. Nessa categoria, dos 18 requisitos, seis foram considerados como implementados e dois foram considerados implementados de forma parcial.

Tabela 11 – Resultados da categoria: Necessidade - Conecte SUS

Resultados da categoria: Necessidad - Conecte SUS		
Requisito	Situação	Justificativa
RQ031	Implementado	De acordo com o consentimento presente no Anexo B, é possível permitir o tratamento de dados quando o titular autoriza de forma específica e destacada.
RQ037	Implementado	De acordo com a Seção E.6 da nota informativa, em casos excepcionais, o profissional de saúde responsável pelo seu atendimento poderá acessar seus dados de saúde nas seguintes situações: (i) a partir de autorização expressa de seu representante legal ou acompanhante; ou (ii) quando, a partir do julgamento técnico do Profissional de Saúde responsável, você correr risco de lesão grave ou risco de morte.
RQ039	Implementado	Na Seção D.8 da política de privacidade é apresentado o direito à necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
RQ041	Implementado	Na Seção E.1 da nota informativa, é apresentado que o Conecte SUS utilizará a RNDS para cumprir as obrigações com a população brasileira, pois através de dados de saúde eles podem avaliar, formular e executar políticas públicas mais eficazes, estabelecendo condições para promoção, proteção, tratamento e recuperação da sua saúde e da população.

RQ044	Implementado	De acordo com a Seção D.3 da política de privacidade é apresentado um parágrafo sobre o uso compartilhado de dados, comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos ou entes privados.
RQ048	Implementado	De acordo com a Seção D.3 da política de privacidade é apresentado um parágrafo sobre o uso compartilhado de dados, comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos ou entes privados.
RQ035	Implementado de forma parcial	Na Seção D.5 da política de privacidade, há menção ao direito de não ser submetido a decisões automatizadas, que incluem as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito. Isso atende parcialmente ao RQ035, pois não há citação em relação a processos administrativos e arbitrais.
RQ042	Implementado de forma parcial	Na Seção D.3 da política de privacidade, há apenas citação do uso compartilhado de dados. Porém, não há evidências suficientes para considerar o requisito totalmente implementado.

Fonte: Autor.

Os resultados apresentados na Tabela 11 mostram a situação dos requisitos na categoria “Necessidade” do sistema Conecte SUS. De acordo com a tabela, os requisitos RQ031, RQ037, RQ039, RQ041, RQ044 e RQ048 estão implementados. Para cada requi-

sito implementado, são fornecidas justificativas e referências aos documentos relevantes que respaldam a implementação. No entanto, os requisitos RQ035 e RQ042 são considerados implementados de forma parcial. Embora o RQ035 seja abordado parcialmente na política de privacidade, uma questão específica relacionada a processos administrativos e arbitrais não é mencionada. No caso do RQ042, embora haja citação do uso compartilhado de dados na política de privacidade, não há informações suficientes para afirmar com certeza que o requisito foi totalmente implementado. Em geral, os resultados destacam a implementação adequada dos requisitos na categoria "Necessidade", mas ressaltam a necessidade de aprimoramentos para atender completamente a todos os requisitos.

4.4 Livre Acesso

A categoria livre acesso é composta por dois requisitos que pertencem ao contexto de Software. A Tabela 12 mostra os resultados de forma resumida.

Tabela 12 – Resultados da categoria livre acesso - Conecte SUS

Resultados da categoria: Livre Acesso - Conecte SUS		
Requisito	Situação	Justificativa
RQ049	Implementado de forma parcial	Esse requisito foi considerado implementado de forma parcial, pois é possível acessar e revisar as informações do titular da conta. No entanto, não é possível obter cópia eletrônica dos dados.
RQ050	Implementado de forma parcial	Esse requisito foi considerado como implementado de forma parcial, pois de acordo com a Seção D.5 da política de privacidade, é mencionado o direito de não ser submetido a decisões automatizadas. Porém, não é possível comprovar a aplicação desse direito.

Fonte: Autor.

Os resultados apresentados na Tabela 12 mostram a situação dos requisitos na categoria "Livre Acesso" do sistema Conecte SUS. De acordo com a tabela, os requisitos RQ049 e RQ050 estão implementados de forma parcial. Para o requisito RQ049, é possível acessar e revisar as informações do titular da conta, mas não é viável obter uma cópia eletrônica dos dados, o que indica uma implementação parcial desse requisito. No caso do requisito RQ050, a política de privacidade (Anexo D) menciona o direito de não ser submetido a decisões automatizadas, conforme a Seção D.5. No entanto, não há evidências suficientes para comprovar a aplicação desse direito, resultando em uma implementação parcial.

4.5 Qualidade dos dados

A categoria qualidade dos dados é dividida em três contextos: Governança, Software e Gestão Pública. Nessa categoria, foram avaliados sete requisitos, dos quais apenas três foram considerados como totalmente implementados e o restante considerado como inválido. A Tabela 13 mostra os resultados obtidos nesta categoria.

Tabela 13 – Resultados da categoria: Qualidade dos dados. - Conecte SUS

Resultados da categoria: Qualidade de dados - Conecte SUS		
Requisito	Situação	Justificativa
RQ051	Implementado	Na Seção C.6 do termo de uso, é mencionado que a responsabilidade de manter os dados atualizados é do usuário e que alguns dados, como nome, data de nascimento, sexo, e-mail e inclusão/exclusão de nome social, são coletados automaticamente do sistema Cadastro Nacional de Usuários do SUS - CadSUS.
RQ052	Implementado	Na política de privacidade, na Seção D.6, cita-se que para atualização e correção, o usuário deve solicitar perante a Receita Federal e/ou solicitar junto a qualquer estabelecimento de saúde.
RQ055	Implementado	Na Seção D.12 da política de privacidade, é apresentado como cada dado é coletado.

Fonte: Autor.

Conforme a Tabela 13, os requisitos RQ051, RQ052 e RQ055 estão implementados. Para o requisito RQ051, é mencionado na Seção D.6 do termo de uso (Anexo C) que a responsabilidade de manter os dados atualizados é do usuário, e alguns dados são coletados automaticamente do sistema Cadastro Nacional de Usuários do SUS - CadSUS. Isso demonstra que o requisito foi implementado adequadamente. No caso do requisito RQ052, a política de privacidade (Anexo D), na Seção D.6, indica que o usuário deve solicitar a atualização e correção dos dados perante a Receita Federal e/ou qualquer estabelecimento de saúde, o que confirma a implementação desse requisito. Por fim, o requisito RQ055 é considerado implementado, pois a política de privacidade, na Seção D.12, apresenta como cada dado é coletado, demonstrando atenção à transparência nesse aspecto.

Em suma, os resultados mostram que o Conecte SUS atende aos requisitos relacionados à qualidade dos dados, fornecendo mecanismos para atualização, correção e transparência na coleta dessas informações.

4.6 Transparência

A categoria transparência é composta por 13 requisitos que estão dentro dos contextos: Software e Governança. Dos 13 requisitos, sete foram considerados como imple-

mentados, um como implementados de modo parcial e o restante considerados como não implementados. A Tabela 14 mostra os resultados obtidos nessa categoria.

Tabela 14 – Resultados da categoria: Transparência - Conecte SUS.

Resultados da categoria: Transparência - Conecte SUS.		
Requisito	Situação	Justificativa
RQ061	Implementado	Esse requisito foi considerado como implementado, pois no Anexo B, o usuário tem a opção de revogar o consentimento a qualquer momento.
RQ063	Implementado	Na nota informativa, de acordo com a Seção E.9, é apresentado ao leitor um canal de atendimento ao usuário.
RQ065	Implementado	Na Seção C.5 do termo de uso, são apresentados os direitos do usuário e a finalidade do tratamento nos termos de uso.
RQ066	Implementado	Esse requisito foi considerado como implementado, pois toda a documentação e a aplicação apresentam linguagem de fácil entendimento e explicativa para o usuário.
RQ067	Implementado de forma parcial	Na Seção D.9 da política de privacidade, são apresentadas informações claras e acessíveis sobre as políticas do controlador; porém, não são apresentadas informações sobre procedimentos com relação ao processamento dos dados.
RQ068	Implementado	Na Seção D.13 da política de privacidade, há uma lista com os dados que são coletados, contendo o motivo e como são coletados.
RQ069	Implementado	Na Seção D.14 da política de privacidade, é apresentada a forma de tratamento dos dados pessoais.
RQ070	Implementado	Na Seção D.9 da política de privacidade, cita-se que as secretarias municipais e estaduais de saúde exercem o papel de controladores de dados.

Fonte: Autor.

Os resultados apresentados na Tabela 14 mostram a situação dos requisitos na categoria “Transparência” do sistema Conecte SUS. Note que os requisitos RQ061, RQ063, RQ065, RQ066, RQ068, RQ069 e RQ070 estão implementados. Para o requisito RQ061, é mencionado no Anexo correspondente que o usuário tem a opção de revogar o consentimento a qualquer momento, evidenciando a implementação desse requisito. No caso do requisito RQ063, é apresentado na nota informativa (Anexo E), conforme a Seção E.9 da

Nota Informativa (Anexo E), cita o canal de atendimento ao usuário, atendendo à necessidade de transparência e comunicação. O requisito RQ065 é considerado implementado, pois a Seção C.5 (Anexo C) do Termos de Uso apresenta os direitos do usuário e a finalidade do tratamento de acordo com os termos estabelecidos. O requisito RQ066 também é implementado, já que toda a documentação e a aplicação utilizam uma linguagem de fácil entendimento e explicativa para o usuário. No caso do requisito RQ067, a implementação é parcial, pois embora a política de privacidade, na Seção D.9, forneça informações claras e acessíveis sobre as políticas do controlador, não são apresentadas informações sobre procedimentos relacionados ao processamento dos dados. Já os requisitos RQ068, RQ069 e RQ070 são considerados implementados, pois a política de privacidade, nas Seções D.13, D.14 e D.9 apresentam informações sobre os dados coletados, o tratamento dos dados pessoais e o papel das secretarias municipais e estaduais de saúde como controladores de dados.

Em suma, os resultados mostram que o Conecte SUS atende aos requisitos relacionados à transparência, fornecendo informações claras e acessíveis aos usuários, embora algumas melhorias sejam necessárias para garantir a divulgação de informações específicas sobre procedimentos de processamento de dados.

4.7 Segurança

A categoria segurança engloba 16 requisitos que são divididos em contextos como Software, Estudos e Pesquisa, Governança e Infraestrutura. 12 dos 16 requisitos foram considerados inválidos por não ser possível avaliá-los, dois foram considerados como implementados de forma parcial e outros dois requisitos foram considerados como totalmente implementados. A Tabela 15 mostra os resultados obtidos.

Tabela 15 – Resultados da categoria: Segurança - Conecte SUS

Resultados da categoria: Segurança - Conecte SUS		
Requisito	Situação	Justificativa
RQ072	Implementado	Esse requisito foi considerado como implementado, pois no Anexo B, o usuário tem a opção de limitar o tratamento e de acordo com a Seção D.5 da política de privacidade é citado o direito à limitação.

RQ081	Implementado	Na Seção E.1 da nota informativa, é apresentada a possibilidade de o usuário não compartilhar seus dados. Com isso, os dados ficarão restritos aos sistemas do Ministério da Saúde e o usuário não terá prejuízo no atendimento.
RQ078	Implementado de forma parcial	De acordo com a Seção D.16 da política de privacidade, é apresentado como os dados são protegidos. Porém, não há forma de comprovação.
RQ084	Implementado de forma parcial	Na Seção E.6 da nota informativa, é citado que os dados de saúde serão coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança proporcionais a sua sensibilidade, o que implica na criação de ambientes físicos e lógicos aderentes ao estado da técnica e às melhores práticas em gestão do sigilo e segurança da informação, inclusive aqueles específicos à área de saúde.

Fonte: Autor.

Conforme a Tabela 15, os requisitos RQ072 e RQ081 estão implementados. Para o requisito RQ072, é mencionado na Seção D.5 da política de privacidade (Anexo D) correspondente que o usuário tem a opção de limitar o tratamento dos seus dados, e a seção referente da política de privacidade também cita o direito à limitação. Isso confirma a implementação adequada desse requisito. No caso do requisito RQ081, na Seção K.1 da nota informativa (Anexo E) é apresentada a possibilidade de o usuário não compartilhar seus dados, garantindo que esses dados fiquem restritos aos sistemas do Ministério da Saúde sem prejuízo ao atendimento. Portanto, o requisito também é considerado implementado. Os requisitos RQ078 e RQ084 são considerados implementados de forma parcial. No caso do requisito RQ078, a Seção D.16 da politica de privacidade (Anexo D) apresenta informações sobre como os dados são protegidos, mas não há evidências suficientes para comprovar essa proteção. No requisito RQ084 é citado que os dados de saúde são coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança. Embora essa citação implique a criação de ambientes físicos e lógicos aderentes às melhores práticas de segurança da informação, não há informações específicas ou evidências de implementação.

Em resumo, os resultados mostram que o Conecte SUS aborda a segurança dos dados e oferece opções de limitação e não compartilhamento, mas são necessárias melhorias para garantir a comprovação da proteção dos dados e fornecer informações mais detalhadas

sobre as medidas de segurança implementadas.

4.8 Prevenção

A categoria prevenção apresenta cinco requisitos que estão divididos em três contextos: Software, estudo e pesquisa e governança. Dos cinco requisitos, três foram considerados como inválidos e apenas um foi considerado como implementado de forma parcial. A Tabela 16 mostra de forma resumida os resultados obtidos.

Tabela 16 – Resultados da categoria: Prevenção - Conecte SUS

Resultados da categoria: Prevenção - Conecte SUS.		
Requisito	Situação	Justificativa
RQ087	Implementado de forma parcial	Na seção C.6 do termo de uso, há citação de que é responsabilidade do usuário e, em caso de problemas com a veracidade e consistência dos dados, pode implicar na impossibilidade de utilizar o serviço.

Fonte: Autor.

Conforme a tabela 16, o requisito RQ087 está implementado de forma parcial. Na Seção C.6 do termo de uso (Anexo E) é mencionado que é responsabilidade do usuário garantir a veracidade e consistência dos dados fornecidos. Além disso, é destacado que problemas com a veracidade e consistência dos dados podem implicar na impossibilidade de utilizar o serviço. Isso indica uma abordagem de prevenção ao incentivar os usuários a fornecerem informações corretas e completas. No entanto, é importante observar que a implementação é considerada parcial, pois não são fornecidos detalhes sobre como essa prevenção é efetivamente realizada ou quais medidas são tomadas para garantir a veracidade e consistência dos dados.

Em resumo, embora o Conecte SUS reconheça a importância da prevenção ao mencionar a responsabilidade do usuário, é necessário fornecer mais informações e evidências sobre as medidas implementadas para garantir a prevenção efetiva de problemas relacionados à veracidade e consistência dos dados.

4.9 Não discriminação

A categoria não discriminação contém apenas dois requisitos no contexto de software. Dos requisitos dessa categoria, apenas um foi considerado como implementado de forma parcial. A Tabela 17 apresenta a análise desse requisito.

Tabela 17 – Resultados da categoria: Não descriminação - Conecte SUS.

Resultados da categoria: Não discriminação - Conecte SUS.		
Requisito	Situação	Justificativa
RQ092	Implementado de forma parcial	Na seção C.7 do termo de uso, há citação de que a administração pública se compromete a cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados no serviço, bem como a garantir todos os direitos e garantias legais dos titulares dos dados. Em virtude disso, o uso correto dos dados pessoais está incluído a não utilização dos dados afim de prejudicar o titular.

Fonte: Autor.

4.10 Responsabilidade e prestação de contas

Essa categoria é composta por 36 requisitos de privacidade, que estão divididos em três contextos: Software, Governança e Infraestrutura. Dos 36 requisitos, nove foram considerados como implementados, três foram considerados como implementados de forma parcial e os outros 24 foram considerados inválidos por não ser possível avaliá-los. A Tabela 18 mostra os resultados obtidos.

Tabela 18 – Resultados da categoria: Responsabilização e prestação de contas - Conecte SUS.

Resultados da categoria: Responsabilização e prestação de contas - Conecte SUS.		
Requisito	Situação	Justificativa
RQ094	Implementado	Na Seção C.6 do termo de uso, há citação de que é responsabilidade do usuário e, em caso de problemas com a veracidade e consistência dos dados, pode implicar na impossibilidade de utilizar o serviço.

RQ101	Implementado	Na Seção D.13 da política de privacidade, há explicação para a utilização de dados sensíveis, como sexo, dados de saúde, dados relacionados com a COVID-19, entre outros.
RQ102	Implementado	Na Seção D.12 da política de privacidade, é apresentado como os dados são coletados.
RQ103	Implementado	Através da aplicação, conforme as imagens presentes no Anexo B, é possível corrigir e atualizar os dados do usuário.
RQ104	Implementado	Através da aplicação, conforme as imagens presentes no Anexo B, é possível limitar ou não conceder a permissão do tratamento de dados pessoais.
RQ106	Implementado de forma parcial	Através da aplicação, é possível selecionar a opção de parar de compartilhar os dados. Porém, não há explicações detalhadas.
RQ110	Implementado	Na Seção D.5 da política de privacidade, é apresentado o direito de retificação, que consiste no direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.
RQ111	Implementado	Na Seção D.5 da política de privacidade, é apresentado o direito de confirmação e acesso, que consiste no direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe dizem respeito são ou não objeto de tratamento, e, se for esse o caso, o direito de acessar os seus dados pessoais.
RQ112	Implementado de forma parcial	Na Seção D.5 da política de privacidade, é citado o direito de portabilidade dos dados, que garante ao usuário o direito de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. Porém, não há forma de comprovação da aplicação desse direito.

RQ115	Implementado	Na Seção D.11, é apresentado ao usuário uma lista com todos os dados que são tratados pelo Conecte SUS. Além disso, na Seção E.1, cita-se a possibilidade de não compartilhar os dados. Ao escolher esta opção, os dados de saúde compartilhados com os profissionais de assistência à saúde responsáveis pelos atendimentos, e que possuem acesso ao Conecte SUS Profissional, ficarão restritos aos sistemas do Ministério da Saúde. Esta possibilidade poderá ser revista a qualquer momento, ocasião em que o usuário será devidamente informado a respeito. Cabe salientar que o usuário não terá prejuízo no atendimento caso não queira compartilhar os seus dados de saúde.
RQ121	Implementado de forma parcial	Na Seção D.8, é citado que o Conecte SUS se compromete com o princípio da segurança, que consiste na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Além disso, na Seção D.16, é citado que, para a garantia da segurança, serão adotadas soluções que levem em consideração as técnicas adequadas, os custos de aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento, e os riscos para os direitos e liberdades do usuário. Porém, não é possível verificar a aplicação desses princípios e técnicas de segurança.
RQ129	Implementado	Na Seção D.10 da política de privacidade, é citado que o Conecte SUS compartilha dados com uma empresa terceirizada, desenvolvedora da aplicação. Sendo assim, é um operador de dados. Todos os controles administrativos e lógicos de segurança foram exigidos à empresa terceirizada na política de privacidade.

Fonte: Autor.

De acordo com a Tabela 18 os requisitos que foram considerados como totalmente implementados foram: RQ094, RQ101, RQ102, RQ103, RQ104, RQ110, RQ111 e RQ115. Para o requisito RQ094, a Seção C.6 do termo de uso (Anexo E) menciona a responsabilidade do usuário em garantir a veracidade e consistência dos dados, o que evidencia a

implementação. Já o RQ101 é considerado implementado, pois na Seção D.13 da política de privacidade, há explicações sobre a utilização de dados sensíveis, como dados de saúde e dados relacionados à COVID-19.

O requisito RQ102 também foi considerado implementado, visto que na Seção D.12 da política de privacidade (Anexo D), é apresentada a forma como os dados são coletados. Além disso, a aplicação do Conecte SUS permite a correção e atualização dos dados do usuário que atende ao RQ103 e a limitação ou não concessão de permissão para o tratamento de dados pessoais que atende ao RQ104, conforme imagens presentes no Anexo B.

Outros requisitos também foram considerados como totalmente implementados. O RQ110 foi pois a Seção D.5 da política de privacidade (Anexo D) apresenta o direito de retificação, permitindo que o usuário solicite a correção de dados incompletos, inexatos ou desatualizados. Da mesma forma, o RQ111 é considerado implementado, pois na Seção D.5 da política de privacidade (Anexo D) é apresentado o direito de confirmação e acesso, assegurando ao usuário a confirmação do tratamento de seus dados pessoais e o direito de acessá-los.

No entanto, alguns requisitos foram considerados como implementados de forma parcial. O RQ106 é um exemplo disso, já que a aplicação permite que o usuário pare de compartilhar seus dados, mas não fornece explicações detalhadas sobre essa funcionalidade. Outro requisito com implementação parcial é o RQ112, que trata do direito de portabilidade dos dados. Embora a política de privacidade (Anexo D) mencione esse direito na Seção D.5, não há comprovação da aplicação dessa possibilidade.

O RQ121 também é considerado implementado de forma parcial, uma vez que nas Seções D.8 e D.16 da política de privacidade (Anexo D), são citados os princípios e técnicas de segurança adotados, mas não há evidências que comprovem sua aplicação na prática.

Por fim, o RQ129 foi considerado implementado, visto que na Seção D.10 da política de privacidade (Anexo D), é mencionado que o Conecte SUS compartilha dados com uma empresa terceirizada, desenvolvedora da aplicação, e exige controles administrativos e lógicos de segurança dessa empresa.

Em resumo, os resultados apontam que o Conecte SUS cumpre boa parte dos requisitos relacionados à responsabilização e prestação de contas. A aplicação permite que o usuário corrija e atualize seus dados, bem como limite o compartilhamento de informações sensíveis. Além disso, são apresentados os direitos de retificação, confirmação, e acesso aos dados pessoais. No entanto, algumas melhorias são necessárias, como fornecer explicações detalhadas sobre certas funcionalidades, comprovar a aplicação de determinados direitos e demonstrar a efetiva implementação dos princípios e técnicas de segurança mencionados

na política de privacidade. Com essas melhorias, o Conecte SUS poderá garantir uma maior transparência e segurança no tratamento de dados dos usuários.

4.11 Melhorias sugeridas no Conecte SUS

No aplicativo Conecte SUS foram identificadas algumas lacunas em relação aos requisitos de privacidade e transparência. Primeiramente, é sugerido que sejam incluídas informações sobre a portabilidade dos dados pessoais, esclarecendo que essa portabilidade não inclui dados que já tenham sido anonimizados pelo controlador. Essa informação pode ser disponibilizada no aplicativo, na política de privacidade e na nota informativa, a fim de garantir que os usuários estejam cientes dessa limitação. Com isso o requisito RQ007 será considerado como totalmente implementado.

Outra sugestão é dispensar a exigência de consentimento para dados manifestamente públicos, desde que sejam resguardados os direitos do titular e os princípios de tratamento de dados. Nesses casos, os usuários devem ser informados de que o consentimento não é necessário, quando seus dados são considerados manifestamente públicos. Com isso o requisito RQ012 será considerado como totalmente implementado.

Além disso, é recomendado obter consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores, ressalvadas as hipóteses de dispensa do consentimento legais. Essa medida visa garantir a transparência e o controle dos usuários sobre o compartilhamento de seus dados pessoais. Com isso o requisito RQ013 será considerado como totalmente implementado.

No que diz respeito à conservação dos dados pessoais para estudos por órgãos de pesquisa, sugere-se que seja informado aos usuários sobre essa possibilidade, garantindo sempre que possível a anonimização dos dados pessoais. Essa informação pode ser incluída no aplicativo, na política de privacidade e na nota informativa. Com isso o RQ016 será considerado como totalmente implementado.

Por fim, é importante apresentar as informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível. Considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos usuários, recursos audiovisuais podem ser utilizados quando adequado, a fim de proporcionar as informações necessárias aos pais ou responsáveis legais e de forma compreensível para as crianças. Com isso o RQ058 será considerado como totalmente implementado.

5 Sabin

A coleta de dados para o presente estudo foi realizada por meio de um questionário que está presente no Apêndice A. No aplicativo Sabin, realizou-se a avaliação da própria aplicação e da política de privacidade descrita no Apêndice F.

No total foram examinados 129 requisitos de privacidade, conforme a classificação proposta por Ferrão (2022). No entanto, como demonstrado na Tabela 19, 68 desses requisitos foram considerados inválidos. Em outras palavras, eles não se adequam ao contexto da aplicação ou não foi possível avaliá-los devido a limitações técnicas ou à falta de acesso às informações necessárias.

Ainda na Tabela 19, constatou-se que 28 requisitos foram considerados implementados, o que indica que a aplicação adotou medidas adequadas para garantir a privacidade dos dados dos usuários. Outros 31 requisitos foram classificados como implementados parcialmente, sugerindo que há espaço para melhorias em áreas específicas ou que necessitam de mais detalhes para serem considerados totalmente implementados. Por fim, dois requisitos foram identificados como não implementados, apontando as áreas em que a aplicação precisa aprimorar suas medidas de privacidade.

Tabela 19 – Resultados da aplicação Sabin.

Resultados da aplicação: Sabin		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	129	100%
Requisitos implementados	28	21.70%
Requisitos implementados de forma parcial	31	24.03%
Requisitos inválidos	68	52.71%
Requisitos não implementados	2	1.56%

Fonte: Autor.

Descartando-se os dados que foram considerados como inválidos, é possível perceber que o Sabin, 45.90% dos requisitos foram considerados como totalmente implementados 50.90% foram considerados como implementados de forma parcial, e 3.20% foram considerados como não implementados. A Tabela 20 mostra esses resultados.

Tabela 20 – Resultados da aplicação Sabin desconsiderando os dados inválidos

Resultados da aplicação Sabin desconsiderando os dados inválidos		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	61	100%
Requisitos implementados	28	45.90%
Requisitos implementados de forma parcial	31	50.90%
Requisitos não implementados	2	3.20%

Fonte: Autor.

A seguir, serão apresentados detalhadamente os resultados conforme as categorias definidas na taxonomia proposta por Ferrão (2022), destacados na Tabela 20. O questionário utilizado pode ser encontrado no Apêndice C.

5.1 Finalidade

Nessa categoria há três contextos: Software, Estudo e Pesquisa, e Gestão Pública. A Tabela 21 apresenta de forma resumida os resultados obtidos nessa categoria.

Dos 25 requisitos analisados, 11 foram considerados inválidos por não ser possível avaliá-los na aplicação em questão. Entretanto, quatro requisitos foram considerados como tolamente implementados e oito foram implementados de forma parcial. Além disso, dois requisitos foram considerados como não implementados.

Tabela 21 – Resultados da categoria: Finalidade - Sabin

Resultados da categoria: Finalidade - Sabin		
Requisito	Situação	Justificativa
RQ001	Implementado	Na política de privacidade, apresenta a área de consentimento. Em que o usuário para exercer seus direitos, é necessário acessar a área de consentimento.
RQ002	Implementado de forma parcial	Implementados de forma parcial, na política de privacidade na Seção F.11 é apresentado que o sabin se compromete a utilizar toda e qualquer informação pessoal dentro dos limites legais e contratuais e que não disponibilizaremos seus dados pessoais a terceiros sem a observância da devida base legal e os demais procedimentos operacionais e técnicos necessários. Porém não foi possível verificar a implementação desse requisito.

RQ003	Implementado de forma parcial	Na política de privacidade na Seção F.9, é citado que quando não mais justificar a manutenção dos dados, estes serão apagados completamente ou alterados de forma que seja impossível identificar o titular dos dados pessoais em questão. Porém não foi possível verificar a implementação desse requisito.
RQ005	Implementado de forma parcial	Na política de privacidade, na Seção F.9 é citado que os dados serão armazenados pelo Sabin nas hipótese pelo prazo legal do possível ajuizamento de demandas por ou em face do Sabin e que em caso de qualquer das hipóteses acima não mais justificar a manutenção desses dados, estes serão apagados completamente ou alterados de forma que seja impossível identificar o titular dos dados pessoais em questão. Porém não foi possível verificar a implementação desse requisito.
RQ006	Não implementado	Não foi possível identificar essa opção nem na política de privacidade e nem no aplicativo. Há apenas o portal da privacidade. Porém não foi possível ter acesso até a data de coleta desse requisito
RQ007	Não implementado	Na Seção F.11 é citado que é direito do titular: Solicitar a portabilidade dos seus dados para outros fornecedores de produtos e serviços similares, de acordo com as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD); porém não é informado que os dados já tenham sido anonimizados pelo controlados não são incluídos na portabilidade.
RQ008	Implementado	No sabin é apresentado uma Seção G que contém os dados coletados e as finalidades.
RQ013	Implementado de forma parcial	Na política de privacidade, na Seção F.13 é apresentado que em todas as ocasiões que o Sabin considera necessário ou que houver obrigação legal/regulatória neste sentido, o Sabin pode solicitar o consentimento de forma expressa e inequívoca, e terem o cuidado de garantir que o usuário é livre para recusar ou retirar o consentimento sem qualquer empecilho. Porém não foi possível verificar a implementação desse requisito.

RQ015	Implementado de forma parcial	Na política de privacidade, Na Seção F.8 o sabin se compromete a utilizar toda e qualquer informação pessoal dentro dos limites legais e contratuais e que não disponibilizará os dados pessoais a terceiros sem a observância da devida base legal e os demais procedimentos operacionais e técnicos necessários. Porém, não foi possível verificar a implementação desse requisito.
RQ016	Implementado	Na política de privacidade cita que o atendimento à criança (todo aquele com até 12 anos de idade) será realizado mediante assinatura de termo de consentimento consignado por um dos pais, ou o pelo responsável legal, autorizando o tratamento dos dados pessoais, em conformidade com o artigo 14° §§ 1° e 3° da Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).
RQ018	Implementado de forma parcial	Na Tabela H de atendimento à menores de 18 anos apresenta que o atendimento a menores de 15 anos sempre precisa de atendimento.
RQ019	Implementado de forma parcial	Na Seção F.9 da politica de privacidade é cita que quando houver base legal ou regulatória que possibilite o armazenamento pelo Sabin . De forma implícita aborda estudo por órgão de pesquisa. Porém em nenhum momento cita de forma explícita e não cita a parte de anonimização.
RQ022	Implementado	Há politica de privacidade em um sítio eletrônico de fácil acesso.

RQ024	Implementado de forma parcial	Apesar de não ter citação explícita, de forma implícita esse requisito é atendido de forma parcial. Há citação na Seção F.8 que o Sabin somente compartilhará dados pessoais com terceiros quando houver a sua devida anuência, existindo alguma obrigação legal neste sentido ou nos casos que o compartilhamento for indispensável para a prestação dos nossos serviços e desenvolvimento de produtos e que o Sabin se compromete a utilizar toda e qualquer informação pessoal dentro dos limites legais e contratuais e que não disponibilizaremos seus dados pessoais a terceiros sem a observância da devida base legal e os demais procedimentos operacionais e técnicos necessários.

Fonte: Autor.

A Tabela 21 apresenta os resultados da avaliação dos requisitos relacionados à finalidade na política de privacidade do Sabin (Anexo F). O requisito RQ001 foi implementado, pois a política de privacidade do Sabin inclui uma área de consentimento para que os usuários possam exercer seus direitos. Por outro lado, os requisitos RQ002, RQ003, RQ005, RQ006, RQ007, RQ013, RQ015, RQ019 e RQ024 foram implementados de forma parcial ou não implementados. Embora a política mencione aspectos relacionados a esses requisitos, não foi possível verificar sua implementação ou não foram fornecidas informações claras sobre como eles são atendidos. No entanto, o requisito RQ008 foi implementado, pois é apresentada uma tabela com os dados coletados e suas finalidades. O requisito RQ016 também foi implementado, pois a política de privacidade do Sabin estabelece a necessidade de consentimento dos pais ou responsáveis legais para o tratamento de dados de crianças até 12 anos de idade. Além disso, o requisito RQ018 foi implementado de forma parcial, pois a tabela de atendimento a menores de 18 anos indica que o atendimento a menores de 15 anos sempre requer acompanhamento.

Em resumo, a política de privacidade do Sabin apresenta implementações parciais e não implementações em relação aos requisitos de finalidade avaliados. Embora aspectos relacionados a alguns requisitos sejam mencionados na política, não há informações claras sobre sua implementação. No entanto, o Sabin atendeu aos requisitos de consentimento, apresentando uma área para os usuários exercerem seus direitos, e estabeleceu a necessidade de consentimento dos pais para o tratamento de dados de crianças.

5.2 Adequação

Nessa categoria há cinco requisitos em dois contextos: Software e Estudo e Pesquisa, sendo que quatro dos cinco requisitos foram considerados como foram considerados inválidos por não ser possível avaliá-los para a aplicação em questão. A Tabela 22 mostra, de forma resumida, os resultados obtidos. Nessa categoria, apenas um dos requisitos foi considerado como implementado de forma parcial.

Tabela 22 – Resultados da categoria: Adequação - Sabin

Resultados da categoria: Adequação - Sabin		
Requisito	Situação	Justificativa
RQ028	Implementado de forma parcial	De acordo com a política de privacidade, na Seção F.11 é citado que é direito do titular: Retirar qualquer consentimento para o processamento de dados pessoais a qualquer momento. Porém, não foi possível verificar essa informação.

Fonte: Autor.

Conforme a Tabela 22 o requisito RQ028 foi implementado de forma parcial, pois a política de privacidade (Anexo F) menciona o direito do titular de retirar o consentimento para o processamento de dados pessoais a qualquer momento. No entanto, não foi possível verificar essa informação ou obter mais detalhes sobre como esse direito é exercido.

Em resumo, a política de privacidade do Sabin atende parcialmente ao requisito RQ028, que diz respeito ao direito do titular de retirar o consentimento para o processamento de dados pessoais a qualquer momento. Embora a política mencione esse direito, não há informações claras sobre como ele pode ser exercido ou quais são os procedimentos para sua efetivação. Portanto, é necessário fornecer mais detalhes e informações sobre como os usuários podem exercer esse direito de forma prática e eficaz.

5.3 Necessidade

A categoria necessidade contém 18 requisitos em cinco contextos: Software, Estudo e Pesquisa, Gestão Pública e Infraestrutura. A Tabela 23 mostra os resultados de forma resumida. Nessa categoria, quatro requisitos foram considerados como implementados e um foi considerado implementado de forma parcial.

Tabela 23 – Resultados da categoria: Necessidade - Sabin

Resultados da categoria: Necessidade - Sabin		
Requisito	Situação	Justificativa
RQ031	Implementado de forma parcial	Não há menção de forma explícita. Porém, há a informação na Seção F.13 que em todas as ocasiões que o Sabin considerar necessário ou que houver obrigação legal/regulatória neste sentido, poderá solicitar o consentimento de forma expressa e inequívoca, e se terá o cuidado de garantir que o usuário é livre para recusar ou retirar o consentimento sem qualquer empecilho.
RQ033	Implementado	Na Seção F.13 está citado que para a realização de exames: laboratoriais, de imagem, vacinas e as respectivas atividades administrativas, como a comunicação do resultado e o fornecimento de login e senhas para acesso remoto. Também contem que o Sabin em todas as ocasiões que considerar necessário ou que houver obrigação legal/regulatória neste sentido, poderá ser solicitado o consentimento de forma expressa e inequívoca, e terão o cuidado de garantir que o usuário é livre para recusar ou retirar o consentimento sem qualquer empecilho.
RQ034	Implementado	Na Seção F.13 está citado que o Sabin informa que nessa ocasião, para o desenvolvimento de novos produtos e serviços, bem como a divulgação deles os dados pessoais serão utilizados.
RQ042	Implementado	Está citado que em casos específicos e para cumprimento de fins contratuais o Sabin poderá realizar a transferência internacional de dados pessoais com empresas, institutos e outras organizações internacionais. Quando esse for o caso, os dados serão tratados e transmitidos dentro da observância da legislação nacional pertinente e só serão transferidos para países que detenham leis de proteção de dados pessoais similares ao Brasil

RQ046	Implementado	Na política de privacidade, na Seção F.8 é citado que proteção da vida e da saúde: Em situações de emergência, onde a vida, saúde ou bem-estar do titular dos dados ou de seus familiares estejam em risco iminente, o Grupo Sabin poderá compartilhar os dados necessários para proteger e preservar a integridade física do indivíduo conforme Art. 7º VII e Art. 11 II e).

Fonte: Autor.

A Tabela 23 apresenta os resultados da avaliação dos requisitos relacionados à necessidade na política de privacidade do Sabin (Anexo F). O requisito RQ031 foi implementado de forma parcial, pois embora não haja menção explícita, a política de privacidade indica que o Sabin poderá solicitar o consentimento do usuário de forma expressa e inequívoca em todas as ocasiões que considerar necessário ou que houver obrigação legal/regulatória. No entanto, é necessário fornecer mais informações claras sobre as situações em que o consentimento pode ser solicitado. Os requisitos RQ033, RQ034, RQ042 e RQ046 foram implementados.

Em resumo, a política de privacidade do Sabin atende parcialmente ao requisito RQ031, que aborda a necessidade de consentimento expresso e inequívoco do usuário. Embora a política indique que o consentimento será solicitado em situações consideradas necessárias ou exigidas por obrigações legais/regulatórias, não são fornecidas informações claras sobre as circunstâncias específicas em que o consentimento pode ser requerido. Por outro lado, os requisitos RQ033, RQ034, RQ042 e RQ046 foram implementados satisfatoriamente, não havendo maiores problemas em relação a eles.

5.4 Livre Acesso

A categoria livre acesso é composta por dois requisitos que pertencem ao contexto de Software. A Tabela 24 mostra os resultados de forma resumida.

Tabela 24 – Resultados da categoria Livre Acesso - Sabin

Resultados da categoria: Livre Acesso - Sabin		
Requisito	Situação	Justificativa
RQ049	Implementado	Esse requisito foi considerado implementado. Através do portal de privacidade é possível solicitar uma cópia de seus dados pessoais mantidos em nossa base de dados. Além disso na Seção F.11 cita que o titular tem esse direito.

Fonte: Autor.

Conforme a Tabela 24 é possível observar que o requisito RQ049 foi considerado implementado. Através do portal de privacidade, é possível solicitar uma cópia dos dados pessoais mantidos pelo Sabin em sua base de dados. Além disso, na Seção F.11, é mencionado que o titular tem o direito de solicitar essa cópia. Portanto, o Sabin atende a esse requisito fornecendo aos usuários uma maneira de acessar seus dados pessoais. No entanto, é importante garantir que o processo de solicitação e acesso aos dados seja transparente e eficiente, de acordo com as diretrizes estabelecidas na legislação de proteção de dados.

Em resumo, o Sabin atende ao requisito RQ049 relacionado ao livre acesso dos usuários aos seus dados pessoais, permitindo que eles solicitem e obtenham uma cópia dos dados através do portal de privacidade. Esse acesso é mencionado na Seção F.11, onde é destacado o direito do titular de solicitar essas informações. No entanto, é fundamental garantir que o processo de solicitação e acesso seja transparente e eficiente, em conformidade com as diretrizes estabelecidas na legislação de proteção de dados. Assegurar uma experiência clara e facilitada para os usuários no acesso às suas informações pessoais é essencial para cumprir adequadamente as obrigações de privacidade.

5.5 Qualidade dos dados

A categoria qualidade dos dados é dividida em três contextos: Governança, Software e Gestão Pública. Nessa categoria, foram avaliados sete requisitos, dos quais apenas um foi considerado como totalmente implementado e outro requisito considerado como implementado de forma parcial. O restante dos requisitos foram considerados como inválidos. A Tabela 25 mostra os resultados obtidos nesta categoria.

Tabela 25 – Resultados da categoria: Qualidade dos dados - Sabin

Resultados da categoria: Qualidade de dados - Sabin		
Requisito	Situação	Justificativa
RQ051	Implementado de forma parcial	Na Seção F.11 há apenas citação de que é direito do titular solicitar que os seus dados sejam corrigidos se estiverem imprecisos, desatualizados ou incompletos. Porém, não foi possível verificar a implementação desse requisito.
RQ052	Implementado	Na Seção F.11 é citado que é direito do titular solicitar que os seus dados sejam corrigidos se estiverem imprecisos, desatualizados ou incompletos. Isso pode ser feito pelo e-mail disponibilizado ou pelo portal de privacidade.

Fonte: Autor.

A Tabela 25 apresenta os resultados da categoria “Qualidade dos dados” para o aplicativo Sabin. O primeiro requisito, RQ051, é classificado como implementado de forma parcial, indicando que há uma menção na Seção F.11 de que é um direito do titular solicitar a correção de dados imprecisos, desatualizados ou incompletos. No entanto, não foi possível verificar a implementação desse requisito. Por outro lado, o requisito RQ052 é classificado como implementado, sendo mencionado na Seção F.11 que o titular tem o direito de solicitar a correção de dados por e-mail ou pelo portal de privacidade.

Esses resultados indicam que o aplicativo Sabin aborda a qualidade dos dados em seu contexto, porém, o requisito RQ051 ainda precisa ser verificado em termos de implementação. O requisito RQ052, por sua vez, está adequadamente implementado, fornecendo aos titulares a opção de corrigir dados imprecisos, desatualizados ou incompletos por meio de canais específicos.

Esses resultados mostram que o Sabin aborda a qualidade dos dados em sua política, mas é importante verificar e garantir a efetiva implementação do requisito RQ051 para fornecer aos titulares o direito de correção de dados. O fato de o requisito RQ052 estar adequadamente implementado oferece aos usuários canais específicos para corrigir suas informações imprecisas, desatualizadas ou incompletas. Assegurar a qualidade dos dados é fundamental para garantir a precisão e integridade das informações mantidas pelo aplicativo.

5.6 Transparência

A categoria transparência é composta por 13 requisitos que estão dentro dos contextos: Software e Governança. Dos 13 requisitos, oito foram considerados como implementados, quatro como implementados de forma parcial e o restante considerado como não implementado. A Tabela 26 mostra os resultados obtidos nessa categoria.

Tabela 26 – Resultados da categoria: Transparência - Sabin

Resultados da categoria: Transparência - Sabin		
Requisito	Situação	Justificativa
RQ058	Implementado	Na Seção G mostra como os dados são tratados
RQ060	Implementado de forma parcial	Apesar da Seção G apresentar a finalidade do tratamento e na Seção F cita os canais de atendimento encarregado@sabin.com.br privacidade@sabin.com.br. Porém, não foi possível verificar a implementação desse requisito.

RQ061	Implementado de forma parcial	Na política de privacidade, na Seção F.11 cita que é direito do titular retirar o consentimento o processamento dos seus dados pessoais a qualquer momento. Porém não foi possível verificar a implementação desse requisito.
RQ062	Implementado	Na Seção G é apresentada a justificativa e a base legal para a coleta dos dados.
RQ063	Implementado	Além dos e-mails para contato há ainda uma central de atendimento.
RQ064	Implementado de forma parcial	Na Seção G de política de privacidade há citação de como os dados são armazenados. Porém não foi possível verificar a implementação desse requisitos.
RQ065	Implementado	A Seção F.11 apresenta todos os direitos do titular dos dados.
RQ066	Implementado	A política de privacidade apresenta uma linguagem clara e apropriada.
RQ067	Implementado	Na política de privacidade há a Seção F.13 mostra a justificativa da coleta de dados. Além disso, na Seção G também é apresentada a finalidade e a base legal.
RQ068	Implementado de forma parcial	Há o portal de privacidade. Porém não foi possível verificar a funcionalidade dele no momento de coleta desse requisito.
RQ069	Implementado	Há na Seção G como os dados são armazenados e como são descartados.
RQ070	Implementado	Na política de privacidade há a Seção F.12 que aborda a indicação do encarregado de dados.

Fonte: Autor.

Conforme mostra a Tabela 26, o requisito RQ058 é relatado como implementado, indicando que a Seção G mostra como os dados são tratados. Isso demonstra um nível adequado de transparência na forma como a empresa lida com as informações pessoais dos indivíduos.

Já o requisito RQ060 é classificado como implementado de forma parcial, pois a Seção G apresenta a finalidade do tratamento e a Seção F cita os canais de atendimento. No entanto, não foi possível verificar a implementação desse requisito, o que sugere que pode haver lacunas na transparência relacionada aos canais de contato específicos para questões de privacidade.

O requisito RQ061 também é classificado como implementado de forma parcial.

Embora a Seção F.11 da política de privacidade mencione que é um direito do titular retirar o consentimento para o processamento de seus dados pessoais a qualquer momento, não foi possível verificar a implementação desse requisito. Isso pode indicar que não há uma maneira clara para os titulares exercerem esse direito de retirada de consentimento.

Por outro lado, os requisitos RQ062, RQ063, RQ065, RQ066, RQ067, RQ069 e RQ070 são relatados como implementados. O Anexo G, a Seção F.11 e a Seção F.13 da política de privacidade fornecem informações claras e abrangentes sobre a finalidade do tratamento de dados, os direitos dos titulares, a base legal para a coleta e o armazenamento adequado dos dados. Além disso, a existência de um portal de privacidade e a indicação do encarregado de dados na Seção F.12 demonstram o compromisso da empresa com a transparência e a conformidade com a legislação de proteção de dados.

No entanto, os requisitos RQ064 e RQ068 são classificados como implementados de forma parcial, pois embora haja menção no Anexo G e na política de privacidade (Anexo F) sobre como os dados são armazenados, não foi possível verificar a implementação desses requisitos. Isso sugere a necessidade de uma avaliação adicional para confirmar se as práticas de armazenamento de dados estão em conformidade com as políticas estabelecidas.

5.7 Segurança

Nesta categoria que engloba 16 requisitos que são divididos em contextos como Software, Estudos e Pesquisa, Governança e Infraestrutura. 11 dos 16 requisitos, foram considerados inválidos por não ser possível avaliá-los. Além disso, dois foram considerados como implementados de forma parcial e outros dois requisitos foram considerados como totalmente implementados. A Tabela 27 mostra os resultados obtidos.

Tabela 27 – Resultados da categoria: Segurança - Sabin

Resultados da categoria: Segurança - Sabin		
Requisito	Situação	Justificativa
RQ072	Implementado de forma parcial	Há citação na política de privacidade, na Seção F.11 que cita como um direito dos titulares o de solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. Porém não foi possível verificar a implementação deste requisito.

RQ073	Implementado de forma parcial	Há citação na política de privacidade, na Seção F.11 que cita como um direito dos titulares o de solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. Porém não foi possível verificar a implementação deste requisito.
RQ075	Implementado	Na Seção F.8, tem a informação que em situações de emergência, onde a vida, saúde ou bem-estar do titular dos dados ou de seus familiares estejam em risco iminente, o Grupo Sabin poderá compartilhar os dados necessários para proteger e preservar a integridade física do indivíduo conforme Art. 7º VII e Art. 11 II e). Além disso, na tutela da saúde está citado que: O compartilhamento pode ser realizado para tutela da saúde, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias. Também na pesquisa científica está citado que: O sabin ressalta que, em todas essas hipóteses, eles garantem que o compartilhamento é realizado de forma segura, protegendo a privacidade e cumprindo as demais disposições da LGPD.
RQ076	Implementado	Na Seção F.8, tem a informação que dados pessoais e dados pessoais sensíveis podem ser compartilhados para fins de pesquisa científica, desde que os dados utilizados nas pesquisas estejam anonimizados. O sabin ressalta que, em todas essas hipóteses, eles garantem que o compartilhamento é realizado de forma segura, protegendo a privacidade e cumprindo as demais disposições da LGPD.

Fonte: Autor.

O requisito RQ072 é classificado como implementado de forma parcial. Na Seção F.11 da política de privacidade, há uma citação que menciona o direito dos titulares de solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. No entanto, não foi possível verificar a implementação desse requisito no momento da análise.

Da mesma forma, o requisito RQ073 também é relatado como implementado de forma parcial. Na Seção F.11 da política de privacidade, é mencionado o direito dos titu-

lares de solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. No entanto, a implementação concreta desse requisito não pôde ser verificada no momento da análise.

Já o requisito RQ075 é considerado implementado. Na Seção F.8 da política de privacidade, é mencionado que, em situações de emergência que envolvam risco iminente à vida, saúde ou bem-estar do titular dos dados ou de seus familiares, o Grupo Sabin poderá compartilhar os dados necessários para proteger e preservar a integridade física do indivíduo, em conformidade com as disposições da LGPD. Além disso, o compartilhamento de dados também pode ocorrer para tutela da saúde e em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias, bem como para fins de pesquisa científica. O Sabin ressalta que, em todas essas hipóteses, o compartilhamento é realizado de forma segura, protegendo a privacidade e cumprindo as demais disposições da LGPD.

Similarmente, o requisito RQ076 é relatado como implementado. Na Seção F.8 da política de privacidade, é mencionado que dados pessoais e dados pessoais sensíveis podem ser compartilhados para fins de pesquisa científica, desde que os dados utilizados estejam anonimizados. O Sabin assegura que, nessas circunstâncias, o compartilhamento é realizado de forma segura, respeitando a privacidade e obedecendo às demais disposições da LGPD.

O requisito RQ084 é considerado implementado de forma parcial. Na Seção F.3 da política de privacidade, o Sabin declara que protege os dados por meio de medidas técnicas e operacionais adequadas, exigindo o mesmo nível de excelência de seus parceiros. Embora essa declaração indique uma abordagem de segurança, a implementação concreta desse requisito não pôde ser verificada no momento da análise.

5.8 Prevenção

A categoria prevenção apresenta cinco requisitos que estão divididos em três contextos que são: Software, estudo e pesquisa e governança. Dos cinco requisitos, três foram considerados como inválidos apenas um foi considerado como implementado de forma parcial e outro como totalmente implementado. A Tabela 28 mostra de forma resumida os resultados obtidos.

Tabela 28 – Resultados da categoria: Prevenção - Sabin

Resultados da categoria: Prevenção - Sabin		
Requisito	Situação	Justificativa
RQ090	Implementado	Na política de privacidade na Seção F.8 apresenta que na pesquisa científica: Dados pessoais e dados pessoais sensíveis podem ser compartilhados para fins de pesquisa científica, desde que os dados utilizados nas pesquisas estejam anonimizados.
RQ091	Implementado de forma parcial	na Seção F.8 da política de privacidade é citado que o Sabin em todas essas hipóteses, garantem que o compartilhamento é realizado de forma segura, protegendo a sua privacidade e cumprindo as demais disposições da LGPD. Portanto de forma implícita esse requisito foi considerado como implementado de forma parcial

Fonte: Autor.

A Tabela 28 apresenta os resultados da categoria “Prevenção” para o aplicativo Sabin. O requisito RQ090 é avaliado como implementado, indicando que na Seção F.8 da política de privacidade (Anexo F) é mencionado que dados pessoais e dados pessoais sensíveis podem ser compartilhados para fins de pesquisa científica, desde que os dados utilizados estejam anonimizados. Isso demonstra um compromisso com a prevenção de riscos ao compartilhar dados sensíveis apenas quando devidamente protegidos e anonimizados para fins científicos.

Por outro lado, o requisito RQ091 é avaliado como implementado de forma parcial. Na Seção F.8 da política de privacidade, é mencionado que o Sabin garante que o compartilhamento de dados é realizado de forma segura, protegendo a privacidade dos indivíduos e cumprindo as disposições da LGPD. Embora esse compromisso implique que o requisito foi considerado implementado de forma parcial, não foi fornecida uma justificativa explícita para confirmar a implementação completa do requisito.

Esses resultados indicam que o aplicativo Sabin demonstra uma preocupação com a prevenção de riscos relacionados ao compartilhamento de dados. O requisito RQ090 é implementado, garantindo que dados sensíveis sejam compartilhados apenas quando anonimizados para fins de pesquisa científica. No entanto, o requisito RQ091 é implementado de forma parcial, sugerindo a necessidade de uma justificativa mais explícita ou informações adicionais para confirmar a implementação completa das medidas de segurança e proteção de privacidade durante o compartilhamento de dados.

5.9 Não discriminação

A categoria não discriminação contém apenas dois requisitos no contexto de software. Todos os requisitos dessa categoria foram considerados como inválidos.

5.10 Responsabilidade e prestação de contas

Essa categoria é composta por 36 requisitos de privacidade, que estão divididos em três contextos: Software, Governança e Infraestrutura. Dos 36 requisitos, sete foram considerados como implementados, 12 foram considerados como implementados de forma parcial e os outros 16 foram considerados inválidos por não ser possível avaliá-los. A Tabela 29 mostra os resultados obtidos.

Tabela 29 – Resultados da categoria: Responsabilização e prestação de contas - Sabin

Resultados da categoria: Responsabilização e prestação de contas - Sabin		
Requisito	Situação	Justificativa
RQ094	Implementado	Na Tabela I de inventário de dados pessoais apresenta os tipos de dados que são coletados dos titulares de dados que são crianças.
RQ095	Implementado de forma parcial	Na Seção F.13 há o seguinte parágrafo: Comunicação e notificações: Utilizamos seus dados para enviar informações relevantes sobre seus exames, intercorrências, comunicados de resultados críticos, confirmações de agendamentos, resultados de exames, lembretes de vacinas, coleta de reações adversas de vacinas e outras comunicações relacionadas aos serviços prestados. Por isso, esse requisito foi considerado como implementado de forma parcial, mesmo de forma implícita.
RQ101	Implementado	Na Tabela de finalidade de dados pessoais I, há o grupo de dados sensíveis, com explicações para a coleta com a devida base legal.
RQ102	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular confirmar a existência de tratamento dos seus dados pessoais; Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.

RQ103	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular: Solicitar a correção de dados imprecisos, desatualizados ou incompletos; Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.
RQ104	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular: Solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.
RQ106	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular solicitar a exclusão ou indisponibilização dos seus dados pessoais, observada a obrigação legal de manutenção;. Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.
RQ107	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular solicitar a exclusão ou indisponibilização dos seus dados pessoais, observada a obrigação legal de manutenção. Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.
RQ108	Implementado de forma parcial	Na Seção F.11 da política de privacidade é citado que é direito do titular ser informado sobre a possibilidade de não fornecer consentimento e as respectivas consequências. Porém não foi possível verificar a aplicação desse requisito no portal de privacidade no momento da coleta desse requisito.
RQ109	Implementado	Há a Seção I que apresenta o inventário de dados pessoais
RQ110	Implementado de forma parcial	Na Seção F.11 é citado que é direito do titular solicitar a correção de dados imprecisos, desatualizados ou incompletos. Porém não foi possível verificar a implementação deste requisito

RQ111	Implementado de forma parcial	Na Seção F.11 é citado que é direito do titular solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei. Porém não foi possível verificar a implementação deste requisito
RQ112	Implementado de forma parcial	Na Seção F.11 é citado que é direito do titular solicitar a portabilidade dos seus dados para outros fornecedores de produtos e serviços similares, de acordo com as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD). Porém não foi possível verificar a implementação deste requisito.
RQ114	Implementado de forma parcial	Na Seção F.11 é citado que é direito do titular solicitar informações sobre as entidades públicas e privadas com as quais compartilhamos os seus dados. Porém não foi possível verificar a implementação deste requisito.
RQ115	Implementado de forma parcial	Na Seção F.11 é citado que é direito do titular ser informado sobre a possibilidade de não fornecer consentimento e as respectivas consequências. Porém não foi possível verificar a implementação deste requisito.
RQ121	Implementado de forma parcial	Na Seção F.13 é citado que segurança e prevenção de fraudes: Ocorre a utilização de dados para garantir a segurança dos pacientes, detecção e prevenção de fraudes, monitoramento de acessos não autorizados a prontuários e sistemas de informação, implementação de medidas de segurança da informação, entre outras atividades relacionadas à segurança dos dados pessoais. Porém não foi possível verificar a implementação deste requisito.
RQ123	Implementado de forma parcial	O Sabin possui uma página com as certificações, inclusive de gestão de riscos.
RQ124	Implementado	Na Seção F.12 cita que o sabin tem um setor exclusivo composto por uma equipe dedicada para gerenciar e proteger seus dados pessoais. O objetivo principal desse setor é garantir um tratamento seguro e adequado das informações pessoais, demonstrando assim o compromisso em proteger a privacidade

RQ126	Implementado	O Sabin possui um portal de privacidade.
RQ129	Implementado	Na Seção F.8 é mencionada que em determinadas circunstâncias, o sabin pode realizar compartilhamentos internacionais de dados com fornecedores de serviços em nuvem para hospedagem de dados. No entanto, o sabin ressalta que esses compartilhamentos são sempre realizados em conformidade com as leis internacionais de privacidade e com o artigo 33 da LGPD. Além disso, é citado que o sabin somente realiza a hospedagem de dados em países que possuem leis de proteção de dados equivalentes ou superiores às estabelecidas pela LGPD.

Fonte: Autor.

A análise dos resultados da categoria "Responsabilização e prestação de contas" para o Sabin mostra que o requisito RQ094 é considerado implementado, uma vez que no Anexo I, são apresentados os tipos de dados coletados dos titulares que são crianças. Isso demonstra que a aplicação está ciente da importância de identificar e proteger os dados pessoais de crianças, em conformidade com as regulamentações aplicáveis.

Já o requisito RQ095 é avaliado como implementado de forma parcial. Na Seção F.13 da política de privacidade, é mencionado que os dados pessoais são utilizados para enviar informações relevantes sobre exames, intercorrências, resultados críticos, agendamentos, vacinas, entre outros. Embora esse uso implique uma implementação parcial do requisito, a justificativa não é explícita o suficiente para confirmar totalmente a conformidade com o requisito.

O requisito RQ101 é relatado como implementado, pois no Anexo I, há um grupo de dados sensíveis com explicações sobre a coleta e a base legal correspondente. Isso indica que o aplicativo reconhece e documenta a finalidade da coleta de dados sensíveis, atendendo ao requisito.

No caso do requisito RQ102, ele é classificado como implementado de forma parcial. Na Seção F.11 da política de privacidade é mencionado que é direito do titular confirmar a existência do tratamento de seus dados pessoais. No entanto, a aplicação desse requisito não pôde ser verificada no portal de privacidade no momento da análise pois não foi possível ter acesso ao portal.

Os requisitos RQ103, RQ104, RQ106, RQ107, RQ108, RQ110, RQ111, RQ112, RQ114, RQ115, RQ121, RQ123, RQ126 e RQ129 são considerados implementados de forma parcial. Embora a política de privacidade (Seção F.11 e F.13) mencione os direitos

dos titulares relacionados a correção, anonimização, bloqueio, eliminação, portabilidade, informações sobre compartilhamento e consentimento, a implementação desses requisitos não pôde ser verificada no portal de privacidade no momento da análise.

Por outro lado, o requisito RQ124 é relatado como implementado, mencionando que o Sabin possui um setor exclusivo e uma equipe dedicada para gerenciar e proteger os dados pessoais dos indivíduos. Isso indica um compromisso com a proteção adequada e segura das informações pessoais.

Em geral, embora o aplicativo Sabin demonstre esforços em atender aos requisitos de responsabilização e prestação de contas, é importante verificar e garantir a implementação efetiva de alguns desses requisitos para cumprir totalmente com as normas de proteção de dados e assegurar os direitos dos titulares.

5.11 Melhorias sugeridas no Sabin

No aplicativo Sabin, são sugeridas melhorias relacionadas aos requisitos de privacidade. Primeiramente, recomenda-se disponibilizar, em área pública, os procedimentos necessários para revogar o consentimento. Dessa forma, os usuários terão fácil acesso às informações e aos procedimentos para revogar o consentimento previamente dado.

Outra sugestão é informar aos usuários que a portabilidade dos dados pessoais não inclui dados que já foram anonimizados pelo controlador. Essa informação pode ser claramente apresentada na seção de direitos dos titulares de dados, a fim de evitar qualquer confusão sobre a portabilidade de dados anonimizados.

Adicionalmente, é fundamental destacar que um detalhamento mais abrangente da política de privacidade traria uma melhora significativa para todas as categorias. Atualmente, a política de privacidade do aplicativo é genérica em muitos pontos, o que levou à avaliação de muitos requisitos como parcialmente implementados ou não implementados para todas as categorias. Com uma política mais detalhada, os usuários poderão compreender melhor como seus dados são coletados, armazenados, utilizados e protegidos, aumentando assim a transparência e a confiança no aplicativo.

Com essas medidas, haverá uma melhora geral na avaliação dos requisitos implementados em todas as categorias. Por fim, outra sugestão é disponibilizar a escolha de consentimento diretamente pelo aplicativo, de forma similar ao que acontece com o Conecte SUS. Assim, o usuário terá a liberdade de escolher o tipo de consentimento de forma prática e rápida.

6 Saúde Mob

A coleta de dados para o presente estudo foi realizada por meio de um questionário que está presente no Apêndice A. O questionário foi aplicado no aplicativo Saúde Mob e está presente no Apêndice D. Nas Seções seguintes, serão apresentados os resultados para a aplicação em questão. No Saúde Mob, realizou-se uma avaliação da própria aplicação e da política de privacidade descrita no Apêndice J.

No total foram examinados 129 requisitos de privacidade, conforme a classificação proposta por Ferrão (2022). No entanto, como demonstrado na Tabela 30, 66 desses requisitos foram considerados inválidos. Em outras palavras, eles não se adequam ao contexto da aplicação ou não foi possível avaliá-los devido a limitações técnicas ou à falta de acesso às informações necessárias.

A Tabela 30 mostra também que 20 requisitos foram considerados implementados, o que indica que a aplicação adotou medidas adequadas para garantir a privacidade dos dados dos usuários. Outros 41 requisitos foram classificados como implementados parcialmente, sugerindo que há espaço para melhorias em áreas específicas ou que necessitam de mais detalhes para serem considerados totalmente implementados. Por fim, dois requisitos foram identificados como não implementados, apontando as áreas em que a aplicação precisa aprimorar suas medidas de privacidade.

Tabela 30 – Resultados da aplicação Saúde Mob.

Resultados da aplicação: Saúde Mob		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	129	100%
Requisitos implementados	20	15.50%
Requisitos implementados de forma parcial	41	31.78%
Requisitos inválidos	66	51.16%
Requisitos não implementados	2	1.56%

Fonte: Autor.

A Tabela 31 mostra os resultados descartando-se os requisitos considerados inválidos. Nesse contexto, 31.75% dos requisitos foram considerados como totalmente implementados. 65.08% foram considerados como implementados de forma parcial e 3.17% foram considerados como não implementados.

Tabela 31 – Resultados da aplicação Saúde Mob desconsiderando os dados inválidos

Resultados da aplicação Sabin desconsiderando os dados inválidos		
Requisitos	**Quantidade**	**Porcentagem**
Requisitos avaliados	63	100%
Requisitos implementados	20	31.75%
Requisitos implementados de forma parcial	41	65.08%
Requisitos não implementados	2	3.17%

Fonte: Autor.

Nas seções seguintes, os resultados apresentados na Tabela 31 são detalhados, considerando as categorias definidas na taxonomia de Ferrão (2022). O questionário utilizado pode ser encontrado no Apêndice D.

6.1 Finalidade

Nessa categoria há três contextos: Software, Estudo e Pesquisa, e Gestão Pública. A Tabela 32 mostra que dos 25 requisitos analisados, 12 foram considerados inválidos por não ser possível avaliá-los na aplicação em questão. Dos requisitos considerados como válidos, quatro requisitos foram considerados como totalmente implementados e sete foram avaliados como implementados de forma parcial. Além disso, dois requisitos foram considerados como não implementados.

Tabela 32 – Resultados da categoria: Finalidade - Saúde Mob

Resultados da categoria: Finalidade - Saúde Mob		
Requisito	Situação	Justificativa
RQ001	Implementado de forma parcial	Pelo aplicativo ou site não é pedido o consentimento. Porém na política de privacidade na Seção J.2 há a definição de consentimento: manifestação livre, informada e inequívoca do titular do dado confirmando sua concordância quanto ao tratamento de seus dados pessoais. Além disso há também na Seção J.6 cita que mediante o fornecimento do consentimento do usuário para tratamento de seus dados pessoais, como por exemplo, para conceder acesso ao site, aplicativo ou outras plataformas mantidas pelo grupo Hermes Pardini ou receber informações via e-mail sobre interesses do usuário.

RQ002	Implementado	Na Seção J.10 está descrito que há limitação do acesso a dados pessoais por parte dos colaboradores, prestadores de serviços e visitantes, restringindo-o apenas nos limites da necessidade e finalidade de tratamento dos dados pessoais.
RQ003	Implementado de forma parcial	Na Seção J.2 cita que há eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados Pessoais – "LGPD";
RQ006	Implementado de forma parcial	É apresentado na Seção J.2 que é um direito do titular a revogação do consentimento. Porém não foi possível verificar a possibilidade de revogação.
RQ007	Não implementado	Não há nenhuma informação na política de privacidade de que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador.
RQ008	Implementado de forma parcial	Na Seção J.10 cita que o tratamento inclui a limitação do acesso a dados pessoais por parte dos colaboradores, prestadores de serviços e visitantes, restringindo-o apenas nos limites da necessidade e finalidade de tratamento dos dados pessoais. Porém não foi possível verificar a implementação desse requisito.
RQ009	Implementado	Na Seção J.6 cita que o tratamento acontece para exercer regularmente os direitos em contratos, processos judiciais, administrativos ou arbitrais.
RQ010	Implementado de forma parcial	Na Seção J.6 é citado que o tratamento ocorre quando existem legítimos interesses para tratamento de dados pessoais como no oferecimento e entrega de serviços, bem como para o funcionamento eficaz e lícito da prestação de serviços, desde que tais interesses não sejam superados pelos interesses do usuário, direitos e liberdades fundamentais.
RQ011	Implementado	Na Seção J.6 da política de privacidade há a possibilidade de tratar os dados para proteção crédito.

RQ014	Implementado de forma parcial	Na política de privacidade, na Seção J.6 é citado que o tratamento ocorre também para o cumprimento de obrigações legais e regulatórias que podem exigir a coleta, armazenamento e compartilhamento de dados pessoais e dados pessoais sensíveis, tais como manutenção de registros para fins fiscais ou fornecimento de informações a um órgão público ou entidade reguladora de leis/atividades do objeto social do grupo Hermes Pardini e cumprimento de obrigações de combate à corrupção, lavagem de dinheiro, fraude e condutas irregulares.
RQ015	Implementado	É citado na política de privacidade na Seção J.6 que o tratamento de dados pessoais também ocorre para executar eventual contrato, bem como para fornecer serviços ao usuário.
RQ016	Implementado de forma parcial	Na política de privacidade, na Seção J.8 é citado que para crianças: O tratamento de dados pessoais de crianças será realizado mediante consentimento específico e em destaque de pelo menos um de seus pais ou responsável legal. Porém não foi possível verificar a implementação desse requisito.
RQ021	Não implementado	Não há nenhuma menção disso na política de privacidade ou nos termos de uso.

Fonte: Autor.

A Tabela 32 apresenta os resultados da categoria “Finalidade” para o aplicativo Saúde Mob. Após análise dos dados, verificou-se que alguns requisitos foram implementados de forma parcial, enquanto outros foram implementados de forma completa ou não implementados.

Um dos requisitos avaliados, o RQ001, foi implementado de forma parcial. Embora a definição de consentimento seja mencionada na política de privacidade (Anexo J), não foi possível verificar a solicitação de consentimento pelo aplicativo ou site. Já o requisito RQ002 foi implementado de forma completa, com a restrição do acesso aos dados pessoais pelos colaboradores, prestadores de serviços e visitantes.

Em relação ao requisito RQ003, constatou-se que houve implementação parcial. A política de privacidade menciona a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, porém não foi possível verificar a implementação específica desse requisito.

Outro requisito, o RQ006, foi implementado de forma parcial. Embora seja citado na política de privacidade o direito do titular de revogar o consentimento, não foi possível verificar a disponibilidade dessa opção.

No entanto, o requisito RQ007 não foi implementado, pois não há informações na política de privacidade sobre a portabilidade dos dados pessoais já anonimizados pelo controlador.

Em relação ao RQ008, verificou-se que houve implementação parcial. Embora a política de privacidade mencione a limitação do acesso aos dados pessoais, não foi possível verificar a implementação desse requisito.

Por outro lado, alguns requisitos foram implementados de forma completa. É o caso do RQ009, que descreve o tratamento dos dados para exercer regularmente os direitos em contratos, processos judiciais, administrativos ou arbitrais. O requisito RQ011 também foi implementado, com a possibilidade de tratar os dados para proteção de crédito.

Já o requisito RQ014 foi implementado de forma parcial, pois embora a política de privacidade mencione o cumprimento de obrigações legais e regulatórias, não foi possível verificar a implementação específica desse requisito.

Outros requisitos, como o RQ015, RQ009 e RQ016, foram implementados de forma completa ou parcial. No entanto, o requisito RQ021 não foi implementado, pois não há menção na política de privacidade ou nos termos de uso sobre o tratamento de dados pessoais para fins de pesquisa científica.

Em resumo, a análise dos resultados da categoria "Finalidade" para o aplicativo Saúde Mob revela que alguns requisitos foram implementados de forma parcial, enquanto outros foram completamente atendidos ou não foram implementados. Foram encontradas limitações na implementação de requisitos essenciais, como a verificação da solicitação de consentimento, a disponibilidade da opção de revogação do consentimento e a eliminação específica de dados desnecessários. Além disso, a política de privacidade não aborda informações sobre a portabilidade de dados pessoais já anonimizados e não detalha a implementação de algumas medidas de segurança. Por outro lado, requisitos importantes, como o tratamento de dados para exercer direitos contratuais e processuais, bem como a proteção de crédito, foram totalmente atendidos. No entanto, ainda são necessárias melhorias para garantir a completa conformidade com as normas de proteção de dados e fornecer informações mais detalhadas sobre as medidas de segurança adotadas pelo aplicativo.

6.2 Adequação

Nessa categoria há cinco requisitos distribuídos em dois contextos: Software e Estudo e Pesquisa, sendo que um dos cinco requisitos foi considerado como inválido por não ser possível de avaliar para a aplicação em questão. A Tabela 33 mostra, de forma resumida, os resultados obtidos.

Tabela 33 – Resultados da categoria: Adequação - Saúde Mob

Resultados da categoria: Adequação - Saúde Mob		
Requisito	Situação	Justificativa
RQ026	Implementado de forma parcial	Na Seção J.10 há a descrição que o Saúde Mob implementa medidas de segurança técnica e organizacional apropriadas projetadas para proteger a integridade e confidencialidade dos dados pessoais. Porém não foi possível verificar a implementação dessas medidas e técnicas de seguranças.
RQ028	Implementado	Na Seção J.12 cita que é um direito do titular revogar o consentimento concedido, solicitar a eliminação dos dados pessoais tratados com base em consentimento, bem como de ter acesso a informações sobre a possibilidade de você não fornecer o consentimento e as respectivas consequências da negativa.
RQ029	Implementado	Na Seção J.7 é citado que empresas de tecnologia que fazem a gestão dos sistemas integrados ou responsáveis pelo armazenamento e garantia de segurança no tratamento dos dados pessoais; internamente para áreas que necessitam ter acesso aos dados pessoais, tais como: área técnica responsável pelos exames, área de atendimento ao cliente e área jurídica para cumprir alguma obrigação legal regulatória ou exercício regular dos direitos.

RQ030	Implementado de forma parcial	Na Seção J.9 Cita que quando necessário para atividade ou serviços relevantes. De forma implícita, esse requisito foi considerado como implementado de forma parcial. Apesar de não cita de forma clara e também não citar a anonimização dos dados pessoais.

Fonte: Autor.

A Tabela 33 apresenta os resultados da categoria "Adequação" para o aplicativo Saúde Mob. Ao analisar os requisitos, verificou-se que alguns foram implementados de forma parcial, enquanto outros foram implementados integralmente.

O requisito RQ026 foi implementado de forma parcial. Na Seção J.10 é mencionado que o Saúde Mob adota medidas de segurança técnica e organizacional para proteger a integridade e confidencialidade dos dados pessoais. No entanto, não foi possível verificar a implementação específica dessas medidas e técnicas de segurança.

Já o requisito RQ028 foi implementado integralmente. Na Seção J.12 é descrito que o titular dos dados possui o direito de revogar o consentimento, solicitar a eliminação dos dados pessoais tratados com base no consentimento e ter acesso a informações sobre as consequências da negativa em fornecer o consentimento.

O requisito RQ029 também foi implementado integralmente. Na Seção J.7 é mencionado que empresas de tecnologia são responsáveis pela gestão dos sistemas integrados e pelo armazenamento seguro dos dados pessoais. Além disso, é citado que áreas internas, como a área técnica responsável pelos exames, a área de atendimento ao cliente e a área jurídica, têm acesso aos dados pessoais para cumprir obrigações legais ou exercer direitos.

Em relação ao requisito RQ030 constatou-se que foi implementado de forma parcial. Na Seção J.9, é citado que a coleta de dados ocorre quando necessário para atividades ou serviços relevantes. No entanto, não há uma menção explícita sobre a anonimização dos dados pessoais.

Em resumo, os resultados da categoria "Adequação" para o aplicativo Saúde Mob demonstram que alguns requisitos foram implementados de forma parcial, enquanto outros foram completamente atendidos. O requisito RQ026 foi parcialmente implementado, pois apesar de mencionar a adoção de medidas de segurança técnica e organizacional para proteger os dados pessoais, não há informações específicas sobre as técnicas empregadas. Por outro lado, os requisitos RQ028 e RQ029 foram integralmente atendidos, abordando a possibilidade de revogação do consentimento pelo titular dos dados e o acesso restrito e responsável aos dados por diferentes áreas internas da empresa. Quanto ao requisito RQ030, foi implementado de forma parcial, pois, embora mencione a coleta de dados

apenas quando necessário e relevante, não há uma explicitação sobre a anonimização dos dados pessoais. Melhorias nesse sentido são necessárias para garantir maior conformidade e transparência nas práticas de privacidade do aplicativo Saúde Mob.

6.3 Necessidade

A categoria necessidade contém 18 requisitos distribuídos em cinco contextos: Software, Estudo e Pesquisa, Gestão Pública e Infraestrutura. A Tabela 34 mostra que dois requisitos foram considerados como implementados e três foram considerados como implementados de forma parcial.

Tabela 34 – Resultados da categoria: Necessidade - Saúde Mob

Resultados da categoria: Necessidade - Saúde Mob		
Requisito	Situação	Justificativa
RQ031	Implementado de forma parcial	Não há menção de forma explícita. Porém, há a informação na Seção F.13 que em todas as ocasiões que o Sabin considerar necessário ou que houver obrigação legal/regulatória neste sentido, poderá solicitar o consentimento de forma expressa e inequívoca, e se terá o cuidado de garantir que o usuário é livre para recusar ou retirar o consentimento sem qualquer empecilho.
RQ033	Implementado	Na Seção J.6 é citado que o tratamento ocorre mediante o fornecimento do consentimento para tratamento dos dados pessoais, como por exemplo, para o concedimento de acesso ao site, aplicativo ou outras plataformas mantidas pelo grupo Hermes Pardini ou receber informações via e-mail sobre interesses do titular.

RQ034	Implementado	Na Seção J.3 apresenta que a coleta de dados pessoais ocorre diretamente do titular: a coleta de dados pessoais que o usuário fornece quando, por exemplo, contrata para prestação de serviços, quando está na condição de doador (por exemplo, para realizar um exame de sangue), porque o paciente nos (por exemplo, o médico e seu paciente irá realizar algum exame em algum de nossos laboratórios), ou porque estão publicamente disponíveis. Ainda, pode-se coletar dados pessoais de incapazes e relativamente incapazes, como por exemplo crianças, adolescentes, interditados e curatelados, fornecidos pelo próprio titular ou por seus pais ou responsáveis legais.
RQ035	Implementado de forma parcial	Na Seção J.6 cita que o tratamento pode ocorrer para o cumprimento de obrigações legais e regulatórias que podem exigir a coleta, armazenamento e compartilhamento dos dados pessoais e dados pessoais sensíveis, tais como manutenção de registros para fins fiscais ou fornecimento de informações a um órgão público ou entidade reguladora de leis/atividades do objeto social do grupo Hermes Pardini e cumprimento de obrigações de combate à corrupção, lavagem de dinheiro, fraude e condutas irregulares. Porém, não cita a dispensa do fornecimento do consentimento do titular.
RQ037	Implementado de forma parcial	Na Seção J.6 cita que ocorre o tratamento de dados pessoais sensíveis para proteção da vida ou da sua incolumidade física. Porém não cita que é sem fornecimento de consentimento do titular.
RQ039	Implementado de forma parcial	Na Seção J.10 cita que a limitação do acesso a dados pessoais por parte dos colaboradores, prestadores de serviços e visitantes, restringe apenas nos limites da necessidade e finalidade de tratamento dos dados pessoais. Porém não foi possível verificar a implementação desse requisito.

Fonte: Autor.

A Tabela 34 apresenta os resultados da categoria "Necessidade" para o aplicativo Saúde Mob. Ao analisar os dados, é possível observar que a implementação dos requisitos varia entre parcial e completa.

Alguns requisitos, como RQ033 e RQ034, são considerados implementados, uma vez que a política de privacidade menciona explicitamente a necessidade de consentimento para o tratamento dos dados pessoais e descreve as situações em que ocorre a coleta desses dados.

Por outro lado, requisitos como RQ031, RQ035, RQ037 e RQ039 são classificados como implementados de forma parcial. Embora haja menções relacionadas a esses requisitos na política de privacidade, algumas especificidades não são abordadas ou não ficam claras o suficiente.

Em resumo, os resultados da categoria "Necessidade" para o aplicativo Saúde Mob mostram uma variação na implementação dos requisitos, abrangendo tanto a forma parcial quanto a completa. Os requisitos RQ033 e RQ034 são considerados implementados, pois a política de privacidade aborda explicitamente a necessidade de consentimento para o tratamento dos dados pessoais e detalha as situações de coleta desses dados. No entanto, alguns requisitos, como RQ031, RQ035, RQ037 e RQ039, foram implementados de forma parcial. Embora haja menções relacionadas a esses requisitos na política de privacidade, algumas especificidades não são devidamente abordadas ou permanecem pouco claras. Essas lacunas podem ser aprimoradas para garantir uma abordagem mais abrangente e transparente em relação à necessidade de tratamento dos dados no aplicativo Saúde Mob.

6.4 Livre Acesso

A categoria livre acesso é composta por dois requisitos que pertencem ao contexto de Software. A Tabela 35 mostra os resultados de forma resumida.

Tabela 35 – Resultados da categoria Livre Acesso - Saúde Mob

Resultados da categoria: Livre Acesso - Saúde Mob		
Requisito	Situação	Justificativa
RQ049	Implementado de forma parcial	Na Seção J.12 cita que é direito do titular a confirmação de que estão tratando seus dados pessoais e acessar os dados pessoais que são tratados sobre o titular. Porém, não foi possível verificar a implementação desse requisito.
RQ050	Implementado de forma parcial	Na Seção J.12 cita que é direito do titular solicitar a revisão do tratamento de dados pessoais com base em decisões automatizadas. Porém, não foi possível verificar a implementação desse requisito.

Fonte: Autor.

Na Tabela 35 observa-se que a implementação de todos os requisitos da categoria "Livre Acesso" para o aplicativo Saúde Mob forama avaliados como parcialmente implementados.

O requisito RQ049 refere-se ao direito do titular de confirmar que seus dados pessoais estão sendo tratados e acessar esses dados. Embora a Seção J.12 faça referência a esse direito, não foi possível verificar a implementação desse requisito com clareza pois não foi possível verificar a confirmação de tratamentos dos dados pessoais.

O requisito RQ050 trata do direito do titular de solicitar a revisão do tratamento de dados pessoais com base em decisões automatizadas. Da mesma forma que o requisito anterior, a Seção J.12 faz menção a esse direito, mas não é possível afirmar com certeza a implementação adequada desse requisito pois não foi possível solicitar a revisão do tratamento.

Em resumo, na categoria "Livre Acesso" do aplicativo Saúde Mob, todos os requisitos foram avaliados como parcialmente implementados. O requisito RQ049, referente ao direito do titular de confirmar o tratamento de seus dados pessoais e acessá-los, foi mencionado na Seção J.12, porém a implementação desse direito não pôde ser verificada com clareza, devido à falta de confirmação dos tratamentos dos dados pessoais. Da mesma forma, o requisito RQ050, que aborda o direito do titular de solicitar a revisão do tratamento com base em decisões automatizadas, também foi mencionado na mesma seção, mas não foi possível afirmar com certeza a implementação adequada, pois não houve a possibilidade de solicitar a revisão do tratamento. Essas questões pendentes de implementação devem ser aprimoradas para garantir o efetivo exercício dos direitos dos titulares em relação ao acesso e revisão de seus dados pessoais no aplicativo Saúde Mob.

6.5 Qualidade dos dados

A categoria qualidade dos dados é dividida em três contextos: Governança, Software e Gestão Pública. Nessa categoria, foram avaliados sete requisitos, dos quais quatro requisitos foram considerados como implementados de forma parcial. O restante dos requisitos foram considerados como inválidos. A Tabela 36 mostra os resultados obtidos nesta seção.

Tabela 36 – Resultados da categoria: Qualidade dos dados - Saúde Mob

Resultados da categoria: Qualidade dos dados - Saúde Mob		
Requisito	Situação	Justificativa
RQ052	Implementado de forma parcial	Na Seção J.12 é citado que é direito do titular solicitar a alteração ou atualização de seus dados pessoais quando estiverem incorretos, incompletos ou inexatos. Porém não foi possível verificar a implementação desse requisito.
RQ055	Implementado de forma parcial	Na Seção J.10 é citado que ocorre a garantia de que todos os colaboradores cumprem esta política, são constantemente treinados e capacitados para realizar procedimentos adequados para o correto tratamento dos dados pessoais. Porém não foi possível verificar a implementação desse requisito.
RQ056	Implementado de forma parcial	Na Seção J.10 cita que ocorre a adoção de sistemas estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e também ocorre a manutenção recorrente do banco de dados. Por isso, esse requisito foi considerado como implementado de forma parcial.

RQ057	Implementado de forma parcial	Na Seção J.9 da política de privacidade cita que o Saúde MOB armazena e mantém os dados pessoais de forma segura em data centers localizados no Brasil, em conformidade com a legislação aplicável e pelo período necessário ou permitido em vista das finalidades para as quais os dados pessoais foram coletados. Já na nota informativa, na Seção K.4 cita que oss dados pessoais tratados pelo Instituto Hermes Pardini S/A em consequência do uso do Saúde Mob serão armazenados em servidores próprios do Instituto Hermes Pardini S/A. Fica eleito o Foro da cidade de Belo Horizonte, Estado de Minas Gerais, para dirimir quaisquer questões decorrentes destes Termos de Uso, que será regido pelas leis brasileiras.

Fonte: Autor.

Observe, na Tabela 36, que a implementação de todos os requisitos é considerada parcial.

O requisito RQ052 refere-se ao direito do titular de solicitar a alteração ou atualização de seus dados pessoais quando estiverem incorretos, incompletos ou inexatos. Embora haja menção a esse direito na Seção J.12, não foi possível verificar de forma conclusiva a implementação desse requisito.

O requisito RQ055 trata da garantia de que todos os colaboradores cumpram a política de privacidade e recebam treinamento adequado para o tratamento correto dos dados pessoais. Embora a Seção J.10 faça referência a essas práticas, não foi possível verificar a implementação adequada desse requisito.

Já o requisito RQ056 diz respeito à adoção de sistemas estruturados que atendam aos requisitos de segurança, boas práticas e governança, conforme previsto na LGPD. A Seção J.10 faz referência a essas práticas, mas não é possível afirmar com certeza a implementação completa desse requisito.

Por fim, o requisito RQ057 aborda o armazenamento seguro dos dados pessoais em conformidade com a legislação aplicável. Embora a política de privacidade faça menção a essa prática, as informações fornecidas na Seção J.9 e na Seção K.4 da nota informativa não permitem uma verificação completa da implementação desse requisito.

Em resumo, na categoria "Qualidade dos Dados"do aplicativo Saúde Mob, a imple-

mentação de todos os requisitos foi considerada parcial. Portanto, são necessárias melhorias para garantir a implementação plena desses requisitos, visando assegurar a qualidade e segurança dos dados pessoais tratados pelo aplicativo Saúde Mob.

6.6 Transparência

A categoria transparência é composta por 13 requisitos que estão dentro dos contextos: Software e Governança. Dos 13 requisitos, nove foram considerados como implementados, um como implementado de forma parcial e o restante considerado como não implementado. A Tabela 37 mostra os resultados obtidos nessa categoria.

Tabela 37 – Resultados da categoria: Transparência - Saúde Mob

Resultados da categoria: Transparência - Saúde Mob		
Requisito	Situação	Justificativa
RQ058	Implementado	Há a Seção J.8 que aborda o tratamento de crianças e adolescentes.
RQ059	Implementado de forma parcial	Na Seção J.2 cita que é um direito do titular a revogação do consentimento. Porém não foi possível verificar a implementação desse requisito.
RQ061	Implementado de forma parcial	Na Seção J.2 cita que é um direito do titular a revogação do consentimento. Porém não foi possível verificar a implementação desse requisito.
RQ062	Implementado	Na Seção J.10 cita que ocorre a limitação do acesso a dados pessoais por parte dos colaboradores, prestadores de serviços e visitantes, restringindo-o apenas nos limites da necessidade e finalidade de tratamento dos dados pessoais.
RQ063	Implementado	Na Seção J.12 cita que o usuário possui vários direitos em relação aos seus dados pessoais, nos termos da LGPD. Para tanto, implementamos controles adicionais de transparência e acesso na área de privacidade para disponibilizar aos usuários o acesso livre e gratuito a esses direitos.
RQ065	Implementado	Há a política de privacidade e antes de se cadastrar, aparece os termos de uso.
RQ066	Implementado	Há uma linguagem clara e apropriada em todo aplicativo e nos documentos oficiais.

RQ068	Implementado	Na Seção J.12 além dos direitos elencados há também a informação se o usuário tiver alguma dúvida, observação, solicitação, reclamação ou revisão sobre a coleta ou o uso de seus dados pessoais ou sobre a política de privacidade e proteção de dados pessoais, pode entrar em contato com o DPO/Encarregado(a), através do envio de e-mail para o endereço eletrônico privacidade@grupopardini.com.br.
RQ069	Implementado	Há na Seção J.9 explicações sobre a retenção de dados e há também explicação sobre a eliminação na Seção J.2.
RQ070	Implementado	Na Seção J.1, há indicação do DPO/Encarregado(a), Fabiana Ricco, através do e-mail privacidade@grupopardini.com.br.

Fonte: Autor.

A Tabela 37 mostra que, na categoria "Transparência" a maioria dos requisitos foram implementados, embora alguns deles tenham sido implementados de forma parcial.

O requisito RQ058, que trata do tratamento de crianças e adolescentes, foi implementado e encontra-se detalhado na Seção J.8.

Os requisitos RQ059 e RQ061 referem-se ao direito do titular de revogar o consentimento. Embora a Seção J.2 faça menção a esse direito, não foi possível verificar de forma conclusiva a implementação desses requisitos.

O requisito RQ062, relacionado à limitação do acesso a dados pessoais, foi implementado. Conforme descrito na Seção J.10, o acesso aos dados é restrito aos colaboradores, prestadores de serviços e visitantes apenas nos limites necessários para o tratamento dos dados pessoais.

O requisito RQ063 diz respeito aos direitos do usuário em relação aos seus dados pessoais, conforme previsto na LGPD. A implementação desse requisito é confirmada na Seção J.12, onde são disponibilizados controles adicionais de transparência e acesso na área de privacidade, visando proporcionar aos usuários acesso livre e gratuito a esses direitos.

Os requisitos RQ065, RQ066, RQ068, RQ069 e RQ070 foram todos implementados. O RQ065 é atendido por meio da existência de uma política de privacidade presente no Anexo J e dos termos de uso exibidos antes do cadastro. O RQ066 é cumprido por meio do uso de uma linguagem clara e apropriada em todo o aplicativo e nos documentos oficiais. O RQ068 é satisfeito pela disponibilização das informações de contato do

DPO/Encarregado na Seção J.12. O RQ069 é contemplado por explicações sobre a retenção e a eliminação de dados nas Seções J.9 e J.2. Por fim, o RQ070 é atendido com a indicação do DPO/Encarregado e seu e-mail de contato na Seção J.1.

Em resumo, na categoria "Transparência" do aplicativo Saúde Mob, a maioria dos requisitos foi implementada, embora alguns deles tenham sido atendidos de forma parcial. Essas medidas têm como objetivo garantir uma maior transparência, controle e acesso dos usuários em relação aos seus dados pessoais no aplicativo Saúde Mob.

6.7 Segurança

A categoria segurança apresenta 16 requisitos que estão divididos em três contextos que são: Software, Estudo e pesquisa e Governança. Dos 16 requisitos, três foram avaliados como implementados de forma parcial e outro como totalmente implementado. A Tabela 38 mostra de forma resumida os resultados obtidos.

Tabela 38 – Resultados da categoria: Segurança - Saúde Mob

Resultados da categoria: Segurança - Saúde Mob		
Requisito	Situação	Justificativa
RQ075	Implementado de forma parcial	Na Seção J.6 cita que o tratamento de dados pode ocorrer para para proteção da vida ou da incolumidade física. Porém, não é citado que é realizado por profissionais de saúde ou por entidades sanitárias.
RQ076	Implementado de forma parcial	Na Seção J.6 pessoais cita que ocorre o tratamento de dados para o cumprimento de obrigações legais e regulatórias que podem exigir a coleta, armazenamento e compartilhamento de seus dados pessoais e dados pessoais sensíveis, tais como manutenção de registros para fins fiscais ou fornecimento de informações a um órgão público ou entidade reguladora de leis/atividades do objeto social do grupo Hermes Pardini e cumprimento de obrigações de combate à corrupção, lavagem de dinheiro, fraude e condutas irregulares. Porém, não cita a anonimização de dados.

RQ078	Implementado de forma parcial	Há a Seção J.10 que detalhada os procedimentos de segurança. Essa Seção aborda a utilização de medidas técnicas capazes de inibir/mitigar riscos de eventuais maliciosos nos sistemas, com a utilização de tecnologias concebidas para proteger os dados pessoais durante o compartilhamento com empresas terceiras.
RQ084	Implementado	Há a Seção J.10 que detalhada os procedimentos de segurança. Essa Seção aborda a utilização de medidas técnicas capazes de inibir/mitigar riscos de eventuais maliciosos nos sistemas, com a utilização de tecnologias concebidas para proteger os dados pessoais durante o compartilhamento com empresas terceiras.

Fonte: Autor.

A Tabela 38 mostra que a maioria dos requisitos foram implementados, embora alguns deles tenham sido implementados de forma parcial.

O requisito RQ075, relacionado ao tratamento de dados para proteção da vida ou da incolumidade física, foi implementado de forma parcial. A Seção J.6 cita o tratamento de dados para esse fim, mas não menciona especificamente que é realizado por profissionais de saúde ou por entidades sanitárias.

O requisito RQ076, referente ao tratamento de dados para o cumprimento de obrigações legais e regulatórias, também foi implementado de forma parcial. A Seção J.6 descreve o tratamento de dados para cumprir essas obrigações, como a manutenção de registros para fins fiscais e o fornecimento de informações a órgãos públicos ou entidades reguladoras. No entanto, não menciona explicitamente a anonimização de dados.

Já o requisito RQ078, que aborda a utilização de medidas técnicas para inibir ou mitigar riscos de eventuais ataques maliciosos nos sistemas, foi implementado de forma parcial. A Seção J.10 detalha os procedimentos de segurança adotados, incluindo a utilização de tecnologias para proteger os dados pessoais durante o compartilhamento com empresas terceiras.

Por fim o requisito RQ084, relacionado à proteção dos dados pessoais durante o compartilhamento com empresas terceiras, foi implementado. A Seção J.10 descreve os procedimentos de segurança adotados, que incluem o uso de medidas técnicas para inibir ou mitigar riscos de ataques maliciosos nos sistemas.

Em resumo, na categoria “Segurança” do aplicativo Saúde Mob, a maioria dos

requisitos foi implementada, embora alguns deles tenham sido atendidos de forma parcial. Portanto esforços adicionais são necessários para garantir a implementação plena dos requisitos parcialmente atendidos e proporcionar uma segurança abrangente dos dados pessoais tratados pelo aplicativo Saúde Mob.

6.8 Prevenção

A categoria prevenção apresenta cinco requisitos que estão divididos em três contextos que são: Software, Estudo e pesquisa e Governança. Dos cinco requisitos, três foram avaliados como inválidos e apenas dois foram avaliados como implementados de forma parcial. A Tabela 39 mostra de forma resumida os resultados obtidos.

Tabela 39 – Resultados da categoria: Prevenção - Saúde Mob

Resultados da categoria: Prevenção - Saúde Mob		
Requisito	Situação	Justificativa
RQ088	Implementado de forma parcial	Na Seção J.10 há citação que o SaudeMOB está comprometido em proteger a privacidade e os dados. Para isso, é adotado medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Porém não foi possível verificar a implementação desse requisito.
RQ091	Implementado de forma parcial	Na Seção J.10 há citação que o Saúde MOB está comprometido em proteger a privacidade e os dados. Para isso, é adotado medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Porém não foi possível verificar a implementação desse requisito.

Fonte: Autor.

Na Tabela 39 é possível observar que o requisito RQ088, relacionado à proteção da privacidade e dos dados, foi implementado de forma parcial. A Seção J.10 descreve que o Saúde Mob adota medidas de segurança, técnicas e administrativas para proteger

os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. No entanto, não foi possível verificar a implementação específica desse requisito.

O requisito RQ091, que também aborda a proteção da privacidade e dos dados, foi implementado de forma parcial. A Seção J.10 descreve que o Saúde Mob adota medidas de segurança, técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. No entanto, não foi possível verificar a implementação específica desse requisito.

Em resumo, na categoria "Prevenção" do aplicativo Saúde Mob, os requisitos relacionados à proteção da privacidade e dos dados (RQ088 e RQ091) no entanto, não foram fornecidos detalhes específicos sobre a implementação desses requisitos. Esforços adicionais são necessários para garantir a implementação completa desses requisitos e fortalecer a prevenção e proteção da privacidade e dos dados pessoais tratados pelo aplicativo Saúde Mob.

6.9 Não discriminação

A categoria não discriminação contém apenas dois requisitos no contexto de software. Todos os requisitos dessa categoria foram considerados como inválidos.

6.10 Responsabilidade e prestação de contas

Essa categoria é composta por 36 requisitos de privacidade, que estão divididos em três contextos: Software, Governança e Infraestrutura. Dos 36 requisitos, apenas dois foram considerados como implementados, 17 foram considerados como implementados de forma parcial e os outros 17 foram considerados inválidos por não ser possível avaliá-los. A Tabela 40 mostra os resultados obtidos.

Tabela 40 – Resultados da categoria: Responsabilização e prestação de contas - Saúde Mob

Resultados da categoria: Responsabilização e prestação de contas - Saúde Mob		
Requisito	Situação	Justificativa
RQ094	Implementado de forma parcial	Na Seção J.4 cita os dados pessoais que são coletados. Porém, não há divisão para os dados que são crianças.
RQ101	Implementado	Na Seção J.4 há um parágrafo sobre a coleta de dados pessoais.

RQ102	Implementado de forma parcial	Na Seção J.12 é informado que é direito do titular a confirmação de que estão tratando os dados pessoais; Se o usuário tiver alguma dúvida, observação, solicitação, reclamação ou revisão sobre a coleta ou o uso de seus dados pessoais ou sobre a política de privacidade e proteção de dados pessoais, pode entrar em contato com o(a) DPO/Encarregado(a), através do envio de e-mail para o endereço eletrônico privacidade@grupopardini.com.br. Porém não apresenta todos os procedimentos necessários.
RQ103	Implementado de forma parcial	Na Seção J.12 é informado que é direito do titular solicitar a alteração ou atualização de seus dados pessoais quando estiverem incorretos, incompletos ou inexatos. Porém não foi possível verificar a implementação desse requisito.
RQ104	Implementado de forma parcial	Na Seção J.12 é informado que é direito do titular solicitar que os dados pessoais que você entenda como desnecessários, excessivos ou tratados em desconformidade com a LGPD sejam anonimizados, bloqueados ou eliminados, desde que permitido pelas legislações/regulamentos que estejam relacionados ao objeto social do grupo HERMES PARDINI.
RQ105	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. Porém não apresenta os procedimentos necessários.
RQ106	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: eliminação dos dados pessoais tratados com o consentimento do titular. Porém não apresenta os procedimentos necessários.
RQ107	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: obter informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados. Porém não apresenta os procedimentos necessários.

RQ108	Implementado	Na Seção J.2 é citado como um direito do titular: ter acesso a informações sobre a possibilidade de você não fornecer o consentimento e as respectivas consequências da negativa.
RQ109	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: acessar os dados pessoais que tratamos sobre o usuário; Porém não foi possível verificar a implementação desse requisito.
RQ110	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: solicitar a alteração ou atualização de seus dados pessoais quando estiverem incorretos, incompletos ou inexatos. Porém não foi possível verificar a implementação desse requisito.
RQ111	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: solicitar que os dados pessoais que o usuário entenda como desnecessários, excessivos ou tratados em desconformidade com a LGPD sejam anonimizados, bloqueados ou eliminados, desde que permitido pelas legislações/regulamentos que estejam relacionados ao objeto social do grupo HERMES PARDINI;Porém não foi possível verificar a implementação desse requisito.
RQ112	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. Porém não foi possível verificar a implementação desse requisito.
RQ113	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: solicitar a eliminação dos dados pessoais tratados com o consentimento do titular. Porém não foi possível verificar a implementação desse requisito.

RQ114	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: solicitar eliminação dos dados pessoais tratados com o consentimento do titular. Porém não foi possível verificar a implementação desse requisito
RQ115	Implementado de forma parcial	Na Seção J.2 é citado como um direito do titular: obter informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa. Porém não foi possível verificar a implementação desse requisito
RQ119	Implementado de forma parcial	Na Seção F.13 é citado que o tratamento pode ocorrer para manutenção de registros.
RQ121	Implementado de forma parcial	na Seção J.10 cita que ocorre adoção de sistemas estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD.
RQ125	Implementado de forma parcial	Há na Seção J.10 a citação de que todos os colaboradores cumprem a política, são constantemente treinados e capacitados para realizar procedimentos adequados para o correto tratamento dos dados pessoais. Porém não foi possível verificar a implementação desse requisito.
RQ129	Implementado de forma parcial	Na Seção J.7 está descrito que de qualquer forma, o grupo Hermes Pardini exigirá que os terceiro: Comprometam-se a cumprir as leis de proteção de dados e os princípios da política de privacidade. Somente processem os dados pessoais para os fins descritos nesta política, e implementem medidas de segurança técnica e organizacional apropriadas projetadas para proteger a integridade e confidencialidade dos dados pessoais.

Fonte: Autor.

A Tabela 40 apresenta a implementação parcial do requisito RQ094, que trata da divisão dos dados pessoais coletados em relação a crianças. Embora a Seção J.4 descreva os dados pessoais coletados, não há uma divisão específica para os dados das crianças.

Quanto ao requisito RQ101, relacionado à coleta de dados pessoais, foi completamente implementado. A Seção J.4 contém um parágrafo que aborda esse requisito.

O requisito RQ102, que trata dos procedimentos para confirmação do tratamento de dados pessoais e para entrar em contato com o DPO/Encarregado, foi implementado parcialmente. Embora a Seção J.12 forneça informações sobre a possibilidade de entrar em contato com o DPO/Encarregado, não apresenta todos os procedimentos necessários.

Já o requisito RQ103, referente à solicitação de alteração ou atualização de dados pessoais incorretos, incompletos ou inexatos, foi implementado parcialmente. A Seção J.12 informa que é um direito do titular, mas não especifica os procedimentos específicos para sua concretização.

O requisito RQ104, que aborda a solicitação de anonimização, bloqueio ou exclusão de dados pessoais tratados em desconformidade com a LGPD, também foi implementado de forma parcial. A Seção J.1 menciona o direito do titular, mas não apresenta os procedimentos necessários.

De maneira similar, o requisito RQ105, relacionado à portabilidade dos dados para outro fornecedor de serviço ou produto, foi implementado parcialmente. A Seção J.2 menciona esse direito do titular, mas não detalha os procedimentos necessários.

O requisito RQ106, que trata da solicitação de exclusão de dados pessoais tratados com consentimento do titular, foi implementado de forma parcial. A Seção J.2 menciona esse direito do titular, mas não apresenta os procedimentos necessários.

No caso do requisito RQ107, que diz respeito à obtenção de informações sobre o uso compartilhado de dados com entidades públicas e privadas, sua implementação também foi parcial. A Seção J.2 menciona esse direito do titular, mas não apresenta os procedimentos necessários.

O requisito RQ108, relacionado ao acesso às informações sobre a possibilidade de não fornecer consentimento e suas consequências, foi implementado completamente. A Seção J.2 aborda esse direito do titular.

Os requisitos RQ109, RQ110, RQ111, RQ112, RQ113, RQ114, RQ115, RQ119, RQ121, RQ125 e RQ129 também foram implementados de forma parcial. As Seções J.2, J.10 e J.7 fornecem informações sobre esses direitos dos titulares, mas não foi possível verificar a implementação específica de cada requisito.

Em resumo, na categoria “Responsabilização e Prestação de Contas” do aplicativo Saúde Mob, a maioria dos requisitos foi implementada de forma parcial. Alguns requisitos não apresentam detalhes específicos para uma implementação completa. Esforços adicionais são necessários para garantir a implementação plena dos requisitos e fortalecer a responsabilização e prestação de contas em relação aos dados pessoais tratados pelo

aplicativo.

6.11 Sugestões de Melhorias no Saúde Mob

O aplicativo Saúde Mob pode ser aprimorado em relação aos requisitos de privacidade. Primeiramente, sugere-se informar aos usuários que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador. Essa informação deve ser claramente apresentada na política de privacidade, garantindo que os usuários estejam cientes dessa particularidade. Com isso, haveria uma melhora significativa na categoria de transparência.

Além disso, é importante informar ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor. Essa informação pode ser incluída tanto na política de privacidade quanto nos termos de uso do aplicativo, garantindo que os usuários conheçam todas as opções disponíveis para exercer seus direitos em relação aos seus dados pessoais.

Adicionalmente, é fundamental destacar que um detalhamento mais abrangente da política de privacidade traria melhorias significativas para todas as categorias. Atualmente, a política de privacidade do aplicativo é genérica em muitos pontos, o que levou à avaliação de muitos requisitos como parcialmente implementados ou não implementados para todas as categorias. Com uma política mais detalhada, os usuários poderão compreender melhor como seus dados são coletados, armazenados, utilizados e protegidos, aumentando assim a transparência e a confiança no aplicativo.

Por fim, a última sugestão é disponibilizar a escolha de consentimento diretamente pelo aplicativo, de forma similar ao que acontece com o Conecte SUS. Assim, o usuário tem a liberdade de escolher o tipo de consentimento de forma prática e rápida. Essas melhorias ajudariam a fortalecer a privacidade e a responsabilidade no tratamento dos dados pessoais dos usuários do Saúde Mob.

7 Discussão e análise dos resultados

A Figura 9 apresenta de forma gráfica os resultados obtidos para os três aplicativos analisados. A seguir, serão discutidos os resultados obtidos.

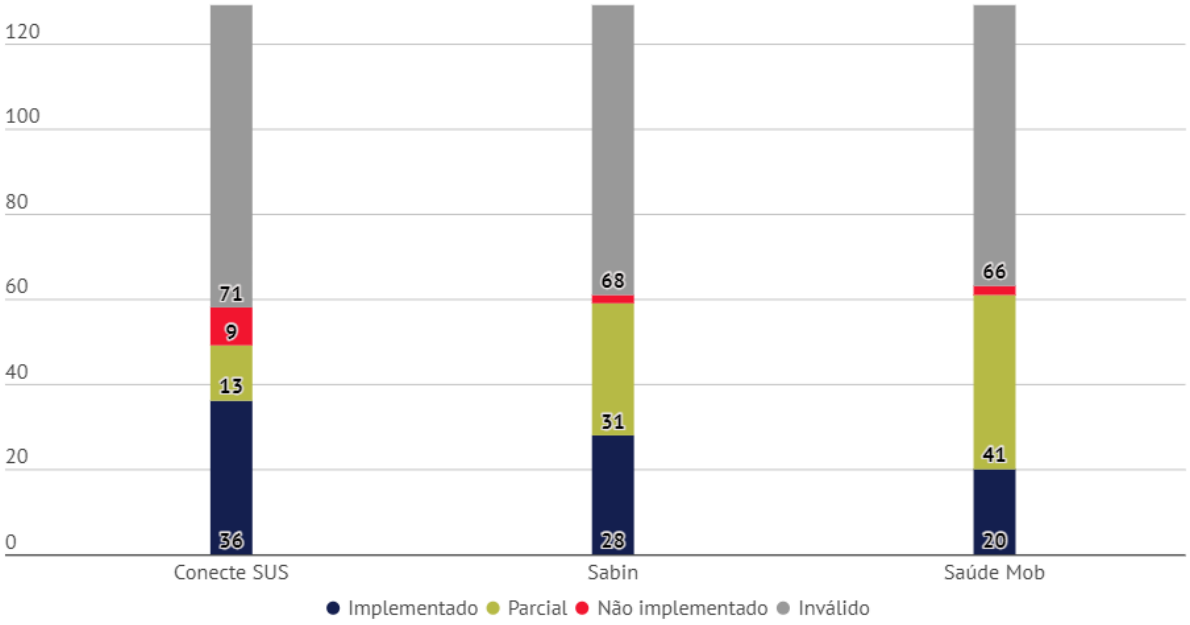

Figura 9 – Resultado dos três aplicativos. Fonte: Autor.

Conforme pode ser observado na Figura 9, a análise dos três aplicativos de saúde: Conecte SUS, Sabin e Saúde Mob, revelou resultados distintos quanto à implementação dos requisitos avaliados. O Conecte SUS obteve a maior quantidade de requisitos considerados como implementados, em comparação com os demais, o que pode ser atribuído à sua política de privacidade, termos de uso e nota informativa mais detalhada em relação aos outros dois aplicativos.

A política de privacidade é um aspecto essencial quando se trata de aplicativos que lidam com dados sensíveis de saúde. No caso do Conecte SUS, sua política de privacidade parece ser mais abrangente e minuciosa, o que pode ter levado à maior implementação dos requisitos. Ao fornecer informações claras e detalhadas sobre como os dados são coletados, armazenados, usados e compartilhados, os usuários tendem a ter mais confiança no aplicativo e, consequentemente, maior aderência às medidas de privacidade e segurança.

Além disso, os termos de uso e a nota informativa no Conecte SUS podem ter sido fatores que influenciaram a maior implementação dos requisitos. Esses documentos são fundamentais para informar aos usuários sobre suas responsabilidades e direitos ao utilizar o aplicativo, garantindo transparência e clareza nas interações com os serviços de

saúde.

Um aspecto interessante observado durante a análise foi que os documentos do Conecte SUS seguiam uma organização por tópicos, alinhada com as diretrizes da Lei Geral de Proteção de Dados (LGPD). Essa abordagem pode ter facilitado a incorporação dos requisitos necessários para estar em conformidade com a legislação, tornando mais claro para os desenvolvedores quais aspectos precisavam ser atendidos.

No caso do aplicativo Sabin, embora tenha sido avaliada a política de privacidade, notou-se que ela apresentava pontos genéricos. A falta de detalhamento e especificidade pode ter influenciado na implementação parcial de requisitos e também prejudicado a taxa de aderência, especialmente em áreas críticas relacionadas à privacidade dos dados.

O Sabin tinha um portal de privacidade, mas a indisponibilidade no momento da coleta de dados pode ter contribuído para resultados inferiores em relação à implementação. A falta de acesso ao portal pode ter limitado a análise completa e detalhada das políticas e diretrizes de privacidade, resultando em uma avaliação menos completa do aplicativo.

No caso do aplicativo Saúde Mob, também foi constatado que a política de privacidade era genérica em vários pontos. Essa falta de especificidade pode ter impactado na implementação parcial dos requisitos.

Em resumo, a análise dos três aplicativos indicou que o Conecte SUS se destacou na quantidade de requisitos implementados, possivelmente devido a sua política de privacidade, termos de uso e nota informativa mais detalhada em comparação com o Sabin e o Saúde Mob. A abordagem organizada por tópicos, alinhada com a LGPD, também pode ter facilitado o processo de implementação. Enquanto isso, os outros aplicativos apresentaram desafios relacionados à falta de detalhamento nas políticas de privacidade e problemas de acessibilidade durante a coleta de dados, o que impactou negativamente sua taxa de aderência aos requisitos de segurança e privacidade.

8 Considerações finais

Este trabalho teve como objetivo verificar a aderência das aplicações selecionadas em relação à LGPD (BRASIL, 2018) e à norma ISO 29100 (ISO/IEC, 2011), utilizando-se a taxonomia proposta por Ferrão (2022). Foram avaliados 129 requisitos de privacidade nos três aplicativos dos quais em média 46.25% dos requisitos foram avaliados como implementados, indicando que as aplicações possuem medidas adequadas para garantir a privacidade dos dados dos usuários. Além disso, em média 46.56% dos requisitos foram considerados parcialmente implementados, sugerindo oportunidades de melhoria em algumas áreas específicas ou que precisam de mais detalhes para serem considerados totalmente implementados. Por outro lado, em média 3.37% dos requisitos foram considerados como não implementados, destacando áreas em que as aplicações precisam aprimorar suas medidas de privacidade. Esses resultados foram alcançados através dos objetivos específicos.

O objetivo **(OE-1)** que consistia em realizar um estudo e seleção de sistemas para avaliação foi feito e está documentado na Seção 3.3. Para a seleção dos aplicativos, foi levado em consideração os documentos oficiais, como a política de privacidade, notas informativas e termos de uso do usuário. O objetivo **(OE-2)** também foi atendido através da realização do referencial teórico presente no Capítulo 2, em que houve estudos sobre os principais assuntos abordados neste trabalho.

Os objetivos **(OE-3)** e **(OE-4)** foram atendidos nos Capítulos 4, 5 e 6 através de um estudo nas aplicações citadas anteriormente. Para isso, foi utilizado um modelo de questionário que está presente no Apêndice A para verificar a implementação dos requisitos. Já o objetivo **(OE-5)** foi atendido nas Seções 4.11, 5.11 e 6.11 onde há o detalhamento dos pontos encontrados que são passíveis de melhorias nas aplicações. Além disso, a taxonomia desenvolvida por Ferrão (2022) em relação aos requisitos de privacidade, de acordo com a LGPD e a ISO 29100, é abrangente e organizada, atendendo de forma geral ao objetivo proposto.

A taxonomia desenvolvida por Ferrão (2022) facilita aos desenvolvedores e gerentes de projetos a verificar e implementar requisitos de privacidade durante o desenvolvimento de software. Essa abordagem taxonômica apresenta uma estrutura organizada e clara, classificando os requisitos de privacidade em categorias e subcategorias, o que torna mais fácil para os profissionais de tecnologia compreenderem e aplicarem as medidas necessárias para estar em conformidade com a LGPD e a ISO 29100.

A grande vantagem da utilização dessa taxonomia é a tradução dos termos legais e complexos presentes na legislação em termos técnicos mais acessíveis. Desenvolvedores

e gerentes de projetos, que muitas vezes não têm formação jurídica, podem enfrentar dificuldades na interpretação das leis e regulamentos de privacidade, podendo cometer equívocos ao aplicá-los no desenvolvimento de software. A taxonomia proporciona uma linguagem comum entre as áreas jurídica e de tecnologia, tornando a comunicação e colaboração mais fluidas.

Ao utilizar a taxonomia proposta por Ferrão (2022), os profissionais podem identificar facilmente quais requisitos de privacidade são aplicáveis ao contexto de seus projetos e, assim, adotar as medidas necessárias para garantir a privacidade dos dados dos usuários. Essa abordagem também permite que as equipes de desenvolvimento compreendam melhor os princípios e diretrizes da LGPD e da ISO 29100, evitando interpretações equivocadas e, consequentemente, reduzindo o risco de não conformidade com a legislação.

Outro ponto relevante é que a taxonomia oferece uma visão geral dos requisitos de privacidade, facilitando a identificação de lacunas e oportunidades de melhoria nas aplicações em análise. Ao organizar os requisitos em categorias, os desenvolvedores e gerentes de projetos podem visualizar de forma mais clara as áreas em que suas aplicações estão mais ou menos aderentes às normas de privacidade. Isso possibilita o direcionamento de esforços para aprimorar as medidas de privacidade nas áreas que mais precisam de atenção.

Além disso, o uso da taxonomia permite que as avaliações de conformidade sejam mais consistentes e padronizadas. Ao seguir a estrutura definida pela taxonomia, diferentes equipes de desenvolvimento e projetos podem conduzir suas análises de maneira uniforme, garantindo resultados mais precisos e comparáveis. Essa padronização também facilita a comunicação entre diferentes stakeholders, como auditores, reguladores e clientes, que poderão entender melhor os relatórios de conformidade produzidos com base na taxonomia. No entanto, uma sugestão de melhoria é observada na identificação de uma possível duplicidade entre os requisitos RQ091 e RQ088. Recomenda-se uma revisão e consolidação desses requisitos, a fim de evitar redundâncias e facilitar a compreensão e aplicação da taxonomia.

É importante ressaltar que este estudo apresenta algumas limitações. Um aspecto relevante a ser mencionado é que a avaliação da implementação de requisitos de privacidade foi realizada considerando a perspectiva do usuário, sem acesso aos códigos fonte dos sistemas analisados. Essa limitação implica que a análise se baseou nas informações disponíveis para os usuários nos documentos oficiais, como políticas de privacidade, notas informativas e termos de uso. Portanto, não foi possível realizar uma avaliação em profundidade do código-fonte dos sistemas selecionados.

Além disso, a falta de acesso aos códigos também pode ter limitado a identificação de possíveis vulnerabilidades de segurança ou problemas na implementação dos requisitos de privacidade.

Dessa forma, é importante considerar que o estudo se concentrou principalmente na perspectiva do usuário e nas informações fornecidas pelos sistemas avaliados. Recomenda-se que estudos futuros possam abordar a análise do código-fonte ou considerar outras abordagens complementares para uma avaliação mais abrangente da implementação de requisitos de privacidade em sistemas de saúde.

Este estudo contribui para o desenvolvimento de aplicações de saúde mais adequadas do ponto de vista da privacidade e proteção de dados, promovendo a conscientização sobre a importância desses aspectos na área da saúde e fornecendo diretrizes para aprimorar a conformidade das aplicações com as normas vigentes. As sugestões em pontos específicos das aplicações analisadas permitem uma melhoria significativa na garantia da privacidade dos usuários, tornando-as mais confiáveis e alinhadas com as legislações vigentes.

Uma sugestão para trabalhos futuros é a criação de uma ferramenta para auxiliar na avaliação de requisitos de privacidade, considerando a taxonomia proposta por Ferrão (2022). Essa ferramenta poderia automatizar parte do processo de análise, agilizando e facilitando a verificação da conformidade das aplicações com as normas de privacidade e proteção de dados. Além disso, Recomenda-se que estudos futuros possam abordar a análise do código-fonte ou considerar outras abordagens complementares para uma avaliação mais abrangente da implementação de requisitos de privacidade em sistemas de saúde.

Referências

ANTóN, A. Goal-based requirements analysis. In: . [S.l.: s.n.], 1996. p. 136–144. ISBN 0-8186-7252-8. Citado na página 46.

BARNES, S. Data privacy management, autonomous spontaneous security, and security by design. In: _____. *Complexity in Information Systems Development*. [S.l.]: Springer, 2013. p. 59–69. Citado 2 vezes nas páginas 43 e 44.

BAYONA-ORÉ, S. et al. Critical success factors taxonomy for software process deployment. *Software Quality Journal*, Springer, v. 22, p. 21–48, 2014. Citado 2 vezes nas páginas 44 e 45.

Brasil. *Constituição da República Federativa do Brasil*. Brasília, DF: Presidência da República, 1988. Disponível em: <https://normas.leg.br/?urn=urn:lex:br:federal:constituicao:1988-10-05;1988#/con1988_05.10.1988/index.asp>. Citado 2 vezes nas páginas 34 e 38.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Citado na página 34.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Citado 13 vezes nas páginas 27, 31, 34, 35, 36, 37, 41, 45, 46, 51, 52, 53 e 121.

CAETANO, J. V. L. O regulamento geral de proteção de dados (gdpr). *Cadernos Eletrônicos Direito Internacional Sem Fronteiras*, v. 2, n. 1, p. e20200111–e20200111, 2020. Citado na página 31.

CASTRO, M. F. R. d. Levantamento de boas práticas e desafios na elicitação de requisitos de software. 2015. Citado 2 vezes nas páginas 39 e 42.

CEPETIC.BR. *Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. Comitê Gestor da Internet no Brasil, 2021. [Acesso em: 06 mar. 2023]. Disponível em: <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/>. Citado na página 27.

COSTA, E. M. V. d. *Processo de solicitação de acesso aos dados em um departamento da saúde, sob a ótica da LGPD*. Dissertação de mestrado — Universidade de São Paulo, 2022. Citado na página 37.

COSTA, J. M. da; ROSA, S. de O. Lei geral de proteção de dados aplicada à saúde. *Humanidades & Inovação*, v. 8, n. 45, p. 136–143, 2021. Citado na página 37.

DIGITAL, O. *Brasil é o 6º país com mais vazamentos de dados no planeta, aponta levantamento*. 2022. <https://olhardigital.com.br/2022/03/17/seguranca/brasil-e-o-6o-pais-com-mais-vazamentos-de-dados-no-planeta-aponta-levantamento/>. Acesso em: 26 fev. 2023. Citado 2 vezes nas páginas 37 e 53.

European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. European Commission, 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Citado 5 vezes nas páginas 31, 32, 33, 34 e 41.

FERRÃO, S. É. R. Proposta de uma taxonomia de requisitos de privacidade baseada na lgpd e iso/iec 29100: aplicação prática no open banking brasil. 2022. Citado 26 vezes nas páginas 11, 13, 15, 27, 28, 43, 45, 46, 47, 48, 49, 51, 52, 53, 54, 57, 58, 75, 76, 95, 96, 121, 122, 123, 245 e 257.

FIOCRUZ. Disponível online: https://observatoriohospitalar.fiocruz.br/conteudo-interno/sites-e-aplicativos-ajudam-monitorar-pandemia-de-covid-19-no-brasil-e-no-mundo. *Acessado em abril*, 2023. Citado 2 vezes nas páginas 31 e 53.

FRETTA, D. d. S. Lgpd: principais aspectos e sua implementação na área da saúde. 2021. Citado 2 vezes nas páginas 35 e 37.

GERHARDT, T.; SILVEIRA, D. *Métodos de pesquisa*. 1. ed. Porto Alegre: Editora da UFRGS, 2009. 120 p. Citado 2 vezes nas páginas 51 e 52.

GIL, A. *Como Elaborar Projetos de Pesquisa*. 6. ed. Brasil: Atlas, 2017. 192 p. ISBN 9788597012613. Citado na página 51.

ISO/IEC. *Information technology – Security techniques – Privacy framework*. Genebra: ISO/IEC, 2011. Citado 9 vezes nas páginas 27, 31, 38, 41, 45, 46, 51, 53 e 121.

JÚNIOR, Á. C.; VASCONCELOS, A. P. V. de; SILVA, S. V. Análise comparativa de métodos de elicitação de requisitos de software a partir de modelos de processos de negócio. Citado na página 40.

KITCHENHAM, B.; CHARTERS, S. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. [S.l.], 2007. Citado na página 46.

LI, H.; YU, L.; HE, W. *The impact of GDPR on global technology development*. [S.l.]: Taylor & Francis, 2019. 1–6 p. Citado na página 32.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. *Revista de Direito, Tecnologia e Inovação*, FGV, v. 8, n. 2, p. 101–128, 2021. Citado na página 31.

MARTINS, G. M.; TELES, C. A. C. A telemedicina na saúde suplementar e a responsabilidade civil do médico no tratamento de dados à luz da lgpd. *REI-REVISTA ESTUDOS INSTITUCIONAIS*, v. 7, n. 1, p. 182–197, 2021. Citado na página 37.

MENDES, L. M.; ROSA, F. de F.; BONACIN, R. Uma revisão sobre o uso da semiótica na análise e especificação de requisitos de privacidade. *Anais do WCF*, v. 6, p. 31–36, 2019. Citado na página 44.

Ministério da Saúde. *Acessar a plataforma móvel de serviços digitais do Ministério da Saúde*. 2023. <https://www.gov.br/pt-br/servicos/acessar-a-plataforma-movel-de-servicos-digitais-do-ministerio-da-saude>. Acesso em: 26 mar. 2023. Citado na página 54.

MOB, S. *SAÚDE MOB*. 2022. <https://www.saudemob.com.br/>. Acesso em: 26 mar. 2023. Citado na página 54.

NEVES, R. d. A. P. Gdpr e lgpd: estudo comparativo. 2021. Citado na página 31.

Presidência da República Federativa do Brasil. *Emenda Constitucional nº 115/2022*. 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Citado na página 34.

PRESSMAN, R. S.; MAXIM, B. R. *Engenharia de software: uma abordagem profissional*. 9. ed. [S.l.]: AMGH, 2016. Citado 7 vezes nas páginas 39, 40, 41, 42, 43, 44 e 45.

Sabin. *Sabin Medicina Diagnóstica*. 2022. <https://www.sabin.com.br/o-sabin/quem-somos/?cidade=brasilia-df>. Acesso em: 26 mar. 2023. Citado na página 55.

SILVA, S. Engenharia de requisitos: Uma análise das técnicas de levantamento de requisitos. *Belo Horizonte. Disponível em:. Acessado em*, v. 28, 2020. Citado 2 vezes nas páginas 39 e 40.

SILVA, T. V. S. O tratamento de dados pessoais sensíveis nas empresas do setor da saúde, segundo a lei geral de proteção de dados (lgpd). Universidade do Vale do Rio dos Sinos, 2020. Citado na página 34.

SOARES, F. R. Consentimento no direito da saúde nos contextos de atendimento médico e de lgpd. *Revista IBERC*, v. 4, n. 2, p. 18–46, 2021. Citado na página 34.

SOLOVE, D. J. A taxonomy of privacy. *University of Pennsylvania Law Review*, JSTOR, v. 154, n. 3, p. 477–564, 2006. Citado 2 vezes nas páginas 43 e 44.

SOMMERVILLE, I. *Engenharia de software*. 9. ed. São Paulo: Pearson Education do Brasil, 2011. Citado 6 vezes nas páginas 15, 39, 40, 41, 42 e 43.

UNTERKALMSTEINER, M.; FELDT, R.; GORSCHEK, T. A taxonomy for requirements engineering and software test alignment. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, ACM New York, NY, USA, v. 23, n. 2, p. 1–38, 2014. Citado na página 45.

USMAN, M. et al. Taxonomies in software engineering: A systematic mapping study and a revised taxonomy development method. *Information and Software Technology*, Elsevier, v. 85, p. 43–59, 2017. Citado 2 vezes nas páginas 44 e 45.

VEGAS, S.; JURISTO, N.; BASILI, V. R. Maturing software engineering knowledge through classifications: A case study on unit testing techniques. *IEEE Transactions on Software Engineering*, IEEE, v. 35, n. 4, p. 551–565, 2009. Citado na página 44.

WARREN, S.; BRANDEIS, L. The right to privacy. *civilistica.com*, v. 2, n. 3, p. 1–22, out. 2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/127>. Citado na página 31.

Apêndices

APÊNDICE A – Modelo de questionário

A seguir está o questionário utilizado para coleta de dados, contendo quatro opções: sim, parcial, não e inválido. A opção "sim" é escolhida quando é possível identificar o requisito completamente. A opção "parcial" é escolhida quando é possível identificar o requisito de maneira parcial. A opção "não" é escolhida quando o requisito não foi implementado. E a opção "inválido" é escolhida quando não foi possível implementar o requisito devido à falta de recursos ou porque não se aplica ao contexto analisado.

1. É possível coletar e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, específica e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

2. É possível limitar o uso de dados à finalidade da coleta a menos que uma finalidade seja explicitamente exigida por lei aplicável?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

3. É possível verificar se os dados são apagados sempre que a finalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

4. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador?
( ) Sim

( ) Não
( ) Parcial
( ) Inválido

5. É possível verificar se o tratamento de dados pessoais é finalizado no fim do período de tratamento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

6. É possível verificar se está disponível em área pública os procedimentos necessários para revogação do consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

7. É possível verificar se é informado que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

8. É possível verificar se é coletado somente dos dados pessoais estritamente necessários para a finalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

9. É possível verificar se o tratamento de dados é permitido para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação?
( ) Sim
( ) Não

( ) Parcial
( ) Inválido

10. É possível verificar se o controlador de dados é permitido de fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exigindo a proteção dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

11. É possível verificar se o controlador de dados é permitido fazer o tratamento de dados pessoais para a proteção do crédito?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

12. É possível verificar se é dispensado a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

13. É possível verificar se é possível obter o consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

14. É possível verificar se é permitido ao controlador que seja feito o tratamento de dados para a finalidade de apoio e promoção a atividades?
( ) Sim

( ) Não
( ) Parcial
( ) Inválido

15. É possível verificar se é permitido o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

16. É possível verificar se é possível coletar consentimento específico concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

17. É possível verificar se é possível coletar dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

18. É possível verificar se é realizado todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

19. É possível verificar se é permitido a conservação dos dados pessoais após o

término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

20. É possível verificar se é tornada pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

21. É possível verificar se é informado ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

22. É possível verificar se é notificado o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

23. É possível verificar se é fornecido por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades públicas?

( ) Sim
( ) Não
( ) Parcial
( ) Inválido

24. É possível verificar se é garantido que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

25. É possível verificar se é permitido por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

26. É possível verificar se é possível usar ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

27. É possível verificar se é vedado o tratamento de dados mediante vicio de con-

sentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

28. É possível verificar se é permitido ao titular a qualquer momento e mediante requisição, a revogação do consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

29. É possível verificar se é permitido que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

30. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

31. É possível verificar se é permitido o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

32. É possível verificar se é permitido o tratamento de dados pessoais sensíveis

sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

33. É possível verificar se é permitido o tratamento de dados pessoais mediante o consentimento expresso do titular de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

34. É possível verificar se é comunicado ao titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

35. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

36. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis?
( ) Sim
( ) Não

( ) Parcial
( ) Inválido

37. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

38. É possível verificar se é permitido a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

39. É possível verificar se é assegurado a adoção de um princípio de "necessidade de conhecimento", ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções oficiais no âmbito do propósito legítimo do processamento de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

40. É possível verificar se é informado a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

41. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

42. É possível verificar se é permitido a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

43. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

44. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

45. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

46. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

47. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

48. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

49. É possível verificar se é fornecido aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

50. É possível verificar se é permitido ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

51. É possível verificar se é garantido que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a finalidade de uso?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

52. É possível verificar se é permitido que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto específico?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

53. É possível verificar se é fornecido qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

54. É possível verificar se é por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado?
( ) Sim

( ) Não
( ) Parcial
( ) Inválido

55. É possível verificar se é estabelecido procedimentos de coleta de dados para ajudar a garantir precisão e qualidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

56. É possível verificar se é estabelecido mecanismos de controle para verificar periodicamente a precisão e a qualidade das informações coletadas e armazenadas?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

57. É possível verificar se os dados são armazenados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

58. É possível verificar se é apresentado informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

59. É possível verificar se é informado ao titular dos dados, antes de qualquer novo

processamento, de forma explícita, o teor das alterações de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; e informações de contato do controlador, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

60. É possível verificar se é permitido e providenciado ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a confirmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, a critério do titular?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

61. É possível verificar se é permitido ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

62. É possível verificar se é apresentada a finalidade, a boa-fé e o interesse público que justificaram o tratamento de dados pessoais de acesso público?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

63. É possível verificar se é permitido que o requerimento de informações sobre

seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

64. É possível verificar se é os dados pessoais são armazenados em formato que favoreça o exercício do direito de acesso por parte do titular de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

65. É possível verificar se é informado aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especificidades exigidas para a finalidade especificada no consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

66. É possível verificar se é usado uma linguagem para esta especificação que seja clara e apropriadamente adaptada a circunstâncias?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

67. É possível verificar se é fornecido aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

68. É possível verificar se é divulgado as opções e os meios oferecidos pelo contro-

lador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

69. É possível verificar se é permitido que o titular de dados entenda os requisitos especificados de retenção e eliminação de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

70. É possível verificar se é o encarregado é indicado para tratamento de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

71. É possível verificar se é impedido a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

72. É possível bloquear os dados pessoais a que se refere a infração até a sua regularização?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

73. É possível verificar se os dados pessoais são apagados ao que se refere a infra-

ção quando aplicável e de forma legal?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

74. É possível verificar se é implementado as preferências do titular de dados conforme expresso em seu consentimento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

75. É possível verificar se é permitido o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por entidades sanitárias?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

76. É possível verificar se é permitido o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

77. É possível verificar se é garantido que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

78. É possível verificar se é protegido as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a inte-

gridade, confidencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modificação, divulgação ou perda ao longo do todo o seu ciclo de vida?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

79. É possível verificar se é assegurado esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

80. É possível verificar se é implementado controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

81. é possível limitar o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

82. É possível verificar se riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

83. É possível verificar se há submissão dos controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo ?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

84. É possível verificar se há controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

85. É possível verificar se é desenvolvido e mantido avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

86. É possível verificar se é selecionado processadores de dados que forneçam garantias suficientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles ?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

87. É possível verificar se é o consentimento do titular é tornado nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim

( ) Não
( ) Parcial
( ) Inválido

88. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

89. É possível verificar se é o consentimento do titular é tornado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

90. É possível verificar se é protegido a divulgação de dados pessoais em resultados de pesquisas de saúde?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

91. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

92. É possível verificar se é ocorre a proteção para que os dados pessoais do titular

não sejam utilizados em seu prejuízo?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

93. É possível verificar se é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

94. É possível verificar se é disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

95. É possível verificar se ocorre a notificação de todas as partes interessadas de privacidade relevantes sobre violações de privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

96. É possível verificar se é permitido que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e eficazes, como retificação, expurgo ou restituição se ocorrer uma violação de privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

97. É possível verificar se é finalizado o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional?

( ) Sim
( ) Não
( ) Parcial
( ) Inválido

98. É possível verificar se ocorre notificação ao titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

99. É possível notificar o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

100. É possível verificar se é fornecido ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

101. É possível verificar se é apresentado quando aplicável explicações suficientes para a necessidade de processar dados sensíveis?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

102. É possível verificar se é mantido em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular e as formas para o seu

acesso?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

103. É possível verificar se é mantido em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

104. É possível verificar se é mantido em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

105. É possível verificar se é mantido em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

106. É possível verifica se é disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

107. É possível verificar se é mantido em área pública os procedimentos necessários

para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

108. É possível verificar se é mantido em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

109. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

110. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

111. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

112. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

113. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

114. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

115. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

116. É possível verificar se é adotado medidas para garantir a transparência do tratamento de dados por parte do controlador?
( ) Sim

( ) Não
( ) Parcial
( ) Inválido

117. É possível verificar se é apresentado a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

118. É possível verificar se é atendido a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

119. É possível verificar se é garantido a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

120. É possível verificar se é comunicado à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

121. É possível verificar se é implementado os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

122. É possível verificar se é publicizado a infração após devidamente apurada e confirmada a sua ocorrência?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

123. É possível verificar se é documentado e comunicado, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

124. É possível verificar se é atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

125. É possível verificar se é fornecido treinamento adequado para o pessoal do controlador de dados que terá acesso a informações?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

126. É possível verificar se é estabelecido procedimentos internos eficientes de tratamento de reclamações e reparação para uso pelos titulares de dados?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

127. É possível verificar se há ponderação nos procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

128. É possível verificar se há verificação e demonstração que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados confiáveis?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

129. É possível garantir que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados)?
( ) Sim
( ) Não
( ) Parcial
( ) Inválido

APÊNDICE B – Aplicação do questionário no aplicativo Conecte SUS

A seguir está o questionário utilizado para coleta de dados na aplicação Conecte Sus.

1. É possível coletar e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, específica e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

2. É possível limitar o uso de dados à finalidade da coleta a menos que uma finalidade seja explicitamente exigida por lei aplicável?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

3. É possível verificar se os dados são apagados sempre que a finalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

4. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador?
( ) Sim
( ) Não
(x) Parcial

( ) Inválido

5. É possível verificar se o tratamento de dados pessoais é finalizado no fim do período de tratamento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

6. É possível verificar se está disponível em área pública os procedimentos necessários para revogação do consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

7. É possível verificar se é informado que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

8. É possível verificar se é coletado somente dos dados pessoais estritamente necessários para a finalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

9. É possível verificar se o tratamento de dados é permitido para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

10. É possível verificar se o controlador de dados é permitido de fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exigindo a proteção dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

11. É possível verificar se o controlador de dados é permitido fazer o tratamento de dados pessoais para a proteção do crédito?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

12. É possível verificar se é dispensado a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

13. É possível verificar se é possível obter o consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

14. É possível verificar se é permitido ao controlador que seja feito o tratamento de dados para a finalidade de apoio e promoção a atividades?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

15. É possível verificar se é permitido o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

16. É possível verificar se é possível coletar consentimento específico concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

17. É possível verificar se é possível coletar dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

18. É possível verificar se é realizado todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

19. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?

( ) Sim
(x) Não
( ) Parcial
( ) Inválido

20. É possível verificar se é tornada pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

21. É possível verificar se é informado ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

22. É possível verificar se é notificado o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

23. É possível verificar se é fornecido por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades públicas?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

24. É possível verificar se é garantido que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

25. É possível verificar se é permitido por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

26. É possível verificar se é possível usar ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

27. É possível verificar se é vedado o tratamento de dados mediante vicio de consentimento?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

28. É possível verificar se é permitido ao titular a qualquer momento e mediante requisição, a revogação do consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

29. É possível verificar se é permitido que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

30. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

31. É possível verificar se é permitido o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

32. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador?

( ) Sim
( ) Não
( ) Parcial
(x) Inválido

33. É possível verificar se é permitido o tratamento de dados pessoais mediante o consentimento expresso do titular de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

34. É possível verificar se é comunicado ao titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

35. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

36. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

37. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

38. É possível verificar se é permitido a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

39. É possível verificar se é assegurado a adoção de um princípio de "necessidade de conhecimento", ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções oficiais no âmbito do propósito legítimo do processamento de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

40. É possível verificar se é informado a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

41. É possível verificar se é permitido o tratamento de dados pessoais sensíveis

sem fornecimento de consentimento do titular, quando indispensável para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

42. É possível verificar se é permitido a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

43. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

44. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

45. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional

entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

46. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

47. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

48. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

49. É possível verificar se é fornecido aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

50. É possível verificar se é permitido ao titular dos dados solicitar a revisão de

decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

51. É possível verificar se é garantido que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a finalidade de uso?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

52. É possível verificar se é permitido que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto específico?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

53. É possível verificar se é fornecido qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

54. É possível verificar se é por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

55. É possível verificar se é estabelecido procedimentos de coleta de dados para ajudar a garantir precisão e qualidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

56. É possível verificar se é estabelecido mecanismos de controle para verificar periodicamente a precisão e a qualidade das informações coletadas e armazenadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

57. É possível verificar se os dados são armazenados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

58. É possível verificar se é apresentado informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

59. É possível verificar se é informado ao titular dos dados, antes de qualquer novo processamento, de forma explícita, o teor das alterações de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial;

identificação do controlador; e informações de contato do controlador, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

60. É possível verificar se é permitido e providenciado ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a confirmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, a critério do titular?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

61. É possível verificar se é permitido ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

62. É possível verificar se é apresentada a finalidade, a boa-fé e o interesse público que justificaram o tratamento de dados pessoais de acesso público?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

63. É possível verificar se é permitido que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento?

(x) Sim
( ) Não
( ) Parcial
( ) Inválido

64. É possível verificar se é os dados pessoais são armazenados em formato que favoreça o exercício do direito de acesso por parte do titular de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

65. É possível verificar se é informado aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especificidades exigidas para a finalidade especificada no consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

66. É possível verificar se é usado uma linguagem para esta especificação que seja clara e apropriadamente adaptada a circunstâncias?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

67. É possível verificar se é fornecido aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

68. É possível verificar se é divulgado as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações?

(x) Sim
( ) Não
( ) Parcial
( ) Inválido

69. É possível verificar se é permitido que o titular de dados entenda os requisitos especificados de retenção e eliminação de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

70. É possível verificar se é o encarregado é indicado para tratamento de dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

71. É possível verificar se é impedido a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

72. É possível bloquear os dados pessoais a que se refere a infração até a sua regularização?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

73. É possível verificar se os dados pessoais são apagados ao que se refere a infração quando aplicável e de forma legal?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

74. É possível verificar se é implementado as preferências do titular de dados conforme expresso em seu consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

75. É possível verificar se é permitido o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por entidades sanitárias?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

76. É possível verificar se é permitido o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

77. É possível verificar se é garantido que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

78. É possível verificar se é protegido as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, confidencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modificação, divulgação ou perda ao longo

do todo o seu ciclo de vida?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

79. É possível verificar se é assegurado esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

80. É possível verificar se é implementado controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

81. é possível limitar o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

82. É possível verificar se riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

83. É possível verificar se há submissão dos controles a revisão e reavaliação pe-

riódicas em um gerenciamento contínuo de riscos de segurança processo ?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

84. É possível verificar se há controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

85. É possível verificar se é desenvolvido e mantido avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

86. É possível verificar se é selecionado processadores de dados que forneçam garantias suficientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles ?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

87. É possível verificar se é o consentimento do titular é tornado nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
(x) Parcial

( ) Inválido

88. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

89. É possível verificar se é o consentimento do titular é tornado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

90. É possível verificar se é protegido a divulgação de dados pessoais em resultados de pesquisas de saúde?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

91. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

92. É possível verificar se é ocorre a proteção para que os dados pessoais do titular não sejam utilizados em seu prejuízo?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

93. É possível verificar se é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

94. É possível verificar se é disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

95. É possível verificar se ocorre a notificação de todas as partes interessadas de privacidade relevantes sobre violações de privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

96. É possível verificar se é permitido que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e eficazes, como retificação, expurgo ou restituição se ocorrer uma violação de privacidade?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

97. É possível verificar se é finalizado o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

98. É possível verificar se ocorre notificação ao titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

99. É possível notificar o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

100. É possível verificar se é fornecido ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

101. É possível verificar se é apresentado quando aplicável explicações suficientes para a necessidade de processar dados sensíveis?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

102. É possível verificar se é mantido em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular e as formas para o seu acesso?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

103. É possível verificar se é mantido em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

104. É possível verificar se é mantido em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

105. É possível verificar se é mantido em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

106. É possível verifica se é disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

107. É possível verificar se é mantido em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?

(x) Sim
( ) Não
( ) Parcial
( ) Inválido

108. É possível verificar se é mantido em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

109. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

110. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

111. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

112. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade

dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

113. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

114. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

115. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

116. É possível verificar se é adotado medidas para garantir a transparência do tratamento de dados por parte do controlador?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

117. É possível verificar se é apresentado a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

118. É possível verificar se é atendido a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

119. É possível verificar se é garantido a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

120. É possível verificar se é comunicado à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

121. É possível verificar se é implementado os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos

e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

122. É possível verificar se é publicizado a infração após devidamente apurada e confirmada a sua ocorrência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

123. É possível verificar se é documentado e comunicado, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

124. É possível verificar se é atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

125. É possível verificar se é fornecido treinamento adequado para o pessoal do controlador de dados que terá acesso a informações?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

126. É possível verificar se é estabelecido procedimentos internos eficientes de tratamento de reclamações e reparação para uso pelos titulares de dados?

( ) Sim
( ) Não
( ) Parcial
(x) Inválido

127. É possível verificar se há ponderação nos procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

128. É possível verificar se há verificação e demonstração que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados confiáveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

129. É possível garantir que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados)?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

APÊNDICE C – Aplicação do questionário no aplicativo Sabin

A seguir está o questionário respondido para a aplicação Sabin.

1. É possível coletar e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, específica e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

2. É possível limitar o uso de dados à finalidade da coleta a menos que uma finalidade seja explicitamente exigida por lei aplicável?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

3. É possível verificar se os dados são apagados sempre que a finalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

4. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

5. É possível verificar se o tratamento de dados pessoais é finalizado no fim do período de tratamento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

6. É possível verificar se está disponível em área pública os procedimentos necessários para revogação do consentimento?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

7. É possível verificar se é informado que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

8. É possível verificar se é coletado somente dos dados pessoais estritamente necessários para a finalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

9. É possível verificar se o tratamento de dados é permitido para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

10. É possível verificar se o controlador de dados é permitido de fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exigindo a proteção dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

11. É possível verificar se o controlador de dados é permitido fazer o tratamento de dados pessoais para a proteção do crédito?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

12. É possível verificar se é dispensado a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

13. É possível verificar se é possível obter o consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

14. É possível verificar se é permitido ao controlador que seja feito o tratamento de dados para a finalidade de apoio e promoção a atividades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

15. É possível verificar se é permitido o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

16. É possível verificar se é possível coletar consentimento específico concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

17. É possível verificar se é possível coletar dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

18. É possível verificar se é realizado todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

19. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim

( ) Não
(x) Parcial
( ) Inválido

20. É possível verificar se é tornada pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

21. É possível verificar se é informado ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

22. É possível verificar se é notificado o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

23. É possível verificar se é fornecido por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades públicas?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

24. É possível verificar se é garantido que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

25. É possível verificar se é permitido por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

26. É possível verificar se é possível usar ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

27. É possível verificar se é vedado o tratamento de dados mediante vicio de consentimento?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

28. É possível verificar se é permitido ao titular a qualquer momento e mediante requisição, a revogação do consentimento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

29. É possível verificar se é permitido que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

30. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

31. É possível verificar se é permitido o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

32. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

33. É possível verificar se é permitido o tratamento de dados pessoais mediante o consentimento expresso do titular de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

34. É possível verificar se é comunicado ao titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

35. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

36. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

37. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

38. É possível verificar se é permitido a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

39. É possível verificar se é assegurado a adoção de um princípio de "necessidade de conhecimento", ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções oficiais no âmbito do propósito legítimo do processamento de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

40. É possível verificar se é informado a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

41. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento

compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

42. É possível verificar se é permitido a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

43. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

44. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

45. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os

instrumentos de direito internacional?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

46. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

47. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

48. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

49. É possível verificar se é fornecido aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

50. É possível verificar se é permitido ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais

que afetem seus interesses?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

51. É possível verificar se é garantido que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a finalidade de uso?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

52. É possível verificar se é permitido que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto específico?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

53. É possível verificar se é fornecido qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

54. É possível verificar se é por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

55. É possível verificar se é estabelecido procedimentos de coleta de dados para ajudar a garantir precisão e qualidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

56. É possível verificar se é estabelecido mecanismos de controle para verificar periodicamente a precisão e a qualidade das informações coletadas e armazenadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

57. É possível verificar se os dados são armazenados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

58. É possível verificar se é apresentado informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

59. É possível verificar se é informado ao titular dos dados, antes de qualquer novo processamento, de forma explícita, o teor das alterações de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; e informações de contato do controlador, podendo o titular,

nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

60. É possível verificar se é permitido e providenciado ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a confirmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, a critério do titular?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

61. É possível verificar se é permitido ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

62. É possível verificar se é apresentada a finalidade, a boa-fé e o interesse público que justificaram o tratamento de dados pessoais de acesso público?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

63. É possível verificar se é permitido que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

64. É possível verificar se é os dados pessoais são armazenados em formato que favoreça o exercício do direito de acesso por parte do titular de dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

65. É possível verificar se é informado aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especificidades exigidas para a finalidade especificada no consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

66. É possível verificar se é usado uma linguagem para esta especificação que seja clara e apropriadamente adaptada a circunstâncias?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

67. É possível verificar se é fornecido aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

68. É possível verificar se é divulgado as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações?
( ) Sim

( ) Não
(x) Parcial
( ) Inválido

69. É possível verificar se é permitido que o titular de dados entenda os requisitos especificados de retenção e eliminação de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

70. É possível verificar se é o encarregado é indicado para tratamento de dados pessoais?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

71. É possível verificar se é impedido a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

72. É possível bloquear os dados pessoais a que se refere a infração até a sua regularização?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

73. É possível verificar se os dados pessoais são apagados ao que se refere a infração quando aplicável e de forma legal?
( ) Sim
( ) Não

(x) Parcial
( ) Inválido

74. É possível verificar se é implementado as preferências do titular de dados conforme expresso em seu consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

75. É possível verificar se é permitido o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por entidades sanitárias?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

76. É possível verificar se é permitido o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

77. É possível verificar se é garantido que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

78. É possível verificar se é protegido as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, confidencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modificação, divulgação ou perda ao longo do todo o seu ciclo de vida?

( ) Sim
( ) Não
( ) Parcial
(x) Inválido

79. É possível verificar se é assegurado esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

80. É possível verificar se é implementado controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

81. é possível limitar o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

82. É possível verificar se riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

83. É possível verificar se há submissão dos controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo ?

( ) Sim
( ) Não
( ) Parcial
(x) Inválido

84. É possível verificar se há controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

85. É possível verificar se é desenvolvido e mantido avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

86. É possível verificar se é selecionado processadores de dados que forneçam garantias suficientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles ?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

87. É possível verificar se é o consentimento do titular é tornado nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

88. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

89. É possível verificar se é o consentimento do titular é tornado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

90. É possível verificar se é protegido a divulgação de dados pessoais em resultados de pesquisas de saúde?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

91. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

92. É possível verificar se é ocorre a proteção para que os dados pessoais do titular não sejam utilizados em seu prejuízo?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

93. É possível verificar se é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

94. É possível verificar se é disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

95. É possível verificar se ocorre a notificação de todas as partes interessadas de privacidade relevantes sobre violações de privacidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

96. É possível verificar se é permitido que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e eficazes, como retificação, expurgo ou restituição se ocorrer uma violação de privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

97. É possível verificar se é finalizado o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

98. É possível verificar se ocorre notificação ao titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

99. É possível notificar o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

100. É possível verificar se é fornecido ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

101. É possível verificar se é apresentado quando aplicável explicações suficientes para a necessidade de processar dados sensíveis?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

102. É possível verificar se é mantido em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular e as formas para o seu acesso?
( ) Sim
( ) Não

(x) Parcial
( ) Inválido

103. É possível verificar se é mantido em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

104. É possível verificar se é mantido em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

105. É possível verificar se é mantido em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

106. É possível verifica se é disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

107. É possível verificar se é mantido em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim

( ) Não
(x) Parcial
( ) Inválido

108. É possível verificar se é mantido em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

109. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

110. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

111. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

112. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de

acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

113. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

114. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

115. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

116. É possível verificar se é adotado medidas para garantir a transparência do tratamento de dados por parte do controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

117. É possível verificar se é apresentado a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

118. É possível verificar se é atendido a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

119. É possível verificar se é garantido a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

120. É possível verificar se é comunicado à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

121. É possível verificar se é implementado os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados

pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

122. É possível verificar se é publicizado a infração após devidamente apurada e confirmada a sua ocorrência?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

123. É possível verificar se é documentado e comunicado, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

124. É possível verificar se é atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

125. É possível verificar se é fornecido treinamento adequado para o pessoal do controlador de dados que terá acesso a informações?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

126. É possível verificar se é estabelecido procedimentos internos eficientes de tratamento de reclamações e reparação para uso pelos titulares de dados?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

127. É possível verificar se há ponderação nos procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

128. É possível verificar se há verificação e demonstração que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados confiáveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

129. É possível garantir que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados)?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

APÊNDICE D – Aplicação do questionário no aplicativo Saúde Mob

A seguir está o questionário respondido para a aplicação Saúde Mob.

1. É possível coletar e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, específica e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

2. É possível limitar o uso de dados à finalidade da coleta a menos que uma finalidade seja explicitamente exigida por lei aplicável?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

3. É possível verificar se os dados são apagados sempre que a finalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

4. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

5. É possível verificar se o tratamento de dados pessoais é finalizado no fim do período de tratamento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

6. É possível verificar se está disponível em área pública os procedimentos necessários para revogação do consentimento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

7. É possível verificar se é informado que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

8. É possível verificar se é coletado somente dos dados pessoais estritamente necessários para a finalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

9. É possível verificar se o tratamento de dados é permitido para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

10. É possível verificar se o controlador de dados é permitido de fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exigindo a proteção dos dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

11. É possível verificar se o controlador de dados é permitido fazer o tratamento de dados pessoais para a proteção do crédito?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

12. É possível verificar se é dispensado a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

13. É possível verificar se é possível obter o consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

14. É possível verificar se é permitido ao controlador que seja feito o tratamento de dados para a finalidade de apoio e promoção a atividades?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

15. É possível verificar se é permitido o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

16. É possível verificar se é possível coletar consentimento específico concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

17. É possível verificar se é possível coletar dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

18. É possível verificar se é realizado todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

19. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

20. É possível verificar se é tornada pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

21. É possível verificar se é informado ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor?
( ) Sim
(x) Não
( ) Parcial
( ) Inválido

22. É possível verificar se é notificado o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

23. É possível verificar se é fornecido por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades públicas?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

24. É possível verificar se é garantido que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

25. É possível verificar se é permitido por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

26. É possível verificar se é possível usar ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

27. É possível verificar se é vedado o tratamento de dados mediante vicio de consentimento?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

28. É possível verificar se é permitido ao titular a qualquer momento e mediante requisição, a revogação do consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

29. É possível verificar se é permitido que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

30. É possível verificar se é permitido a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

31. É possível verificar se é permitido o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

32. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

33. É possível verificar se é permitido o tratamento de dados pessoais mediante o consentimento expresso do titular de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

34. É possível verificar se é comunicado ao titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

35. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

36. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

37. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

38. É possível verificar se é permitido a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

39. É possível verificar se é assegurado a adoção de um princípio de "necessidade de conhecimento", ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções oficiais no âmbito do propósito legítimo do processamento de dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

40. É possível verificar se é informado a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

41. É possível verificar se é permitido o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento

compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

42. É possível verificar se é permitido a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

43. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

44. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

45. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os

instrumentos de direito internacional?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

46. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

47. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

48. É possível verificar se é permitido a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

49. É possível verificar se é fornecido aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

50. É possível verificar se é permitido ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais

que afetem seus interesses?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

51. É possível verificar se é garantido que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a finalidade de uso?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

52. É possível verificar se é permitido que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto específico?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

53. É possível verificar se é fornecido qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

54. É possível verificar se é por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

55. É possível verificar se é estabelecido procedimentos de coleta de dados para ajudar a garantir precisão e qualidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

56. É possível verificar se é estabelecido mecanismos de controle para verificar periodicamente a precisão e a qualidade das informações coletadas e armazenadas?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

57. É possível verificar se os dados são armazenados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

58. É possível verificar se é apresentado informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

59. É possível verificar se é informado ao titular dos dados, antes de qualquer novo processamento, de forma explícita, o teor das alterações de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; e informações de contato do controlador, podendo o titular,

nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

60. É possível verificar se é permitido e providenciado ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a confirmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, a critério do titular?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

61. É possível verificar se é permitido ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

62. É possível verificar se é apresentada a finalidade, a boa-fé e o interesse público que justificaram o tratamento de dados pessoais de acesso público?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

63. É possível verificar se é permitido que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

64. É possível verificar se é os dados pessoais são armazenados em formato que favoreça o exercício do direito de acesso por parte do titular de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

65. É possível verificar se é informado aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especificidades exigidas para a finalidade especificada no consentimento?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

66. É possível verificar se é usado uma linguagem para esta especificação que seja clara e apropriadamente adaptada a circunstâncias?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

67. É possível verificar se é fornecido aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

68. É possível verificar se é divulgado as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

69. É possível verificar se é permitido que o titular de dados entenda os requisitos especificados de retenção e eliminação de dados?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

70. É possível verificar se é o encarregado é indicado para tratamento de dados pessoais?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

71. É possível verificar se é impedido a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

72. É possível bloquear os dados pessoais a que se refere a infração até a sua regularização?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

73. É possível verificar se os dados pessoais são apagados ao que se refere a infração quando aplicável e de forma legal?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

74. É possível verificar se é implementado as preferências do titular de dados conforme expresso em seu consentimento?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

75. É possível verificar se é permitido o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por entidades sanitárias?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

76. É possível verificar se é permitido o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

77. É possível verificar se é garantido que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

78. É possível verificar se é protegido as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, confidencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modificação, divulgação ou perda ao longo do todo o seu ciclo de vida?

( ) Sim
( ) Não
(x) Parcial
( ) Inválido

79. É possível verificar se é assegurado esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

80. É possível verificar se é implementado controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

81. é possível limitar o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

82. É possível verificar se riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

83. É possível verificar se há submissão dos controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo ?

( ) Sim
( ) Não
( ) Parcial
(x) Inválido

84. É possível verificar se há controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

85. É possível verificar se é desenvolvido e mantido avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

86. É possível verificar se é selecionado processadores de dados que forneçam garantias suficientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles ?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

87. É possível verificar se é o consentimento do titular é tornado nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

88. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

89. É possível verificar se é o consentimento do titular é tornado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

90. É possível verificar se é protegido a divulgação de dados pessoais em resultados de pesquisas de saúde?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

91. É possível verificar se é garantido a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

92. É possível verificar se é ocorre a proteção para que os dados pessoais do titular não sejam utilizados em seu prejuízo?
( ) Sim
( ) Não

( ) Parcial
(x) Inválido

93. É possível verificar se é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

94. É possível verificar se é disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

95. É possível verificar se ocorre a notificação de todas as partes interessadas de privacidade relevantes sobre violações de privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

96. É possível verificar se é permitido que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e eficazes, como retificação, expurgo ou restituição se ocorrer uma violação de privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

97. É possível verificar se é finalizado o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional?
( ) Sim
( ) Não
( ) Parcial

(x) Inválido

98. É possível verificar se ocorre notificação ao titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

99. É possível notificar o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

100. É possível verificar se é fornecido ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

101. É possível verificar se é apresentado quando aplicável explicações suficientes para a necessidade de processar dados sensíveis?
(x) Sim
( ) Não
( ) Parcial
( ) Inválido

102. É possível verificar se é mantido em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular e as formas para o seu acesso?
( ) Sim
( ) Não

(x) Parcial
( ) Inválido

103. É possível verificar se é mantido em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

104. É possível verificar se é mantido em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

105. É possível verificar se é mantido em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

106. É possível verifica se é disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

107. É possível verificar se é mantido em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
(x) Sim

( ) Não
( ) Parcial
( ) Inválido

108. É possível verificar se é mantido em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

109. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

110. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

111. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

112. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de

acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

113. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

114. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

115. É possível verificar se é possível obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

116. É possível verificar se é adotado medidas para garantir a transparência do tratamento de dados por parte do controlador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

117. É possível verificar se é apresentado a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

118. É possível verificar se é atendido a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

119. É possível verificar se é garantido a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

120. É possível verificar se é comunicado à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

121. É possível verificar se é implementado os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados

pessoais?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

122. É possível verificar se é publicizado a infração após devidamente apurada e confirmada a sua ocorrência?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

123. É possível verificar se é documentado e comunicado, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

124. É possível verificar se é atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade?
( ) Sim
( ) Não
(x) Parcial
( ) Inválido

125. É possível verificar se é fornecido treinamento adequado para o pessoal do controlador de dados que terá acesso a informações?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

126. É possível verificar se é estabelecido procedimentos internos eficientes de tratamento de reclamações e reparação para uso pelos titulares de dados?
( ) Sim

( ) Não
( ) Parcial
(x) Inválido

127. É possível verificar se há ponderação nos procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

128. É possível verificar se há verificação e demonstração que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados confiáveis?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

129. É possível garantir que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados)?
( ) Sim
( ) Não
( ) Parcial
(x) Inválido

Anexos

ANEXO A – Requisitos Identificados

Nesse anexo é apresentado a tabela com todos os 129 requisitos proposto por Ferrão (2022).

Tabela 41 – Requisitos de privacidade de acordo com a taxonomia proposta

Requisito	Descrição
RQ001	COLETAR e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, específica e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento
RQ002	LIMITAR o uso de dados à finalidade da coleta a menos que uma finalidade seja explicitamente exigida por lei aplicável
RQ003	APAGAR os dados sempre que a finalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las
RQ004	PERMITIR a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador
RQ005	FINALIZAR o tratamento de dados pessoais no fim do período de tratamento
RQ006	MANTER disponível em área pública os procedimentos necessários para revogação do consentimento
RQ007	INFORMAR que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador
RQ008	COLETAR somente dos dados pessoais estritamente necessários para a finalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse
RQ009	PERMITIR o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação

Continua na próxima página

Requisito	Descrição
RQ010	PERMITIR o controlador de dados fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exigindo a proteção dos dados pessoais
RQ011	PERMITIR o controlador de dados fazer o tratamento de dados pessoais para a proteção do crédito
RQ012	DISPENSAR a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados.
RQ013	OBTER consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais
RQ014	PERMITIR ao controlador que seja feito o tratamento de dados para a finalidade de apoio e promoção a atividades
RQ015	PERMITIR o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido
RQ016	COLETAR consentimento específico concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças
RQ017	COLETAR dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento
RQ018	REALIZAR todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador
RQ019	PERMITIR a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
RQ020	TORNAR pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições

Continua na próxima página

Requisito	Descrição
RQ021	INFORMAR ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor
RQ022	NOTIFICAR o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público
RQ023	FORNECER por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades públicas
RQ024	GARANTIR que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.
RQ025	PERMITIR por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades
RQ026	USAR ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas
RQ027	VEDAR o tratamento de dados mediante vicio de consentimento
RQ028	PERMITIR ao titular a qualquer momento e mediante requisição, a revogação do consentimento

Continua na próxima página

Requisito	Descrição
RQ029	PERMITIR que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular
RQ030	PERMITIR a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
RQ031	PERMITIR o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
RQ032	PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador
RQ033	PERMITIR o tratamento de dados pessoais mediante o consentimento expresso do titular de dados
RQ034	COMUNICAR o titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito
RQ035	PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos
RQ036	PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis
RQ037	PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

Continua na próxima página

Requisito	Descrição
RQ038	PERMITIR a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres
RQ039	ASSEGURAR a adoção de um princípio de "necessidade de conhecimento", ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções oficiais no âmbito do propósito legítimo do processamento de dados
RQ040	INFORMAR a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado
RQ041	PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública.
RQ042	PERMITIR a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos.
RQ043	PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política.
RQ044	PERMITIR a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.
RQ045	PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional.

Continua na próxima página

Requisito	Descrição
RQ046	PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro.
RQ047	PERMITIR a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência.
RQ048	PERMITIR a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional
RQ049	FORNECER aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais.
RQ050	PERMITIR ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.
RQ051	GARANTIR que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a finalidade de uso.
RQ052	PERMITIR que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto específico.
RQ053	FORNECER qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos
RQ054	VERIFICAR, por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado.
RQ055	ESTABELECER procedimentos de coleta de dados para ajudar a garantir precisão e qualidade
RQ056	ESTABELECER mecanismos de controle para verificar periodicamente a precisão e a qualidade das informações coletadas e armazenadas
RQ057	ARMAZENAR os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral

Continua na próxima página

Requisito	Descrição
RQ058	APRESENTAR as informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.
RQ059	INFORMAR ao titular dos dados, antes de qualquer novo processamento, de forma explícita, o teor das alterações de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; e informações de contato do controlador, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.
RQ060	PERMITIR e providenciar ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a confirmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, a critério do titular;
RQ061	PERMITIR ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.
RQ062	APRESENTAR a finalidade, a boa-fé e o interesse público que justificaram o tratamento de dados pessoais de acesso público.
RQ063	PERMITIR que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento
RQ064	ARMAZENAR os dados pessoais em formato que favoreça o exercício do direito de acesso por parte do titular de dados.
RQ065	INFORMAR aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especificidades exigidas para a finalidade especificada no consentimento.

Continua na próxima página

Requisito	Descrição
RQ066	USAR uma linguagem para esta especificação que seja clara e apropriadamente adaptada a circunstâncias.
RQ067	FORNECER aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados.
RQ068	DIVULGAR as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações.
RQ069	PERMITIR que o titular de dados entenda os requisitos especificados de retenção e eliminação de dados.
RQ070	INDICAR o encarregado pelo tratamento de dados pessoais.
RQ071	IMPEDIR a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades.
RQ072	BLOQUEAR os dados pessoais a que se refere a infração até a sua regularização.
RQ073	APAGAR os dados pessoais a que se refere a infração quando aplicável e legal.
RQ074	IMPLEMENTAR as preferências do titular de dados conforme expresso em seu consentimento.
RQ075	PERMITIR o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por entidades sanitárias.
RQ076	PERMITIR o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
RQ077	GARANTIR que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro
RQ078	PROTEGER as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, confidencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modificação, divulgação ou perda ao longo do todo o seu ciclo de vida.

Continua na próxima página

Requisito	Descrição
RQ079	ASSEGURAR esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício
RQ080	IMPLEMENTAR controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas
RQ081	LIMITAR o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções
RQ082	RESOLVER riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos
RQ083	SUBMETER os controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo
RQ084	POSSUIR controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade
RQ085	DESENVOLVER e manter avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade.
RQ086	SELECIONAR processadores de dados que forneçam garantias suficientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles.
RQ087	TORNAR o consentimento do titular nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
RQ088	GARANTIR a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento.

Continua na próxima página

Requisito	Descrição
RQ089	TORNAR o consentimento do titular nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
RQ090	PROTEGER a divulgação de dados pessoais em resultados de pesquisas de saúde.
RQ091	GARANTIR a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito por parte dos agentes de tratamento.
RQ092	PROTEGER para que os dados pessoais do titular não sejam utilizados em seu prejuízo.
RQ093	VEDAR às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.
RQ094	MANTER disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças.
RQ095	NOTIFICAR todas as partes interessadas de privacidade relevantes sobre violações de privacidade.
RQ096	PERMITIR que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e eficazes, como retificação, expurgo ou restituição se ocorrer uma violação de privacidade.
RQ097	FINALIZAR o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional.
RQ098	NOTIFICAR o titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente.
RQ099	NOTIFICAR o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência.

Continua na próxima página

Requisito	Descrição
RQ100	FORNECER ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial.
RQ101	APRESENTAR quando aplicável explicações suficientes para a necessidade de processar dados sensíveis.
RQ102	MANTER disponível em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular e as formas para o seu acesso.
RQ103	MANTER disponível em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados.
RQ104	MANTER disponível em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
RQ105	MANTER disponível em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
RQ106	MANTER disponível em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
RQ107	MANTER disponível em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
RQ108	MANTER disponível em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
RQ109	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados.
RQ110	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados.

Continua na próxima página

Requisito	Descrição
RQ111	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade
RQ112	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
RQ113	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas.
RQ114	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
RQ115	OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
RQ116	ADOTAR medidas para garantir a transparência do tratamento de dados por parte do controlador.
RQ117	APRESENTAR a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial.
RQ118	ATENDER a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial.
RQ119	GARANTIR a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador.

Continua na próxima página

Requisito	Descrição
RQ120	COMUNICAR à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador.
RQ121	IMPLEMENTAR os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados pessoais..
RQ122	PUBLICIZAR a infração após devidamente apurada e confirmada a sua ocorrência.
RQ123	DOCUMENTAR e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade.
RQ124	ATRIBUIR a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade.
RQ125	FORNECER treinamento adequado para o pessoal do controlador de dados que terá acesso a informações.
RQ126	ESTABELECER procedimentos internos eficientes de tratamento de reclamações e reparação para uso pelos titulares de dados.
RQ127	PONDERAR os procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido.
RQ128	VERIFICAR e demonstrar que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados confiáveis.
RQ129	GARANTIR que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados).

Retirado de Ferrão (2022)

ANEXO B – Consentimento

Neste anexo serão apresentados as imagens do aplicativo Conecte SUS para obter o consentimento do usuário. As imagens presentes na figura 10 foram obtidas no dia 16/04/2023.

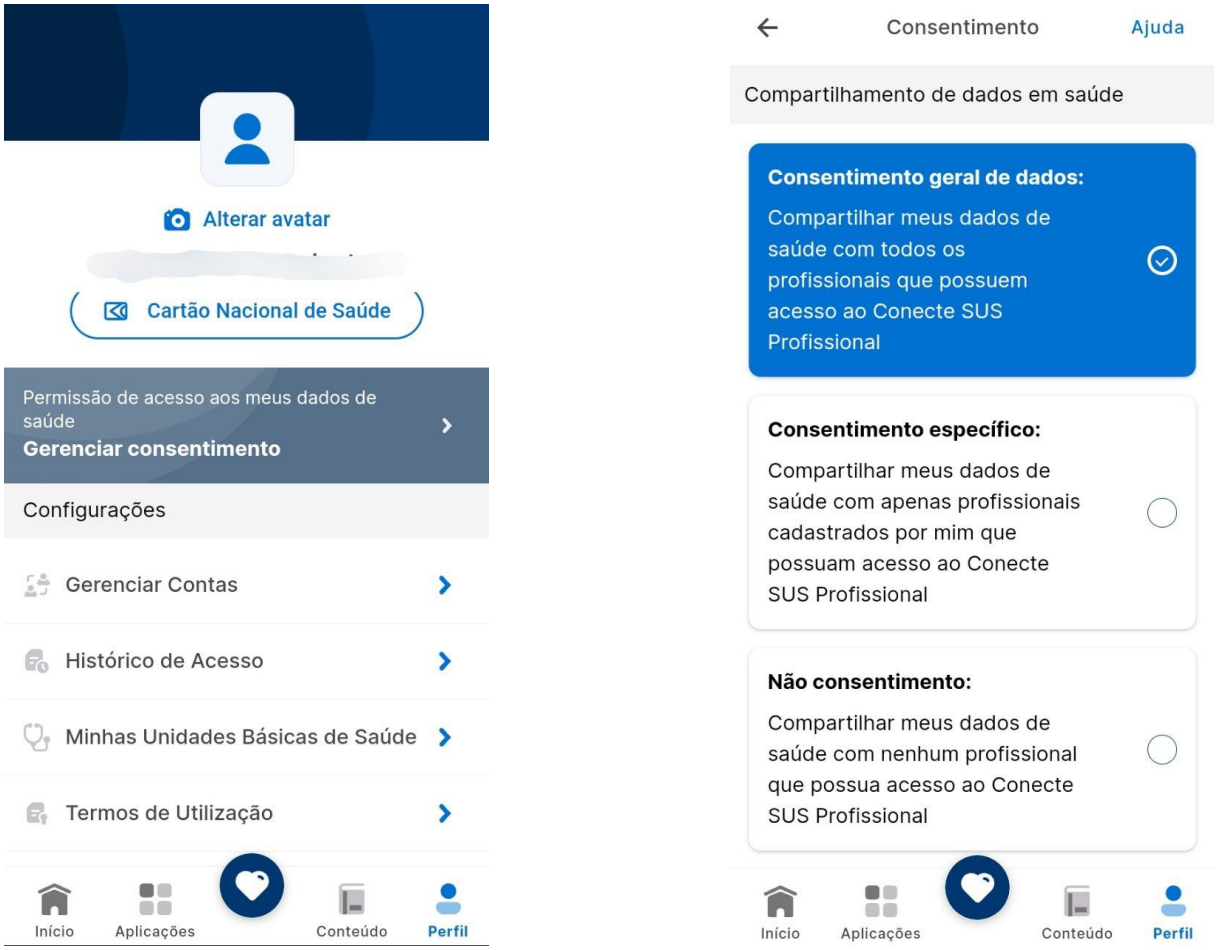

Figura 10 – Solicitação de consentimento para compartilhamento de dados.

De acordo com a figura 10, na aba **Perfil** do aplicativo Conecte SUS, há a opção de **Gerenciar consentimento**. Nessa seção do aplicativo, há 3 opções que são:

(Opção-1) **Consentimento geral de dados:** Compartilhar meus dados de saúde com todos os profissionais que possuem acesso ao Conecte SUS Profissional"

(Opção-2) **Consentimento específico:** Compartilhar meus dados de saúde com apenas profissionais cadastrados por mim que possuam acesso ao Conecte SUS Profissional.

(Opção-3) Não consentimento: Compartilhar meus dados de saúde com nenhum profissional que possua acesso ao Conecte SUS Profissional.

ANEXO C – Termo de uso

A seguir é apresentado o termo de uso disponibilizado pelo Conecte SUS transcrito para texto. A transcrição foi obtida no dia 16/04/2023.

Transcrição

C.1 ACEITAÇÃO DO TERMO DE USO

O presente Termo de Uso se refere a um contrato de adesão firmado entre o usuário e o fornecedor deste serviço, o Ministério da Saúde, localizado em Endereço: Ministério da Saúde - Esplanada dos Ministérios Bloco G, Zona Cívico-Administrativa, Brasília - DF - CEP 70058900. O uso deste serviço está condicionado à aceitação dos termos e das políticas associadas. O usuário deverá ler tais termos e políticas, certificar-se de havê-los entendido, estar consciente de todas as condições estabelecidas no Termo de Uso e se comprometer a cumpri-las. Ao utilizar o serviço, o usuário manifesta estar de acordo com relação ao conteúdo deste Termo de Uso e estará legalmente vinculado a todas as condições aqui previstas.

C.2 DEFINIÇÕES DO TERMO DE USO

Para os fins deste Termo de Uso, são aplicáveis as seguintes definições: Agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta. Agentes de Estado: Inclui órgãos e entidades da Administração pública além dos seus agentes públicos. Códigos maliciosos: São qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores. Sítios e aplicativos: Sítios e aplicativos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados. Terceiro: Pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico. Internet: Sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. Usuários: (ou "Usuário", quando individualmente considerado): Todas as pessoas naturais que utilizarem o serviço (citar o serviço).

C.3 ARCABOUÇO LEGAL

O arcabouço legal aplicável ao serviço Conecte SUS compreende os seguintes atos legislativos e normativos: - Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. - Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação: Regula o acesso a informações previsto na Constituição Federal. - Lei nº 13.460, de 26 de junho de 2017: Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. - Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. - Lei nº 13.444, de 11 de maio de 2017: Dispõe sobre a Identificação Civil Nacional (ICN). - Decreto nº 8.777, de 11 de maio de 2016: Institui a Política de Dados Abertos do Poder Executivo federal. - Decreto nº 7.724, de 16 de maio de 2012: Regulamenta a Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição. - Decreto nº 7.845, de 14 de novembro de 2012: Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. - Decreto nº 10.046, de 09 de outubro de 2019: Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. - Normas complementares do Gabinete de Segurança da Informação da Presidência (GSI/PR): Disciplinam a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. - Decreto nº 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. - Lei nº 12.737, de 30 de novembro de 2012:Dispõe sobre a tipificação criminal de delitos informáticos. - Portaria GM/MS nº 69, de 14 de Janeiro de 2021: Institui a obrigatoriedade de registro de aplicação de vacinas contra a Covid-19 nos sistemas de informação do Ministério da Saúde. - Portaria GM/MS nº 1.434, de 28 de maio de 2020: Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. - Portaria GM/MS nº 1.792, de 17 de julho de 2020: Altera a Portaria nº 356/GM/MS, de 11 de março de 2020, para dispor sobre a obrigatoriedade de notificação ao Ministério da Saúde de todos os resultados de testes diagnóstico para SARS-CoV-2 realizados por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional.

- Portaria GM/MS nº 1.768, de 30 de julho de 2021: Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). - Portaria GM/MS nº 3.632, de 21 de dezembro de 2020: Altera a Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017, para instituir a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28).

C.4 DESCRIÇÃO DO SERVIÇO

O Conecte SUS é o aplicativo oficial do Ministério da Saúde que permite ao cidadão acompanhar na palma de sua mão o seu histórico clínico, a partir das informações de saúde do Sistema Único de Saúde (SUS). Atualmente o aplicativo apresenta o registro de vacinas aplicadas e exames laboratoriais de Covid-19 realizados, internações, medicamentos dispensados, além da emissão do Certificado Nacional de Vacinação Covid-19 e da Carteira nacional de Vacinação. Os dados do aplicativo são em sua maioria provenientes da Rede Nacional de Dados em Saúde (RNDS), plataforma nacional de interoperabilidade de dados em saúde, que integra diferentes sistemas de informação alimentados por profissionais de saúde. Instituída pela portaria GM/MS n. 1.434, de 28 de maio de 2020, a Rede é um projeto estruturante do programa do Governo Federal para a transformação digital da saúde no Brasil e tem o objetivo de promover a troca de informações entre os pontos da Rede de Atenção à Saúde, permitindo a transição e continuidade do cuidado nos setores público e privado. O Conecte SUS também é disponível em na web https://conectesus-paciente.saude.gov.br/.

C.5 DIREITOS DO USUÁRIO DO SERVIÇO:

De acordo com a Lei nº 13.460, de 26 de junho de 2017, são direitos básicos do usuário:

Participação no acompanhamento da prestação e na avaliação dos serviços; Obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação; Acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados, observado o disposto no inciso X do caput do art. 5º da Constituição Federal e na Lei nº 12.527, de 18 de novembro de 2011; Proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011; Atuação integrada e sistêmica na expedição de atestados, certidões e documentos comprobatórios de regularidade; Obtenção de informações precisas e de fácil acesso nos locais de prestação do serviço, assim como sua disponibilização na internet, especialmente sobre:

Horário de funcionamento das unidades administrativas; Serviços prestados pelo

órgão ou entidade, sua localização exata e a indicação do setor responsável pelo atendimento ao público; Acesso ao agente público ou ao órgão encarregado de receber manifestações; Situação da tramitação dos processos administrativos em que figure como interessado; Valor das taxas e tarifas cobradas pela prestação dos serviços, contendo informações para a compreensão exata da extensão do serviço prestado.

C.6 RESPONSABILIDADES DO USUÁRIO

RQ087 - IP

6. Quais são as obrigações dos usuários que utilizam o serviço? O usuário se responsabiliza pela precisão e pela veracidade dos dados informados e reconhece que a inconsistência deles poderá implicar a impossibilidade de se utilizar o serviço Conecte SUS. Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros. O login e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer

RQ051 - I

hipótese, a alegação de uso indevido após o ato de compartilhamento. O usuário do serviço é responsável pela atualização dos seus dados pessoais e pelas consequências em caso de omissão ou erros nos dados fornecidos. O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários; de terceiros, inclusive direitos de propriedade intelectual; de sigilo; e de personalidade), que sejam causados à Administração Pública, a qualquer outro Usuário, ou ainda a qualquer terceiro, inclusive em virtude do descumprimento do disposto nestes Termos de Uso e Política de Privacidade ou de qualquer ato praticado a partir de seu acesso ao serviço. O Ministério da Saúde não poderá ser responsabilizado pelos seguintes fatos:

6.1 Equipamento infectado ou invadido por atacantes; 6.2 Equipamento avariado no momento do consumo de serviços; 6.3 Proteção do computador; 6.4 Proteção das informações baseadas nos computadores dos usuários; 6.5 Abuso de uso dos computadores dos usuários; 6.6 Monitoração clandestina do computador dos usuários; 6.7 Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários; 6.8 Perímetro inseguro. Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação, no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

C.7 RESPONSABILIDADE DA ADMINISTRAÇÃO PÚBLICA

RQ092 - IP

Quais são as responsabilidades da Administração Pública com meus dados? A Administração Pública se compromete a cumprir todas as legislações inerentes ao uso correto

dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados no serviço, bem como a garantir todos os direitos e garantias legais dos titulares dos dados. Ela também se obriga a promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas. É de responsabilidade da Administração Pública implementar controles de segurança para proteção dos dados pessoais dos titulares. A Administração Pública poderá, quanto às ordens judiciais de pedido das informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o Serviço ou de outra forma necessárias para cumprir com obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

C.8 POLÍTICA DE PRIVACIDADE

A Política de Privacidade estabelecida pelo Ministério da Saúde e utilizada pelo Conecte SUS trata da utilização de dados pessoais. Essa Política específica faz parte de forma inerente do presente Termo de Uso, ressaltando-se que os dados pessoais mencionados por esse Serviço serão tratados nos termos da legislação em vigor. Para mais informações acesse nossa política de privacidade em https://conectesus-paciente.saude.gov.br/menu/termo-politica

C.9 MUDANÇAS NO TERMO DE USO

Este Termo de Uso pode ser alterado? A presente versão (Conecte SUS) deste Termo de Uso foi atualizada pela última vez em: 22/07/2022. O editor se reserva o direito de modificar no site, a qualquer momento, as presentes normas, especialmente para adaptá-las às evoluções do serviço Conecte SUS, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Qualquer alteração e/ou atualização do Termos de Uso e da Política de Privacidade passará a vigorar a partir da data de sua publicação no sítio do serviço e deverá ser integralmente observada pelos Usuários.

C.10 INFORMAÇÕES PARA CONTATO

Em caso de dúvidas relacionadas ao Conecte SUS, entre em contato através dos nossos canais de atendimento: https://webatendimento.saude.gov.br/faq/conectesus.

C.11 FORO

Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida exclusivamente pela comarca/seção judiciária de Brasília, Distrito Federal, Tribunal de Justiça do Distrito Federal Sem prejuízo de qualquer outra via administrativa ou judicial disponível, todos os titulares de dados pessoais têm direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados (ANPD).

ANEXO D – Política de privacidade

A seguir é apresentado a transcrição em texto da política de privacidade disponibilizada pelo Conecte SUS. O texto foi obtido no dia 16/04/2023.

Transcrição

D.1 Quais informações estão presentes neste documento?

Nesta Política de Privacidade, o usuário do serviço Conecte SUS encontrará informações sobre: o funcionamento do serviço e as regras aplicáveis a ele; o arcabouço legal relacionado à prestação do serviço; as responsabilidades do usuário ao utilizar o serviço; as responsabilidades da administração pública ao prover o serviço; informações para contato, caso exista alguma dúvida ou seja necessário atualizar informações; e o foro responsável por eventuais reclamações caso questões desta Política tenham sido violadas. Além disso, na Política de Privacidade, o usuário do serviço Conecte SUS encontrará informações sobre: qual o tratamento dos dados pessoais realizados, de forma automatizada ou não, e a sua finalidade; os dados pessoais dos usuários necessários para a prestação do serviço; a forma como eles são coletados; se há o compartilhamento de dados com terceiros; e quais as medidas de segurança implementadas para proteger os dados.

RQ003 IP

D.2 Aceitação da Política de Privacidade

Ao utilizar os serviços, o usuário confirma que leu e compreendeu as Políticas aplicáveis ao serviço Conecte SUS e concorda em ficar vinculado a eles.

D.3 Definições

Para melhor compreensão deste documento, nesta Política de Privacidade, consideram-se: Agentes de tratamento: o controlador e o operador. Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Controlador: pessoa natural ou jurídica, de direito público ou

privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Encarregado de Dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entes privados. Lei Geral de Proteção de Dados: Lei Federal n. 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Usuários (ou "Usuário", quando individualmente considerado): todas as pessoas naturais que utilizarem o serviço Conecte SUS. ANPD: autoridade nacional de proteção de dados pessoais é órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

RQ044, RQ048 - I e RQ042 - IP

D.4 Quais são as leis e normativos aplicáveis a esse serviço?

-Lei nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação – Regula o acesso a informações previsto na Constituição Federal. -Lei nº 13.460, de 26 de junho de 2017: Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. -Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. -Decreto nº 7.724, de 16 de maio de 2012: Regulamenta a Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição. -LEI n. 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. -Decreto nº 10.046, de 09 de outubro de 2019: Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. -Decreto nº

9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. - Portaria GM/MS nº 69, de 14 de Janeiro de 2021: Institui a obrigatoriedade de registro de aplicação de vacinas contra a Covid-19 nos sistemas de informação do Ministério da Saúde. - Portaria GM/MS nº 1.434, de 28 de maio de 2020: Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. - Portaria GM/MS nº 1.792, de 17 de julho de 2020: Altera a Portaria nº 356/GM/MS, de 11 de março de 2020, para dispor sobre a obrigatoriedade de notificação ao Ministério da Saúde de todos os resultados de testes diagnóstico para SARS-CoV-2 realizados por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional. - Portaria GM/MS nº 1.768, de 30 de julho de 2021: Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). - Portaria GM/MS nº 3.632, de 21 de dezembro de 2020: Altera a Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017, para instituir a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28).

D.5 Descrição do serviço

O Conecte SUS é o aplicativo oficial do Ministério da Saúde que permite ao cidadão acompanhar na palma de sua mão o seu histórico clínico, a partir das informações de saúde do Sistema Único de Saúde (SUS). Atualmente o aplicativo apresenta o registro de vacinas aplicadas e exames laboratoriais de Covid-19 realizados, internações, medicamentos dispensados, além da emissão do Certificado Nacional de Vacinação Covid-19 e da Carteira nacional de Vacinação. Os dados do aplicativo são em sua maioria provenientes da Rede Nacional de Dados em Saúde (RNDS), plataforma nacional de interoperabilidade de dados em saúde, que integra diferentes sistemas de informação alimentados por profissionais de saúde. Instituída pela portaria GM/MS n. 1.434, de 28 de maio de 2020, a Rede é um projeto estruturante do programa do Governo Federal para a transformação digital da saúde no Brasil e tem o objetivo de promover a troca de informações entre os pontos da Rede de Atenção à Saúde, permitindo a transição e continuidade do cuidado nos setores público e privado. O Conecte SUS também é disponível em na web https://conectesus-paciente.saude.gov.br/. Quais são os direitos do usuário do serviço? O usuário do serviço possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais: - Direito de confirmação e acesso (Art. 18, I e II): é o direito do usuário de obter

RQ111 - I

RQ110 - I

RQ008, RQ021 e RQ072 - I

RQ112 - IP

RQ035 e RQ050 - IP

do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais. Direito de retificação (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados. - Direito à limitação do tratamento dos dados (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados. - Direito de oposição (Art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados. - Direito de portabilidade dos dados (Art. 18, V): é o direito do usuário de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. - Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

D.6 Quais são as obrigações dos usuários que utilizam o serviço?

O usuário se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes poderá implicar a impossibilidade de se utilizar o serviço Conecte SUS. Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros. O login e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese e, a alegação de uso indevido, após o ato de compartilhamento. O usuário do serviço é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas. Não é possível realizar retificação de informação pelo Conecte SUS, salvo aquelas consideradas como “Registros e Contatos”, que se referem a informações autodeclaradas de Índice de Massa Corpórea (IMC), Alergias, Pressão Arterial, Glicose e Doações de Sangue. Dados cadastrais, como nome, data de nascimento, sexo, e-mail, inclusão/exclusão de nome social, são recebidos pelo sistema Cadastro Nacional de Usuários do SUS - CadSUS, onde, a partir do Cartão Nacional de Saúde – CNS, são validados com as informações disponíveis na Receita Federal. Para a correção desses dados, o cidadão deverá atualizar as informações na Receita Federal e/ou solicitar junto a qualquer estabelecimento de saúde (Alteração de dados na Receita Federal pode ser realizado em: https://servicos.receita.fazenda.gov.br/Servicos/As

RQ052 - I

secre/alterar/default.asp). Os dados de saúde são inseridos nos sistemas de informação diretamente por profissionais de saúde, nos estabelecimentos assistenciais. A visualização das informações no Conecte SUS é possível após o devido envio destes dados à Rede Nacional de Dados em Saúde (RNDS). Para qualquer tipo de correção e alteração de dados de saúde, deve-se entrar em contato com o estabelecimento onde foi realizada a ação ou serviço de saúde, ou secretaria estadual ou municipal de saúde e solicitar a correção do registro. Compete ao gestor local de saúde, responsável pela coleta dos dados, a correção de dados incompletos, inexatos ou desatualizados, requisitada pelo cidadão, conforme Inciso III do Art. 18 da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais. O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nesta Política de Privacidade ou de qualquer ato praticado a partir de seu acesso ao serviço. O Órgão não poderá ser responsabilizado pelos seguintes fatos:

Equipamento infectado ou invadido por atacantes; Equipamento avariado no momento do consumo de serviços; Proteção do computador; Proteção das informações baseadas nos computadores dos usuários; Abuso de uso dos computadores dos usuários; Monitoração clandestina do computador dos usuários; Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

D.6.1 Perímetro inseguro;

O uso comercial das expressões utilizadas em aplicativos como marca, nome empresarial ou nome de domínio, além dos conteúdos do serviço, assim como os programas, bancos de dados, redes, arquivos que permitem que o usuário acesse sua conta estão protegidos pelas leis e tratados internacionais de direito autoral, marcas, patentes, modelos e desenhos industriais. Ao acessar o aplicativo, os usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes e/ou desenhos industriais, depositados ou registrados em, bem como todos os direitos referentes a terceiros que porventura estejam, ou estiverem de alguma forma, disponíveis no serviço. O simples acesso ao serviço não confere aos usuários qualquer direito ao uso dos nomes, títulos, palavras, frases, marcas, patentes, imagens, dados e informações, dentre outras, que nele estejam ou estiverem disponíveis. A reprodução de conteúdo descritos anteriormente está proibida, salvo com prévia autorização por escrito ou caso se destinem ao uso exclusivamente pessoal e sem que em nenhuma circunstância os usuários adquiram qualquer direito sobre esses conteúdos. É vedada a utilização do serviço para finalidades comerciais, publicitárias ou qualquer outra que contrarie a finalidade para a qual foi

concebido, conforme definido neste documento, sob pena de sujeição às sanções cabíveis na Lei nº 9.610/1998, que protege os direitos autorais no Brasil. Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, imagens, enfim, todo e qualquer direito de propriedade intelectual ou industrial do serviço. Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

D.7 Quais são as responsabilidades da administração pública com meus dados?

A Administração Pública, no papel de custodiante das informações pessoais dos Usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma. Publicar e informar ao Usuário as futuras alterações a esta Política de Privacidade por meio do sítio (https://sso.acesso.gov.br/), conforme o princípio da publicidade estabelecido no artigo 37, caput, da Constituição Federal. Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário. Em hipótese alguma, o serviço e seus colaboradores responsabilizam-se por eventuais danos diretos, indiretos, emergentes, especiais, imprevistos ou multas causadas, em qualquer matéria de responsabilidade, seja contratual, objetiva ou civil (inclusive negligência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos. Tendo em vista que o serviço lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como “spiders” ou “scrapers”), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão. Em se tratando de aplicativos em dispositivos móveis sua comercialização é expressamente proibida. Ao concordar com esta Política e utilizar o aplicativo móvel, o usuário receberá uma permissão do órgão para uso não comercial dos serviços oferecidos pelo aplicativo, o que, em nenhuma hipótese, fará dele proprietário do aplicativo móvel. Caso o usuário descumpra a Política de Privacidade, ou seja, investigado em razão de má conduta, o órgão poderá restringir seu acesso. O usuário também deverá responder legalmente por essa conduta. A Administração Pública poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou to-

RQ009 - IP

mar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça. A Administração pública se compromete a preservar a funcionalidade do serviço ou aplicativo, utilizando um layout que respeite a usabilidade e navegabilidade, facilitando a navegação sempre que possível, e exibir as funcionalidades de maneira completa, precisa e suficiente, de modo que as operações realizadas no serviço sejam claras.

D.8 Qual o contato pelo qual o usuário do serviço pode tirar suas dúvidas?

Caso o usuário tenha alguma dúvida sobre esta Política de Privacidade, ele poderá entrar em contato pelo canal de atendimento ao suporte ao usuário: https://webatendimento.saude.gov.br/faq/conectesus . Esta Política de Privacidade foi elaborada em conformidade com a Lei Federal n. 12.965 de 23 de abril de 2014 (Marco Civil da Internet) e com a Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais). Esta Política de Privacidade poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção. O site se compromete a cumprir as normas previstas na Lei Geral de Proteção de Dados (LGPD), e respeitar os princípios dispostos no Art. 6º: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; RQ039 - I

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos RQ121 - IP

em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

D.9 Agentes de tratamento

A quem compete as decisões referentes ao tratamento de dados pessoais realizado no serviço Conecte SUS (Controlador)? A Lei Geral de Proteção de Dados define como controlador, em seu artigo 5º: Art. 5º, VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; Para o serviço Conecte SUS, as decisões referentes ao tratamento de dados pessoais são de responsabilidade do Ministério da Saúde. Endereço: Ministério da Saúde - Esplanada dos Ministérios Bloco G, Zona Cívico-Administrativa, Brasília - DF - CEP 70058900. E-mail: datasus@saude.gov.br. Telefone: 61 3315 3900. As secretarias municipais e estaduais de saúde exercem o papel de controladores de dados, devido as mesmas terem suas próprias legislações e realizarem também o tratamento de dados de saúde.

RQ067 - IP e RQ070 - I

D.10 Quem realiza o tratamento de dados (Operador)?

A Lei Geral de Proteção de Dados define como operador, em seu artigo 5º: Art. 5º, VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Para o serviço Conecte SUS, o Controlador Ministério da Saúde também atua como operador, ou seja, além de ser responsável pelas decisões referentes ao tratamento de dados pessoais, também realiza o tratamento de dados pessoais. O Conecte SUS compartilha dados com uma empresa terceirizada, desenvolvedora da aplicação, sendo assim, é um operador de dados. Todos os controles administrativos e lógicos de segurança foram exigidos à empresa terceirizada. O Conecte SUS armazena seus dados em nuvem privada, sendo assim o serviço de nuvem também se configura como operador de dados.

RQ0129 - I

D.11 Quais dados pessoais são tratados pelo serviço?

A utilização, pelo usuário, de determinadas funcionalidades do serviço dependerá do tratamento dos seguintes dados pessoais:

RQ0115 - I

-Nome completo -Data de nascimento -Sexo -Filiação -Nacionalidade -Número de inscrição no As secretarias municipais e estaduais de saúde -Endereço de e-mail -Endereço -Número de telefone -Localização do usuário -Foto do usuário -Dados de Saúde (Alergias, IMC, Pressão Arterial, Glicose, Doações de Sangue) -Vacinação Covid-19 - Vacinação de Rotina -Resultado de Exame Covid-19 -Internações Hospitalares -Contatos de emergência e de profissionais de saúde (Nome e Telefone) -Medicamentos Dispensados (Programa Farmácia Popular) -Situação Cadastral no Sistema Nacional de Transplantes. RQ016 - IP e RQ094 -I

O serviço Conecte SUS realiza o tratamento de dados de crianças e adolescentes e se compromete a fornecer maior proteção a esses dados. Além disso, o serviço Conecte SUS se compromete a cumprir todas as disposições legais pertinentes, como o Estatuto da Criança e do Adolescente. Alguns recursos ou informações, quando necessários pela primeira vez ou mesmo na instalação, serão solicitados por este aplicativo e notificados por meio do sistema operacional do seu dispositivo móvel, por exemplo: Acesso à rede (internet móvel ou WiFi); Acesso à identificação do dispositivo; Acesso à câmera e fotos, mídia e arquivos de áudio e vídeo de seu aparelho. Além disso, o aplicativo pode acessar, ler e gravar arquivos ou documentos do seu dispositivo

D.12 Como os dados são coletados?

RQ055 - I

- Nome completo: Obtido de terceiros (Login Único, Cadastro Nacional de Usuários do SUS - CADSUS) - Data de nascimento: Obtido de terceiros (CADSUS) - Sexo: Obtido de terceiros (CADSUS) - Filiação: Obtido de terceiros (CADSUS) - Nacionalidade: Obtido de terceiros (CADSUS) - Número de inscrição no As secre: Obtido de terceiros (CADSUS) - Endereço de e-mail: Obtido de terceiros (CADSUS) - Endereço: Obtido de terceiros (CADSUS) - Número de telefone: Obtido de terceiros (CADSUS) - Localização do usuário: Obtida pelo dispositivo de acesso, após autorização do usuário - Foto do usuário: câmera e fotos, mídia e arquivos de áudio e vídeo do dispositivo, após autorização do usuário -Dados de Saúde (Alergias, IMC, Pressão, Glicose, Doações de Sangue): Informado pelo usuário -Vacinação Covid-19: Obtido de terceiros (Rede Nacional de Dados em Saúde - RNDS) -Resultado de Exame Covid-19 : Obtido de terceiros (RNDS) -Internações Hospitalares : Obtido de terceiros (RNDS) -Contatos de emergência e de profissionais de saúde (Nome e Telefone) : Informado pelo usuário -Medicamentos Dispensados (Programa Farmácia Popular – Sistema Horus) : Obtido de terceiros -Situação Cadastral no Sistema Nacional de Transplantes : Obtido de terceiros (Sistema Nacional de Transplantes)

D.13 Para que fim utilizamos seus dados?

RQ068 e RQ101 - I

-Nome completo: O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Va-

cinação e Certificado de Vacinação Covid-19. -Data de nascimento: O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação Covid-19. -Sexo: O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação Covid-19. -Filiação: O dado é necessário para melhorar e personalizar a experiência do usuário. O aplicativo permite adicionar outras contas. O nome da mãe é apresentado na Carteira Nacional de Vacinação e no Certificado Nacional de Vacinação Covid-19. -Nacionalidade: O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação Covid-19. -Número de inscrição no As secre: O dado é necessário para manter o usuário logado. -Endereço de e-mail: O dado é necessário para identificação do usuário dentro do serviço e envio de notificações. -Endereço: O dado é necessário para identificação do usuário dentro do serviço. -Número de telefone: O dado é necessário para envio de notificações. -Localização do usuário: O dado é necessário para melhorar e personalizar a experiência do usuário. A localização do usuário é acionada na funcionalidade Serviços que apresenta a geolocalização dos estabelecimentos de saúde mais próximos. Dado opcional. -Foto do usuário: O dado é necessário para melhorar e personalizar a experiência do usuário no menu do aplicativo. A câmera e fotos, mídia e arquivos de áudio e vídeo do dispositivo também é utilizada para escanear códigos QR para autenticação e validação dos documentos emitidos pelo aplicativo. -Dados de Saúde (Alergias, IMC, Pressão, Glicose, Doações de Sangue) : O dado é necessário para melhorar e personalizar a experiência do usuário. Dados registrados pelo próprio usuário. -Vacinação Covid-19: O dado é necessário para melhorar e personalizar a experiência do usuário. São dados da RNDS, coletados por profissionais de saúde nos serviços de vacinação, sob gestão de secretarias municipal ou estadual de saúde. Dados: nome da vacina; tipo de dose aplicada; data da vacinação; número do lote da vacina; nome do fabricante; identificação do vacinador; e identificação do serviço de vacinação. -Resultado de Exame Covid-19: O dado é necessário para melhorar e personalizar a experiência do usuário. Dados da RNDS, coletados por profissionais de saúde de laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional. -Internações Hospitalares: O dado é necessário para melhorar e personalizar a experiência do usuário. Dados da RNDS, coletados por profissionais de saúde da atenção hospitalar. -Contatos de emergência e de profissionais de saúde (Nome e Telefone) : O dado é necessário para melhorar e personalizar a experiência do usuário. Dados registrados pelo próprio usuário. -Medicamentos Dispensados (Programa Farmácia Popular e Sistema Horus) : O dado é necessário para melhorar e personalizar a experiência do usuário. Dados coletados por profissionais de saúde para dispensação de medicamento do Programa Farmácia Popular. -Situação Cadastral no Sistema Nacional de Transplantes: O dado é necessário para

melhorar e personalizar a experiência do usuário. Dados coletados pelas Secretarias Estaduais de Transplantes (Centrais Estaduais de Transplantes) que apresentam informações sobre o status e posição do usuário na lista de espera para transplante de órgão e tecido.

D.14 Qual o tratamento realizado com os dados pessoais?

RQ069 - I

-Nome Completo: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Data De Nascimento: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Sexo: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Filiação: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Nacionalidade: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Número de Inscrição no As secre: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Endereço de e-mail: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Endereço: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Número de Telefone: Acesso, Armazenamento, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Localização Do Usuário: Acesso, Coleta -Foto Do Usuário: Acesso, Coleta -Dados De Saúde (Alergias, IMC, Pressão, Glicose, Doações De Sangue): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Vacinação Covid-19: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Resultado De Exame Covid-19: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Internações Hospitalares: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Contatos De Emergência E De Profissionais De Saúde (Nome E Telefone): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Medicamentos Dispensados (Programa Farmácia Popular e Sistema Horus): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção -Situação Cadastral No Sistema Nacional De Transplantes: Acesso, Armazenamento, Avaliação,

Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção

D.15 Os dados pessoais utilizados no serviço são compartilhados?

Os dados pessoais do usuário poderão ser compartilhados com as seguintes pessoas ou empresas: profissionais de saúde com acesso ao Conecte SUS Profissional, Secretarias Estaduais e Municipais de Saúde, Agência Nacional de Vigilância Sanitária (ANVISA), Controladoria-Geral da União (CGU), Tribunal de Contas da união (TCU), Operador que desenvolve o Conecte SUS e o serviço de nuvem que armazena os dados.

D.16 Segurança no tratamento dos dados pessoais do usuário

RQ121 - IP

O serviço Conecte SUS se compromete a aplicar as medidas técnicas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão de tais dados. Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e

RQ078 - IP

os riscos para os direitos e liberdades do usuário. O site utiliza criptografia para que os dados sejam transmitidos de forma segura e confidencial, de maneira que a transmissão dos dados entre o servidor e o usuário, e em retroalimentação, ocorra de maneira totalmente cifrada ou encriptada. No entanto, o site se exime de responsabilidade por culpa exclusiva de terceiro, como em caso de ataque de hackers ou crackers, ou culpa exclusiva do usuário, como no caso em que ele mesmo transfere seus dados a terceiro. O serviço Conecte SUS se compromete, ainda, a comunicar o usuário em prazo adequado caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa lhe causar um alto risco para seus direitos e liberdades pessoais. A violação de dados pessoais é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Por fim, o site se compromete a tratar os dados pessoais do usuário com confidencialidade, dentro dos limites legais.

D.17 O serviço Conecte SUS utiliza cookies?

Cookies são pequenos arquivos de texto enviados pelo site ao computador do usuário e que nele ficam armazenados, com informações relacionadas à navegação do site. Por meio dos cookies, pequenas quantidades de informação são armazenadas pelo navegador do usuário para que nosso servidor possa lê-las posteriormente. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo usuário, bem como seu local e horá-

rio de acesso ao site. É importante ressaltar que nem todo cookie contém dados pessoais do usuário, já que determinados tipos de cookies podem ser utilizados somente para que o serviço funcione corretamente. As informações eventualmente armazenadas em cookies também são consideradas dados pessoais e todas as regras previstas nesta Política de Privacidade também são aplicáveis a eles. O serviço Conecte SUS não utiliza cookies.

D.18 Esta Política de Privacidade pode ser alterada?

A presente versão desta Política de Privacidade foi atualizada pela última vez em: 13/12/2022 O editor se reserva o direito de modificar, a qualquer momento o site as presentes normas, especialmente para adaptá-las às evoluções do serviço Conecte SUS, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Qualquer alteração e/ou atualização desta Política de Privacidade passará a vigorar a partir da data de sua publicação no sítio do serviço e deverá ser integralmente observada pelos Usuários.

D.19 Qual o foro aplicável caso o usuário queira realizar alguma reclamação?

Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados. Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida exclusivamente pela Justiça Federal, na seção judiciária do domicílio do usuário, por previsão do artigo 109, §§ 1º, 2º e 3º, da Constituição Federal.

ANEXO E – Nota Informativa

A seguir é apresentado a nota informativa disponibilizada pelo Conecte SUS transcrito para texto. A transcrição foi obtida no dia 16/04/2023.

Transcrição

LEIA COM ATENÇÃO. ESTE DOCUMENTO APRESENTA AS INFORMAÇÕES NECESSÁRIAS PARA QUE VOCÊ COMPREENDA SOBRE O COMPARTILHAMENTO DOS SEUS DADOS DE SAÚDE.

E.1 CONTEXTO

Todas as vezes em que você recebe cuidados de um profissional de saúde registrado, para diagnóstico, tratamento, ou prevenção de uma enfermidade ou orientação sobre sua saúde, seja no sistema de saúde público ou privado, Dados de Saúde desse encontro assistencial são coletados, registrados e armazenados eletronicamente nos sistemas locais de informação. Esses dados são usados para documentação desse encontro e para comunicação do seu histórico para outros profissionais de saúde que estiverem colaborando para que você recupere sua saúde totalmente e permaneça saudável. A coleta, o registro e o armazenamento de Dados de Saúde são etapas muito importantes para garantir que você tenha acesso a ações e serviços de saúde de qualidade, no momento em que você precisa. Além de agilizar seu atendimento e possibilitar que você receba os cuidados mais adequados para o seu caso, a documentação do seu histórico de saúde serve também para o cumprimento de obrigações éticas, regulatórias e legais por parte de quem lhe presta os cuidados – profissionais e instituições de saúde. A Rede Nacional de Dados em Saúde (RNDS), mantida pelo Ministério da Saúde, nasceu para que os Dados de Saúde possam ser trocados de forma responsável, segura e confidencial, entre os profissionais de saúde que cuidam para que você receba uma atenção integral e de qualidade, garantindo que as informações essenciais para dar continuidade de seu tratamento estejam disponíveis sempre que você necessitar, mesmo que você seja tratado com profissionais que não trabalham em um mesmo estabelecimento, ou nem no mesmo município, estado ou país. Através do armazenamento dos seus Dados de Saúde na RNDS, você poderá ter um atendimento de qualidade em qualquer lugar e em qualquer momento! Atualmente, os profissionais de saúde têm acesso aos dados de saúde por meio do Conecte SUS Profissional. A Lei Geral de Proteção de Dados Pessoais (LGPD) considera os Dados de Saúde, ou seja, dados referentes à sua saúde, à vida sexual, dado genético ou biométrico, como dados pessoais sensíveis. Isso significa que seus Dados de Saúde, registrados em meio eletrônico ou físico, têm de ser protegidos e tratados com mais atenção, pois são dados que podem predispor a algum

tipo de discriminação. Por isso, para a RNDS, todas as atividades que envolvam a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, ou ainda, o compartilhamento dos seus Dados de Saúde com terceiros, seguirão os princípios e obrigações dispostos na Lei Geral de Proteção de Dados e demais normas que regulem estas atividades. Todos os cidadãos, usuários do SUS, participam da RNDS automaticamente, pois o país coleta os dados de todos os brasileiros e estrangeiros usuários do SUS para conhecer a situação de saúde da população. Nós utilizaremos a RNDS para cumprir nossas obrigações com a população brasileira, pois porque através de Dados de Saúde poderemos avaliar, formular e executar políticas públicas mais eficazes, estabelecendo condições para promoção, proteção, tratamento e recuperação da sua saúde e da população. No entanto, neste momento, você poderá escolher não compartilhar os seus Dados de Saúde com a RNDS. Ao escolher esta opção, seus Dados de Saúde compartilhados com os profissionais de assistência à saúde responsáveis pelos seus atendimentos, e que possuem acesso ao Conecte SUS Profissional, serão ficarão restritos aos sistemas do Ministério da Saúde. Esta possibilidade poderá ser revista a qualquer momento, ocasião em que você será devidamente informado a respeito. Cabe salientar que você não terá prejuízo no atendimento caso não queira compartilhar os seus dados de saúde.

RQ 041 - I

RQ072 e RQ115 - I

E.2 COMO FUNCIONA O COMPARTILHAMENTO DOS DADOS DE SAÚDE?

Os seus Dados de Saúde estarão disponíveis por trinta minutos ao Profissional de Saúde que esteja prestando atendimento a você ou à pessoa que você seja responsável legal. Este Profissional de Saúde deverá estar habilitado a acessar os dados da Rede Nacional de Dados em Saúde, do Ministério da Saúde, por meio do Conecte SUS Profissional.

E.3 QUAIS DADOS SERÃO ACESSADOS?

O Profissional de Saúde terá acesso a informações de caráter administrativo (por exemplo: data e horários de atendimento, entrada e saída do estabelecimento), informações relativas a medicamentos distribuídos, internações hospitalares, atendimentos ambulatoriais, de vacinação e resultados de exames. Novos dados de saúde serão apresentados, conforme o projeto da RNDS seja desenvolvido, alinhado à Estratégia de Saúde Digital para o Brasil (2020-2028), e priorizados pelo Comitê Gestor de Saúde Digital.

E.4 POR QUEM E COMO SEUS DADOS DE SAÚDE SERÃO ACESSADOS?

O Profissional de Saúde que, no exercício regular de sua profissão, esteja diretamente envolvido nas ações e serviços de saúde prestados a você, e tenha acesso à RNDS, estará autorizado a acessar seus Dados de Saúde.

E.5 BENEFÍCIOS

RQ022 - I

O objetivo da RNDS é facilitar o acesso dos Profissionais de Saúde que venham a cuidar de você, às informações precisas e atualizadas sobre seu histórico e condições presentes de saúde. O acesso aos seus Dados de Saúde poderá estar disponível para esses Profissionais no exato momento em que você precisa. Isso é muito importante para que possamos lhe prestar um atendimento mais individualizado e direcionado às suas necessidades. Através da RNDS se espera melhorar a comunicação entre todos profissionais que cuidam de você, de modo que eles atuem de forma integrada e contínua para o seu benefício, evitando que você tenha que repetir exames ou outros procedimentos desnecessariamente. Essa integração contribui, ainda, para que as decisões deles sejam melhor informadas e que você tenha uma atenção personalizada, segura e mais adequada às suas necessidades. Você será atendido com muito mais rapidez, qualidade, eficiência e segurança. Afinal, quanto mais o seu profissional de saúde conhecer sobre você, seus hábitos e seu histórico de saúde, melhor e mais assertivo poderá ser sua prevenção, diagnóstico e tratamento, mesmo que esteja atendendo você pela primeira vez. Outro exemplo: saber, imediatamente, quais medicamentos você usa ou já usou, se você tem alergias, quais os resultados dos exames já realizados, assim como ter acesso a relatórios cirúrgicos e notas de internação é muito importante para evitar diagnósticos e tratamentos inadequados ou ineficientes e, como consequência, eventuais prejuízos à sua saúde. Outra vantagem é que quando estiver em um Atendimento de Emergência, nos quais, por exemplo, você esteja inconsciente e/ou desacompanhado e, portanto, incapaz de fornecer informações sobre seu estado ou histórico de saúde, o profissional de saúde que estiver lhe atendendo será capaz de acessar seus Dados de Saúde e conhecer sua história clínica.

E.6 SEGURANÇA DA INFORMAÇÃO

RQ084 - IP

Os Dados de Saúde serão coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança proporcionais a sua sensibilidade, o que implica na criação de ambientes físicos e lógicos aderentes ao estado da técnica e às melhores práticas em gestão do sigilo e segurança da informação, inclusive aqueles específicos à área de saúde. Embora os Estabelecimentos de Saúde integrantes da RNDS e a própria RNDS

estejam cercados de todos os cuidados voltados ao sigilo e a segurança de seus Dados de Saúde, é impossível garantir a inviolabilidade de seus sistemas, seja em razão da ocorrência de casos fortuitos, motivos de força maior ou em razão de ataques cibernéticos que possam vir a ocorrer. Todos os acessos aos seus Dados de Saúde serão registrados eletronicamente e você será notificado no Aplicativo Conecte SUS sempre que seu registro for acessado. Os acessos não autorizados e usos indevidos por usuários da RNDS estão sujeitos a penalidades previstas na legislação. É seu direito, a qualquer momento, ter conhecimento dos acessos realizados aos seus Dados de Saúde. Caso você decida não compartilhar seus Dados de Saúde, seus atendimentos nos Estabelecimentos de Saúde não sofrerão qualquer restrição. Nesse caso, o Estabelecimento de Saúde somente compartilhará seus Dados de Saúde com terceiros nos casos exigidos por lei ou pelos códigos e normas de ética médica (por exemplo, em caso de ordem judicial, hipóteses de comunicado compulsório de doenças).

RQ004 IP

RQ037 - I

Em casos de Atendimento de Emergência, em que não haja registro de autorização para compartilhamento de seus Dados de Saúde, ou quando você não estiver em condições de dar esse consentimento, o Profissional de Saúde responsável pelo seu atendimento poderá acessar seus Dados de Saúde, nas seguintes situações: (i) a partir de autorização expressa de seu representante legal ou acompanhante; ou (ii) quando, a partir do julgamento técnico do Profissional de Saúde responsável, você corra risco de lesão grave ou risco de morte. O acesso aos Dados de Saúde nessa segunda hipótese deverá ser devidamente justificado e registrado na RNDS para futura auditoria.

E.7 GESTÃO DA BASE DE DADOS DA RNDS

A Rede Nacional de Dados em Saúde utiliza uma tecnologia de armazenamento em nuvem, o que permite guardar dados na internet por meio de um servidor online. A aquisição, instalação e manutenção dessa tecnologia, bem como a gestão da base de dados estão sob responsabilidade do Departamento de Informática do SUS – DATASUS – Ministério da Saúde. Caso a gestão da base de Dados de Saúde seja transferida a terceiros, você será notificado da ocorrência dessa mudança com a devida antecedência. As Secretarias de Saúde do estado e do município aos quais o Estabelecimento de Saúde integrante da RNDS estiver vinculado poderão ter acesso a essas informações de forma que você não poderá ser identificado, ou seja, os dados serão anonimizados.

E.8 E SE EU OPTAR POR NÃO COMPARTILHAR MEUS DADOS DE SAÚDE?

O modelo adotado pela RNDS para garantir o seu consentimento é o opt-out, ou seja, você sempre terá seus dados compartilhados dentro dos serviços de saúde, alinhado ao modelo de atenção à saúde preconizado. Caso você decida não compartilhar seus Dados de Saúde, seus atendimentos nos Estabelecimentos de Saúde não sofrerão qualquer restrição. Nesse caso, o Estabelecimento de Saúde somente compartilhará seus Dados de Saúde com terceiros nos casos exigidos por lei ou pelos códigos e normas de ética médica (por exemplo, em caso de ordem judicial, hipóteses de comunicado compulsório de doenças). Mas é importante ressaltar que, caso necessite de um atendimento onde você não possa dar o seu consentimento, o profissional de saúde não terá como acessar seus dados de saúde, que podem conter informações valiosas para o atendimento que ele vai lhe prestar, como alergias a medicamentos, sua história clínica, cirurgias que realizou, dentre outros. Esteja ciente que estas informações podem ser de muita importância numa situação de urgência onde você esteja desacordado, por exemplo.

E.9 CANAIS DE ATENDIMENTO

Sempre que desejar, você poderá entrar em contato com a equipe da RNDS. Em caso de dúvidas, reclamações ou perguntas sobre os seus direitos, você poderá entrar em contato no canal de atendimento ao usuário do Conecte SUS: https://webatendimento.saude.gov.br/fa

RQ061 - I

ANEXO F – Política de Privacidade - Sabin

A seguir é apresentado a política de privacidade disponibilizada pelo Sabin transcrito para texto. A transcrição foi obtida no dia 24/06/2023.

Transcrição

POLÍTICA DE PRIVACIDADE

Bem-vindo(a) à Política de Privacidade ("Política") do Grupo Sabin ("SABIN"), somos uma pessoa jurídica de direito privado, com sede em SAAN Quadra 03, Lotes 165 e 245, Brasília – DF, Brasil, CEP: 70.632-300, inscrita no CNPJ sob o nº 00.718.528/0001-09.

No Grupo Sabin, valorizamos e respeitamos a privacidade de nossos clientes, colaboradores, fornecedores e parceiros. Comprometemo-nos a assegurar a confidencialidade e a segurança de todos os dados pessoais durante a prestação de nossos serviços e em todas as atividades relacionadas ao nosso negócio. Nossa prioridade é manter a integridade, confidencialidade e disponibilidade dos seus dados em todas as etapas do processo.

Este documento tem o objetivo de esclarecer, de forma clara e objetiva, como coletamos e tratamos os dados pessoais e dados pessoais sensíveis para a prestação dos serviços executados pelo Sabin, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

RQ060 - IP

Se você tiver alguma dúvida ou quiser discutir qualquer questão relacionada aos seus dados, nossa equipe estará à disposição para ajudar. Você pode entrar em contato conosco através dos seguintes canais:

Encarregado de Proteção de Dados: encarregado@sabin.com.br Privacidade e Proteção de Dados: privacidade@sabin.com.br

Aqui no Grupo Sabin, prezamos pela proteção dos seus direitos, em conformidade com o artigo 18 da LGPD. Se você deseja fazer alguma solicitação relacionada aos seus direitos, convidamos você a visitar nosso portal de privacidade no link abaixo:

F.1 O QUE SÃO DADOS PESSOAIS? Art. 5º, I da LGPD

São quaisquer informações referentes a uma pessoa que a identifiquem ou permitam sua identificação, por exemplo nome, RG, CPF, carteiras profissionais (CRM, OAB, CREA, CRC), endereço, telefone, e-mail, certidão de nascimento, dados de Geolocalização, endereço de lP de computador, cookies entre outros.

F.2 O QUE SÃO DADOS PESSOAIS SENSÍVEIS? Art. 5º, Ii da LGPD

São informações de natureza sensível que podem ser utilizadas de forma discriminatória, exigindo atenção especial. Esses dados incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, orientação sexual, dados biométricos (como características faciais, digitais ou genéticas), pedidos médicos, peso, altura e todos os seus dados relacionados à saúde.

É crucial reconhecer a importância e sensibilidade dessas informações, considerando os potenciais riscos e impactos negativos que podem surgir se forem utilizadas de maneira inadequada ou discriminatória.

Portanto, estamos comprometidos em garantir a proteção e confidencialidade desses dados sensíveis, adotando medidas de segurança rigorosas e garantindo sua privacidade. Valorizamos sua confiança em nós e nos esforçamos para cumprir os mais altos padrões de proteção de dados.

Se você tiver alguma preocupação ou precisar de mais informações sobre como lidamos com esses dados sensíveis, entre em contato conosco. Estamos aqui para oferecer suporte e esclarecer quaisquer dúvidas que possa ter.

F.3 SEGURANÇA DOS DADOS PESSOAIS - Art. 46 da LGPD

RQ084 - IP

Nós do SABIN garantimos que cuidamos de seus dados por meio de medidas técnicas e operacionais adequadas, e exigimos o mesmo nível de excelência de nossos parceiros, nós não lhe solicitaremos outros dados fora de nossos canais de contato oficiais;

Caso você suspeite de qualquer violação de dados relacionadas à privacidade e segurança de seus dados pessoais, solicitamos que entre em contato conosco imediatamente. Estamos prontos para investigar prontamente qualquer incidente relatado e tomar as medidas necessárias previstas em lei.

Se você receber algum e-mail indesejado de uma de nossas empresas, solicitamos gentilmente que entre em contato conosco pelo endereço de e-mail privacidade@sabin.com.br. Valorizamos a sua privacidade e nos esforçamos para garantir uma experiência livre de comunicações indesejadas.

Canais de atendimento: E-mail: encarregado@sabin.com.br Portal da Privacidade Sabin

F.4 DADOS PESSOAIS COLETADOS – art. 6º, VI, da LGPD

Para a prestação dos nossos serviços, é possível que sejam coletados dados pessoais e dados pessoais sensíveis, de acordo com suas respectivas finalidades. Para obter informações mais detalhadas sobre os dados que poderão ser coletados consulte nossa tabela de finalidades e inventário de dados nos links abaixo:

Clique e acesse a Tabela de Finalidades

Clique e acesso o Inventário de Dados

Nestes links, você encontrará informações específicas sobre quais dados são coletados, como são utilizados, os fundamentos legais para o tratamento dos dados e o período de retenção dos dados. O objetivo é fornecer a você uma visão clara e abrangente do ciclo de vida dos seus dados pessoais, garantindo transparência em relação à sua utilização, armazenamento e tempo de retenção.

A coleta dos dados pessoais pelo Sabin poderá ocorrer através de diferentes canais de comunicação, como: pessoalmente em nossas unidades, e-mail, telefone, website, serviços de teleatendimento, entre outros.

F.5 PARA QUE UTILIZAMOS SEUS DADOS? Art. 6º, I, da LGPD

Principais finalidades de tratamento dos seus dados:

Prestação de serviços: Utilizamos seus dados para fornecer serviços de realização de exames de medicina diagnóstica e imunizações.

Gerenciamento da sua saúde: Seus dados são utilizados para garantir um histórico completo e atualizado dos exames e imunizações executados conosco.

RQ095 - IP

Comunicação e notificações: Utilizamos seus dados para enviar informações relevantes sobre seus exames, intercorrências, comunicados de resultados críticos, confirmações de agendamentos, resultados de exames, lembretes de vacinas, coleta de reações adversas de vacinas e outras comunicações relacionadas aos serviços prestados.

Faturamento e cobrança: Utilizamos seus dados para fins de faturamento, emissão de notas fiscais e cobrança pelos serviços realizados.

Cumprimento de obrigações legais: Lei 13.787/18 – Lei do Prontuário Eletrônico, RCD 768/23, RDC 330/19 e RDC 197/17.

Notificações compulsórias: Uma de nossas obrigações legais é permitir que as autoridades de saúde monitorem e acompanhem a ocorrência de doenças, bem como adotem medidas preventivas e de controle, como o planejamento de ações de saúde pública, a identificação de surtos epidêmicos, a implementação de medidas de prevenção e tratamento

RQ121 - IP

adequados e a proteção da saúde da população em geral.

Segurança e prevenção de fraudes: Utilização de dados para garantir a segurança dos pacientes, detecção e prevenção de fraudes, monitoramento de acessos não autorizados a prontuários e sistemas de informação, implementação de medidas de segurança da informação, entre outras atividades relacionadas à segurança dos dados pessoais.

Ressaltamos que todas as finalidades mencionadas estão em conformidade com a LGPD e são realizadas com o objetivo de fornecer um serviço de qualidade, respeitando sua privacidade e segurança.

F.6 ATENDIMENTO À CRIANÇA – Art. 14, I, da LGPD

RQ016 - I

O atendimento às crianças, compreendendo aquelas com até 12 anos de idade, será efetuado mediante a assinatura de um termo de consentimento por parte de um dos pais ou do responsável legal. Esse termo autorizará o tratamento dos dados pessoais em conformidade com o artigo 14°, parágrafos 1° e 3°, da Lei nº 13.709, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Os dados de crianças com menos de 12 anos serão utilizados exclusivamente para a execução dos serviços contratados pelos pais ou responsáveis legais.

F.7 LEI APLICÁVEL E FORO – Art. 3º da LGPD

A legislação aplicável a esta Política de Privacidade será sempre as leis da República Federativa do Brasil. Em caso de quaisquer demandas decorrentes desta política, o foro competente para discussão será a Circunscrição Judiciária de Brasília – DF, onde está localizada a sede do SABIN, prevalecendo sobre qualquer outra jurisdição, independentemente de privilégios que possam existir.

F.8 COMPARTILHAMENTO DE DADOS - Art. 18, VII, da LGPD

O SABIN poderá compartilhar dados pessoais nas seguintes hipóteses:

Quando você titular der seu consentimento de forma livre, informada e inequívoca, para uma finalidade específica, ou:

Cumprimento de obrigação legal ou regulatória: podemos compartilhar seus dados pessoais para cumprir obrigações legais ou regulatórias impostas por autoridades competentes, como órgãos de saúde, fiscalização ou controle.

Execução de contrato ou procedimento preliminar: O compartilhamento pode ocorrer quando necessário para a execução de um contrato ou de medidas preliminares relaci-

onadas ao contrato.

Fique tranquilo, caso você queira executar exames para os quais ainda não possuímos a metodologia internalizada, contamos com uma rede de laboratórios de apoio para garantir a realização dos exames. Nossos parceiros laboratoriais seguem os mesmos critérios de conformidade com a LGPD e possuem certificações de qualidade, assim como o Grupo Sabin.

Nesse contexto, o compartilhamento de seus dados pessoais com esses laboratórios é respaldado por duas bases legais: a tutela da saúde, uma vez que seus dados são recebidos por profissionais de saúde, e a execução do contrato que mantemos com nossos laboratórios de apoio.

Caso tenha alguma dúvida adicional ou necessite de mais informações sobre os compartilhamentos com laboratórios de apoio, estamos à disposição para esclarecer suas questões pelos canais já informados.

Proteção da vida e da saúde: Em situações de emergência, onde a vida, saúde ou bem-estar do titular dos dados ou de seus familiares estejam em risco iminente, o Grupo Sabin poderá compartilhar os dados necessários para proteger e preservar a integridade física do indivíduo conforme Art. 7º VII e Art. 11 II e). RQ046, RQ075 - I

Tutela da saúde: O compartilhamento pode ser realizado para tutela da saúde, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias. RQ090, RQ076 - I

Pesquisa científica: Dados pessoais e dados pessoais sensíveis podem ser compartilhados para fins de pesquisa científica, desde que os dados utilizados nas pesquisas estejam anonimizados. RQ091 - IP

Ressaltamos que, em todas essas hipóteses, garantimos que o compartilhamento é realizado de forma segura, protegendo a sua privacidade e cumprindo as demais disposições da LGPD. RQ129 - I

É importante mencionar que, em determinadas circunstâncias, podemos realizar compartilhamentos internacionais de dados com fornecedores de serviços em nuvem para hospedagem de dados. No entanto, ressaltamos que esses compartilhamentos são sempre realizados em conformidade com as leis internacionais de privacidade e com o artigo 33 da LGPD. Somente realizamos hospedagem de dados em países que possuem leis de proteção de dados equivalentes ou superiores às estabelecidas pela LGPD.

Poderemos compartilhar seus dados pessoais entre as empresas do Grupo Sabin. Esse compartilhamento tem como objetivo a execução de serviços, visando proporcionar uma melhor experiência e atender às suas necessidades. Ressaltamos que todas as empresas do Grupo Sabin estão comprometidas em proteger a privacidade e a confidencialidade

dos dados, garantindo que sejam tratados de acordo com as leis de proteção de dados aplicáveis, incluindo a LGPD.

RQ024 - IP

O Instituto Sabin somente compartilhará dados pessoais com terceiros quando houver a sua devida anuência, existir alguma obrigação legal neste sentido ou nos casos que o compartilhamento for indispensável para a prestação dos nossos serviços e desenvolvimento de produtos.

RQ015 - IP

Nos comprometemos autilizar toda e qualquer informação pessoal dentro dos limites legais e contratuais e que não disponibilizaremos seus dados pessoais a terceiros sem a observância da devida base legal e os demais procedimentos operacionais e técnicos necessários.

F.9 TEMPO DE ARMAZENAMENTO DOS DADOS PESSOAIS - Art. 16 da LGPD

Seus dados são armazenados em conformidade com a Lei 13.787/18, conhecida como Lei do Prontuário Eletrônico. Essa abordagem garante que você tenha facilidade de acesso às suas informações de saúde, nos comprometemos a respeitar o prazo mínimo de 20 anos estabelecido por lei.

Se, por algum motivo, você desejar que seus dados fiquem indisponíveis em nossa base de dados, solicitamos que entre em contato conosco pelos canais de atendimento mencionados anteriormente. Estaremos prontos para atender sua solicitação e garantir que suas informações sejam tratadas de acordo com suas preferências. Sua privacidade é uma prioridade para nós, e estamos comprometidos em respeitar suas escolhas e tomar as medidas necessárias para atender às suas necessidades.

Os dados serão armazenados pelo Instituto Sabin nas seguintes hipóteses:

Enquanto forem necessários para cumprir as finalidades descritas acima;
Enquanto durar uma obrigação legal ou regulatória que obrigue o Instituto Sabin a manter os dados;

RQ005 - IP

Pelo prazo legal do possível ajuizamento de demandas por ou em face do Instituto Sabin;
Quando houver base legal ou regulatória que possibilite o armazenamento pelo Instituto Sabin.

RQ019 - IP

Em caso de qualquer das hipóteses acima não mais justificar a manutenção desses dados, estes serão apagados completamente ou alterados de forma que seja impossível identificar o titular dos dados pessoais em questão.

RQ003 - IP

F.10 UTILIZAÇÃO DE COOKIES - GUIA ORIENTATIVO ANPD 18/10/2022

Visando garantir sua privacidade e proporcionar uma experiência personalizada em nossos sites, as empresas do Grupo Sabin oferecem a você o direito de livre escolha em relação à ativação ou não de cookies.

Os cookies são pequenos arquivos de texto que são armazenados no seu dispositivo quando você acessa um site. Eles desempenham diferentes funções, como permitir o funcionamento adequado do site, lembrar suas preferências e personalizar sua experiência de navegação.

Entendemos a importância de sua privacidade e, seguindo as diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), adotamos a abordagem de desativar os cookies por padrão em nossos sites. Isso significa que, ao visitar nossas páginas, os cookies não serão ativados automaticamente, a menos que você escolha fazê-lo.

Dessa forma, você tem total controle sobre quais informações são coletadas e compartilhadas por meio dos cookies. Ao desativá-los, você pode optar por não fornecer determinados dados e limitar o rastreamento de sua atividade online.

Ressaltamos que cumprimos o guia orientativo "Cookies e Proteção de Dados Pessoais" publicado em 18/10/2022 às 09h29 pela ANPD. Essa orientação reforça nossa dedicação em proteger sua privacidade e garantir que suas informações pessoais sejam tratadas de acordo com as melhores práticas de proteção de dados.

Caso decida ativar os cookies, estaremos em conformidade com a legislação aplicável, fornecendo transparência sobre quais tipos de cookies utilizamos, os propósitos para os quais são utilizados.

É importante destacar a existência dos cookies obrigatórios. Esses cookies são essenciais para o funcionamento adequado do site e não podem ser desativados pelo titular dos dados, essa obrigatoriedade está em conformidade com a LGPD e Marco Civil da Internet.

Os cookies obrigatórios desempenham funções cruciais, como permitir o acesso seguro às áreas restritas do site, lembrar informações de login, manter as preferências de idioma, garantir a correta exibição do conteúdo e cumprimento de obrigações legais.

F.11 DIREITO DOS TITULARES DE DADOS – Art.18 da LGPD

RQ102 - IP

De acordo com o artigo 18 da LGPD, você possui os seguintes direitos em relação aos seus dados pessoais:

RQ049 - I

Confirmar a existência de tratamento dos seus dados pessoais; • Solicitar uma cópia dos seus dados pessoais mantidos em nossa base de dados; • Solicitar a correção de dados imprecisos, desatualizados ou incompletos;

RQ051, RQ103 e RQ110 - IP RQ052 - I

• Solicitar a exclusão ou indisponibilização dos seus dados pessoais, observada a obrigação legal de manutenção; • Solicitar a anonimização, bloqueio ou eliminação de dados excessivos ou tratados de forma contrária à lei; Solicitar a portabilidade dos seus dados para outros fornecedores de produtos e serviços similares, de acordo com as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD); • Solicitar informações sobre as entidades públicas e privadas com as quais compartilhamos os seus dados; • Ser informado sobre a possibilidade de não fornecer consentimento e as respectivas consequências; • Retirar o consentimento o processamento dos seus dados pessoais a qualquer momento.

RQ106 e RQ107 - IP

Durante o atendimento presencial em nossas unidades, não é necessário coletar explicitamente seu consentimento para o tratamento dos seus dados pessoais, isso ocorre porque, ao contratar serviços do Grupo Sabin, estamos estabelecendo um contrato de prestação de serviços, seja para a realização de exames ou de imunização. No caso de atendimento de menores de 12 anos, seguimos as disposições do artigo 14, parágrafo 1º da LGPD, onde coletamos o seu consentimento livre e esclarecido para o tratamento dos dados pessoais de seus dependentes nessa faixa etária.

RQ104 e RQ111, RQ072 - IP

RQ112 - IP

Respeitamos rigorosamente as diretrizes legais e nos comprometemos a proteger a privacidade e a segurança dos dados dos nossos clientes, garantindo o cumprimento das normas aplicáveis à privacidade e proteção de dados.

RQ114 - IP

Para exercer seus direitos em relação aos seus dados pessoais, você pode acessar o Portal da Privacidade Sabin, onde encontrará opções para realizar solicitações específicas. Além disso, também é possível entrar em contato conosco por e-mail, utilizando os canais abaixo indicados:

RQ108 e RQ115 - IP

E-mails: encarregado@sabin.com.br privacidade@sabin.com.br

F.12 NOMEAÇÃO DO ENCARREGADO DE DADOS Art. 41, I e II da LGPD

RQ028 e RQ061 - IP

RQ002 - IP

Para garantir o cumprimento dos seus direitos de acordo com a legislação de proteção de dados, o Grupo Sabin nomeou seu Encarregado de Dados em 2020. Essa função

é desempenhada por um profissional responsável por receber reclamações e comunicações dos titulares dos dados, fornecer esclarecimentos e lidar com as comunicações da Autoridade Nacional, representando todas as empresas do Grupo. RQ123 - I

Além disso, temos um setor exclusivo composto por uma equipe dedicada para gerenciar e proteger seus dados pessoais. Nosso objetivo principal é garantir um tratamento seguro e adequado das suas informações pessoais, demonstrando assim o nosso compromisso em proteger a sua privacidade.

Se você tiver alguma dúvida ou quiser discutir qualquer questão relacionada aos seus dados, nossa equipe estará à disposição para ajudar. Você pode entrar em contato conosco através dos seguintes canais: RQ070 - I

Encarregado de Dados: Welisom Ferreira Encarregado de Proteção de Dados: encarregado@sabin.com.br Equipe de Privacidade e Proteção de Dados: privacidade@sabin.com.br

Referência versão: POL.TIC.06 V.05

F.13 PARA QUE UTILIZAMOS SEUS DADOS? Art. 6º, I, da LGPD

O Instituto Sabin necessita dos seus dados pessoais para diversas finalidades distintas inerentes ao nosso negócio, elencamos as principais: RQ033 - I

Para a realização de exames: laboratoriais, de imagem, vacinas e as respectivas atividades administrativas, como a comunicação do resultado e o fornecimento de login e senhas para acesso remoto;// Para o cumprimento de obrigações legais e/ou regulatórias que estamos sujeitos; Para o desenvolvimento de novos produtos e serviços, bem como a divulgação deles;// Para possibilitar a comunicação com o nosso suporte técnico; RQ034 - I

Informamos que em todas as ocasiões que considerarmos necessário ou que houver obrigação legal/regulatória neste sentido, poderemos solicitar o seu consentimento de forma expressa e inequívoca, e teremos o cuidado de garantir que você é livre para recusar ou retirar o consentimento sem qualquer empecilho. RQ013 e RQ031 - IP

ANEXO G – TABELA DE FINALIDADES DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS - Sabin

TABELA DE FINALIDADES DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Processo	Titulares	Grupo de Dados	Dados	Finalidade	Base Legal	Armazenamento	Descarte
Cadastro de clientes: unidades de coleta, sites, aplicativos, pré-cadastros, e-commerce, hospitais parceiros, clínicas de medicina ocupacional, execução de exames e notificações à secretaria de saúde e vigilância sanitária	Clientes	Dado pessoal	Nome, telefone, endereço, data de nascimento, sexo biológico.	Cadastro do cliente nos sistemas de informação (LIS e PACS) para execução do(s) exame(s).	Cumprimento de obrigação legal (RDC-786)	Os dados de clientes e respectivos resultados ficam armazenados localmente em nosso datacenter, nos sistemas de informação. (LIS e PACS)	Os dados ficam armazenados sem um tempo máximo para comodidade de acesso pelos nossos clientes ou até que seja solicitada a sua exclusão, respeitado o prazo mínimo legal de 20 anos.
			RG/CPF	Identificação única do paciente/evitar homônimos Diretriz do controlador com foco na integridade dos dados	Legítimo interesse do controlador		
			e-mail	Envio de nota fiscal em atendimentos particulares e recuperação de acesso aos resultados pelo site Sabin.	Execução de contrato (prestação de serviços de medicina diagnóstica)		
		Dados pessoais sensíveis	Requisição de exames (pedidos médicos ou autopedido)	Realização de exames.	Execução de contrato (prestação de serviços de medicina diagnóstica		
			Resultados de exames anteriores	Apoio diagnóstico, análise comparativa	Consentimento		
			Anamnese (Peso, Altura, Medicação em Uso, Abstinência sexual, atividades físicas, data última menstruação, etc.)	Identificar possibilidades de interferência em resultados de exames.	Execução de contrato (prestação de serviços de medicina diagnóstica)		
	Médico Solicitante	Dados pessoal	Nome e CRM	Registro do solicitante dos exames	Cumprimento de obrigação legal (RDC-786)		
Recrutamento e Seleção	Candidatos	Dado Pessoal	Nome, e-mail, Data de nascimento, filiação, RG, CPF, Estado Civil, Telefones, Redes sociais, Endereço, Currículo contendo dados pessoais e de contato do candidato.	Realizar seleção e entrevistas de candidatos	Interesses legítimos do controlador, para avaliação de perfil profissional com o objetivo de contratação de pessoal.	São impressos e ficam arquivados na pasta do RH no setor administrativo, com acesso exclusivo pelo pessoal do setor	Os currículos são armazenados por pelo menos um ano, mediante autorização dos candidatos, e posteriormente descartados.
		Dado Pessoal Sensível	deficiência, laudo médico, raça gênero,		Exercício regular de direito, consentimento, inclusão social e programa de diversidade	Plataforma de Seleção	
RH e DP	Colaboradores	Dado Pessoal	Nome completo, data de nascimento, RG, CPF, Carteira de Trabalho, PIS, Título de Eleitor, Carteira de Motorista, Certidão de Casamento, Foto 3x4, histórico acadêmico, registro em conselho profissional, Contrato de Trabalho, Ficha de Registro de colaborador	Cadastro do colaborador no sistema do RH (protheus), do departamento pessoal e da contabilidade para manutenção do trabalhador e emissão de benefícios	Cumprimento de obrigação legal ou regulatória (CLT, convenções sindicais)	ERP	A documentação referente ao contrato de trabalho e a ficha de registro ficam armazenadas por 30 anos após a rescisão.
		Dado Pessoal Sensível	ASO, exames periódicos, carteirinha de vacinação, histórico de solicitação de descontos para exames	Manutenção do vínculo empregatício, seguir com obrigação específica para colaboradores de laboratórios de análises clínicas	Cumprimento de obrigação legal ou regulatória (CLT, convenções sindicais)	ERP	
	Dependentes	Dado pessoal	Certidão de Nascimento (menores de idade), RG, CPF	Cadastro dos dependentes dos colaboradores para liberação de benefícios	Cumprimento de obrigação legal ou regulatória (CLT, convenções sindicais)	ERP	Ainda não há rotina de descarte dos dados dos dependentes, seguindo eles o mesmo roteiro que os dados dos colaboradores.
		Dado Pessoal Sensível	Histórico de solicitação de descontos para exames	Cadastro dos dependentes dos colaboradores para liberação de benefícios	Cumprimento de obrigação legal ou regulatória (CLT, convenções sindicais)	ERP	

ANEXO H – Figura de atendimento à Menores de 18 anos - Sabin

Tabela de atendimento à Menores de 18 anos

Faixa Etária	Menores de 12 anos	De 12 a 15 anos	16 e 17 anos
Assinatura de Termo de consentimento de menores	Sempre	Não	Não
Necessita de acompanhamento de um adulto?	Sempre	Sempre	Não, **exceto:** exames de BHCG, HIV e exames de imagem.
Quais exames podem ser feitos e qual o procedimento?	Pode executar qualquer exame de análises clínicas desde apresente pedido médico ou auto pedido preenchido pelos pais ou responsável legal no ato do atendimento **Exceção:** execução de exames de BHCG, HIV e exames de Imagem, pois é necessário o pedido médico, o menor deverá estar também acompanhado por um dos pais ou responsável legal.	Pode executar qualquer exame de análises clínicas desde apresente pedido médico ou auto pedido preenchido pelos pais ou responsável legal no ato do atendimento **Exceção:** execução de exames de BHCG, HIV e exames de Imagem, pois é necessário o pedido médico, o menor deverá estar também acompanhado por um dos pais ou responsável legal.	Pode executar qualquer exame de análise clínica desde apresente pedido médico ou auto pedido preenchido pelo jovem no ato do atendimento. **Exceção:** execução de exames de BHCG, HIV e exames de Imagem, pois é necessário o pedido médico, o menor deverá estar também acompanhado por um dos pais ou responsável legal.
Entrega de resultados e senha de acesso	Somente para os pais, responsável legal ou terceiro que assinou o termo de consentimento de menor. Neste caso o documento do terceiro deverá estar anexado no cadastro da criança.	Para o próprio menor, para os pais, responsável legal.	Para o próprio menor ou para os pais e responsável legal.

ANEXO I – Inventário de dados pessoais e dados pessoais sensíveis - Sabin

INVENTÁRIO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

DADOS PESSOAIS TRATADOS	
Dados pessoais	**Justificativa**
nome	obrigação legal - RDC 786
telefone	obrigação legal - RDC 786
endereço	obrigação legal - RDC 786
Data de nascimento	obrigação legal - RDC 786
Sexo	obrigação legal - RDC 786
CPF	Evitar homônimos
RG	Evitar homônimos
Convênio médico	execução de contrato
Matrícula do beneficiário convênio	execução de contrato
Nome responsável	obrigação legal - RDC 786
Data de nascimento responsável	obrigação legal - RDC 786
Sexo responsável	obrigação legal - RDC 786
RG responsável	obrigação legal - RDC 786
CPF responsável	obrigação legal - RDC 786
e-mail responsável	obrigação legal - RDC 786
Grau de parentesco do responsável	obrigação legal - RDC 786
Nome do médico que solicitou exames	obrigação legal - RDC 786
CRM do médico que solicitou exames	obrigação legal - RDC 786
Tipo da amostra	obrigação legal - RDC 786

DADOS PESSOAIS SENSÍVEIS TRATADOS	
Dados pessoais sensíveis	**Justificativa**
pedidos médicos	execução de contrato
doenças diagnosticadas	informação importante para determinados exames
medicamentos	obrigação legal - RDC 786
terapias	Interferência em exames
Tempo de abstinencia sexual	Interferência em exames
Gravidez	Interferência em exames
Ciclo menstrual	obrigação legal - RDC 786
possui marcapasso	Interferência em exames
CID	execução de contrato
relatórios médicos	execução de contrato
Informações de transfusão	informação importante para determinados exames
Informação de vasectomia	informação importante para determinados exames
Informação de transplantado	informação importante para determinados exames
Informação de tabagismo	informação importante para determinados exames
Informação sobre sono	informação importante para determinados exames
Alergias	informação importante para determinados exames
peso	informação importante para determinados exames
altura	informação importante para determinados exames
local de coleta do material	obrigação legal - RDC 786
Informações de animal de estimação	informação importante para determinados exames
Informações sobre atividade física	Interferência em exames
Sintomas	informação importante para determinados exames
Tempo de jejum	informação importante para determinados exames
Tempo de gestação	informação importante para determinados exames
Quantidade de embriões	informação importante para determinados exames
Uso de materiais de higiene	informação importante para determinados exames
Uso de esmalte	informação importante para determinados exames
auto-pedido	execução de contrato

ANEXO J – Política de Privacidade - Saude Mob

A seguir é apresentado a política de privacidade disponibilizada pelo Saúde Mob transcrito para texto. A transcrição foi obtida no dia 25/06/2023. Transcrição

J.1 Introdução

O grupo Hermes Pardini cumpridor de seus deveres e obrigações adota medidas rigorosas de privacidade e proteção de dados pessoais. Entendemos que você está ciente e se preocupa com seus interesses pessoais de privacidade.

Esta Política de Privacidade e Proteção de Dados Pessoais expressa nosso compromisso com o tratamento de seus dados pessoais de modo responsável, ético, em linha com nossos princípios e valores e, especialmente, de acordo com as regras da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - "LGPD") e demais legislações vigentes aplicáveis. Reconhecemos que esta é uma responsabilidade constante e, portanto, atualizaremos periodicamente esta Política à medida que se fizerem necessários novos procedimentos de privacidade e proteção de seus dados pessoais.

Ao utilizar nossos serviços, bem como nosso site ou aplicativo, você concorda com o tratamento de seus dados pessoais como está descrito nesta Política de Privacidade e Proteção de Dados Pessoais.

Se você tiver alguma dúvida sobre esta Política de Privacidade e Proteção de Dados Pessoais, entre em contato com o(a) nosso(a) DPO/Encarregado(a), Fabiana Ricco, através do e-mail privacidade@grupopardini.com.br. RQ070 - I

J.2 Definições

Adolescente: pessoa física entre 12 (doze) e 18 (dezoito) anos de idade, segundo o Estatuto da Criança e do Adolescente ("ECA").

Agentes de tratamento: controlador e/ou operador.

Autoridade Nacional de Proteção de Dados – ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do

tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal.

Cliente: pessoa física que utiliza os serviços do grupo Hermes Pardini.

Criança: pessoa física com até 12 (doze) anos de idade incompletos, segundo o Estatuto da Criança e do Adolescente ("ECA").

Compartilhamento: transferência ou interconexão de dados pessoais com áreas internas ou terceiros.

Confidencialidade: garantia de que os dados pessoais não serão divulgados para pessoas não autorizadas.

Controlador: pessoa física ou jurídica, de direito público ou privado, a quem compete a decisão sobre o tratamento do dado pessoal.

RQ001 - I

Consentimento: manifestação livre, informada e inequívoca do titular do dado confirmando sua concordância quanto ao tratamento de seus dados pessoais.

Cookies: pequenos arquivos de texto enviados pelo site ao computador do Usuário e que nele ficam armazenados com informações relacionadas à navegação do site. São utilizados para fazer o site funcionar ou funcionar de forma mais eficiente, bem como para fornecer informações aos proprietários do site, de forma que seja possível reconhecer e lembrar de suas preferências. Essas informações podem ser utilizadas para fornecer um serviço mais personalizado e ágil.

Dado Pessoal: informação que individualmente ou em conjunto com outras, permite a identificação do indivíduo de forma direta ou indireta, tal como, nome, endereço, e-mail, CPF, RG, título de eleitor, telefone (s), profissão, sexo, data de nascimento, estado civil, grau de instrução, nacionalidade, dados do cônjuge/dependentes, entre outros.

Dado Pessoal Sensível: categoria de dado pessoal que, pelo seu potencial discriminatório, requer um nível extra de proteção e um elevado dever de cuidado. São dados pessoais que podem revelar origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dado Pessoal de Geolocalização: categoria de dados pessoais referentes à localização via GPS e WIFI obtidos a partir do dispositivo móvel do usuário, a fim de proporcionar aos usuários a melhor experiência dentro do app do grupo Hermes Pardini.

Acesso aos arquivos: Utilizaremos a escrita ou gravação (WRITE$_{E}XTERNAL_{S}TORAGE$)$eleitura$

Direitos do titular: o titular do dado tem o direito de obter informações e realizar solicitações junto ao controlador, tais como: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados Pessoais – "LGPD"; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados com o consentimento do titular; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) revogação do consentimento.

RQ003 - IP

RQ105, RQ112 - IP

RQ106, RQ113, RQ114 - IP

RQ107 - IP

RQ115

RQ006, RQ059 - IP

RQ069 - I

Doador: pessoa física que realiza doação de sangue ou outro material genético para realização de algum exame ou transfusão.

Encarregado/DPO: pessoa física ou jurídica indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Eliminação: exclusão de dado pessoal ou de conjunto de dados pessoais armazenados em banco de dados, independentemente do procedimento empregado.

LGPD: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) que traz regras e disposições sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador, sem tomar qualquer decisão sobre como tratar os dados.

Marco Civil da Internet: Lei 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Pseudonimização: processo a ser aplicado em um dado pessoal para torná-lo pseudonimizado, ou seja, dado pessoal que tenha sido descaracterizado ou codificado de modo que não permita a identificação do titular em um primeiro momento, mas que, após associação com outros dados, leva à sua identificação. Os dados pseudonimizados são aqueles que permitem a associação a um indivíduo a partir de informações mantidas pelo controlador em ambiente separado e seguro, como no caso da segregação da base de dados ou da atribuição de identificadores a indivíduos.

Retenção dos dados pessoais: período pelo qual os dados pessoais permanecem armazenados mesmo após o término da finalidade do tratamento.

Terceiros: pessoas físicas ou jurídicas parceiras do grupo Hermes Pardini, prestadores de serviços, médicos ou fornecedores.

Titular: pessoa física a quem se referem os dados pessoais que são objeto do tratamento.

Tratamento de Dados: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuário: pessoa física que navega no site do grupo Hermes Pardini. O Usuário é Titular de dados pessoais.

Vazamento: divulgação ilícita ou acesso não autorizado a dados pessoais.

Seções desta Política de Privacidade e Proteção de Dados Pessoais Esta Política de Privacidade e Proteção de Dados Pessoais informa quais dados pessoais coletamos sobre você, para o que usamos, como e onde armazenamos e com quem compartilhamos. Também define os seus direitos em relação aos seus dados pessoais e quem você pode contatar para obter mais informações ou esclarecimentos a respeito desse tema. Veja abaixo as seções desta Política:

Como coletamos os seus dados pessoais; Tipos de dados pessoais que coletamos; Como utilizamos seus dados pessoais; Fundamentos legais para tratar os seus dados pessoais; Compartilhamento de seus dados pessoais; Dados de Crianças e Adolescentes; Retenção de seus dados pessoais; Segurança de seus dados pessoais; Gestão de Cookies; Seus direitos; Alterações nesta Política de Privacidade e Proteção de Dados Pessoais; Reclamações, dúvidas e/ou solicitações;

J.3 1. Como coletamos os seus dados pessoais

Coletamos seus dados pessoais e dados pessoais sensíveis (em conjunto referidos nesta Política simplesmente como “dados pessoais”) automaticamente quando você visita nosso site, utiliza nossos aplicativos, e-mails ou anúncios. Também coletamos seus dados pessoais durante a prestação de nossos serviços. Assim, a coleta de dados pode advir das seguintes fontes:

RQ034 - I

Diretamente do titular: podemos coletar dados pessoais que você nos forneceu quando, por exemplo, você nos contrata para prestação de serviços, quando está na condição de doador (por exemplo, para realizar um exame de sangue), porque seu paciente nos forneceu (por exemplo, se você é médico e seu paciente irá realizar algum exame em algum de nossos laboratórios), ou porque estão publicamente disponíveis. Ainda, podemos coletar dados pessoais de incapazes e relativamente incapazes, como por exemplo

crianças, adolescentes, interditados e curatelados, fornecidos pelo próprio titular ou por seus pais ou responsáveis legais. Via interação com o nosso site e/ou aplicativo: através de sua interação em nosso site, nosso aplicativo, podemos coletar dados pessoais sobre você para a prestação de serviços (por exemplo, podemos coletar seus dados pessoais para: o agendamento de um exame, divulgar resultados ou registrar uso de medicamentos). Também podemos coletar ou obter dados pessoais sobre você pela maneira como você interage com nosso site e/ou aplicativo, para fornecer informações que acreditamos ser de seu interesse. Ainda, podemos coletar dados referente à geolocalização do dispositivo utilizado para garantir agilidade nos atendimentos e indicar a nossa unidade de atendimento ou colhedor em domicílio mais próximo de você. Por fim, podemos utilizar a sua câmera para que nosso sistema consiga executar o módulo de realidade aumentada com objetivo de melhorar a interação e experiência durante a visualização do resultado no app. Através de terceiros: também podemos coletar seus dados pessoais através de parceiros, médicos ou fornecedores. Neste caso, adotamos medidas para garantir que foram cumpridas as regras de privacidade e proteção de dados pessoais, dispostas na LGPD, incluindo a coleta de termo de consentimento, se assim for necessário. Via sistemas integrados: através de sistemas integrados entre laboratórios do grupo Hermes Pardini e entre estes e laboratórios conveniados, para realizar exames e/ou checar o histórico de exames e demais informações necessárias para realizar a nossa prestação de serviços.

J.4 2. Tipos de dados pessoais que coletamos

Clientes e usuários do nosso site/aplicativo: durante a prestação de nossos serviços ou mesmo durante a navegação em nosso site e aplicativo, podemos coletar alguns dados pessoais sobre você, tais como:

RQ094 - IP

Dados de identificação: nome, RG, CPF, idade, sexo, endereço de e-mail, endereço comercial/residencial, telefone, data de nascimento, estado civil, carteirinha do plano, filiação, convênio médico, documentos para fins de identidade (tais como documentos de conselho de classe, carteira nacional de habilitação, número do passaporte e outros documentos oficiais) e imagens de circuito interno de câmeras. Dados sensíveis: dados relacionados a sua saúde, relatórios médicos, solicitações médicas, resultados de exames, medicamentos que você utiliza, dados genéticos, dados biométricos, etnia, orientação sexual e religião Dados financeiros: informações sobre pagamento, conta bancária e dados de cartões de crédito. Dados de navegação: login e senha de acesso, postagens em nossas mídias sociais, endereço IP, tipo de navegador e idioma, horários de acesso, detalhes de solicitações e de como você usa nossos serviços e de sua interação conosco. Além disso e prezando pela transparência na relação com nossos clientes sinalizamos, também coletamos cookies quando você acessa nosso site e/ou aplicativo, para melhor experiência do usuário, seguindo as regras da nossa Política de Cookies. Acompanhantes de clien-

tes: durante a prestação de nossos serviços podemos coletar dados de identificação sobre seus acompanhantes presentes durante a realização de algum exame ou procedimento, tais como: Nome, RG, CPF e imagens de circuito interno de câmeras. Médicos: durante a prestação de nossos serviços podemos coletar dados de identificação sobre os médicos responsáveis pelas solicitações dos exames, a saber: nome, especialidade profissional e CRM

J.5 3. Como utilizamos seus dados pessoais

Coletamos, armazenamos e tratamos seus dados pessoais para diversas finalidades ligadas ao nosso negócio, tais como:

Clientes e usuários do nosso site/aplicativo Dados identificação: para identificar e confirmar sua identidade para atendimentos, solicitar autorização junto às operadoras de planos de saúde, realizar agendamentos, informar preparos para exames, divulgar produtos e serviços, assegurar o acesso às unidades do grupo Hermes Pardini e atender às determinações legais e regulatórias. Dados sensíveis: entender histórico clínico, apoiar na descrição de resultados e direcionamento de diagnósticos e realizar exames. Dados financeiros: identificar, agendar e faturar pagamentos e atender questões fiscais, legais e regulatórias. Dados de navegação: agendar procedimentos e realizar atendimentos on-line, cumprir determinações legais de coleta de dados pessoais dispostas no Marco Civil da Internet (Lei nº 12.965/2014), promover melhorias na experiência de navegação e realizar análises estatísticas. Dados de navegação: Dados de identificação: para fins de identificação e controle de acesso. Médicos Dados de identificação: para fins de identificação, confirmação da solicitação médica e registro.

J.6 4. Fundamentos legais para tratar os seus dados pessoais

A LGPD dispõe que o tratamento de dados pessoais apenas deve ocorrer mediante fundamento legal. Assim, destacamos abaixo as hipóteses legais em que os seus dados pessoais poderão ser tratados, quando estamos na posição de Controlador, aplicando-se de acordo com a categoria dos dados (dados pessoais ou dados pessoais sensíveis):

RQ001 - IP e RQ033 - I

Mediante o fornecimento do seu consentimento para tratamento de seus dados pessoais, como por exemplo, para lhe conceder acesso ao site, aplicativo ou outras plataformas mantidas pelo grupo Hermes Pardini ou receber informações via e-mail sobre seus interesses;

RQ010 - IP

Quando existentes legítimos interesses para tratamento de seus dados pessoais como no oferecimento e entrega de nossos serviços para você, bem como para o funcionamento eficaz e lícito de nossa prestação de serviços, desde que tais interesses não sejam superados pelos seus interesses, direitos e liberdades fundamentais;

RQ014, RQ035, RQ076 - IP

Para o cumprimento

de obrigações legais e regulatórias que podem exigir a coleta, armazenamento e compartilhamento de seus dados pessoais e dados pessoais sensíveis, tais como manutenção de registros para fins fiscais ou fornecimento de informações a um órgão público ou entidade reguladora de leis/atividades do objeto social do grupo Hermes Pardini e cumprimento de obrigações de combate à corrupção, lavagem de dinheiro, fraude e condutas irregulares; Para executar eventual contrato, bem como para fornecer nossos serviços a você; Para exercer regularmente nossos direitos em contratos, processos judiciais, administrativos ou arbitrais; Para proteção da vida ou da sua incolumidade física; Para tutelar sua saúde; para proteção de nosso crédito; Para garantir a prevenção à fraude e à sua segurança, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Quando o grupo Hermes Pardini atuar na posição de Operador, a hipótese legal em que os dados pessoais serão tratados será definida pelo Controlador do dado pessoal.

RQ015 - I

RQ009 - I

RQ075 - IP

RQ011 - I

J.7 5. Compartilhamento de seus dados pessoais

No decorrer da prestação de nossos serviços, poderemos compartilhar seus dados pessoais com:

Laboratórios, hospitais, profissionais médicos, e unidades de atendimento do grupo Hermes Pardini para, por exemplo, exercer regularmente algum direito ou executar devidamente os serviços contratados; Terceiros que nos prestam serviços nas condições de operadores de tratamento de dados pessoais; Autoridades competentes (incluindo tribunais e autoridades que nos regulam); Empresas de tecnologia que fazem a gestão dos nossos sistemas integrados ou responsáveis pelo armazenamento e garantia de segurança no tratamento de seus dos dados pessoais; internamente para áreas que necessitam ter acesso aos dados pessoais, tais como: área técnica responsável pelos exames, área de atendimento ao cliente e área jurídica para cumprir alguma obrigação legal regulatória ou exercício regular dos nossos direitos. De qualquer forma, o grupo Hermes Pardini exigirá que os terceiros acima indicados:

RQ029 - I

RQ129 - IP

Comprometam-se a cumprir as leis de proteção de dados e os princípios desta Política; Somente processem os Dados Pessoais para os fins descritos nesta Política; Implementem medidas de segurança técnica e organizacional apropriadas projetadas para proteger a integridade e confidencialidade de seus Dados Pessoais. Ao realizar interação com nosso site ou aplicativo, que eventualmente permitam compartilhar conteúdo com outros usuários, os dados pessoais e informações que você publicar podem ser lidas, coletadas e usadas por outros usuários do site ou aplicativo. Temos pouco ou nenhum controle sobre esses outros usuários e, portanto, não podemos garantir que qualquer informação ou dado pessoal que você forneça nesse contexto será tratado de acordo com esta Política de Privacidade e Proteção de Dados Pessoais.

RQ026 - IP

Além disso, ao realizar solicitações de atendimento, agendamentos, pré-atendimentos e falar conosco pelo nosso site, seus dados pessoais serão compartilhados com nossos atendentes e prestadores de serviços de infraestrutura dos sistemas geridos pelo grupo Hermes Pardini, os quais são treinados e capacitados a tratar seus dados pessoais de forma ética e em linha com esta Política. Outros compartilhamentos podem ser realizados com a finalidade de atender as suas solicitações e prestar devidamente os serviços contratados. Para informações detalhadas sobre os nomes dos terceiros com os quais compartilhamos seus dados pessoais, entre em contato com o(a) nosso(a) DPO/Encarregado(a) através do e-mail privacidade@grupopardini.com.br.

J.8 6. Dados de Crianças e Adolescentes

Durante a prestação de serviços, o grupo Hermes Pardini poderá coletar dados pessoais de crianças e adolescentes e garantirá que o tratamento sempre ocorra no melhor interesse da criança e do adolescente.

RQ016 - IP

Crianças: O tratamento de dados pessoais de crianças será realizado mediante consentimento específico e em destaque de pelo menos um de seus pais ou responsável legal. Em caso de urgência/emergência, a coleta e tratamento dos dados pessoais da criança será realizado imediatamente para proteção de sua vida e, posteriormente, será comunicado a um de seus pais ou responsável legal. As mesmas disposições serão aplicáveis aos dados pessoais de interditados e curatelados. Adolescentes: Em relação ao adolescente, o tratamento de seus dados pessoais poderá ocorrer independentemente do consentimento de um dos pais ou responsável legal, desde que presente outro fundamento legal que autorize o tratamento, nos termos da LGPD.

J.9 7. Retenção de seus dados pessoais

Armazenamos e mantemos seus dados pessoais de forma segura em data centers localizados no Brasil, em conformidade com a legislação aplicável e pelo período necessário ou permitido em vista das finalidades para as quais os dados pessoais foram coletados, conforme exposto nesta Política de Privacidade e Proteção de Dados Pessoais.

Os critérios utilizados para determinar os períodos de retenção incluem, mas não se limitam a:

Duração do nosso relacionamento com você; Enquanto válido seu consentimento, nas hipóteses aplicáveis; Diante de eventual obrigação legal ou regulatória que exija a manutenção dos dados pessoais; Quando necessário para atividade ou serviços relevantes; Para atender prazos prescricionais aplicáveis, conforme previsto em lei ou regulamento.

RQ030 - IP

J.10 8. Segurança de seus dados pessoais

RQ088, RQ091 - IP

Estamos comprometidos em proteger a sua privacidade e seus dados. Para isso, adotamos medidas de segurança, técnicas e administrativas aptas a proteger os seus dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, o que inclui, mas não se limita à:

RQ002 e RQ062 - I e RQ008 - IP

RQ055, RQ125 - IP

RQ084

RQ056, RQ121 - IP

Limitação do acesso a dados pessoais por parte dos colaboradores, prestadores de serviços e visitantes, restringindo-o apenas nos limites da necessidade e finalidade de tratamento dos dados pessoais; Garantia de que todos os nossos colaboradores cumprem esta Política, são constantemente treinados e capacitados para realizar procedimentos adequados para o correto tratamento de seus dados pessoais; Utilização de tecnologias concebidas para proteger seus dados pessoais durante o compartilhamento com empresas terceiras; Utilização de medidas técnicas capazes de inibir/mitigar riscos de eventuais maliciosos em nossos sistemas; Adoção de sistemas estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD; Manutenção recorrente do banco de dados; Utilização de ferramenta de categorização do gartnes, efetuando backup na nuvem com conteúdo criptografado; Utilização de tecnologias concebidas para proteger os dados pessoais durante a sua transmissão, como encriptação SSL dos dados que você fornece em determinadas partes do nosso site e utilização de segurança adequada para proteger os dados pessoais recebidos. Também aplicamos processos e medidas, padrão da indústria para a detecção e resposta a tentativas de violação dos nossos sistemas. Entretanto, não existe um método de transmissão pela Internet ou um método de armazenamento eletrônico que seja 100% seguro. Por conseguinte, não podemos garantir a segurança absoluta das suas informações, apesar de serem tomadas todas as precauções necessárias e exigidas pelos órgãos competentes.

A Internet, dada a sua natureza, é um fórum público e por isso recomendamos que você tenha cautela ao divulgar informações online. Frequentemente, você se encontra na melhor posição para proteger a si mesmo online. Você é responsável pela proteção do seu nome de usuário e senha contra o acesso de terceiros, assim como pela escolha de senhas seguras.

J.11 9. Gestão de Cookies

Sempre que você utilizar nosso site, coletaremos cookies para melhorar sua experiência de navegação. Você poderá se opor a coleta de alguns tipos de cookies através do nosso site, bastando que desative esta opção no seu próprio navegador ou aparelho.

A desativação dos cookies, no entanto, pode afetar a disponibilidade de algumas

ferramentas e funcionalidades do site, comprometendo seu correto e esperado funcionamento. Outra consequência possível é remoção das suas preferências que eventualmente tiverem sido salvas, prejudicando sua experiência.

J.12 10. Seus Direitos

Você possui vários direitos em relação aos seus dados pessoais, nos termos da LGPD. Para tanto, implementamos controles adicionais de transparência e acesso em nossa área de Privacidade para disponibilizar aos usuários o acesso livre e gratuito a esses direitos. Neste contexto, você tem o direito a:

RQ049 e RQ109 - IP

RQ050, RQ051, RQ103, RQ110 - IP

RQ104, RQ111 - IP

RQ028, RQ108 - I

RQ068 - I, RQ102 - IP

Confirmação de que estamos tratando seus dados pessoais; Acessar os dados pessoais que tratamos sobre você; Solicitar a alteração ou atualização de seus dados pessoais quando estiverem incorretos, incompletos ou inexatos; Solicitar que os dados pessoais que você entenda como desnecessários, excessivos ou tratados em desconformidade com a LGPD sejam anonimizados, bloqueados ou eliminados, desde que permitido pelas legislações/regulamentos que estejam relacionados ao objeto social do grupo HERMES PARDINI; Se opor ao tratamento de dados pessoais, quando não tivermos mais necessidade legítima ou legal de tratá-los; Solicitar a transmissão dos dados pessoais que tratamos sobre você para outro fornecedor; Solicitar informações das entidades públicas e privadas com as quais compartilhamos seus dados pessoais; Revogar o consentimento concedido, solicitar a eliminação dos dados pessoais tratados com base em consentimento, bem como de ter acesso a informações sobre a possibilidade de você não fornecer o consentimento e as respectivas consequências da negativa; e Solicitar a revisão do tratamento de dados pessoais com base em decisões automatizadas. Se você tiver alguma dúvida, observação, solicitação, reclamação ou revisão sobre a coleta ou o uso de seus dados pessoais ou sobre esta Política de Privacidade e Proteção de Dados Pessoais, você pode entrar em contato com o(a) nosso(a) DPO/Encarregado(a), através do envio de e-mail para o endereço eletrônico privacidade@grupopardini.com.br

J.13 11. Alterações nesta Política de Privacidade e Proteção de Dados Pessoais

A presente Política de Privacidade e Proteção de Dados Pessoais poderá ser alterada a qualquer tempo. Portanto, recomendamos que você reveja esta Política de tempos em tempos para ser informado sobre como estamos protegendo suas informações.

Todas as alterações serão comunicadas por meio de um aviso em destaque na tela inicial do nosso site/aplicativo ou por meio de qualquer outra forma de comunicação com você.

J.14 12. Reclamações, dúvidas e/ou solicitações

Se você não estiver satisfeito com a maneira como tratamos os seus dados pessoais ou em caso de qualquer dúvida, reclamação, preocupação ou solicitações relacionadas a sua privacidade e proteção de seus dados pessoais, você pode entrar em contato com o(a) nosso(a) DPO/Encarregado(a), através do envio de e-mail para o endereço eletrônico privacidade@grupopardini.com.br

ANEXO K – Nota Informativa - Saúde Mob

A seguir é apresentada a nota informativa disponibilizada pelo Saúde Mob transcrito para texto. A transcrição foi obtida no dia 25/06/2023.

Transcrição

A seguir estão descritas as regras aplicáveis à utilização do Saúde Mob e seus serviços – disponibilizado pelo Instituto Hermes Pardini S/A, inscrita no CNPJ nº 19.378.769/0001-76 e sediado na Rua Aimorés, nº 66, bairro Funcionários, Belo Horizonte, Minas Gerais, CEP 30.140-920, único e exclusivo proprietário do domínio www.hermespardini.com.br.

Ao realizar o acesso ao Saúde Mob, o usuário se submeterá automaticamente às regras e condições destes Termos de Uso.

O uso do Saúde Mob deve ser feito em caráter pessoal e intransferível. Não é permitido compartilhamento dos dados de acesso ao Portal do Conhecimento em qualquer site ou ambiente virtual.

O Instituto Hermes Pardini S/A poderá, sem prévio aviso, bloquear e cancelar o acesso ao Saúde Mob quando verificar que o usuário praticou algum ato ou mantenha conduta que (i) viole as leis e regulamentos federais, estaduais e/ou municipais, (ii) contrarie as regras destes Termos de Uso, ou (iii) viole os princípios da moral e dos bons costumes.

O usuário autoriza o Instituto Hermes Pardini S/A, ou terceiros por ela indicados, a utilizar, por prazo indeterminado, as informações fornecidas durante o uso do Saúde Mob para fins estatísticos e envio de material publicitário, newletters, informes etc.

O Instituto Hermes Pardini S/A se reserva do direito de incluir, excluir ou alterar os conteúdos e funcionalidades do Saúde Mob, bem como suspendê-lo temporariamente ou cancelá-lo, a qualquer momento, independentemente de aviso-prévio ao usuário. Da mesma forma, poderá modificar estes Termos de Uso, cuja versão mais recente estará sempre disponível para consulta no próprio Saúde Mob.

O INSTITUTO HERMES PARDINI S/A SE EXIME DE TODA E QUALQUER RESPONSABILIDADE PELOS DANOS E PREJUÍZOS DE QUALQUER NATUREZA QUE POSSAM DECORRER DO ACESSO, INTERCEPTAÇÃO, ELIMINAÇÃO, ALTERAÇÃO, MODIFICAÇÃO OU MANIPULAÇÃO, POR TERCEIROS NÃO AUTORIZADOS, DOS DADOS DO USUÁRIO DURANTE A UTILIZAÇÃO DO PORTAL DO CONHECIMENTO.

As informações solicitadas ao Usuário no momento do acesso e uso do Saúde Mob serão utilizadas pelo Instituto Hermes Pardini S/A somente para os fins previstos

nestes Termos de Uso e em nenhuma circunstância, tais informações serão cedidas ou compartilhadas com terceiros, exceto por ordem judicial ou de autoridade competente.

K.1 Do uso do Portal do Saúde Mob

O início de utilização do Saúde Mob implica em aceitar todos os termos e condições deste Termo. Caso o usuário não concorde com os termos e condições estipulados neste termo de uso, deverá interromper imediatamente a utilização do Saúde Mob. Direitos de Propriedade: O usuário reconhece expressamente que o Saúde Mob, assim como os logotipos, marcas, insígnias, símbolos, sinais distintivos, manuais, documentação técnica associada e quaisquer outros materiais correlatos ao Saúde Mob, constituem, conforme o caso, direitos autorais, segredos comerciais, e/ou direitos de propriedade do Instituto Hermes Pardini S/A, sendo tais direitos protegidos pela legislação nacional e internacional aplicável à propriedade intelectual e aos direitos autorais, especialmente pelo que contém as Leis números 9.609 e 9.610 de 19/12/1998. Fica expressamente vedado ao usuário, em relação ao Saúde Mob: ceder, doar, alugar, vender, arrendar, emprestar, reproduzir, modificar, adaptar, traduzir, disponibilizar o acesso de terceiros, via on-line, acesso remoto ou de outra forma; incorporar a outros sistemas ou programas, próprios ou de terceiros; oferecer em garantia ou penhor; alienar ou transferir, total ou parcialmente, a qualquer título, de forma gratuita ou onerosa; decompilar, mudar a engenharia (reengenharia), enfim, dar qualquer outra destinação ao Saúde Mob – ou parte dele – que não seja a disposta neste Termo.

K.2 Dos direitos e deveres do usuário

O Usuário será responsável pela correta e idônea utilização do Login e Senha, de seu uso exclusivo durante a utilização do Saúde Mob. O Usuário deverá providenciar, por conta própria, seu acesso ao Saúde Mob e os requisitos mínimos para o funcionamento do mesmo. O Usuário se compromete a comunicar imediatamente ao Instituto Hermes Pardini S/A a eventual perda ou roubo de sua senha de acesso, assim como qualquer risco de acesso a ela por terceiros. Os dados pessoais são de total responsabilidade do Usuário, arcando com sanções civis e penais que eventualmente gerarem no uso indevido do documento de outrem. Lembrando que estes dados deverão ser preenchidos com responsabilidade no Cadastro de Usuário.

K.3 Dos dados pessoais tratados

O Instituto Hermes Pardini S/A, durante a utilização do Saúde Mob, fará o tratamento dos seguintes dados pessoais de seus usuários:

Pacientes: nome completo, nome social, nome da mãe, foto, sexo, data de nascimento, CPF, e-mail, telefone, endereço, localização; Colhedores: nome completo, foto; Médicos: nome completo, CRM.

K.4 Do armazenamento dos dados pessoais

RQ057 - IP

Os dados pessoais tratados pelo Instituto Hermes Pardini S/A em consequência do uso do Saúde Mob serão armazenados em servidores próprios do Instituto Hermes Pardini S/A.

Fica eleito o Foro da cidade de Belo Horizonte, Estado de Minas Gerais, para dirimir quaisquer questões decorrentes destes Termos de Uso, que será regido pelas leis brasileiras.