# Especificação de requisitos de *design* de software para sistemas de IoT conforme a LGPD: Resultados de aplicação em um sistema de assistência para pacientes com Diabetes Mellitus.

**João Pedro Ribeiro**[1], **Lina Garcés**[1]

[1]Instituto de Matemática e Computação – Universidade Federal de Itajubá (UNIFEI)
Av. BPS, 1303. Pinheirinho. CEP: 37500-903 – Itajubá – MG – Brasil

{jpribeiro55, lina}@unifei.edu.br

***Abstract.*** *With the evolution of the Internet of Things (IoT) and its operations in different domains, it is necessary to focus on the security and privacy of user data. This work investigates and proposes an approach for specifying and adapting requirements for IoT systems in healthcare, using the DiaMant@Home application as a scenario for compliance with the General Data Protection Law (LGPD). Goal-Oriented Requirement Engineering (GORE), a software engineering method for requirement specification, was used. As a result, a set of functional and non-functional requirements was proposed that can be reused for healthcare IoT systems that need to comply with the LGPD, supporting the software design phase related to security and privacy aspects in IoT systems for the protection of sensitive data and ensuring application integrity.*

***Resumo.*** *Com a evolução da Internet-das-Coisas (IoT, em inglês) e suas operações em diferentes domínios, se faz necessário focar na segurança e privacidade dos dados dos usuários. Este trabalho investiga e propõe uma abordagem para a especificação e adequação de requisitos para sistemas de IoT na área da saúde, usando a aplicação DiaMant@Home como cenário de adequação à Lei Geral de Proteção de Dados (LGPD). Foi usado o Goal Oriented Requirement Engineering (GORE), um método na engenharia de software para a especificação de requisitos. Como resultado, foi proposto um conjunto de requisitos funcionais e não funcionais que podem ser reutilizados para sistemas de IoT na saúde que precisem se adequar à LGPD, apoiando a etapa de design de software atrelados aos aspectos de segurança e privacidade em sistemas de IoT para proteção de dados sensíveis e garantia de integridade da aplicação.*

## 1. Caracterização do problema

O termo *Internet of Things* (IoT) ou Internet das Coisas pode ser definido como uma rede com dispositivos conectados que podem ser integrados à *internet* e que possuem a função de enviar, receber, coletar e armazenar dados [Kelly et al. 2020], podendo estar presente em diversos cenários tecnológicos. Com a presença da IoT em crescente evolução, principalmente na área da saúde, torna-se necessária a construção e adequação das soluções de IoT, com foco no controle e restrições de segurança, diminuindo os riscos à privacidade de seus usuários [Liu et al. 2018].

Com o intuito de sanar estas questões no meio digital e a ausente padronização nos tratamento de dados, em 2018, foi aprovada no Brasil, a Lei Geral de Proteção de Dados

(LGPD), que visa regulamentar e proteger todos os dados pessoais e intransferíveis de usuários em relação a empresas e sistemas que possuem os mesmos através de normas praticadas pelas organizações [Brasil 2018].

## 2. Motivação

Com base na teoria de especificação de requisitos da engenharia de *software*, é bem conhecido que o sucesso de um sistema depende de uma boa especificação de requisitos, ainda mais quando é necessário considerar as restrições impostas pela LGPD. Devido a sua recente aprovação, conforme estudos realizados na revisão bibliográfica do embasamento teórico, existem poucas diretrizes para orientar a adequação dos requisitos à LGPD, ainda mais considerando o cenário de IoT para a saúde.

## 3. Objetivos e contribuições

Esta pesquisa tem como objetivo investigar e propor uma abordagem de identificação, análise e adequações de requisitos funcionais e não funcionais de *software* com a utilização das técnicas de GORE e demais propostas desenvolvidas por [Mendes et al. 2021]. A pesquisa visa atender critérios da LGPD em sistemas de IoT na saúde, e consequentemente, apoiar a etapa de *design* de *software* para que os sistemas de IoT possam se adequar às restrições de privacidade e segurança impostas pela legislação. Desta forma, espera-se auxiliar os engenheiros de *software* na criação de arquiteturas que representam toda a estrutura para sistemas de IoT na saúde, de forma que sejam seguras e garantam a proteção dos dados dos usuários finais.

A aplicação desta pesquisa no cenário de estudo da arquitetura do sistema DiaManT@Home [Garcés et al. 2020] combinada dos procedimentos de GORE e das aplicações das técnicas de [Mendes et al. 2021] possuem o objetivo de estimular e guiar especialistas de tecnologia da informação na elaboração de requisitos funcionais e não funcionais em sistemas de IoT no âmbito da saúde.

## 4. Trabalhos relacionados

A seguir descrevemos alguns trabalhos relacionados que foram inspiração para a abordagem aqui apresentada.

O trabalho desenvolvido por [Mendes et al. 2021] propõe um *checklist* contendo 52 itens atribuídos sobre transparência, segurança, direitos e responsabilidades para avaliar sistemas em adequação à LGPD. Na pesquisa, os autores utilizam um cenário prático de uma aplicação do Governo Federal Brasileiro, descrevendo as técnicas empregadas para aplicação do *checklist*, incluindo referências a atributos de qualidade.

O trabalho realizado por [Camêlo 2022] aborda conceitos como *Privacy by Design* e *Privacy by Default*, que são metodologias de apoio para garantir a privacidade dos dados pessoais. Além disso, o guia apresenta atividades bem definidas, *templates* e um catálogo com padrões de requisitos de privacidade para auxiliar os analistas de requisitos na especificação dos requisitos de privacidade em conformidade com a LGPD.

Este trabalho traz uma evolução do corpo de conhecimento atual, no sentido que apresenta a aplicação de uma abordagem na adequação dos requisitos do sistema DiaManT@Home, um sistema de IoT de assistência domiciliar para pacientes com diabetes mellitus

## 5. Métodos

Como etapa inicial do projeto, foi necessário um entendimento da especificação de requisitos e da arquitetura do sistema DiaManT@Home [Garcés et al. 2020] antes da sua adequação à LGPD. Uma simplificação da arquitetura deste sistema de IoT é apresentada na Figura 1.

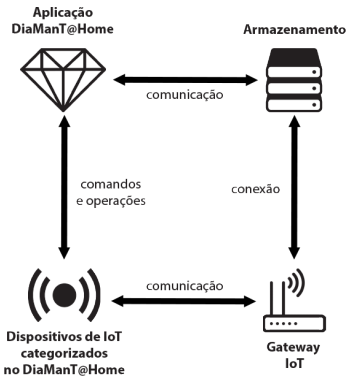


**Figura 1. Modelo de Arquitetura IoT do sistema DiaManT@Home**

DiaMant@Home é um sistema de IoT composto por dispositivos que de forma conjunta são responsáveis por apoiar o paciente com diabetes em atividades como [Garcés et al. 2020]: monitoramento de exercıcios, dieta, medicação, níveis de glicose, sinais vitais, atividades, assim como na geração de alertas, lembretes e relatórios.

Numa segunda etapa, os objetivos do sistema, e a definição requisitos de segurança e privacidade, e suas funcionalidades foram identificados pela estratégia *Goal Oriented Requirement Engineering* (GORE), que fornece um conjunto de "técnicas para elicitar, elaborar, estruturar, especificar, analisar, negociar, documentar e modificar requisitos" [Lamsweerde 2001]. A GORE promove a identificação de metas através do refinamento e abstração de requisitos com perguntas de *COMO*, *QUAIS* e *POR QUE* as funcionalidades e requisitos de adequação são necessárias.

A etapa a seguir consistiu em definir e responder questões relacionadas ao tratamento dos dados obtidos pelo sistema, meios de consentimento e medidas de segurança necessárias no sistema DiaMant@Home para se adequarem aos requisitos funcionais e não funcionais já existentes no sistema em questão. Para isso, foram usadas como base as diretrizes de adequação de requisitos apresentadas em [Mendes et al. 2021].

## 6. Resultados

A aplicação das diretrizes de [Mendes et al. 2021] junto com as técnicas de GORE facilitou a identificação de todos os requisitos de conformidade de segurança e integridade dos dados propostas pela LGPD necessários para aplicação no cenário de estudo, que até então não propunha soluções para o tratamento de dados relacionados à legislação em seus requisitos funcionais e não funcionais.

Como resultado, foram identificados 25 requisitos funcionais (RF) divididos em sete (7) categorias, e 16 requisitos não funcionais (RNF) classificados em cinco (5) categorias. Todos os RF e RNF foram especificamente definidos para possibilitar a conformidade do sistema de IoT DiaMant@Home à LGPD. A Tabela 1 apresenta a descrição de cada requisito especificado neste trabalho.

Tabela 1: Lista de Requisitos Funcionais e Não Funcionais para a Adequação de DiaMant@Home à LGPD

| **REQUISITOS FUNCIONAIS** |
|---|
| **Categoria: Tratamento de Dados de Usuário** |
| **RF01** - O sistema deverá permitir a inclusão, alteração, leitura e exclusão do cadastro de usuários de acordo com o cadastro das informações apresentadas para cada tipo de usuário.<br>**RF02** - O sistema deverá possuir um campo obrigatório de marcação contendo os termos de consentimento para leitura explícita, visando cumprir o Art. 5º, XII da LGPD.<br>**RF03** - O sistema deverá permitir a conclusão do cadastro do usuário exclusivamente após o mesmo concordar com o termo de consentimento que deverá abordar questões do Art. 9º da LGPD.<br>**RF04** - O sistema DiaManT@Home deverá exibir as hipóteses para tratamento de dados durante o cadastro de usuários, visando cumprir o Art. 7º e Art. 11º da LGPD.<br>**RF05** - O sistema deve permitir ao usuário cadastrado consultar seus dados de forma facilitada através de um botão no menu da aplicação.<br>**RF06** - O sistema deve permitir ao usuário revogar seu consentimento ao tratamento de dados dentro da aplicação, conforme preza o Art. 8º, § 5º da LGPD.<br>**RF07** - Caso seja de interesse do paciente, o mesmo poderá consultar os dados registrados sobre sua rotina a qualquer momento, cumprindo o Art. 18º, II, da LGPD. |
| **Categoria: Tratamento de Dados Clínicos do Paciente** |
| **RF08** - O sistema deverá manter de forma segura os dados sensíveis e clínicos dos pacientes, pacientes, como peso, altura, idade, sexo e informações de saúde da rotina do paciente |
| **Categoria: Relatórios** |
| **RF09** - O sistema deve permitir ao usuário o acesso à relatórios com suas informações pessoais, cumprindo o Art. 11º, § 4º, I da LGPD.<br>**RF10** - O sistema deve permitir aos stakeholders o acesso à informação de pacientes vinculados visando cumprir as hipóteses para tratamento dos dados. |
| **Categoria: Requisitos do Encarregado dos Dados** |
| **RF11** - O sistema deve manter em sua interface uma aba com os contatos disponíveis do encarregado pelo tratamento de dados pessoais dos usuários. |
| **Categoria: Atribuição de Responsabilidades** |
| **RF12** - O sistema deverá permitir que profissionais de saúde sejam atribuídos como responsáveis ao acompanhamento de pacientes cadastrados no sistema.<br>**RF13** - O sistema deverá permitir que familiares e amigos de pacientes possuam autonomia para realizar a inserção de dados no sistema. |
| **Categoria: Monitoramento da Rotina do Paciente** |
| **RF14** - Se o usuário paciente realizou o cadastro na aplicação e concordou com o termo de consentimento, o sistema deverá monitorar e registrar suas atividades diárias.<br>**RF15** - O profissional de saúde responsável por pacientes poderá através dos dados, incluir ou modificar o plano de atividades do paciente para cumprir os objetivos do tratamento de dados, conforme Art. 6º, I da LGPD.<br>**RF16** - O sistema deverá permitir que os profissionais de saúde cadastrados na aplicação possam alterar o plano nutricional do paciente, de forma consentida.<br>**RF17** - O sistema deverá permitir que o paciente registre dados sobre sua alimentação na aplicação de maneira consentida<br>**RF18** - O sistema deve informar no termo de consentimento do tratamento de dados que os alimentos cadastrados na aplicação poderão ser consultados por todos os tipos de usuário do *software*.<br>**RF19** - O sistema deverá registrar informações medicamentosas da rotina diária do paciente, sendo estes dados tratados para atingir os objetivos médicos e controle da saúde.<br>**RF20** - O sistema deverá manter dados de acompanhamento do nível de glicose no sangue do paciente. Estes dados deverão ser incluídos pelo paciente, ciente de que as informações serão compartilhadas.<br>**RF21** - O sistema deverá permitir que profissionais de saúde sejam responsáveis pela tutela de pacientes incapacitado. Este atributo está atrelado ao Art. 7º, VIII e Art. 11º, II, "f".<br>**RF22** - O sistema deverá deixar claro os objetivos a serem alcançados com a obtenção dos dados do paciente no controle de sua rotina, cumprindo o Art. 10º da LGPD.<br>**RF23** - O sistema devera manter dados de acompanhamento do nível de glicose no sangue do paciente. Estes dados devem ser incluídos pelo paciente, ciente de que as informações serão compartilhadas com profissionais de saúde, familiares ou amigos relacionados ao seu cadastro.<br>**RF24** - O sistema devera permitir que profissionais de saúde sejam responsáveis pela tutela de pacientes incapacitados para operar seus dados. |
| **Categoria: Finalidade do Uso dos Dados** |
| **RF25** - O sistema devera deixar claro os objetivos a serem alcançados com a obtenção dos dados do paciente no controle de sua rotina. |
| **REQUISITOS NÃO FUNCIONAIS** |
| **Categoria: Privacidade** |

Continua na seguinte página

**Tabela 1 – continuação**

| |
|---|
| **RNF01** - O sistema e seus dispositivos deverão possuir regras de boas práticas definidas pelo controlador e operador da aplicação em relação ao uso e tratamento de dados, a finalidade de manipulação e analise dos dados e possíveis riscos para o titular das informações fornecidas. Art. 50o da LGPD.<br>**RNF02** - O sistema e seus dispositivos deverão funcionar integralmente e evitar o uso de dados indevidos relacionados pelos stakeholders através de boas práticas de governança.<br>**RNF03** - O sistema e seus dispositivos deverão proteger informações confidenciais dos usuários cadastrados para evitar que seus dados sejam usados para outras finalidades externas.<br>**RNF04** - O sistema e seus dispositivos deverão passar por práticas de auditoria em segurança de informação para evitar possıveis ameaças através da abordagem de Privacidade desde a Concepção (PdC)<br>**RNF05** - O sistema e seus dispositivos só deverão permitir suas funcionalidades após consentimento do usuário ao aceitar os termos propostos, exceto na situação descrita no RF24.<br>**RNF06** - O sistema e seus dispositivos deverão manter um arquitetura de *logs* onde todas as operações para tratamento de dados devem ser registradas, incluindo tentativas de acesso não autorizados por usuários sem permissão necessária. |
| **Categoria: Segurança** |
| **RNF07** - O software e dispositivos deverão cumprir as determinações do Art. 2o da LGPD.<br>**RNF08** - O software e dispositivos deverão manter aspectos de qualidade e segurança de informação conforme a [ABNT 2013] explicitada na fundamentação de políticas de segurança e proteção de falhas.<br>**RNF09** - O sistema devera estabelecer conexões seguras em rede para controle das funcionalidades da IoT e das informaç es fornecidas pelos usuários, software e dispositivos, além das demais informações contidas no banco de dados da aplicação<br>**RNF10** - O software e dispositivos deverão manter mecanismos de autenticação para controle de acesso dos usuários e coleta de dados.<br>**RNF11** - O software e dispositivos deverão manter os conceitos de segurança definidos pelo Art. 6o, VII, da LGPD. |
| **Categoria: Confidencialidade** |
| **RNF12** - O software, dispositivos e os diversos componentes que compõe a arquitetura deverão possuir proteção entre a comunicação de dados e o armazenamento para que haja controle da confidencialidade. |
| **Categoria: Interoperabilidade** |
| **RNF13** - O software e dispositivos deverão manter sua interoperabilidade cumprindo a integração de serviços, sistemas e módulos externos. |
| **Categoria: Medidas contra danos** |
| **RNF14** - O software e dispositivos deverao possuir medidas para prevenção de danos realizadas por parte dos stakeholders, conforme destaca o conceito de tratamento de dados pessoais contidos no Art. 6o, VIII da LGPD.<br>**RNF15** - O software e dispositivos não deverão propagar falhas para outros componentes da aplicação.<br>**RNF16** - O software e dispositivos não deverão permitir modificação de dados por pessoas sem a devida autorização. |

A generalização de requisitos conectados aos aspectos de saúde mencionados na categoria “Monitoramento da Rotina do Paciente”elicita questões de consentimento do paciente atrelado aos conceitos de criação, alteração, exclusão e inclusão no tratamento de seus dados por parte dos *stakeholders* do sistema analisado. Portanto, os conceitos da LGPD presentes nesta categoria podem se adequar à outros sistemas de IoT na saúde.

## 7. Avaliação

Com a finalidade de entender a qualidade dos requisitos funcionais e não funcionais de adequação à LGPD do sistema DiaMant@Home, foi realizada uma avaliação qualitativa por três avaliadores (Av). O primeiro avaliador (Av 1) é advogado com especialização em privacidade de dados e é atuante na fiscalização na adequação dos sistemas de software à LGPD. O segundo avaliador (Av 2) é engenheiro de software com experiência na especificação de requisitos e uso do método GORE. O terceiro avaliador (Av 3) é especialista em IoT aplicada à saúde.

Cada avaliador examinou na íntegra o documento de especificação de requisitos. Após a leitura independente, foi realizada uma reunião no Google Meets com os três avaliadores para esclarecer possíveis dúvidas. A seguir, foi solicitado para cada especialista dar uma nota de 1 a 5 para os critérios de avaliação listados na Tabela 2. Cada nota representa um das seguintes opiniões: 1 - Discordo Totalmente; 2 - Discordo; 3 - Neutro; 4 - Concordo; e 5 - Concordo Totalmente.

Tabela 2: Resultado da Avaliação

| Critério de Avaliação | Av 1 | Av 2 | Av 3 |
|---|---|---|---|
| Corretude no uso do método de especificação de requisitos | 4 | 4 | 4 |
| Completude dos requisitos | 5 | 5 | 4 |
| Coerência com o domínio do sistema DiaMant@Home | 4 | 5 | 5 |
| Coerência com a LGPD | 5 | 5 | 5 |
| Clareza na descrição dos requisitos | 4 | 3 | 3 |

É possível concluir que, a especificação de requisitos realizada neste trabalho, para adequar o sistema de IoT DiaMant@Home apresenta níveis razoáveis de qualidade, pois a maioria dos critérios foi avaliada com nota superior ou igual a 4. Os avaliadores concordaram que falta um pouco de clareza na descrição dos requisitos, principalmente, pelo uso de terminologia específica da legislação, o que segundo os avaliadores #2 e #3 poderia dificultar o entendimento dos requisitos por parte dos profissionais de TI.

## 8. Conclusão e Considerações Finais

Visando a possível implementação e gerenciamento dos requisitos funcionais e demais funcionalidades do sistema DiaManT@Home e outros *softwares* ou dispositivos, levantou-se os RF e RNF adequados à LGPD que podem ter suas aplicações reutilizadas em outros sistemas de IoT na saúde, cumprindo todos os aspectos de segurança, privacidade e tratamento de dados. As contribuições aplicadas ao cenário de estudo promovem entendimentos sobre a LGPD e geram facilitações para a criação de *design* de *softwares*. As técnicas de GORE podem ser replicadas em diversos cenários tecnológicos para contribuição em seus requisitos. Por fim, é possível que profissionais da tecnologia utilizem esta pesquisa como base para outros estudos no desenvolvimento e adequações de requisitos para sistemas de IoT, reforçando os conceitos abordados neste trabalho.

## Referências


Brasil (2018). *Lei Geral de Proteção de Dados (LGPD)*. Lei n. 13.709 de 14 de agosto de 2018. Presidência da República, Brasília.

Camêlo, M. N. (2022). G-PRIV: um guia para especificação de requisitos de privacidade em conformidade com a LGPD. Dissertação de Mestrado, Universidade Federal de Pernambuco, Recife.

Garcés, L., Oliveira, B., and Arenas, C. (2020). *Arquiteturas de software para o domínio da saúde*, pages 1–47.

Kelly, J., Campbell, K., Gong, E., and Scuffham, P. (2020). The Internet of Things: impact and implications for healthcare delivery (Preprint). *Journal of Medical Internet Research*, 22.

Lamsweerde, A. (2001). Goal-oriented requirements engineering: a guided tour. In *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, pages 249–262.

Liu, J., Zhang, C., and Fang, Y. (2018). EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. *IEEE Internet of Things Journal*, 5(2):1206–1217.

Mendes, J., Viana, D., and Rivero, L. (2021). Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal. pages 263–268.