V Simpósio de Iniciação Científica 2022
Ciência, Tecnologia e Inovação no Brasil

ABORDAGEM PARA ESPECIFICAÇÃO DE REQUISITOS DE DESIGN DE SOFTWARE PARA SISTEMAS DE INTERNET DAS COISAS (IOT) CONFORME A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

João Pedro L. D. Ribeiro[1] (IC), Lina María Garcés Rodríguez (PQ)[1]
[1]*Universidade Federal de Itajubá*

Palavras-chave: Arquitetura de software. Engenharia de software. Goal-oriented requirement engineering.

Introdução

O termo *Internet of Things* (IoT) 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), presente em diversos cenários tecnológicos. Com a presença da IoT em evolução, tornou-se necessária a adequação da tecnologia para que haja controle e restrições de segurança sem presenças invasivas que geram riscos a privacidade de seus usuários através da manipulação de dados (Liu et al., 2018).

Em consideração, surgiu em 2018, 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. Os fundamentos da LGPD visam manter os direitos dos usuários em sua liberdade e privacidade com o seguimento obrigatório de normas praticadas pelas organizações (Brasil, 2018).

Esta pesquisa tem como objetivo investigar o *design* de *software* para que os sistemas de IoT possam cumprir as restrições de privacidade e segurança impostas pela LGPD, tendo como foco auxiliar os engenheiros de *software* na criação de arquiteturas para sistemas de IoT na saúde, de forma que sejam. O método *design science* foi escolhido e utilizado para realização da pesquisa e formulação do artigo.

A pesquisa se baseia no estudo de fundamentações teóricas sobre os conceitos exigidos na LGPD e demais aspectos de segurança para construção de uma arquitetura tecnológica adequada aos requisitos da legislação. Com a utilização da metodologia e conceitos abordados, tornou-se possível a reutilização de um *checklist* para adequação, verificação e criação de requisitos funcionais e não funcionais de um sistema para melhoria na qualidade de vida de pacientes portadores da doença Diabetes Mellitus. Como base da pesquisa, o sistema DiaManT@Home de Garcés et al. (2019) foi utilizado para aplicação da pesquisa e demonstração dos resultados obtidos.

Metodologia

O método *design science* foi escolhido e utilizado para realização da pesquisa e formulação do artigo. Este método de condução de pesquisas tecnológicas visa criar inovações e práticas através de análises, *design*, gestão e uso dos sistemas de informação no geral para solucionar problemas organizacionais com métodos computacionais avaliando a qualidade e eficácia dos artefatos da pesquisa (Hevner et al., 2004).

O termo *Design Science Research* (DSR) aborda metodologias de pesquisas de porte científico para áreas tecnológicas, com o intuito de inserir áreas acadêmicas do Brasil em áreas com desafios tecnológicos (Lacerda et al., 2013).

De acordo com Hevner et al. (2004), o método DSR deve ser seguido conforme instruções de condução e avaliação, que abordam conceitos de *design* como artefato.

Preservando os conceitos de Hevner et al. (2004) abordados sobre o método de pesquisa DSR, leva-se em consideração a relevância do problema a ser solucionado durante a pesquisa, buscando gerar soluções tecnológicas relevantes. São considerados a avaliação sobre qualidade, usabilidade e eficiência dos artefatos do método executado durante a pesquisa, além das contribuições dos artefatos gerados através dos métodos rigorosos do DSR.

Para entendimento dos conceitos utilizados juntamente com as adequações necessárias exigidas pela LGPD, tornou-se necessário os estudos dos conceitos de processo arquitetural com ênfase na sua etapa de análise e geração de Requisitos Arquiteturalmente Significativos (RAS), IoT, conceitos de segurança da informação e qualidade de *software*.

Na prática, o método de pesquisa foi aplicado neste trabalho através da utilização no sistema DiaManT@Home, que consiste em apoiar pacientes portadores da Diabetes Mellitus através da autogestão e controle da doença em suas rotinas diárias. O sistema DiaManT@Home é orientado a serviços e contempla soluções completas para utilização em casas de saúde e outros ambientes de vida assistida, promovendo mais

autonomia aos pacientes portadores da enfermidade (Garcés et al., 2019). Com a finalidade de elicitar os requisitos funcionais e não funcionais do sistema, Garcés et al. (2019) realizaram a estruturação das funcionalidades de acordo com a arquitetura da aplicação.

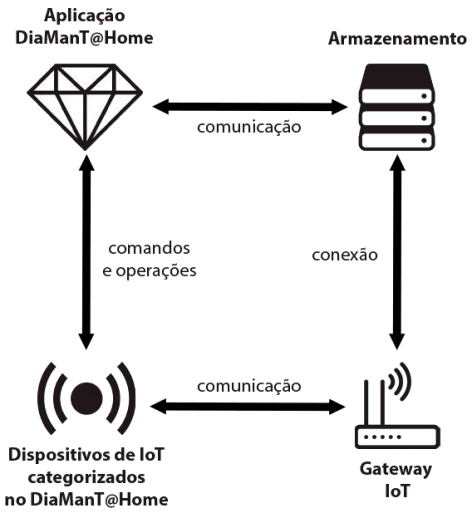
Posteriormente, as categorias da arquitetura foram utilizadas para a realização das adequações dos requisitos contemplando as exigências da LGPD. Os artefatos gerados e os resultados desta adequação estão contidos nos resultados e discussão do artigo.

Resultados e discussão

Considerando os estudos realizados, pôde-se obter os resultados e análises para a implementação da abordagem definida em ambientes de *design* de *software* de sistemas de IoT de acordo com as conformidades da LGPD.

A elicitação de requisitos deste trabalho e abordagem do sistema DiaManT@Home nesta pesquisa visam atualizar funcionalidades e conformidades do sistema de acordo com a LGPD com o uso de tecnologias para promover qualidade da saúde em pessoas com necessidades devido a doenças, de acordo com a arquitetura presente na Figura 1.

Figura 1 – Modelo de Arquitetura IoT do sistema DiaManT@Home



Os objetivos do sistema e a definição dos requisitos e suas funcionalidades foram identificados pela estratégia de *Goal Oriented Requirement Engineering* (GORE), "A GORE visa suas técnicas para elicitar, elaborar, estruturar, especificar, analisar, negociar, documentar e modificar requisitos" (Lamsweerde, 2001).

As metas definidas para o *design* de *software* de um sistema de IoT para o controle de Diabetes Mellitus em um ambiente inteligente devem ser claras e fornecer justificativas para a aplicação de seus requisitos. A aplicação desses requisitos deve conter os aspectos de segurança e abranger as funcionalidades dos dispositivos de IoT, mantendo a integridade dos *stakeholders* (paciente, família, amigos, profissionais da saúde e possíveis outros usuários) e do sistema de forma refinada.

No âmbito de desenvolvimento do *checklist* necessário para elicitação de requisitos e realização das análises, foram utilizados os conceitos abordados por Mendes et al. (2021) de forma aprofundada ao sistema da aplicação DiaManT@Home. O uso desse *checklist* unido com as técnicas de GORE possibilita as conformidades de segurança e integridade propostas pela LGPD. Os treze itens da lista foram definidos de forma exclusiva ao que se exige a Lei Geral de Proteção de Dados, não mapeando questões externas.

Para criação dos requisitos de sistema da aplicação DiaManT@Home foi utilizado o seguinte *checklist* apresentado na Figura 2.

Figura 2 – Checklist para criação de requisitos em conformidade com a LGPD para o sistema DiaManT@Home adaptado de Mendes et al. (2021).

Ordem	Itens
	Checklist Requisitos do Sistema DiaManT@Home
REQ1	O sistema utiliza os dados dos stakeholders de forma clara, legítima e consensual aos mesmos para realização de suas finalidades?
REQ2	O sistema permite aos stakeholders consultar de forma simplificada e sem custos as informações fornecidas ao software?
REQ3	O sistema permite aos stakeholders excluir sua participação no fornecimento de dados para realização das finalidades?
REQ4	O sistema faz o tratamento de dados de maneira segura?
REQ5	O sistema mantém registro do consentimento de uso das informações fornecidas pelos stakeholders?
REQ6	O sistema armazena os dados de forma segura e transparente ao titular dos dados?
REQ7	O sistema permite ao usuário aceitar e retirar sua participação na inclusão de seus dados pessoais para realização das finalidades fornecidas?
REQ8	O sistema possui práticas de segurança à privacidade desde o seu design?
REQ9	O sistema possui meios de prevenção de perda de dados por ataques ou desastres ocasionais?
REQ10	O sistema possui funcionalidades de fácil comunicação de falhas e/ou problemas de segurança aos órgãos de autoridade nacional?
REQ11	O sistema possui um controlador responsável pelos requisitos de proteção e tratamento de dados com informações de contato para sanar possíveis questões dos stakeholders?
REQ12	O sistema possui meios de transferir dados de forma segurança para autoridades internacionais para fins de coperação jurídica de forma consentida aos stakeholders?
REQ13	O sistema possui termos de privacidade, segurança, consentimento e de condições de participação dos stakeholders acessíveis de forma clara e simplificada?

Considerando os itens do *checklist* definidos com as técnicas de GORE para alcançar as metas propostas pela LGPD, torna-se possível traçar os requisitos funcionais e não funcionais para o sistema DiaManT@Home em conformidades com as exigências propostas pela LGPD. Posteriormente, após a elicitação dos requisitos, será possível utilizar o *checklist* para analisar se os aspectos mencionados no mesmo estão condizentes com a legislação.

Considerando o estudo realizado e as análises obtidas, aborda-se abaixo um resumo dos requisitos funcionais adequados à LGPD para sistemas de saúde que englobam a IoT, tendo como base a aplicação DiaManT@Home como objeto de pesquisa e aperfeiçoamento. Estes requisitos visam complementar os requisitos funcionais (RF) e requisitos não funcionais (RNF) já citados por Garcés et al. (2019) e são necessários para que o sistema cumpra as determinações da LGPD.

RF01 - O sistema deverá manter o cadastro de usuários de acordo com o cadastro das informações apresentadas para cada tipo de usuário.

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.

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.

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.

RF05 - O sistema deve permitir ao usuário cadastrado consultar seus dados de forma facilitada através de um botão no menu da aplicação.

RF06 - O sistema deve permitir ao usuário revogar seu consentimento ao tratamento de dados, conforme preza o Art. 8º, § 5º da LGPD.

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.

RF08 - O sistema deverá manter de forma segura os dados sensíveis e clínicos dos pacientes.

RF09 - O sistema deve permitir ao usuário o acesso à relatórios com suas informações pessoais, cumprindo o Art. 11º, § 4º, I da LGPD.

RF10 - O sistema deve permitir aos *stakeholders* o acesso à informação de pacientes vinculados visando cumprir as hipóteses para tratamento 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.

RF12 - O sistema deverá permitir que profissionais de saúde sejam atribuídos como responsáveis ao acompanhamento de pacientes cadastrados no sistema.

RF13 - O sistema deverá permitir que familiares e amigos de pacientes possuam autonomia para realizar a inserção de dados no sistema.

RF14 - Se o usuário paciente realizou o cadastro na aplicação e concordou com o termo de consentimento, o sistema deverá monitorar e registrar seus exercícios físicos diários.

RF15 - O profissional de saúde responsável por pacientes poderá através dos dados, incluir ou modificar o plano de exercícios do paciente para cumprir os objetivos do tratamento de dados, conforme Art. 6º, I da LGPD.

RF16 - O sistema deverá permitir que os profissionais de saúde cadastrados na aplicação possam alterar o plano nutricional do paciente, de forma consentida.

RF17 - O sistema deverá permitir que o paciente registre dados sobre sua alimentação na aplicação de maneira consentida

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*.

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 do paciente.

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.

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”.

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.

Visando manter os requisitos funcionais listados e demais funcionalidades já existentes da elicitação de requisitos do sistema DiaManT@Home e outros

softwares ou dispositivos, levantou-se os requisitos não funcionais (RNF) adequados à LGPD, cumprindo questões de privacidade, conforme exigências do Art. 50º e princípios do Art. 6º, aspectos de segurança conforme Art. 2º e Art. 6º, confidencialidade do tratamento de dados, interoperabilidade do sistema conforme Art. 25º e proteção com medidas preventivas contra danos, conforme Art. 6º, VII e VIII.

Conclusões

Os resultados obtidos neste trabalho concluem que as adaptações nos requisitos para criação de sistemas envolvendo a IoT são fundamentais para um sistema possua transparência com o usuário e segurança de operabilidade. Considerando as análises e conteúdo desenvolvido, é possível notar que todos os atributos elicitados estão de acordo com o que preza a Lei Geral de Proteção de Dados.

Os resultados ainda abordam a amplitude que a LGPD promove nos seus requisitos exigidos, além de uso de documentos complementares à bibliografia do estudo, como as informações contidas na norma ABNT NBR ISO/IEC 27002 de 2013 (ABNT, 2013) e que se contemplam em unir informações pertinentes com os resultados obtidos neste trabalho. Considerando a inclusão da LGPD em *softwares* de IoT, conclui-se que este trabalho atendeu seu objetivo principal de investigar requisitos para que sistemas possam cumprir as imposições da lei, auxiliando profissionais da tecnologia da informação a criarem aplicações seguras e interoperáveis com atributos de qualidade pertinentes.

Por sua vez, a demonstração de conceitos abordados neste artigo promoveu grande impacto nos resultados finais do trabalho, visto que esses conceitos estavam ligados diretamente aos requisitos formados pelas análises do estudo, podendo se conectar diretamente aos artigos da LGPD e aos fundamentos da IoT. Por fim, é possível que engenheiros de *software* e profissionais da área utilizem esta pesquisa como base para outros estudos no desenvolvimento de requisitos para sistemas de IoT, reforçando os conceitos abordados neste trabalho e possibilitando adequações necessárias para o tratamento de dados de modo seguro.

Agradecimento

Agradeço à Deus, minha família e namorada, a empresa NeST Digital, meus amigos e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) que promoveram momentos de conhecimento e incentivo para formulação desta pesquisa.

Referências

ABNT, Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro. ABNT, 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 ago. 2022.

GARCÉS, Lina; VICENTE, Isabella Zanin; NAKAGAWA, Elisa Yumi. Software Architecture for Health Care Supportive Home Systems to Assist Patients with Diabetes Mellitus. 2019. **IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS)**. p. 249-252, 2019.

HEVNER, Alan R., MARCH, Salvatore T.; PARK, Jinsoo; RAM, Sudha. Design Science in Information Systems Research. **MIS Quarterly**. p. 75-105, 2004.

KELLY, Jaimon; CAMPBELL, Catrina; ENYING, Gong; SCUFFHAM, Paul. The Internet of Things: Impact and implications for health care delivery. **Journal of medical Internet research**, v. 22, n. 11, 2020.

LACERDA, Daniel.; DRESCH, Aline.; PROENÇA, Adriano; ANTUNES JUNIOR, José. Design science research: A research method to production engineering**. Gestão & Produção**, 20(4). p. 741-761, 2013.

LAMSWEERDE, Axel. Goal-oriented requirements engineering. **A Guided Tour**. Pro-ceedings Fifth. IEEE International Symposium on Requirements Engineering. p. 249–262, 2001.

LIU, Jianqing; ZHANG, Chi; FANG, Yuguang. Epic: A differential privacy framework to defend smart homes against internet traffic analysis. **IEEE Internet of Things Journal**, v. 5, n. 2. p. 1206-1217, 2018.

MENDES, João; VIANA, Davi; RIVERO, Luis. Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: **An Initial Proposal.** Brazilian Symposium on Software Engineering. p. 263-268, 2021.