UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Levantamento de Requisitos para Internet das Coisas na Saúde com Ênfase em Segurança da Informação

Dissertação de Mestrado

Maiane de Castro Santos

São Cristóvão – Sergipe

2023

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Maiane de Castro Santos

Levantamento de Requisitos para Internet das Coisas na Saúde com Ênfase em Segurança da Informação

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Sergipe como requisito parcial para a obtenção do título de mestre em Ciência da Computação.

Orientador(a): Prof. Dr. Admilson de Ribamar Lima Ribeiro
Coorientador(a): Prof. Dr. Gilton José Ferreira da Silva

São Cristóvão – Sergipe

2023

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Santos, Maiane de Castro
S237l Levantamento de requisitos para internet das coisas na saúde com ênfase em segurança da informação / Maiane de Castro Santos ; orientador Admilson de Ribamar Lima Ribeiro. - São Cristóvão, 2023.
147 f.; il.

Dissertação (mestrado em Ciência da Computação) – Universidade Federal de Sergipe, 2023.

1. Engenharia de software. 2. Internet das coisas. 3. Saúde. 4. Software – Proteção. I. Ribeiro, Admilson de Ribamar Lima orient. II. Título.

CDU 004.05

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
COORDENAÇÃO DE PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Ata da Sessão Solene de Defesa da Dissertação do Curso de Mestrado em Ciência da Computação-UFS.
Candidata: Maiane de Castro Santos

Em 15 dias do mês de fevereiro do ano de dois mil e vinte três, com início às 15h00min, realizou-se na Sala de Seminários do PROCC da Universidade Federal de Sergipe, na Cidade Universitária Prof. José Aloísio de Campos, a Sessão Pública de Defesa de Dissertação de Mestrado da candidata **Maiane de Castro Santos**, que desenvolveu o trabalho intitulado: ***" Levantamento de Requisitos para Internet das Coisas na Saúde com Ênfase em Segurança da Informação"***, sob a orientação do Prof. Dr. **Admilson de Ribamar Lima Ribeiro**. A Sessão foi presidida pelo Prof. Dr. **Admilson de Ribamar Lima Ribeiro** (PROCC/UFS), que após a apresentação da dissertação passou a palavra aos outros membros da Banca Examinadora, Prof. Dr. **José Augusto Andrade Filho** (IFS) e, em seguida, o Prof. Dr. **Rubens de Souza Matos Junior** (PROCC/UFS) e também o Prof. Dr. **Gilton José Ferreira da Silva** (PROCC/UFS). Após as discussões, a Banca Examinadora reuniu-se e considerou o mestrando (a) aprovado *"(aprovado/reprovado)"*. Atendidas as exigências da Instrução Normativa 05/2019/PROCC, do Regimento Interno do PROCC (Resolução 67/2014/CONEPE), e da Resolução nº 04/2021/CONEPE que regulamentam a Apresentação e Defesa de Dissertação, e nada mais havendo a tratar, a Banca Examinadora elaborou esta Ata que será assinada pelos seus membros e pelo mestrando.

Cidade Universitária *"Prof. José Aloísio de Campos"*, 15 de fevereiro de 2023.

Admilson Ribeiro
Prof. Dr. Admilson de Ribamar Lima Ribeiro
(PROCC/UFS)
Presidente

Rubens de Sav. Matos Júnior
Prof. Dr. Rubens de Souza Matos Junior
(PROCC/UFS)
Examinador Interno

José Augusto Andrade Filho
Prof. Dr. José Augusto Andrade Filho
(IFS)
Examinador Externo

Gilton José Ferreira da Silva
Prof. Dr. Gilton José Ferreira da Silva
(PROCC/UFS)
Coorientador
Examinador Interno

Maiane de Castro Santos
Maiane de Castro Santos
Candidato

Agradecimentos

Primeiramente a Deus que permitiu que tudo isso acontecesse ao longo de minha vida, que me deu saúde e forças para superar todos os obstáculos nessa caminhada.

A minha mãe Maria Auxiliadora, pelo seu amor e dedicação em compartilhar meus sonhos, dividir meus medos, por todo apoio e dedicação.

Aos meus irmãos, Maiara, Maíza e Marxs, por sonharem sempre ao meu lado e não permitir que eu desanimasse diante das incertezas e dos obstáculos.

Aos demais familiares, especialmente aos meus tios Reginaldo e Eliane, e a minha vó Paulina pelo apoio e incentivo.

Aos meus amigos: Caio, Natália, Jadson, Mairon e Ricardo, que desde o início, me apoiaram sem medir esforços.

Agradeço ao meu orientador e coorientador Admilson e Gilton Ferreira, respectivamente, por ter sido meu orientador e ter desempenhado tal função com dedicação e amizade.

Enfim, a todos os funcionários do DCOMP/UFS especialmente a secretária Elaine por terem contribuído nesta conquista pessoal e profissional.

Resumo

Os avanços tecnológicos no âmbito da informação, têm contribuindo de forma significativa em diversos setores, de modo que estes novos aparatos ampliem a cada dia as possibilidades de otimização em vários dos seus produtos, através da interação entre sistemas de *software* e usuários. A atual realidade tecnológica que envolve Internet das Coisas do inglês *Internet of Things*(IoT), envolve também coleta e gerenciamento de grandes volumes de dados, através de uma crescente rede de dispositivos e sensores. Entretanto, a grande quantidade de dados gerados por objetos IoT, tende a significar uma séria ameaça à privacidade e segurança dos usuários, já que suas atividades podem ser monitoradas a qualquer hora, em qualquer lugar. No contexto da IoT em saúde, na contramão da praticidade e funcionalidade, o risco de ataques cibernéticos direcionados a aplicativos mHealth pode comprometer a disponibilidade e integridade das informações do paciente, prejudicando a mobilidade do atendimento e, às vezes, ameaçando a vida dos pacientes se as decisões forem tomadas com base em informações inválidas. Frente a esta demanda, o objetivo principal deste trabalho é o de desenvolver um modelo de boas práticas para o levantamento de requisitos de Software voltados para segurança em Internet das Coisas aplicada à saúde.

Palavras-chave: Engenharia de Software; Internet das Coisas; Levantamento de Requisitos; Saúde; Segurança.

Abstract

Technological advances in the field of information are significantly guaranteed in several sectors, so that these new devices expand the possibilities of optimization in several of their products every day, through the interaction between user and software systems. The current technological reality that involves the Internet of Things (IoT), also involves the collection and management of large volumes of data, through a growing network of devices and sensors. However, the large amount of data generated by IoT objects tends to pose a threat to users' privacy and security, as their activities can be monitored anytime, anywhere. In the context of IoT in healthcare, against the grain of practicality and functionality, the risk of cyber-attacks directed at mHealth applications can compromise the availability and integrity of patient information, impairing the mobility of care and, sometimes, threatening the lives of patients if decisions were made based on invalid information. Faced with this demand, the main objective of this work is to develop a model of good practices for the survey of Software requirements aimed at security in the Internet of Things applied to health.

Keywords: Internet of Things, Information Security, Requirements Engineering; healthcare.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
AEC	Arquitetura Engenharia e Construção
abnTeX	ABsurdas Normas para TeX
CE	Critério de Exclusão
CI	Critério de Inclusão
DCOMP	Departamento de Computação
ER	Engenharia de Requisitos
ES	Engenharia de Software
GL	Grey Literature
HIoT	Healthcare Internet of Things
IoT	Internet of Things
IoTsecM	Internet of Things Security Modeling
LGPD	Lei Geral de Proteção de Dados
mApp	Aplicativos móveis
mHealth	aplicativos de prática móvel de saúde
MIoT	Medical Internet of Things
QPP	Questão de Pesquisa Primária
QPS	Questão de Pesquisa Secundária
RF	Requisitos Funcionais
RNF	Requisitos não Funcionais
RFID	Radio Frequency Identification
SDLC	Ciclo de Vida de Desenvolvimento de Software
UML	Unified Modeling Language
UFS	Universidade Federal de Sergipe

Sumário

1 Introdução

Este capítulo apresenta de forma contextualizada uma abordagem sobre Internet das Coisas no contexto de saúde com ênfase em segurança. Em sua estrutura consta também, a motivação da pesquisa, objetivos, a justificativa e a organização do documento.

1.1 Apresentação Geral

A Internet das Coisas, em inglês Internet of Things (IoT) no contexto de saúde é o conjunto de dispositivos e aplicativos médicos que se conectam através de redes de computadores online. Neste sentido, os aparatos interconectados em redes online no setor de saúde, são denominados Healthcare Internet of Things (HIoT) (COSTEA-MARCU; MILITARU et al., 2019).

Com o surgimento da Internet das Coisas, tornou-se possível acessar o prontuário e estado clínico do paciente remotamente, passando a possibilitar ao paciente um acompanhamento contínuo e em tempo real e acompanhar seu estado de saúde onde quer que ele vá, de dentro de casa, na rua, no local de trabalho, etc.(HUANG et al., 2017).

Os novos aparatos tecnológicos conectados em rede, voltados para a prestação de serviços de IoT em Saúde, permitem cuidados de saúde móvel integrados e tomada de decisão informatizada para serviços médicos de emergência, especialmente em caso de desastres, quando cada segundo pode significar a diferença entre a vida ou a morte (AMBROSIO et al., 2019).

Destarte, o Medical Internet of Things (MIoT) oferece soluções inovadoras para uma vida mais saudável, fazendo mudanças radicais na vida das pessoas. Os provedores de saúde podem monitorar contínua e remotamente seus pacientes para muitos problemas médicos fora dos hospitais e escritórios dos provedores de saúde (ALMEHMADI; ALSHEHRI; TAHIR, 2019).

É válido considerar que quando as informações confidenciais e privadas são trocadas entre as coisas, a privacidade se torna uma grande preocupação, entre muitas questões importantes

como: escalabilidade, transparência e confiabilidade são consideradas como novos desafios que diferenciam a IoT da Internet convencional (KIRUBA; VIJAYALAKSHMI, 2018).

A atual realidade tecnológica que envolve IoT, envolve também coleta e gerenciamento de grandes volumes de dados, através de uma crescente rede de dispositivos e sensores. Esses dados acabam sendo compartilhados entre diversos serviços diferentes com a finalidade de criar um modelo inteligente que forneça cada vez mais um valor agregado e customizado para o usuário. Entretanto, a grande quantidade de dados gerados por objetos IoT, tende a significar uma séria ameaça à privacidade e segurança dos usuários, já que suas atividades podem ser monitoradas a qualquer hora, em qualquer lugar (NEISSE et al., 2014).

Para corrigir tal lacuna, conta-se com ferramentas entre as quais se destaca a Internet of Things Security Modeling (IoTsecM) para modelagem de segurança de aplicativos móveis (mApp) em aplicativos de prática móvel de saúde (mHealth). IoTsecM é uma extensão em Unified Modeling Language (UML) capaz de desenvolver controles de segurança identificados contra possíveis ataques para garantir a existência de mecanismos de análise de segurança eficaz (AMBROSIO et al., 2019).

1.2 Motivação

Na contramão da praticidade e funcionalidade da IoT em saúde, o risco de ataques cibernéticos direcionados (mHealth) pode comprometer a disponibilidade e integridade das informações do paciente, prejudicando a mobilidade do atendimento e, às vezes, ameaçando a vida dos pacientes se as decisões forem tomadas com base em informações inválidas (AMBROSIO et al., 2019).

Torna-se difícil aplicar várias tecnologias de segurança existentes no ambiente de IoT porque vários serviços são fornecidos usando dispositivos sensores de baixa qualidade com desempenhos limitados (WILLIAMS; MCCAULEY, 2016). Neste ínterim, quando um sistema não considera a segurança e privacidade dos dados, torna-se vulnerável a uma série de ataques destinados a espionar ou adulterar as informações pessoais dos pacientes. A natureza desses sensores provém de uma conexão sem fio e capacidades limitadas (RGHIOUI et al., 2015).

Os riscos com a IoT em saúde podem ser tratados considerando os controles de segurança da informação apropriados nos estágios iniciais do ciclo devida de desenvolvimento de aplicativos móveis (mApp) para o modelo de atendimento mHealth. No entanto, os dados de saúde são muito confidenciais para seus proprietários e, portanto, é importante garantir a segurança dos dados (AMBROSIO et al., 2019).

A Figura 1 expressa uma representação do uso da Internet no âmbito hospitalar, traz uma ideia aproximada de como os objetos estão interconectados, e de como são monitorados e controlados através de aparelhos como celular, tablet ou similares.

Figura 1 – Internet das Coisas na saúde

Fonte: Página da dataRain [1]

1.3 Justificativa

Os avanços tecnológicos no âmbito da informação, têm contribuindo de forma significativa em diversos setores, de modo que estes novos aparatos ampliem a cada dia as possibilidades de otimização em vários dos seus produtos, através da interação entre sistemas de *software* e usuários. Neste interim, utiliza-se formas até então desconhecidas e inimagináveis de colaboração, comunicação e interação entre as pessoas e as coisas e entre as próprias coisas (PESSOA et al., 2016).

A competição entre os fabricantes de dispositivos médicos pequenos e inteligentes, cria uma complexidade relativa aos dispositivos vestíveis, que resulta em outros problemas, como segurança do paciente, privacidade, confidencialidade e roubo de identidade (AMBROSIO et al., 2019).

No referido contexto, apresenta-se também uma gama de dificuldades acerca da garantia de segurança da informação no que tange a Healthcare Internet of Things (HIoT) e Medical Internet of Things (MIoT). Tais modalidades de interconexão oferecem soluções inovadoras para uma vida mais saudável, fazendo mudanças radicais na vida das pessoas, mas chamam atenção com relação a vulnerabilidade gerada pela exposição de dados em rede.

Faz-se notável e significativa a necessidade de utilizar a IoT no âmbito da saúde, dada a praticidade e as diversas possibilidades. Os trabalhos de Ramanchandran (2016), Rios (2018), Carvalho (2018), e Pressman (2016), apontam falhas no que concerne à análise de requisitos

[1] Disponível em: https://www.datarain.com.br/blog/iot-revolucionando-saude-mundial/

como sendo o maior fator de risco. Frente à relevância dada a esta temática, tomou-se a mesma, enquanto objeto de pesquisa.

1.4 Objetivos

Esta seção trata do objetivo geral deste trabalho, bem como dos objetivos específicos.

1.4.1 Objetivo Geral

Desenvolver um modelo de boas práticas para o levantamento de requisitos de *software* voltados para segurança em Internet das Coisas aplicada à saúde.

1.4.2 Objetivos Específicos

Para alcançar o objetivo principal, foram definidos os seguintes objetivos específicos:

- Fazer levantamento e análise dos trabalhos relacionados ao desenvolvimento de *software* para Dispositivos de IoT aplicados à saúde;
- Descrever os desafios da Segurança da Informação da Internet das Coisas em saúde, analisando as vulnerabilidades da Segurança em IoT;
- Verificar o nível do impacto de ataques a dispositivos de Saúde;
- Desenvolver *framework* enquanto modelo adaptável para o levantamento de requisitos no desenvolvimento de aplicações IoT da saúde com ênfase em segurança.

1.5 Estrutura do Documento

No sentido de imprimir clareza, coesão e facilidade de navegação, este trabalho foi estruturado em capítulos e seções distribuídos da seguinte maneira:

- Capítulo 1 - Introdução: apresenta as definições preliminares da literatura, a questão problematizadora, argumentações e hipóteses sobre o tema, bem como os objetivos;
- Capítulo 2 - Fundamentação teórica: contextualiza a temática, e, se faz mediante a revisão de literatura relacionada à mesma;
- Capítulo 3 - Metodologia, materiais e métodos utilizados na elaboração da pesquisa;
- Capítulo 4 - Mapeamento Sistemático da literatura sobre Segurança em MIoT;
- Capítulo 5 - Revisão Sistemática sobre Levantaento de requisitos para segurança em MIoT;

- Capítulo 6 - Trabalhos relacionados: descreve alguns trabalhos encontrados na literatura, relacionados ao tema deste trabalho;
- Capítulo 7 - Desenvolvimento do Adm. R;
- Capítulo 8 - Considerações Finais.

2

Fundamentação Teórica

Será apresentada neste capítulo, a Fundamentação Teórica cuja abordagem abrange: Engenharia de Software; Levantamento de Requisitos; Internet das Coisas; Tecnologia da Informação e Comunicação para a Saúde; e Segurança da Informação.

2.1 Engenharia de Software

Para Brito (2014) a Engenharia de Software (ES) é um processo que engloba: levantamento, modelagem, especificação, verificação e manutenção das propriedades de um produto ou serviço de software antes, durante e depois da sua realização. Durante o desenvolvimento de um *software*,são descobertas as necessidades e restrições impostas pelo cliente, bem como são identificados seus principais interessados *(stakeholders)*.

Para Portela, Vasconcelos e Oliveira (2017), elaborar um produto de *software* requer o envolvimento de uma grande equipe de especialistas que imprimem nesta construção, um amplo conjunto de habilidades, como: definição de projetos, gerenciamento, programação, validação, análise, estudo dos usuários, documentação, integração de sistemas e técnicas específicas.

É válido considerar que, embora necessário, este conjunto de habilidades se encontra atrelado a um alto custo de gerenciamento. Desta forma, a Engenharia de Software se apresenta multidisciplinar, uma vez que se compõe de uma vasta quantidade de abordagens teóricas que são assimilidas na prática (PORTELA; VASCONCELOS; OLIVEIRA, 2017).

Dentre outras habilidades, os engenheiros de softwares devem compreender processos, sistemas e relacionamentos complexos, bem como abstrair configurações complexas de problemas e encontrar possíveis soluções. Estes, devem estar dispostos e capazes de pensar para além do momento, e, por tanto entender e aceitar a significação e a necessidade de procedimentos e artefatos até então estranhos (SEDELMAIER; LANDES, 2014).

De acordo com Andrade et al. (2016) uma equipe de desenvolvimento de *software* é multifuncional e autossuficiente, uma vez que seus membros deverão ser capazes de desenvolver todas as habilidades necessárias ao alcance do objetivo. Para tanto, cada membro assume compromissos e responsabilidades em relação ao projeto.

Na abordagem de Horita, Neto e Santos (2018) consta que a área de ES dispõe de um acervo muito amplo de métodos experimentais e que, estes apresentam em si, diversos graus de rigor a serem utilizados em pesquisas científicas. Quando aplicados para teorizar fenômenos observados, tais métodos partem sempre de estudos piloto que concernem provas de conceito e abrangem pesquisas de opinião, estudos de caso e experimentos controlados.

2.1.1 Engenharia de Requisitos: Conceito e aplicações

A Engenharia de Requisitos (ER) pode ser entendida como uma prática de Engenharia de Software que consiste em abordagens que convergem para a compreensão dos requisitos pela equipe de desenvolvimento. Sendo assim, é parte integrante do ciclo de vida de desenvolvimento de *software*, e portanto, a base para o desenvolvimento de *software* bem-sucedido (REHMAN; KHAN; RIAZ, 2013).

Além de fornecer processos, ferramentas, técnicas, modelagem, estimativa de custos, planejamento de projetos e acordos contratuais, a Engenharia de Requisitos cria e examina cada elemento do modelo em termos de inconsistência, omissões e ambiguidade, representando-os e agrupando-os em pacotes. Tal esforço colaborativo, envolve muitos participantes, como analistas de negócios, engenheiro de requisitos de software, arquiteto de software e gerentes de testes (PRESSMAN; MAXIM, 2016).

De acordo com Barbosa e Lencastre (2019), trata-se de um processo que envolve inúmeras interações sociais, portanto, requer do analista um nível de cooperação muito alto, bem como empatia com pessoas de personalidades, valores e interesses diferentes. Nas equipes de desenvolvimento de software, independentemente do tamanho que seja o projeto, os conflitos fazem parte do seu ciclo de vida.

Na ER, coletar, analisar e documentar os requisitos, são tarefas básicas para que o produto final tenha a qualidade esperada . Nestes termos, os Processos em RE podem ser desenvolvidos de maneiras distintas, sem no entanto, abrir mão de que se trata de uma parte fundamental do desenvolvimento de um software como um todo (REHMAN; KHAN; RIAZ, 2013).

As especificações que um sistema deve oferecer e como ele deve se comportar mediantes situações específicas, concernem a Requisitos Funcionais, enquanto os Requisitos não Funcionais se inserem nos quesitos referentes à qualidade e aos critérios utilizados no sistema, como usabilidade, desempenho, confiabilidade, etc (SOMMERVILLE, 2011).

Vegendla et al. (2018) apesentam um conceito pontual e simplificado para ER quando afirma que se trata de todo o ciclo de vida do documento de requisitos que inclui as fases de

concepção, elicitação, negociação, análise, especificação, verificação, validação e gestão em sua complexidade, garantindo assim, a construção adequada.

Segundo Pressman e Maxim (2016) a ER permite que os engenheiros de software compreendam melhor o problema a ser resolvido, bem como entendam de que forma o software impactará o negócio ao qual se destina e até como os usuários finais irão interagir com o sistema.

Fagundes et al. (2020) defendem que a ER prevê a construção de sistemas de informação de qualidade e que atendam às necessidades informacionais dos seus usuários, ou seja, sistemas seguros são aqueles cuja estrutura possa prover suporte à indexação e recuperação da informação. Esta caracteristica no entanto, se encontra fortemente relacionada com o processo utilizado no seu desenvolvimento.

Filho (2003) conceitua Engenharia de Requisitos enquanto uma subárea da Engenharia de Software que possui relevância para a elaboração de um software por imprimir a responsabilidade de levantar, uma a uma, as solicitações requeridas pelo stakeholder, e em seguida, elaborar uma documentação e transferir devidamente os requisitos para as partes interessadas de maneira clara, concisa e sem ambiguidades.

É importante que o analista de requisitos possa monitorar continuamente os sinais que apontam a existência de conflitos, evitando o comprometimento do projeto. Tal premissa envolve elicitar, analisar, estruturar e gerenciar os requisitos -o que requer do analista um domínio sólido da linguagem, que saiba ouvir, compreender e consolidar de forma clara as necessidades das partes interessadas (BARBOSA; LENCASTRE, 2019).

Estes requisitos devem imprimir a propriedade de segurança (confidencialidade, integridade e disponibilidade) bem como, devem estar relacionados ao tipo de permissão concedida a seus gestores e usuáros. Os envolvidos podem receber três tipos diferentes de permissões sobre os recursos, a saber: acessar, modificar e gerenciar a permissão (SEQUEIROS et al., 2020).

A modelagem de segurança se torna relevante quando analisado o fato de que a maioria dos ataques se dá devido à configuração incorreta dos dispositivos, cuja vulnerabilidade não é apresentada e corrigida durante o processo de desenvolvimento dos mesmos, apesar dos algoritmos e mecanismos de defesa aplicados a esses ecossistemas (GUPTA; AGRAWAL; YAMAGUCHI, 2016).

O Levantamento de Requisitos parte do princípio de que o bom desenvolvimento de um sistema informatizado deve ser capaz de atender as necessidades específicas do usuário em suas peculiaridades, portanto, como afirmam Vieira et al. (2015), mediante as diretrizes da Engenharia de Software sendo necessário que os seus desenvolvedores detenham conhecimentos específicos.

Abran et al. (2004) afirmam que o bom levantamento requisitos deve levar em conta quem são, e quais as necessidades dos seus atores *(stakeholders)* antes da validação destes requisitos, e só a partir daí, a compilar e verificar com os usuários. Neste contexto, entende-se enquanto *stakeholder*s os seguintes grupos:

- Usuários: envolve toda pessoa que irá utilizar o produto final, sem nenhuma relação com o desenvolvimento de um software;
- Clientes: inclui pessoas que encomendam o software;
- Analistas de mercado: seus atores têm o papel de sondar novas tecnologias e tendências no meio externo, podendo adicionar algumas ideias ao projeto;
- Reguladores: devem possuir domínio na área de atuação para projetos de software que envolvam portarias e outras normas, como bancos, mineração e logística;
- Engenheiros de Software: são os desenvolvedores e possuem a responsabilidade de ouvir os clientes, validar seus requisitos verificando inconsistências, compilar e verificar o sistema junto com os clientes e aguardar *feedback*. Compete a estes considerar a redução nos custos do projeto.

2.2 Levantamento de Requisitos

O levantamento de requisitos é o início para toda a atividade de desenvolvimento de software e faz-se extremamente relevante. Nesta fase, o analista faz as primeiras reuniões com os clientes e/ou usuários com a finalidade de conhecer as funcionalidades do sistema a ser desenvolvido.

O grau de satisfação dos usuários é aferido na fase de levantamento de requisitos do projeto, e a insatisfação destes se faz mediante a não utilização de uma técnica adequada na extração dos requisitos do sistema. Neste contexto, se define enquanto falha do analista a não descrisção dos requisitos ou não fazê-la de foma clara, concisa, consistente e sem ambiguidades, de maneira a apresentar todos os aspectos significativos do sistema proposto (COSTA, 2011).

Os requisitos possuem em suas propriedades a capacidade de expressar as características e restrições do produto de software partindo do pressuposto do nível de satisfação dos usuários a partir das suas reais necessidades. Neste ínterim, torna-se o levantamento de requisitos uma das partes mais críticas e propensas a erros no desenvolvimento de *software*, independentemente da tecnologia utilizada (MACHADO, 2018).

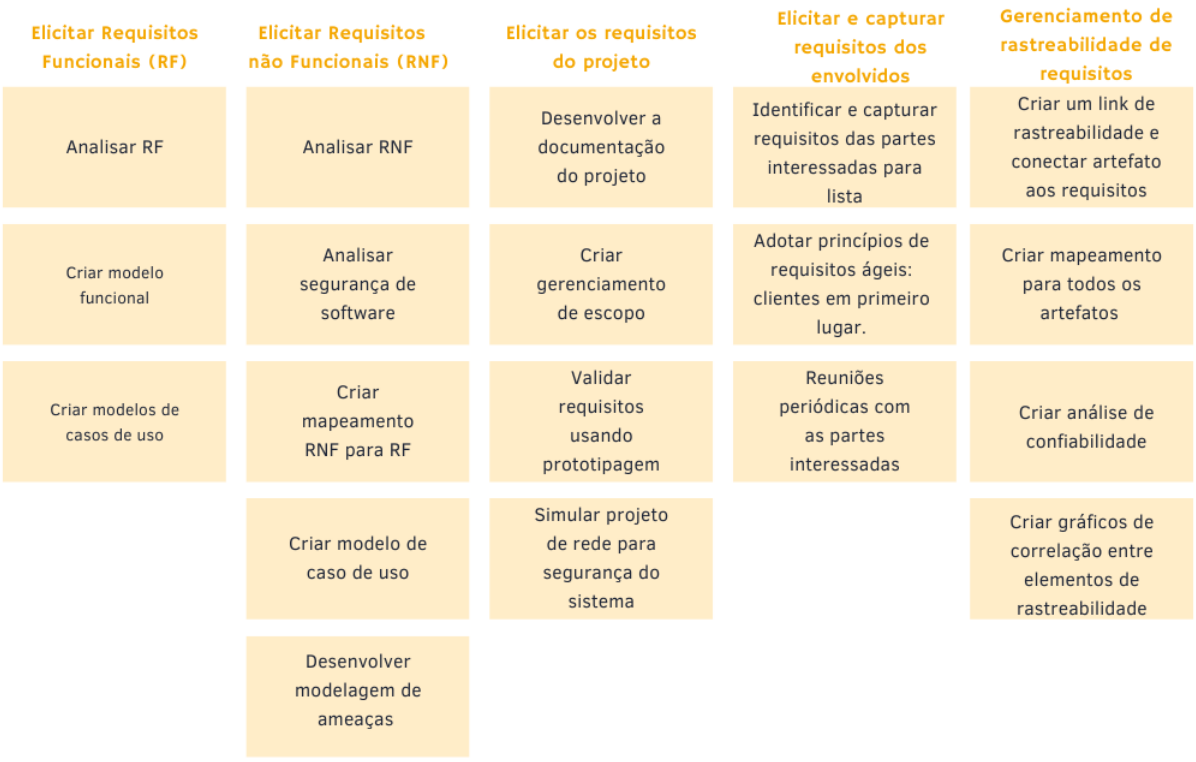
Considera-se ainda enquanto especificação dos requisitos, ser legível e rastreável possibilitando gerenciamento e evolução do sistema no tempo. O gerenciamento dos requisitos muito relevante e faz parte das melhores práticas de Engenharia de Software (JR, 2010).

O ponto de partida responsável pelo bom andamento de qualquer sistema, seja no que concerne a questões legais, contratuais e de governança se faz através dos requisitos, uma vez que são estes que fornecem uma perspectiva funcional completa do sistema que está sendo desenvolvido (RAMACHANDRAN, 2016).

De acordo com Sommerville (2011), no levantamento de requisitos, os engenheiros de software estão em contato direto com clientes e usurários finais do sistema para assim obterem informações necessárias sobre o domínio da aplicação, os serviços que o sistema deve fornecer, o desempenho que o sistema deve apresentar,as restrições de *hardware*, entre outros.

Na Figura 2, apresenta-se um mapa conceitual que sintetiza o gerenciamento de requisitos. Conforme apresentado, o gerenciamento de rastreabilidade de requisitos (RTM) se define enquanto matriz de rastreabilidade de requisitos. Esta funcionalidade é validada durante a fase de desenvolvimento dos mesmos (RAMACHANDRAN, 2016).

Figura 2 – Gerenciamento de Requisitos



Fonte: Adaptado de Ramachandran (2016)

2.3 Internet das Coisas

Akabane (2018) afirma que o termo IoT foi utilizado por Kevin Ashton pela primeira vez em 1999, para denominar uma estrutura de rede abrangente, na qual vários tipos de objetos entre si, processam informações por meio de tecnologias de sensores, e, afirmou que a falta de tempo

das pessoas é fator determinante para que se desenvolvam ferramentas capazes de fazer coisas que não necessitam ser feitas por pessoas.

Frente as abordagens de Alexandrov, Desnitsky e Chaly (2019) o termo, Internet das Coisas, bem como seu conceito e funcionalidade, está cada vez mais presente nas sociedades. Avanços tecnológicos em IoT, são determinantes para oportunizar e desenvolver novos negócios. Em geral, as tecnologias de *internetworking* proporcionam a conectividade entre humanos, bem como entre aparatos tecnológicos.

Nas sociedades atuais, frente às novas configurações e demandas, surge a necessidade de se utilizar dispositivos inteligentes, proativos e sustentáveis. Este *layout* configura total dependência da Internet e, traz consigo, um novo desafio em termos de segurança da informação. Destarte, em uma organização, a segurança em redes deve ser tão levada a sério, quanto a segurança física. Considera-se tambem que a última trabalha com funcionários preparados com habilidades técnicas necessárias (QUSA et al., 2019).

Alexandrov, Desnitsky e Chaly (2019) defendem a importância de se criar um módulo protegido de sistema de informação e telecomunicações capaz de implementar o conceito Internet das Coisas levando em consideração todos os seus aspectos. Para tanto, vale ressaltar que a maioria dos "crimes" virtuais se correlacionam com o estilo de vida adotado nos últimos anos e com o mau uso dos novos aparatos tecnológicos.

Mediante a uma diversidade de dispositivos interconectados, que embarcam importantes inovações e possibilidades tecnológicas facilitadoras, relacionadas a negócios, pesquisas, e nichos mercadológicos em geral, pode-se afirmar se tratar de uma revolução, como aponta (LEMOS; MARQUES, 2018).

Afonso, Pereira e Pereira (2015) emprestam o conceito de Internet das Coisas a um paradigma que ganhou espaço no cenário moderno das telecomunicações *wireless* ao gerar um fluxo de dados em rede, cuja conexão permite a transmissão de dados para outros objetos no meio, formando assim uma Internet de coisas como sensores, *tags* Radio Frequency Identification (RFID), *smartphones*, computadores, bem como objetos de uso comum, entre si.

Filho (2016) explicita que quando há recursos eletrônicos disponíveis, a Internet das Coisas permite que objetos do dia-a-dia se comuniquem com a Internet, e que esta comunicação favorece o compartilhamento de informações em objetos. Neste âmbito, os dispositivos controlam a si mesmos e a outros dispositivos.

2.4 Tecnologia da Informação e Comunicação para a Saúde: o Papel de IoT na Saúde

O exponencial crescimento da Internet das Coisas vem criando possibilidades para o surgimento de inovações tecnológicas. De acordo com Martins et al. (2020) na indústria da saúde,

especificamente, é fácil observar o desenvolvimento destes aparatos, o que gera um impacto significativo para a saúde e bem-estar dos usuários, sendo possível monitorar o estado de saúde e acompanhar doenças e tratamentos.

Para Bertoni et al. (2022), a inovação tecnológica em saúde vem sendo reconhecida como elemento essencial para a equidade e promoção da saúde nas suas diferentes vertentes, seja a prevenção, o diagnóstico, o tratamento, a reabilitação ou assistência. Neste sentido, a adoção de tecnologias digitais imprimem vantagens como a agilidade no acesso à informações para a gestão de processos e serviços de saúde e eficácia no atendimento, bem como possibilita o monitoramento remoto de pacientes.

De acordo com Aledhari et al. (2017) a revolução dos dispositivos inteligentes tem um impacto significativo e positivo na vida de muitas pessoas, no que diz respeito aos cuidados de saúde. Tais avanços tecnológicos permitem aos indivíduos vestir e usar dispositivos médicos para monitorar suas atividades de saúde, de forma remota. Além disso, esses dispositivos médicos inteligentes e vestíveis ajudam os profissionais de saúde a monitorar seus pacientes de forma remota, permitindo assim respostas rápidas em caso de emergência.

Quando se fala em Internet das Coisas na Saúde, é importante analisá-la enquanto aliada aos conhecimentos médicos de maneira a atuar sobretudo na medicina promovendo baixo custo com medicamentos, consultas e outros procedimentos médicos, no entanto, tais benefícios demandam desafios (MASSOLA; PINTO, 2018).

Segundo Mauer (2017) por mais que a indústria médica aposte em tecnologia de ponta para o desenvolvimento de novos produtos, o fato dos processos de certificação serem muito custosos e longos, aumenta a cautela, e às vezes até inviabiliza a adoção de algumas tecnologias, especialmente em equipamentos de suporte a vida. Por isso, a evolução muitas vezes parece ser lenta e menos visível.

Embora existam muitos benefícios da Internet das coisas na área da saúde, não são poucos os seus desafios tendo em vista a complexidade do sistema e a sensibilidade da área. Assim, toda nova tecnologia na área da saúde, implica em preocupações tanto com a segurança dos dados bem como com o gerenciamento dos dispositivos da IoT(MASSOLA; PINTO, 2018).

Tendo em vista que a disseminação não permitida dos dados de saúde gera consequências indesejadas, prejudicando não só aos pacientes, mas também as entidades ou profissionais da área que acessam esses dados, um estudo de Gomes e Coutinho (2022) propõe um sistema *blockchain* enquanto tecnologia capaz de lidar com tais problemas e que possui alto grau de confiabilidade, além de permitir a descentralização dos dados.

São vários os dispositivos utilizados hoje em dia no contexto de IoT em saúde, desde simples a sofisticados dentre os quais se destaca um dispositivo proposto por Bharadwaj et al. (2017) denominado caixa médica inteligente. Trata-se de um dispositivo de assistência baseado em computador de placa única para pessoas que sofrem com perda de memória de curto prazo.

O dispositivo de Bharadwaj et al. (2017) é baseado em alarme que faz com que o paciente possa lembrar sobre sua medicação. Mediante essas inovações, é válido afirmar que os cuidados com a saúde sob o prisma do uso de tecnologias no conceito de Internet das Coisas (IoT) tornam o diagnóstico mais fácil e conveniente para os médicos, bem como para os pacientes.

Uma caixa médica inteligente, similar ao modelo proposto por Bharadwaj et al. (2017) esá expressa na Figura 3. O modelo ora representado, conta com até quatro conjuntos de alarmes ao mesmo tempo e tampas coloridas transparentes para facilitar a visualização. De acordo com as instruções do fabricante, esta é capaz derepetir o lembrete perdido três vezes a cada cinco minutos. Isso ajuda a manter o controle dos medicamentos a serem ingeridos em diferentes momentos do dia.

Figura 3 – Caixa de remédios Inteligente

Fonte: Página da Amazon [1]

[1] Disponível em: https://www.amazon.com.br/comprimidos-SUPVOX compartimentos-inteligente medicamentos/dp/B084RH5GKT?th=1

No trabalho de Kiruba e Vijayalakshmi (2018) é informado que aplicações de saúde baseadas em IoT estão ganhando mais atenção devido às suas vantagens como custos reduzidos, gerenciamento aprimorado de medicamentos bem como monitoramento remoto. No entanto, dados de saúde são muito sensíveis. Desta forma, é de extrema importância que o desenvolvimento destes dispositivos leve em conta a garantia da segurança dos dados dos seus usuários.

2.5 Segurança da Informação

Ao definir formalmente o termo Segurança da informação, Hintzbergen et al. (2018) afirmam ser a proteção da informação contra uma ampla gama de ameaças evitando assim a descontinuidade do serviço, minimizando riscos e maximizando resultados positivos, imprimindo aos sistemas, confidencialidade, integridade e disponibilidade.

De acordo com a ABNT (2005) a perda de confidencialidade; ocorre mediante a quebra de sigilo de uma informação, seja esta qual for. O mesmo ocorre para a perda de integridade, que diz respeito à exposição e manuseio por usuário não autorizado, de maneira a realizar operações não aprovadas e não controladas pelo seu administrador. Este princípio pode vir a ser quebrado mediante falha no dispositivo de armazenamento ou outro fator. A integridade cuida para que haja a certeza de que os dados não são adulterados, destruídos ou corrompidos. Por outro lado, para que um sistema demonstre disponibilidade, deve contar com um sistema computacional, de controles de segurança e canais de comunicação de bom funcionamento.

Um exemplo de integridade da informação é ilustrado por Cipriano (2021) ao apontar que um prontuário médico se acessado e modificado por pessoas não autorizadas pode comprometer inclusive a vida do paciente. Considera-se basicamente dois pontos do processo de transmissão nos quais a integridade pode ser comprometida: na fase de carregamento de dados e/ou na fase de armazenamento ou coleta do banco de dados.

Gouveia (2017) aponta que o que define o valor da informação é o conjunto de caraterísticas que a mesma possui, de maneira que, ao se alterar uma informação altera-se também suas caraterísticas, portanto, seu valor. Assim, o exato momento em que a informação se encontra disponível é um fator crítico para os utilizadores, uma vez que, em muitas situações a informação perde todo o seu valor quando não é entregue em tempo real.

Na visão de Cipriano (2021) um conceito aplicavél a disponibilidade pode ser resumido no fato desta estar disponível sempre que precisar ser utilizada. A maioria dos sistemas disponíveis são acessíveis em todos os momentos e tem garantias contra falhas de energia, desastres naturais, falhas de *hardware* e atualizações de sistemas.

2.5.1 Lei Geral de Proteção de Dados- LGPD

Pinheiro (2020) afirma que a Lei Geral de Proteção de Dados (LGPD) - Lei n. 13.709/2018, enquanto marco legal parte do pressuposto de que todo dado pessoal deve ser preservado pois tem importância e valor. Este marco conceitua dado pessoal como sendo a informação relacionada a pessoa natural identificada ou identificável.

A violação destes dados se dá quando os mesmos são transferidos, cruzados ou organizados, e resultam em dados bastante específicos sobre determinada pessoa, de modo a trazer informações diversas sobre a mesma. De acordo com o que fundamenta a LGPD é a necessidade de proteger os direitos fundamentais da liberdade e da privacidade além do bom desenvolvimento da personalidade da pessoa natural (TEFFÉ; VIOLA, 2020).

O risco real à privacidade ocorre mediante o compartilhamento de dados pessoais com os provedores de serviços. A Vulnerabilidade na internet ocorre frente a inúmeros fatores dentre os quais (CAMARA et al., 2021), aponta o tratamento inadequado dos dados, a falta de conhecimento dos usuários acerca de como são compartilhados os seus dados e o compartilhamento inadequado e a quantidade excessiva de compartilhamento de informações pessoais.

No âmbito da Internet das coisas em Saúde, a LGPD culmina com uma preocupação relevante e recorrente acerca de como como tratar dados pessoais, inclusive os dados sensíveis, de maneira a não ferir direitos e garantias individuais (CAMARA et al., 2021).

o art. 13º da LGPD aponta que na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro. O referido artigo alude também os devidos padrões éticos relacionados a estudos e pesquisas, bem como afirma não ser permitida, em circunstância alguma, a transferência dos dados a terceiro.

Neste sentido, (TEFFÉ; VIOLA, 2020) apresenta o sinaliza que antes da promulgação desta lei, os sistemas de informação primavam a eficiência no compartilhamento das informações médicas e dos registros oficiais no que concerne a fins administrativos, não havendo cautela com a segurança da informação, com o estabelecimento de uma governança de dados.

2.5.2 Segurança em Internet das Coisas

O estudo de Jacobsson, Boldt e Carlsson (2016) refere-se a uma análise de risco cujos resultados apontam para o necessidade de um modelo mais amplo de segurança e privacidade ainda na fase de projeto em IoT, para reforçar a segurança do sistema e aumentar a privacidade do usuário, e ajudando a perceber o potencial de vulnerabilidade em ambientes ou sistemas interconectados.

Lee (2020) recorre às teorias de privacidade e vulnerabilidade para explicar a relevância

da proteção e da privacidade no que concerne à segurança física e de dados no contexto de IoT. Partindo deste pressuposto, além de propor um modelo de protocolo de segurança, utiliza uma análise empírica com 265 amostras para validá-lo.

Mavropoulos et al. (2019) trazem como objeto de estudo o Apparatus Framework, consta uma busca por redefinir a linguagem de modelagem, transformando-a em uma notação que venha a facilitar a análise de segurança em sistemas IoT. Tal estudo foi testado em um sistema de transporte público inteligente. Em análise, os quesitos segurança e visualização do sistema foram facilitadas pelo aplicativo de software desenvolvido como parte do aparato Framework.

De acordo com Yiğit et al. (2019) a equação em si: IoT e usuários, leva a violações e comprometimentos de segurança graves, tendo em vista a natureza interconectada e interdependente destes aparatos, acrescida das capacidades irrestritas em relação aos recursos computacionais. Tais fatores tornam impossível a aplicabilidade de mecanismos convencionais de segurança.

2.5.3 A Segurança da Informação no contexto de Internet das Coisas aplicada à saúde

No contexto do desenvolvimento de dispositivos de prestação de cuidados de saúde online, Ambrosio et al. (2019) consideram que estes ajudam a melhorar qualidade de vida do paciente, embora exija uma análise criteriosa, além de um design de sistema capaz de garantir os equilíbrios de soluções entre o valor que essas aplicativos agregam às vítimas, no que concerne à funcionalidade entre a salvação de suas vidas e os riscos que estes representam.

Rghioui et al. (2015) alertam no entanto que, a principal desvantagem desses aparatos é que geralmente o usuário não leva em consideração a segurança e a privacidade dos dados, tendo em vista a natureza desses sensores, uma vez que a conexão sem fio e a capacidade limitada favorece uma série de ataques cibernéticos que vão desde a espionagem até a adulteração das informações pessoais dos pacientes.

Para Saleem, Ali e AlSalloom (2020), o relevante papel que as novas tecnologias têm exercido na saúde vem imbuído da busca por soluções no que concerne à segurança de dados, uma vez que mediante registros eletrônicos seus usuários ficam vulneráveis a ataques sejam estes intencionais ou não-intencionais. Neste sentido, propõem soluções de segurança e descrevem uma plataforma com capacidade para proteger e aprimorar o processo de acesso e gerenciamento em bancos de dados hospitalares baseadas em IoT para assistência médica.

Ressalta-se portanto, a importância de um modelo eficiente na transmitissão e gerenciamento das informações médicas e de saúde dos pacientes com segurança por meio de autorização no ambiente de IoT, que não permita que membros da equipe de hospitais coletem informações sem o consentimento do paciente e, portanto, reduza o risco de vazamento de informações pessoais (PARK et al., 2016).

Um estudo proposto por Costea-Marcu, Militaru et al. (2019) aplicado a 96 pessoas para as quais foram direcionadas perguntas que apontassem os desafios enfrentados na aceitação de dispositivos de IoT no contexto da Saúde, indicou a privacidade enquanto o principal desafio. Esta por sua vez se agrava quando dispositivos e aplicativos não são testados, resultando em problemas de interoperabilidade, instabilidade, incompatibilidade e segurança de dados.

A pesquisa de Costea-Marcu, Militaru et al. (2019) indicou que aparatos e dispositivos IoT na saúde são facilmente aceitos pelos pacientes quando estes percebem a sua utilidade, bem como a facilidade em manuseá-los ou ainda quando são influenciados por terceiros e por último quando se sentem confiantes em relação a privacidade.

Huang et al. (2017) afirmam que, o florescimento adicional de m-health ainda enfrenta muitos desafios, incluindo segurança da informação e preservação da privacidade, neste sentido, apresenta um modelo de criptografia homomórfica baseada em esquema de matriz capaz de garantir privacidade, analisar os dados médicos embaralhados e fornecer *feedback* dos resultados automaticamente.

Zouka (2017) apresentam um modelo no qual os dados do paciente são capturados em tempo real e enviados para a nuvem/data center de forma assíncrona para serem analisados e armazenados, podendo então, serem acessados de qualquer lugar e por meio de quase todos os dispositivos de computação. Nesse sistema, a comunicação móvel é autenticada e armazenada em um banco de dados criptografado e isolado da Internet. O serviço de segurança da informação será fornecido por uma rede de nuvem altamente confiável que permite a troca e o compartilhamento de informações médicas confidenciais.

Mediante estudos de Almehmadi, Alshehri e Tahir (2019), os dispositivos MIoT geram uma grande quantidade de dados em tempo real, o que torna tais dados altamente vulneráveis. No entanto, sua contribuição relevante no que concerne a soluções inovadoras para uma vida mais saudável, através da promoção de mudanças radicais na vida das pessoas. Através destes dispositivos, os profissionais de saúde monitoram remotamente seus pacientes fora de hospitais e outros ambientes de prestações de serviços em saúde como clínicas e postos médicos. Esta inovação imprime mais disponibilidade, acessibilidade, qualidade e custo-efetividade dos serviços de saúde.

Rizk, Rizk e Hsu (2019) identificam ameaças de segurança potenciais ao MIoT e apresentam os mecanismos de segurança para remover qualquer possível impedimento da segurança da informação imunológica do MIoT. Ao tempo que afirmam que a segurança e privacidade tornam-se grandes preocupações, especialmente na área médica, o que impede o setor de saúde de adotá-las, apesar de seus benefícios e potenciais. A abordagem de Rizk, Rizk e Hsu (2019), faz-se mediante uma estrutura resumida do modelo de segurança em camadas, e, uma revisão de avaliação específica de cada camada.

A garantia da segurança e da privacidade das informações de dispositivos para a saúde

elenca desafios relacionados à quantidade de dados,ao processamento, à memória, à sensibilidade e o alto nível de segurança exigido pelas aplicações (NASCIMENTO; LEAL; FONSECA, 2022).

As premissas de segurança são similares à segurança de outros sistemas, embora haja limitações de recursos dada a natureza destes dispositivos. Desta forma questões relacionadas a pouca memória, a capacidade de processamento limitada e a área física dos dispositivos implicam em diversas vulnerabilidades (NASCIMENTO; LEAL; FONSECA, 2022).

.

3
Metodologia

Este capítulo descreve como a pesquisa foi conduzida no que diz respeito às escolhas dos métodos Científicos.

3.1 Métodos

O desenvolvimento desta dissertação se deu a a partir de Mapeamento Sistemático e Revisão Sistemática. As referidas etapas foram desenvolvidas sob uma perspectiva metodológica de natureza aplicada. A pesquisa aplicada de acordo com Gil (2008) tem como principal característica o interesse na aplicação, utilização e consequentes práticas dos conhecimentos dirigidos à resolução de problemas específicos, perpassando o âmbito da teoria.

De acordo com Gil (2008) em relação ao objetivo geral, o qual define o caráter da pesquisa, pode-se afirmar se tratar de uma pesquisa exploratória, uma vez que no presente trabalho, buscou-se através de levantamento bibliográfico a familiarização do problema, para a devida e imediata aplicação na pratica. Vale ressaltar que o levantamento bibliográfico imprime o caráter científico à pesquisa.

A pesquisa exploratória realizada no âmbito da Internet das Coisas (IoT) no contexto de saúde, iniciou-se mediante a elaboração de um Mapeamento Sistemático, o qual subsidiou a seleção, a revisão e a sintetização dos trabalhos que, de acordo com a relevância, embasaram a pesquisa. Neste ínterim, foram consultadas publicações entre os anos 2015-2020.

Na Revisão Sistemática, aplicou-se um protocolo detalhado que permitiu buscar, selecionar, identificar, avaliar e interpretar toda literatura disponível e relevante frente ao tema proposto ou questão de pesquisa. Mediante estudos de (KITCHENHAM, 2004), toda Revisão Sistemática da Literatura deve apresentar tais aspectos.

No referido levantamento bibliográfico, utilizou-se as seguintes bases de dados: Sprin-

gerLink, ACM Digital Library, IEEE Digital Xplore, ISI Web Of Science, Science Direct e Scopus. Os termos de busca utilizados foram: (IoT, e-health, Internet das coisas, Segurança da informação, Internet of Things, Information security, healthcare). Cabe enfatizar a plataforma Parsifal [1] enquanto ferramenta de apoio utilizada na importação dos artigos.

Os resultados obtidos nas etapas de Mapeamento Sistemático, Revisão Sistemática e Literatura Cinzenta, compõem o corpo de conhecimento deste trabalho. Neste ínterim, o Mapeamento Sistemático pontuou as principais ameaças à segurança em Iot em Saude e os danos causados aos usuários de dispositivos médicos de Internet das Coisas vítimas de ataques cibernéticos, enquanto a Revisão Sistemática buscou subsídios na literatura pertinente, capaz de aprofundar uma pesquisa acerca de como ocorre o desenvolvimento de dispositivos de IoT na saúde com vistas a oferecer uma análise de segurança ainda na fase de levantamento de requisitos.

De acordo com Gama (2022), se um tema é ainda um campo de pesquisa pouco explorado, de modo que sejam poucas as contribuições científicas provenientes de materiais acadêmicos, podem ser analisados textos e artefatos úteis como relatórios técnicos, artigos, revistas, blogs e outros. Esta fonte é denominada Grey Literature (GL). A Literatura Cinzenta analisada neste trabalho propocionou uma discussão acerca dos desafios da segurança em IoT na saúde e possíveis técnicas a serem adotadas no sentido de promover a redução de riscos neste contexto e quais resultados se pretende alcançar.

No intuito de efetivar evidências acerca de problemas reais no que tange o Levantamento de Requisitos, recorreu-se a um método denominado pesquisa-ação-participativa (PAP) para o qual foram envolvidos profissionais e pesquisadores cujo processo e ação se deu através da experiência e da reflexão a partir de métricas capazes de promover mudanças e assim, otimizar as práticas.

No que concerne à PAP empreendida no desenvolvimento deste trabalho, esta ocorreu no contexto acadêmico e teve como público-alvo alunos de graduação de Engenharia de Software e áreas correlatas de diferentes instituições e contou com a participação da própria pesquisadora enquanto moderadora no acompanhamento das atividades.

Para uma sucinta compreensão do conceito de PAP; recorre-se a Coghlan e Brydon-Miller (2014) quando explicitam que na pesquisa-ação participativa a problematização surge do contexto [...]; os envolvidos desenvolvem uma visão informada e crítica sobre o contexto real em que se situa o problema; o pesquisador funciona como mediador da discussão e apoio técnico, o qual faz as abordagens, traça metas, angaria contribuições para a execução do projeto e articula agentes internos e externos, etc.

[1] <https://parsif.al/about/>

3.2 Materiais

Os dados utilizados para este estudo foram gerados a partir da aplicação de 03 questionários online, disponíveis nos apêndices F, G e H , com perguntas fechadas e abertas, por meio das quais foi possível aferir o perfil dos participantes, bem como o nível de conhecimento e habilidade em Engenharia de Software, Desenvolvimento e áreas correlatas.

Por meio do *feedback* dos formulários, foi possível guiar a seleção e recrutamento para a pesquisa (PAP), por meio da qual foi validada a ferramenta Adm. R que concerne em um *framework* conceitual cuja teoria e metodologia serve como base para novos projetos de ES ainda na fase inicial. O levantamento de requisitos feito pelos participantes desta pesquisa gerou documentação que caracteriza a validação da ferramenta

4

Mapeamento Sistemático da Literatura sobre segurança em MIoT

Nos dias atuais, os aplicativos de saúde baseados em IoT têm ganhando mais atenção devido às suas vantagens, como custos reduzidos, gerenciamento aprimorado de doenças e de medicamentos, além de monitoramento remoto. Tal realidade tem tornado a utilização de IoT em alvo lucrativo para a concorrência devido ao seu valioso potencial de oportunidades de negócios.

No entanto, devem ser consideradas algumas ressalvas no uso destes dispositvos, como por exemplo, a segurança e privacidade dos dados, tendo em vista que a natureza desses sensores provém de uma conexão sem fio e capacidades limitadas, tornando-os vulneráveis a uma série de ataques destinados a espionar ou adulterar as informações pessoais dos pacientes.

As abordagens ora apresentadas neste capítulo buscam descrever os riscos à Segurança da Informação através de uma discussão acerca dos desafios da segurança em IoT e das técnicas que podem ser adotadas para a redução de riscos no contexto de Internet das Coisas da saúde, pontuando as principais ameaças à segurança neste contexto e os danos causados aos usuários de dispositivos médicos de Internet das Coisas vítimas de ataques cibernéticos.

4.1 Questões de pesquisa

Esta seção responderá a seguinte Questão de Pesquisa Primária (QPP): Quais principais desafios em sa segurança em IoT e técnicas que podem ser adotadas para redução de riscos no contexto de Internet das Coisas da saúde?. Para a obtenção da resposta a esta questão, foram incluídas Questões de Pesquisa Secundárias (QPS). Ao se concluir a pesquisa procurou-se responder a maioria das questões norteadoras (primária e secundárias) bem como obter os dados propostos para esse mapeamento.

1. Quais técnicas podem ser adotadas para reduzir riscos no contexto de Internet das Coisas da saúde?

2. Quais os principais desafios de segurança em IoT?
3. Quais os danos causados aos usuários de dispositivos médicos de Internet das Coisas vítimas de ataques cibernéticos?
4. Qual o ano de publicação do estudo?
5. Qual o tipo de veículo de publicação da pesquisa?

4.2 Estratégia de busca

A pesquisa foi conduzida mediante bases internacionais sendo ACM Digital Library, IEEE Xplore Digital Library, Science@Direct, Scopus, e ISI Web of Science, totalizando 5 bases.

Foram utilizadas as seguintes bases de pesquisa:

- IEEE Xplore Digital Library <<http://ieeexplore.ieee.org>>;
- ISI Web of Science <<https://www.webofknowledge.com/>>;
- Science Direct <<http://www.sciencedirect.com>>;
- ACM Digital Library <<http://portal.acm.org>>;
- Scopus <https://www-scopus-com.ez20.periodicos.capes.gov.br/>

No Quadro 1 são apresentadas as Palavras-Chave utilizadas utilizadas para formar a *string* de busca.

Quadro 1 – Palavras-Chave utilizadas

Palavra-chave	**Sinônimo em Inglês**
Internet das Coisas,	IoT, Internet of Things
Segurança da Informação	Information security,
——-	healthcare, e-health

Fonte: Autores, 2020

No Quadro 2 é apresentada a *string* utilizada para as buscas nas bases:

Quadro 2 – *String* utilizada para realizar as buscas nas bases

("Internet das Coisas"OR "Internet of Things"OR "IoT"AND "segurança da informação"OR "information security"AND "healthcare"OR "e-health")

Fonte: Autores, 2020

Para filtrar os artigos relevantes foram estabelecidos Critérios de Inclusão (CI) e Exclusão (CE) indicados abaixo. Assim foram selecionados a partir somente da leitura do título e resumo de cada artigo resultando em 15 artigos oriundos de 236 artigos encontrados pela string. Após esta etapa vem o filtro por meio da leitura completa dos artigos resultantes da primeira seleção, analisando-os a partir de Questões de Qualidade.

A seguir os Critérios de Inclusão:

1. Acessível via web de maneira gratuita;
2. Artigos apenas com idioma inglês ou português;
3. Somente estudos primários.

A seguir os Critérios de Exclusão:

1. Estudos Duplicados;
2. Falta de disponibilidade para download de maneira gratuita;
3. Trabalhos publicados como resumos ou resumo expandido ou prefácio de periódicos e eventos;
4. Trabalhos que não contemplam a temática.

O critério de inclusão e exclusão enquanto ferramenta de busca, possibilitou o acesso a estudos de diferentes regiões que apresentam os desafios da segurança da informação no contexto de Internet das Coisas em saúde . Inclui-se neste interim, pesquisas empreendidas através da publicação de artigos em conferências ou periódicos; selecionados mediante tal critério, apenas artigos em inglês e português. Também foram utilizados somente estudos publicados a partir de 2015.

No que concerne à exclusão, não houve ênfase em relação a estudos duplicados, estudos secundários e trabalhos publicados como resumos ou resumo expandido ou prefácio de periódicos e eventos. Também foram excluídas informações incompletas ou aquelas sem disponibilidade para download.

4.3 Respostas

Nas próximas subseções serão analisados os resultados das 04 Questões de Pesquisa Secundárias com o intuito de responder à Questão de Pesquisa Primária; serão apresentados os dados encontrados nos artigos, bem como uma breve análise do mesmos.

4.3.1 QPS 1 - Quais técnicas podem ser adotadas para reduzir riscos no contexto de Internet das Coisas da saúde?

Ambrosio et al. (2019) desenvolveu a Internet of Things Security Modeling (IoTsecM), uma extensão UML para modelar controles de segurança identificados contra possíveis ataques para garantir a existência de análise e mecanismos de segurança.

Khan et al. (2019) propõem um mecanismo de criptografia que emprega operação aritmética de módulo, tem níveis comparativamente mais altos de segurança e que pode se adaptar melhor do que várias criptografias de imagem tradicionais e de última geração.

Zouka (2017) ressalta o armazenamento em um banco de dados criptografado e isolado da Internet. O serviço de segurança da informação será fornecido por uma rede em nuvem altamente confiável que permite a troca e compartilhamento de informações médicas confidenciais.

Williams e McCauley (2016) propõem uma estrutura de proteção de informações com autenticação, controle de acesso, segurança de rede e sistema, integridade e confidencialidade.

Huang et al. (2017) apresentam um modelo de criptografia homomórfica baseada em esquema de matriz capaz de garantir privacidade, analisar os dados médicos embaralhados e fornecer feedback dos resultados automaticamente.

4.3.2 QPS 2- Quais os principais desafios da segurança em IoT?

Aledhari et al. (2017) abordam que os requisitos de privacidade representam um grande desafio no uso dessas tecnologias. Quando os dispositivos e aplicativos não são testados, resultando em problemas de interoperabilidade, estabilidade, compatibilidade e segurança de dados.

Para Williams e McCauley (2016), torna-se difícil aplicar várias tecnologias de segurança existentes no ambiente de IoT porque vários serviços são fornecidos usando dispositivos sensores de baixa qualidade com desempenhos limitados

4.3.3 QPS 3- Quais os danos causados aos usuários de dispositivos médicos de Internet das Coisas vítimas de ataques cibernéticos?

Para Aledhari et al. (2017), se as decisões forem tomadas com base em informações inválidas, podem estar pondo em risco a vida dos pacientes.

Para Kiruba e Vijayalakshmi (2018), informações roubadas podem comprometer a saúde e a vida das pessoas.

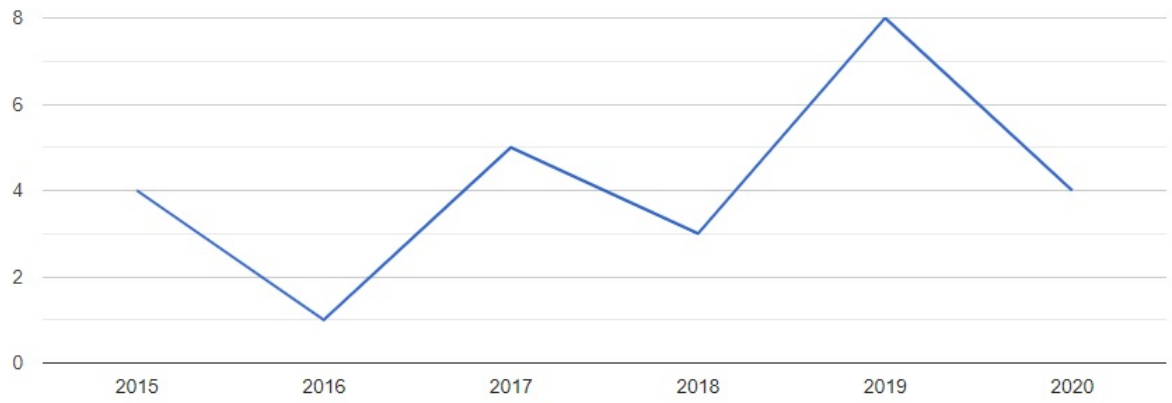
De acordo com Park et al. (2016) o mau funcionamento ou parada do equipamento IoT causado pela falha ao aplicar o módulo de segurança pode ser fatal o suficiente para ameaçar a vida das pessoas.

4.3.4 QPS 4-Em qual ano foi publicado?

Para a elaboração deste trabalho, foram buscados e selecionados estudos relevantes a partir do ano 2015 até o ano de 2022, e selecionados priorizando-se os anos mais recentes. Foram aceitos 04 artigos em 2015, 01 em 2016, 05 em 2017, 04 em 2018, 08 em 2019 e 05 em 2020.

.

Figura 4 – Ano de publicação



Fonte: Autores, 2022

4.4 Considerações do Capítulo

Os resultados encontrados nos artigos selecionados para a presente pesquisa, permitem responder as questões norteadoras que embasaram o Mapeamento Sistemático, o que vem a validar os caminhos percorridos na coleta de dados.

Mediante tal pressuposto, os requisitos de privacidade representaam um grande desafio no uso dessas tecnologias. Quando os dispositivos e aplicativos não são testados, podem resultar em problemas de interoperabilidade, estabilidade, compatibilidade e segurança de dados.

É válido ressaltar que o risco de ataques cibernéticos direcionados a aplicativos mHealth pode comprometer a disponibilidade e integridade das informações do paciente, prejudicando a mobilidade do atendimento e, às vezes, ameaçando a vida dos pacientes se as decisões forem tomadas com base em informações inválidas.

A Internet das Coisas ainda precisa de um mecanismo de segurança melhor que possa proteger a privacidade do paciente, uma vez que os dados de saúde são muito confidenciais para seus proprietários e, portanto, é importante garantir a segurança dos dados.

Segurança e privacidade tornam-se grandes preocupações, especialmente na área médica, o que impede o setor de saúde de adotá-las, apesar de seus benefícios e potenciais.

Torna-se difícil aplicar várias tecnologias de segurança existentes no ambiente de IoT porque vários serviços são fornecidos usando dispositivos sensores de baixa qualidade com desempenhos limitados

Quando um sistema não considera a segurança e privacidade dos dados, torna-se vulnerável a uma série de ataques destinados a espionar ou adulterar as informações pessoais dos pacientes. A natureza desses sensores provém de uma conexão sem fio e capacidades limitadas.

Os dispositivos MIoT geram uma grande quantidade de diversos dados em tempo real, altamente sensíveis. Portanto, proteger os dados médicos é um requisito essencial ao desenvolver arquiteturas MIoT.

Frente à pesquisa empreendida na elaboração deste artigo faz-se notável e significativa a necessidade de utilizar a IoT no âmbito da saúde, dada a praticidade e as diverss possibilidades. No referido contexto, apresenta-se também uma gama de dificuldades acerca da garantia de segurança da informação no que tange a Healthcare Internet of Things (HIoT) e Medical Internet of Things (MIoT). Tais modalidades de interconexão oferecem soluções inovadoras para uma vida mais saudável, fazendo mudanças radicais na vida das pessoas, mas chamam atenção com relação a vulnerabilidade gerada pela exposição de dados em rede.

A literatura corrobora a importância de provermaior segurança nesse contexto, o framework proposto para o levantamento de requisitos busca mitigar essa lacuna.

5

Revisão Sistemática sobre Levantamento de Requisitos para segurança em MIoT

As abordagens presentes nesta revisão, apontam que com o advento da Internet das Coisas (IoT), a área da saúde também inaugurou um novo modelo de funcionamento no qual, tornou-se possível o acompanhamento de pacientes de forma contínua e em tempo real, bem como a monitoração do seu estado de saúde onde quer que esteja. Neste contexto, a Internet das Coisas em Saúde ou *The Medical Internet of Things* (MIoT), pode ser definida como o conjunto de dispositivos e aplicativos médicos que se conectam através de redes de computadores online.

No desenvolvimento deste trabalho, explicita-se que MIoT, oferece soluções inovadoras para uma vida mais saudável, fazendo mudanças radicais na vida das pessoas, e podem monitorar continua e remotamente seus pacientes para muitos problemas médicos fora dos hospitais e clínicas. Cabe a ressalva que aplicativos nesta modalidade podem comprometer a disponibilidade e integridade das informações do paciente, prejudicando a mobilidade do atendimento e, às vezes, ameaçando a vida dos pacientes se as decisões forem tomadas com base em informações inválidas.

Desta forma, cabe um estudo aprofundado sobre levantamento de requisitos e modelagem de segurança em mApp em mHealth através de revisão de literatura. Na conclusão deste trabalho, foram apresentados os principais desafios de pesquisa, bem como projeções para trabalhos futuros neste âmbito.

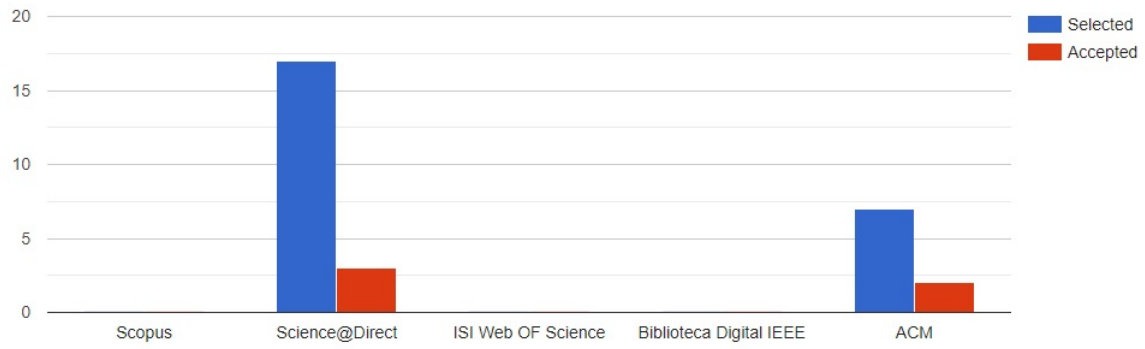
5.1 Estratégia de busca

Para o desenvolvimento desse levantamento bibliográfico foram utilizadas as seguintes bases de dados: SpringerLink, ACM Digital Library, IEEE Digital Library, ISI Web Of Science, Science Direct e Scopus. Os termos de busca utilizados foram: IoT, Requirements engineering, Segurança da informação, Internet das coisas, Engenharia de requisitos, Internet of things, Information security.

A Revisão Sistemática cumpriu um protocolo detalhado, este proposto por Kitchenham (2004) e foi dividida em três etapas: execução da busca, primeira etapa de seleção e segunda etapa de seleção. Para a etapa de execução da busca, foi utilizada a seguinte string, (“Internet das coisas” OR “Internet of Things” OR “IoT”) AND (“segurança da informação” OR "information security”) AND (“healthcare” OR “e-health”) AND ("levantamento de requisitos"OR "requirements engineering").

Desta forma a string é utilizada nas fontes escolhidas e os resultados obitidos são armazenados na ferramenta online Parsifal. A coleta de dados foi realizada no mês de abril de de 2021, não foi definido um tempo limite, foram selecionados apenas artigos publicados em conferências ou periódicos. Assim, a pesquisa teve como resultados um total de 25 artigos, como pode ser visto na Figura 5 , sendo aceitos 5 artigos, 2 na base ACM Digital Library, e 3 artigos na base Science Direct.

Figura 5 – Ano de publicação



Fonte: Autores, 2022

Mediante esta análise, descreve-se uma constante busca por soluções frente à vulnerabilidade referente a IoTHealth à qual os usuários estão expostos. Grande parte dos trabalhos analisados apontam falhas no que concerne à análise de requisitos como sendo o maior fator de risco. Neste contexto toma-se como referência o trabalho de (AMBROSIO et al., 2019), que sugere controles de segurança da informação apropriados nos estágios iniciais do ciclo de vida de desenvolvimento de aplicativos móveis (mApp), enquanto ferramenta necessária para identificar os riscos e tratá-los durante o projeto do aplicativo.

5.2 Resultados

Frente à pesquisa empreendida na elaboração deste artigo faz-se notável e significativa a necessidade de utilizar a IoT no âmbito da saúde, dada a praticidade e as diversas possibilidades.No referido contexto, apresenta-se também uma gama de dificuldades acerca da garantia de segurança da informação no que tange a Healthcare Internet of Things (HIoT) e Medical Internet of Things (MIoT).

Neste ínterim faz-se relevante o desenvolvimento de uma ferramenta de Engenharia de Requisitos capaz de pre-estabelecer protocolos e requisitos que ofereçam segurança desde a fase de projeto destes aparatos. Esta, deve imprimir a compreensão de como é tratada a segurança da informação em (HioT) na fase de desenvolvimento dos softwares, bem como verificar se os requisitos de segurança estão presentes ainda nesta fase ou só são visíveis somente quando este já está pronto para o uso. Para tanto faz-se necessario a elaboração de um modelo de inclusão de segurança que deve ser testado e validado, para a comprovação da sua funcionalidade.

5.3 Considerações do Capítulo

As aplicações de dispositivos para IoT em saúde elaboradas na ausência de requisitos de segurança, impactam na privacidade dos usuários bem como na funcionalidade dos dispositivos. Grande parte dos trabalhos analisados apontam falhas no que concerne à análise de requisitos como sendo o maior fator de risco. Neste contexto, toma-se enquanto referência uma pesquisa que sugere controles de segurança da informação apropriados nos estágios iniciais do ciclo de vida de desenvolvimento de aplicativos móveis (mApp) enquanto ferramenta necessária para identificar os riscos e tratá-los durante o projeto do dispositivo. Ressalta-se ainda, serem poucos os trabalhos voltados para o levantamento de requisitos de segurança aplicados à etapa inicial do ciclo de vida dos dispositivos em saúde. Espera-se que ao final deste trabalho surjam novas linhas de pesquisa que avaliem a importância acerca de como é tratada a segurança da informação em (HioT) na fase de desenvolvimento dos softwares. Para tanto apresenta-se a elaboração de um *framework* que será disponibilizado em site específico enquanto guia para desenvolvedores de aplicações de IoT da sáude.

6

Trabalhos relacionados

Nesta seção, apresentam-se os trabalhos de pesquisa relacionados ao tema, para além da Revisão Sistemática da literatura. Como critério de seleção, foram incluídos os trabalhos que abordam os desafios da segurança da informação no contexto de Internet das Coisas na saúde. Mediante a um restrito número de artigos científicos coletados no primeiro momento da pesquisa, descrito como Mapeamento Sistemático, e ainda observado na Revisão Sistemática, utilizou-se enquanto pesquisa complementar, alguns trabalhos correlatos , oriundos do *Google Scholar*, uma plataforma de publicação de artigos de conferências ou periódicos.

O trabalho de Ramachandran (2016) parte do pressuposto de que o risco de ataques cibernéticos direcionados a aplicativos mHealth pode comprometer a disponibilidade e integridade das informações do paciente, prejudicando a mobilidade do atendimento e, às vezes, ameaçando a vida dos pacientes se as decisões forem tomadas com base em informações inválidas.

Para Rios, Fernandez-Gago e Lopez (2018) as negociações de confiança trazem ameaças à privacidade pessoal se não forem cuidadosamente consideradas. Neste ínterim, propõem uma estrutura para representar negociações de confiança nas fases iniciais do Ciclo de Vida de Desenvolvimento de Software (SDLC), de modo que esta venha a ajudar os engenheiros de software a determinar as políticas mais adequadas para o sistema, detectando conflitos entre os requisitos de privacidade e confiança através da linguagem de modelagem SI.

Na abordagem de Sequeiros et al. (2020) faz-se notável considerar que ao projetar um sistema, o *design* deve organizar e estruturar o processo a partir de uma camada de detecção, de forma a reduzir a complexidade do processo, o que permite a criação de requisitos específicos a partir dos quais se analisa interações e comportamentos diminuindo as chances de erros ainda na fase de elaboração.

Carvalho, Andrade e Oliveira (2018) propõem uma solução para os desenvolvedores. Embora existam vários catálogos de correlações propostos na literatura, eles não levam em conta novas características que surgiram com o ambiente de Computação Ubíqua (UbiComp) e Internet

das Coisas (IoT), como a invisibilidade. Em um estudo anterior, foi proposto um processo para definir um catálogo de correlações para características de qualidade.

Para Carvalho, Andrade e Oliveira (2018) as características de qualidade de um software apresentam inconsistência na maioria das vezes, uma vez que uma característica pode impactar negativamente outra, gerando assim diversas dificuldades a serem abordadas no seu desenvolvimento. Para tanto, Carvalho propõe a utilização de catálogos de requisitos não funcionais (NFRs).

Mantha, Soto e Karri (2021) analisa a ameaça à segurança cibernética relevante para a indústria de Arquitetura Engenharia e Construção (AEC), propondo modelos de ameaça para cada uma das fases do ciclo de vida do projeto. A viabilidade da abordagem é ilustrada e inclui um sistema robótico autônomo para coletar dados como uma possível contramedida. A contramedida ora referida, visa enfrentar alguns dos desafios de cibersegurança presentes no processo de certificação e comissionamento na execução do projeto. Os resultados mostram que a probabilidade de detectar sensores desonestos aumenta com restrições adicionais no robô de monitoramento, como distância mínima e máxima. Os modelos ilustrativos sugerem que a estrutura proposta ajudará a abordar a segurança cibernética dos sistemas e das partes interessadas e durante as fases cruciais dos projetos.

De acordo com Pressman e Maxim (2016) os requisitos de segurança de software não podem ser compreendido apenas enquanto um conjunto de restrições nos sistemas. E sim, devem apresentar um gerenciamento satisfatório que ofereça proteção e confiança. Neste sentido, faz-se pertinente a análise de novas técnicas de ataque, porém observando-se o uso indevido ou abuso na elaboração dos de requisitos. Além de fornecer processos, ferramentas, técnicas, modelagem, estimativa de custos, planejamento de projetos e acordos contratuais , a Engenharia de Requisitos cria e examina cada elemento do modelo em termos de inconsistência, omissões e ambiguidade, representando-os e agrupando-os em pacotes. Tal esforço colaborativo, envolve muitos participantes, como analistas de negócios, engenheiro de requisitos de software, arquiteto de software e gerentes de testes.

No Quadro 3 está disposta a relação de cada trabalho com este.

Quadro 3 – Comparação entre os Trabalhos Relacionados

Autor (ano)	IoT	Desafioos IoT	Desenvolvimento IoT	Engenharia de Software	Segurança	Levantamento de requisitos	eHealth
Ramachandran(2016)				X	X	X	
Rios (2018)				X	X	X	
Sequeiros (2020)	X	X	X		X		
Carvalho (2018)	X	X	X	X		X	
Mantha(2021)					X		
Pressman (2016)				X		X	
Este estudo	X	X	X	X	X	X	X

Fonte: Autores, 2022

7

Desenvolvimento do Adm. R

Neste capítulo será descrito cada artefato desenvolvido durante a pesquisa, os resultados, a avaliação e validação das funcionalidades dos artefatos e a discussão dos resultados.

7.1 Processo de desenvolvimento do Framework

O Adm. R é um *framework* do tipo conceitual. De acordo com Magher (2016), framework conceitual se constitui enquanto estrutura usada para explicar o contexto e direcionar um projeto de pesquisa. Assim, ainda na fase de planejamento, o *framework* oferece um passo a passo com base em pesquisas anteriores determinando a teoria e a metodologia a ser utilizada no projeto de pesquisa atual.

Dadas as carcterísticas específicas do framework ora descrito, e como se trata de uma estrutura de caráter gerencial, atribui-se a este, o título de Adm.R, em alusão à administração de requisitos. Ressalta-se ainda que *frameworks* conceituais são produtos gerados a partir de processos qualitativos compostos por conceitos capazes de fornecer uma compreensão abrangente de um fenômeno em estudo.

Para a elaboração do Adm. R (Framework de elicitação de requisitos) foi realizada inicialmente a construção de um corpo de conhecimento apresentado no capitulo 2, com o intuito de identificar as principais características do sistema de Software IoT, entender a Engenharia de Software, particularidades de sistemas de HIoT, técnicas de elicitação de requisitos e desafios durante essa etapa de desenvolvimento.

De acordo com os trabalhos relacionados, parte dos problemas de segurança nos dispositivos de Internet das Coisas concerne ao desenvolvimento dos mesmos, é perceptível que há desafios para garantia de qualidade de sistemas desse âmbito.

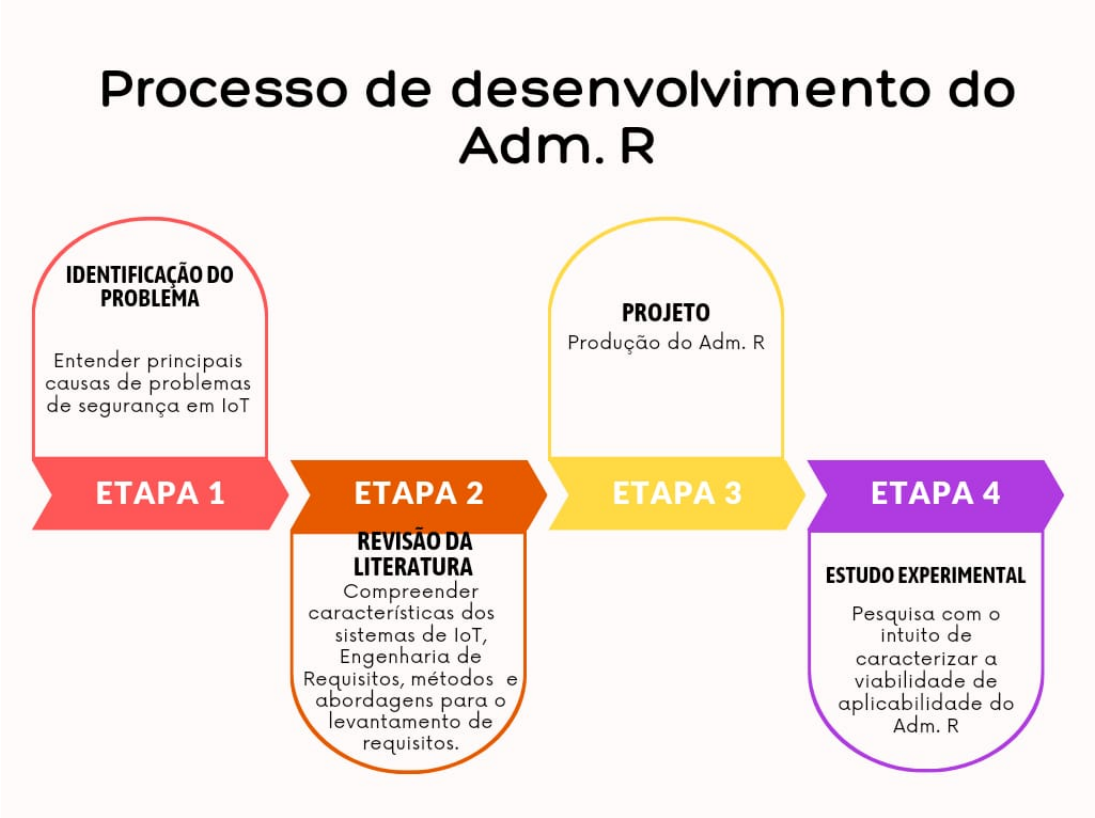
Apesar de existirem técnicas diversas que são utilizadas por engenheiros de software

dentro das indústrias para a atividade de elicitação de requisitos ainda não existe uma técnica padronizada para *software* de IoT, e são poucos os estudos que tratam disso, alguns estudos propõem adaptações dos métodos tradicionais de sistemas (*web* ou *mobile*) no contexto de sistemas de Internet das Coisas.

O Adm. R é um *framework* conceitual que tem como objetivo, apoiar desenvolvedores durante a fase de Elicitação de Requisitos, na tentativa de prover que o sistema funcione como o esperado, minimizando falhas de segurança. Uma vez que o mesmo enfatiza a identificação de requisitos relevantes no que diz respeito à segurança.

Na Figura 6 estão descritas as etapas de desenvolvimento para formação de conhecimento utilizado na construção do *framework*.

Figura 6 – Processo de desenvolvimento do Adm. R

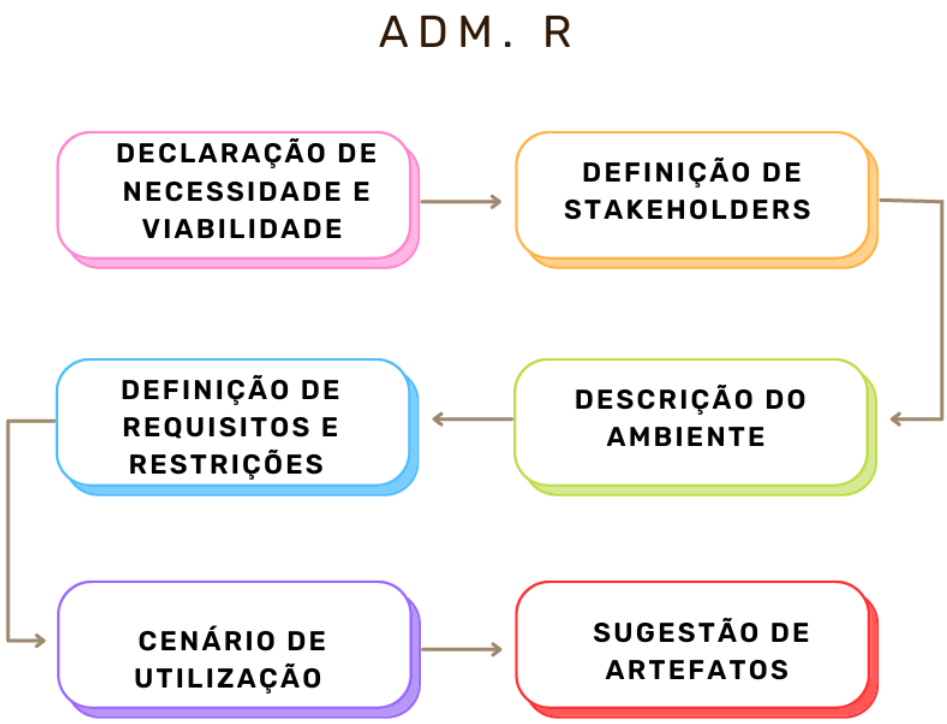


Fonte: Autores, 2022

7.2 Projeto

Na Figura 7 é possível entender como está organizado o Adm. R, disposto por uma sequência de atividades, a fim da obtenção do máximo de informações relacionadas ao sistema, com o objetivo de compreender o mais correto e completo acerca do que é solicitado para aquele sistema de software como propõe Pressman e Maxim (2016).

Figura 7 – Fluxograma de Atividades do ADM. R



Fonte: Autores, 2022

- Declaração de necessidade e viabilidade:

  A primeira etapa do Adm. R se constitui enquanto definição do sistema e limitação do escopo de acordo com Zowghi e Coulin (2005). Entender o domínio do sistema é importante ao iniciar o processo para investigar e examinar em detalhe a situação em que o sistema irá residir o que é chamado de domínio de aplicação.

  O ambiente atual precisa ser explorado, incluindo aspectos políticos, organizacionais e sociais. Aspectos relacionados ao sistema, além de quaisquer restrições sobre o sistema ou

seu desenvolvimento. Processos de trabalho existentes e os problemas a serem resolvidos pelo sistema precisam ser descritos.

- Definição de *Stakeholders*:

  Posteriormente a descrição do sistema, é necessário identificar os envolvidos afetados pelo problema, definindo assim uma possível solução. Envolvido é qualquer um que tenha interesse direto ou que se beneficie do sistema a ser desenvolvido, Pressman e Maxim (2016) recomenda descrever uma lista de pessoas que vão contribuir com sugestões à medida que os requisitos forem obtidos, a lista inicial crescerá à medida que os envolvidos forem contatados, pois para cada um deles, será feita a pergunta: “com quem mais você acha que eu devo falar ?"

- Descrição do ambiente :

  De acordo com Santos et al. (2016) a arquitetura básica dos objetos inteligentes é composta por quatro unidades: processamento/memória, comunicação, energia e sensores/atuadores.

- Definição de requisitos e restrições :

  Sistemas de IoT possuem complexidades e restrições em consequência da integração de componentes de *hardware* e de *software*, tais restrições tornam o projeto desafiador, com isso é essencial considerar detalhadamente o máximo de características durante a sua construção.

  O Adm. R indica a identificação dos requisitos funcionais, requisitos não funcionais e requisitos de segurança, de acordo com Sommerville (2011) os requisitos funcionais são declarações de serviço que o sistema deve fornecer, como o sistema deve reagir a entradas especificas e de como o sistema deve se comportar em determinadas situações, os requisitos não funcionais estão relacionados às restrições dos serviços ou funções oferecidos pelo sistema, incluem restrições de tempo, restrições de processo de desenvolvimento e restrições impostas pelas normas.

  Requisitos de segurança, especificam como um sistema deve se proteger de defeitos internos, para falhas de sistema que causam danos ao meio ambiente, para acidentes ou ataques do ambiente do sistema que estejam danificando o próprio sistema, bem como facilitar a recuperação em caso de falha.

  Ainda de acordo com Sommerville (2011) uma abordagem dirigida a riscos para especificação de requisitos leva em consideração os eventos perigosos que podem ocorrer, a probabilidade de que estes eventos venham a ocorrer, a probabilidade de os resultados desses eventos serem danos e a extensão desses danos.

- Cenário de utilização:

De acordo com Pressman e Maxim (2016) à medida que os requisitos são reunidos, começa a se materializar as funções e características, com isso é difícil passar para as atividades mais técnicas da Engenharia de Software, enquanto não há uma definição clara de como as estas serão usadas pelos diferentes tipos de usuários. No entanto os desenvolvedores podem criar um conjunto de cenários que identifique um roteiro de uso para o sistema a ser construído, os mesmos fornecem uma descrição de como o sistema será utilizado.

- Sugestão de artefatos:

  Por fim o Adm. R sugere artefatos pra melhor interação entre com *Stakeholders*, como entrevista, criação de cenários e casos de uso.

7.3 Avaliação do Framework

A avaliação do Adm. R foi realizada em duas etapas dentro de um contexto acadêmico, a primeira etapa com alunos de graduação do curso de Egenharia de Software da UFS- Universidade Federal de Sergipe, e contou com a participação da própria pesquisadora para servir de moderador para acompanhar as atividades, esta ocorreu durante um período de 30 dias na modalidade de ensino remoto.

Inicialmente os alunos responderam um formulário de caracterização e posteriormente foram aplicadas aulas conceituais cuja abordagem permitiu uma ampla compreensão para a realização da pesquisa. Todos concordaram em participar do estudo e consentiram a utilização dos dados para fins de pesquisa. Em visita e entrevista informal a profissionais de saúde, foram angariados subsídios através da qual foram desenvolvidos os estudos de caso fictícios, disponíveis no apêndice D, que foram entregues aos alunos participantes juntamente com a ferramenta Adm. R, disponível no apêndice E, para apoio na realização da atividade de elicitação de requisitos.

Nesta etapa da pesquisa, os alunos tiveram um prazo de 15 dias para realizar a elicitação de requisitos e ao finalizarem apresentaram os respectivos projetos. Logo após responderam o formulário de acompanhamento que provê informações qualitativas a respeito da viabilidade de aplicação do mesmo. O formulário pós uso contém questões sobre grau de dificuldade em identificar requisitos, o nível de clareza e facilidade ao utilizar a ferramenta e espaço para críticas e sugestões.

Tendo em vista a necessidade de se realizar um novo estudo levando em consideração a sugestões recebidas durante o primeiro uso, foi oferecido um curso online, neste os participantes se inscreveram por meio de um formulário o qual também coletava informações sobre o perfil dos mesmos, principalmente em relação à experiência na área de desenvolvimento, e levantamento de requisitos.

Nessa segunda etapa da pesquisa ambas equipes receberam o mesmo caso, mas apenas uma recebeu a ferramenta de apoio, o Adm. R. O critério para essa escolha foi o grau de

habilidade em engenharia de software. Os participantes tiveram um prazo de 15 dias para realizar a elicitação de requisitos e ao finalizarem apresentaram os projetos.

Os trabalhos das equipes de ambas as fases estão nos apêndices A e B, os nomes dos alunos foram modificados para garantir a privacidade dos mesmos.

Mediante um estudo de caso, a equipe que não teve acesso a ferramenta Adm. R ao apresentarem a documentação, explicitam um levantamento de requisitos que não oferece clareza com relação à identificação do problema e /ou como esse sistema ajudaria na resolução, embora utilizem os termos: pacientes, monitoramento da saúde do paciente, médicos, enfermeiros e emergencista, não explicita o domínio. Observa-se também no levantamento de requisitos desta, que o mesmo não nomeia e caracteriza todas as pessoas envolvidas.

Em contrapartida, as equipes que acessaram a ferramenta, apresentaram uma documentação de levantamento de requisitos cuja estrutura especifica claramente o problema, bem como aponta soluções, indica o domínio do sistema e descreve seus *Stakeholders*, seguindo a teoria e a metodologia expressa no modelo cedido pela ferramenta.

É possível observar também, que participantes que utilizaram o *framework* especificaram o critério da escolha dos recursos a serem utilizados, bem como a fonte de alimentação, processador, protocolos e sensores, justificando o critério de escolha de cada um destes recursos. Considerando aspectos de segurança, como por exemplo minimizar falha no fornecimento de dados como na Figura 8.

Figura 8 – Unidade de Comunicação

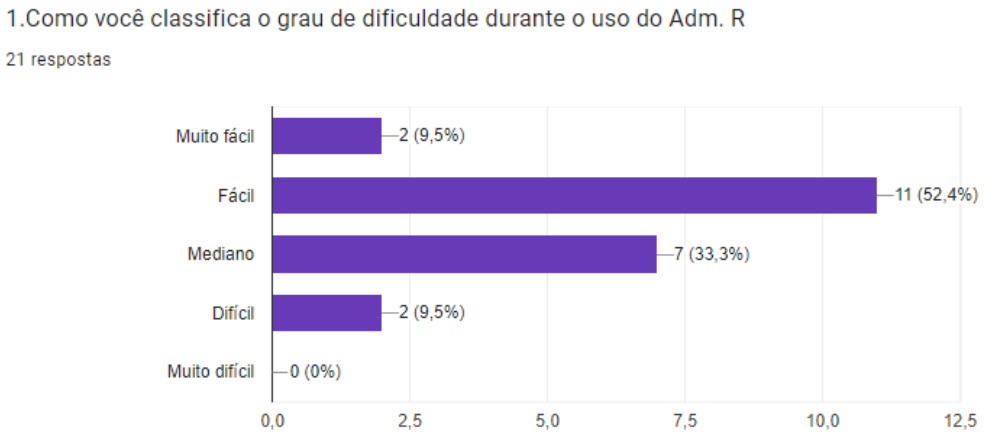
Fonte: Autores, 2022

Como já mencionado, os grupos que utilizaram o Adm.R responderam o formulário sobre o uso da ferramenta, cujos dados obtidos nas duas fases da pesquisa foram sistematizados mediante informações obtidas através de formulários aplicados a estes e estão dispostos no seguinte endereço: <https://forms.gle/MZL4QtBiqawVU2yQ9> Para aferir o grau de dificuldade

enfrentado pelos participantes que utilizaram o Adm.R foram aplicadas as questões abaixo descritas:

A primeira pergunta acerca do grau de dificuldade encontrado no uso do Framework Conceitual, na qual utilizou-se os termos: muito fácil, fácil, mediano, difícil, e muito difícil, retornou 21(vinte e uma respostas, sendo em percentuais: 9,5% para muito fácil; 52,5% para fácil; 33,3% para mediano; nenhuma resposta para muito difícil, abordado na Figura 9.

Figura 9 – Questão 01 Formulário Pós uso do Adm.R



Fonte: Autores, 2022

A segunda pergunta, cuja abordagem discorre sobre a ferramenta enquanto facilitadora de elicitação dos projetos aos quais se aplica, apresentou as alternativas: totalmente, boa parte das vezes e, não. Nesta, obteve-se das 21 respostas, 42,9% para totalmente; 57,1% para boa parte das vezes; e nenhuma resposta para não, como mostra a Figura 10.

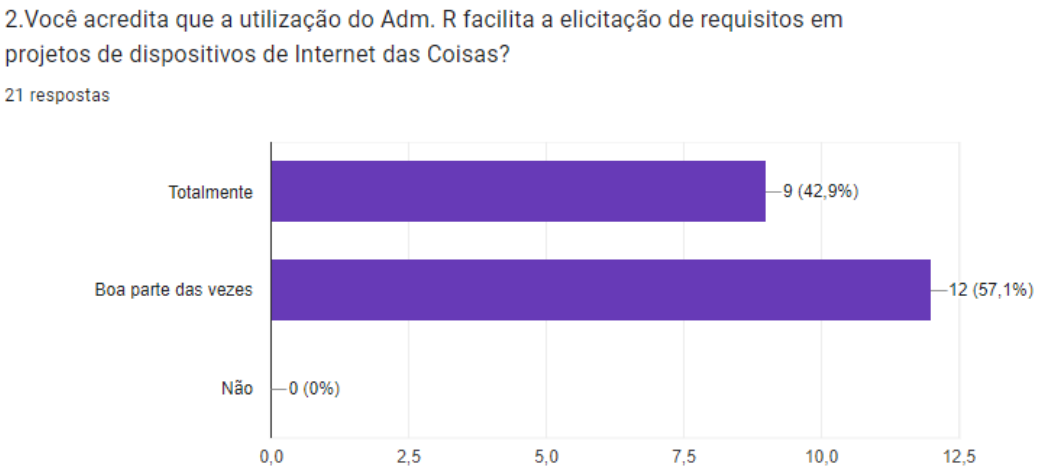
Além dos resultados com perguntas fechadas, foi possível coletar também a opinião dos participantes acerca da metodologia utilizada. Neste sentido, direcionou-se a terceira pergunta: " você acredita que a utilização do Adm. R reduz o tempo de atividade de elicitação de requisitos se comparada a não utilização dele? " Neste ínterim, descreve-se abaixo algumas respostas consideradas relevantes para a sistematização deste estudo:

P1: Sim, pelo fato de ter uma narrativa no campo de necessidade e viabilidade. Facilitando a visualização do problema e pensando nos requisitos que resolvem o problema.

P2: Com certeza, pois a estrutura como um todo faz o levantador de requisitos ganhar tempo, pois as informações estão bem organizadas e suas identificações em tópicos os deixam mais compreensivo na hora de elicitar um requisito.

P3: Sim, porque ele orienta tanto quais pontos, além da ordem em que temos que abordar para levantar os requisitos do sistema.

Figura 10 – Questão 02 Formulário Pós uso do Adm.R

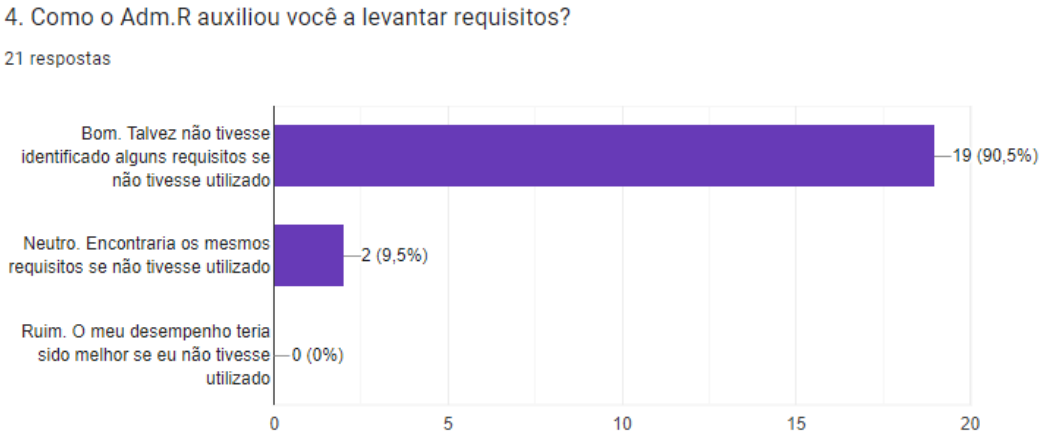


Fonte: Autores, 2022

P4: O *framework* proporciona agilidade no desenvolvimento dos requisitos e por ser muito intuitivo as atividades são realizadas de maneira eficiente de se chegar ao resultado esperado.

A quarta pergunta, de cunho prático, acerca de como a ferramenta em análise auxiliou ao entrevistado no levantamento de requisitos, para a qual se apresentou hipoteticamente: Alternativa 1- Bom. Talvez não tivesse identificado alguns requisitos se não o tivesse utilizado – para a qual se obteve 90,5%; Alternativa 2- Neutro. Encontraria os mesmos requisitos se não tivesse utilizado – com 9,5% das respostas; Ruim. O meu desempenho teria sido melhor se se eu não o tivesse utilizado – para a qual nenhuma resposta retornou, explicito na Figura 11.

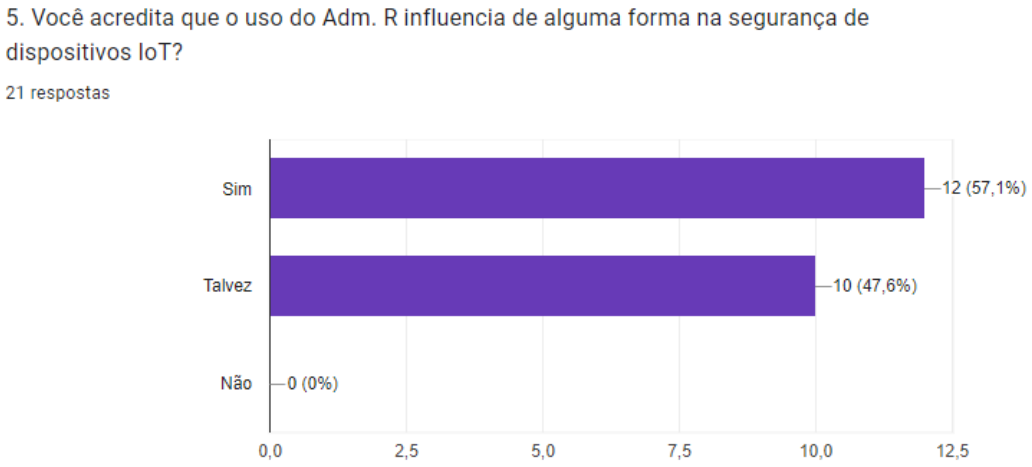
Figura 11 – Questão 04 Formulário Pós uso do Adm.R



Fonte: Autores, 2022

A quinta questão interrogou acerca da influência da ferramenta em estudo no que tange a segurança dos dispositivos IoT, tendo como alternativas: sim, não e talvez, abordado na Figura 12.

Figura 12 – Questão 05 Formulário Pós uso do Adm.R



Fonte: Autores, 2022

A abordagem da questão 6, acerca de sentir, ou não a necessidade de algum artefato adicional no Adm. R, retornou 21 respostas das quais foram selecionadas 2/3, o equivalente a 14 respostas descritas abaixo:

1. Não

2. Não. Só dificuldade de entendimento na aplicação do framework.

3. Uma tabela que narra cada caso de uso. Com fluxo principal, secundário etc. (Se o diagrama de caso de uso não for suficiente).

4. Acrescentar tabelas para "mapear"os requisitos e afins.

5. Acredito que não.

6. Não, não que eu me lembre.

7. Sim.

8. Talvez uma descrição sobre quais diagramas deveriam ser necessários para elicitação.

9. Não, ele foi suficiente.

10. Não. O framework é bem eficiente.

11. Não, mas possa ser que sinta se utilizado em outros projetos com maior complexidade.

12. Nenhum.

13. Acho que precisa em cada tópico que for necessário a menção de alguns diagramas,

por exemplo casos de uso, diagrama de sequência, que na minha opinião ajuda a entender como funciona o sistema.

14. Nas minhas atividades não sentir necessidade de nada além do oferecido pelo framework.

A questão 7, na qual foi solicitada a opinião de cada participante a respeito da ferramenta Adm. R, retornou 21 respostas as quais estão dispostas a seguir:

1. Organiza os critérios de avaliação para levantamento de requisitos.

2. Simples, pequeno e preciso.

3. Fácil compreensão; Estrutura simplificada.

4. Auxílio prático para aprimorar os requisitos.

5. Simplicidade. Tem o essencial.

6. Projeto Padronizado, Maior segurança, reduz tempo.

7. De fácil utilização, com boas descrição sobre cada item. Além de trazer exemplos de como deveria ser feito.

8. Fácil utilização, torna a elicitação de requisitos mais clara e eficiente, além de reduzir os riscos e o tempo do processo.

9. O framework fornece um guia de instruções que auxilia no levantamento dos requisitos, além servir como uma base para o projeto.

10. Fácil entendimento, abrangente, bem estruturado.

11. Facilidade de enxergar as necessidades e requisitos do projeto; capacidade de prever possíveis falhas no sistema na fase de planejamento.

12. Fácil e intuitivo.

13. Contém o necessário para se ter um excelente documento de requisitos.

14. Usar o Adm. R é bom por que como já citei antes nos dá uma direção de como estruturar o levantamento de requisitos.

15. Fácil utilização.

16. É um framework muito conciso, direto. Pode parecer pouca coisa, mas acho importante devido a facilidade de sua aplicabilidade.

17. Fácil de usar. Ajuda a encontrar Requisitos que não são tão óbvios/fáceis de observar.

18. Muito bom, nos orientou muito na melhor forma realizar o levantamento de requisitos além da divisão dos trabalhos entre o grupo.

19. Objetivo, simples e rápido.

20. Agilidade, intuitivo, eficiente.

21. Eficiente, breve.

8

Considerações Finais

Este capítulo decreve as considerações finais acerca dos estudos empreendidosna elaboração desta dissertação.

O objetivo macro desta pesquisa foi desenvolver um modelo de boas práticas para o levantamento de requisitos de *Software* voltados para segurança em Internet das Coisas. O modelo se aplica à IoT em geral, embora com foco na saúde dado o maior nível de vulnerabilidade nesta área. Para o alcance deste objetivo, a primeira etapa deste trabalho consiste em um levantamento e análise dos trabalhos relacionados ao desenvolvimento de *Software* para Dispositivos de IoT aplicados à saúde.

Ainda na primeira etapa, foram descritos os desafios da Segurança da Informação em IoT em saúde, analisando as vulnerabilidades bem como um breve análise e verificação dos impactos de ataques a dispositivos de de IoT em Saúde.

Para o desenvolvimento da primeira etapa, elaborou-se uma questão norteadora capaz de definir o que estaria sendo procurado e quais resultados se pretendia alcançar, para assim, selecionar as bibliografias pertinentes. A questão norteadora possibilitou traçar um panorama da pesquisa e construir uma string de busca que definiu critérios de exclusão e inclusão de publicações dada a relevância acerca do tema.

Já na segunda etapa, a de revisão bibliográfica, buscou-se concentrar um maior número de trabalhos relacionados à IoT, Levantamento de Requisitos, Dispositivos de Internet das Coisas em Saúde e outras abordagens correlatas. No desenvolvimento dessa revisão bibliográfica, utilizou-se as bases de dados Springer Link 1, ACM Digital Library 2, IEEE Digital Library 3, ISI Web Of Science 4, Science Direct 5 e Scopus.

Esta etapa consolidou a revisão sistemática a partir da qual se construiu um corpo de conhecimento com o intuito de identificar as principais características do Sistemas de Software IoT, bem como entender a Engenharia de Software, as particularidades de sistemas de HIoT e

técnicas de Elicitação de Requisitos.

A terceira etapa consiste no desenvolvimento de *framework* conceitual enquanto modelo adaptável para o levantamento de requisitos no desenvolvimento de aplicações IoT da saúde com ênfase em segurança, o qual foi validado através de um curso de levantamento de requisitos online. os participantes se inscreveram por meio de formulário que também coletava informações sobre o perfil dos mesmos, principalmente em relação a experiência na área de Desenvolvimento Levantamento de requisitos. Sendo a não experiência enquanto critério para a utilização do *Framework*.

A documentação resultante do levantamento de Requisitos permitiu uma visão panorâmica do quanto a ferramenta ora descrita identifica requisitos relevantes no que diz respeito à segurança e, portanto, se faz pertinente no sentido de nortear o projeto de desenvolvimento de um software imprimindo a esse, a capacidade de apoiar desenvolvedores durante a fase de Elicitação de Requisitos, provendo que o sistema funcione como o esperado, minimizando assim as falhas de segurança.

Considerando que 55,5% dos participantes da pesquisa, apontaram a Adm. R enquanto ferramenta de fácil utilização, bem como 57,1% responderam que em boa parte das vezes a ferramenta se apresenta como facilitadora na elicitação dos projetos, tais dados a apontam enquanto aparato relevante no âmbito de levantamento de requisitos.

Ressalta-se o quantitativo 90,5% de respostas apontando que talvez não tivessem sido identificados alguns requisitos sem o uso aparto ora descrito, o que permite compreender quão eficiente se apresenta a ferramenta Adm. R. No que tange a percepção da necessidade de um artefato adicional para melhor desempenho da ferramenta em estudo, as respostas da questão 6, apontam não haver tal necessidade.

8.1 Limitações do Trabalho

Mediante observações cabíveis, após análise dos dados obtidos por meio deste questionário, convém conceituar a Adm.R como ferramenta relevante no que concerne a levantamento de requisitos, haja visto o nível de satisfação do público alvo desta abordagem, embora, no âmbito da segurança este estudo ainda necessite de análises futuras mais aprofundadas, dada a insuficiência de pesquisas correlatas.

8.2 Trabalhos Futuros

Nesta seção serão apresentadas algumas contribuições para trabalhos futuros. São elas:

- Disponibilizar o Adm. R em plataformas digitais;

- Elaborar template de acompanhamento para elicitação de requisitos;
- Realizar novos testes.

Referências

ABRAN, A. et al. Software engineering body of knowledge. *IEEE Computer Society, Angela Burgess*, p. 25, 2004. Citado na página 17.

AFONSO, B. S.; PEREIRA, R. B. d. O.; PEREIRA, M. F. L. Utilização da internet das coisas para o desenvolvimento de miniestação de baixo custo para monitoramento de condições do tempo em áreas agrícolas. *Anais da Escola Regional de Informática da Sociedade Brasileira de Computação (SBC)–Regional de Mato Grosso*, v. 6, p. 183–189, 2015. Citado na página 20.

AKABANE, G. Gestão estratégica das tecnologias cognitivas: conceitos, metodologias e aplicações. *São Paulo: Érica*, 2018. Citado na página 19.

ALEDHARI, M. et al. A new cryptography algorithm to protect cloud-based healthcare services. In: IEEE. *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. [S.l.], 2017. p. 37–43. Citado 2 vezes nas páginas 21 e 34.

ALEXANDROV, V.; DESNITSKY, V.; CHALY, D. Design and security analysis of a fragment of internet of things telecommunication system. *Automatic Control and Computer Sciences*, Springer, v. 53, n. 7, p. 851–856, 2019. Citado na página 20.

ALMEHMADI, T.; ALSHEHRI, S.; TAHIR, S. A secure fog-cloud based architecture for miot. In: IEEE. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. [S.l.], 2019. p. 1–6. Citado 2 vezes nas páginas 10 e 26.

AMBROSIO, P. J. E. et al. Securing mhealth applications using iotsecm security modelling: Dentify. me mapp case study for urgent care management. *Computación y Sistemas*, v. 23, n. 4, 2019. Citado 6 vezes nas páginas 10, 11, 12, 25, 34 e 38.

ANDRADE, B. A. L. et al. Aplicando e adaptando a metodologia ágil scrum no processo de ensino e aprendizagem de engenharia de software baseado no desenvolvimento com equipes distribuídas. *XVI ERBASE*, 2016. Citado na página 16.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 14724*: Informação e documentação — trabalhos acadêmicos — apresentação. Rio de Janeiro, 2005. 9 p. Citado na página 23.

BARBOSA, A. F.; LENCASTRE, M. Identificando cenários de conflitos na engenharia de requisitos visando aplicação da comunicação não violenta. In: *WER*. [S.l.: s.n.], 2019. Citado 2 vezes nas páginas 16 e 17.

BERTONI, A. P. S. et al. Internet das coisas de saúde: aplicando iot, interoperabilidade e aprendizado de máquina com foco no paciente. *Sociedade Brasileira de Computação*, 2022. Citado na página 21.

BHARADWAJ, S. A. et al. Enhancing healthcare using m-care box (monitoring non-compliance of medication). In: IEEE. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. [S.l.], 2017. p. 352–356. Citado 2 vezes nas páginas 21 e 22.

BRITO, C. d. S. Uso de mapas mentais no processo de engenharia de requisitos do núcleo de práticas em informática. 2014. Citado na página 15.

CAMARA, M. A. A. et al. Internet das coisas e blockchain no sistema único de saúde: a proteção dos dados sensíveis diante da lei geral de proteção de dados. *Cadernos Ibero-Americanos de Direito Sanitário*, v. 10, n. 1, p. 93–112, 2021. Citado na página 24.

CARVALHO, R. M.; ANDRADE, R. M.; OLIVEIRA, K. M. de. Correlations between invisibility and usability in ubicomp and iot applications: partial results. In: *Proceedings of the XXXII Brazilian Symposium on Software Engineering*. [S.l.: s.n.], 2018. p. 214–219. Citado 2 vezes nas páginas 40 e 41.

CIPRIANO, W. F. A segurança da informação com o advento da internet das coisas em ambientes hospitalares: uma abordagem bibliográfica. 2021. Citado na página 23.

COGHLAN, D.; BRYDON-MILLER, M. *The SAGE encyclopedia of action research*. [S.l.]: Sage, 2014. Citado na página 29.

COSTA, G. H. d. C. Engenharia de requisitos no desenvolvimento de software ágil. *Universidade Federal de Pernambuco, Centro de Informática*, 2011. Citado na página 18.

COSTEA-MARCU, I.-C.; MILITARU, G. et al. Patients' attitudes toward the use of iot medical devices: empirical evidence from romania. In: SCIENDO. *Proceedings of the International Conference on Business Excellence*. [S.l.], 2019. v. 13, n. 1, p. 567–577. Citado 2 vezes nas páginas 10 e 26.

FAGUNDES, P. B. et al. Taxonomias, ontologias e tesauros: possibilidades de contribuição para o processo de engenharia de requisitos. *Em Questão*, v. 26, n. 1, p. 237–254, 2020. Citado na página 17.

FILHO, M. F. Internet das coisas. *Unisul Virtual*, 2016. Citado na página 20.

FILHO, W. de P. P. *Engenharia de software*. [S.l.]: LTC, 2003. v. 2. Citado na página 17.

GAMA, G. A. d. Design arquitetural de software aplicado a sistemas de larga escala: revisão de literatura cinzenta. 2022. Citado na página 29.

GIL, A. C. *Métodos e técnicas de pesquisa social*. [S.l.]: 6. ed. Ediitora Atlas SA, 2008. Citado na página 28.

GOMES, A. N.; COUTINHO, E. F. Uma solucao para compartilhamento de dados de saude baseada em blockchain permissionada e internet das coisas para hospitais inteligentes. In: SBC. *Anais do V Workshop em Blockchain: Teoria, Tecnologias e Aplicações*. [S.l.], 2022. p. 1–14. Citado na página 21.

GOUVEIA, L. B. *Gestão da Segurança da Informação*. 2017. Citado na página 23.

GUPTA, B.; AGRAWAL, D. P.; YAMAGUCHI, S. *Handbook of research on modern cryptographic solutions for computer and cyber security*. [S.l.]: IGI global, 2016. Citado na página 17.

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018. Citado na página 23.

HORITA, F. E. A.; NETO, V. V. G.; SANTOS, R. d. Design science research em sistemas de informação e engenharia de software: Conceitos, aplicações e trabalhos futuros. *I Jornada Latino-Americana de Atualização em Informática*, p. 191–210, 2018. Citado na página 16.

HUANG, H. et al. Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Transactions on Industrial Informatics*, IEEE, v. 13, n. 3, p. 1227–1237, 2017. Citado 3 vezes nas páginas 10, 26 e 34.

JACOBSSON, A.; BOLDT, M.; CARLSSON, B. A risk analysis of a smart home automation system. *Future Generation Computer Systems*, Elsevier, v. 56, p. 719–733, 2016. Citado na página 24.

JR, H. E. *Engenharia de software na prática*. [S.l.]: Novatec Editora, 2010. Citado na página 18.

KHAN, J. et al. Medical image encryption into smart healthcare iot system. In: IEEE. *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*. [S.l.], 2019. p. 378–382. Citado na página 34.

KIRUBA, W. M.; VIJAYALAKSHMI, M. Implementation and analysis of data security in a real time iot based healthcare application. In: IEEE. *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. [S.l.], 2018. p. 1460–1465. Citado 3 vezes nas páginas 11, 23 e 34.

KITCHENHAM, B. Procedures for performing systematic reviews. *Keele, UK, Keele University*, v. 33, n. 2004, p. 1–26, 2004. Citado na página 28.

LEE, H. Home iot resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics*, Elsevier, v. 49, p. 101377, 2020. Citado na página 24.

LEMOS, A.; MARQUES, D. Questoes sobre privacidade na internet das coisas. In: *Congresso do INCT. DD*. [S.l.: s.n.], 2018. Citado na página 20.

MACHADO, F. N. R. *Análise e Gestão de Requisitos de Software Onde nascem os sistemas*. [S.l.]: Saraiva Educação SA, 2018. Citado na página 18.

MAGHER, M. How to make a conceptual framework for a thesis. *Retrieved November*, 2016. Citado na página 43.

MANTHA, B.; SOTO, B. G. de; KARRI, R. Cyber security threat modeling in the aec industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, Elsevier, v. 66, p. 102682, 2021. Citado na página 41.

MARTINS, G. de S. et al. Internet das coisas (iot): Monitoramento remota de sinais biomédicos. *Caleidoscópio*, v. 12, n. 1, p. 23–27, 2020. Citado na página 20.

MASSOLA, S. C.; PINTO, G. S. O uso da internet das coisas (iot) a favor da saúde. *Revista Interface Tecnológica*, v. 15, n. 2, p. 124–137, 2018. Citado na página 21.

MAUER, T. C. Registro eletrônico de saúde: Desafios da implantação. Universidade Federal de São Paulo (UNIFESP), 2017. Citado na página 21.

MAVROPOULOS, O. et al. Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks*, Elsevier, v. 92, p. 101743, 2019. Citado na página 25.

NASCIMENTO, R. L.; LEAL, R. M.; FONSECA, I. E. Demonstraçao experimental de vulnerabilidades em dispositivos internet das coisas. In: SBC. *Anais Estendidos do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2022. p. 298–303. Citado na página 27.

NEISSE, R. et al. Dynamic context-aware scalable and trust-based iot security, privacy framework. *Chapter in Internet of Things Applications-From Research and Innovation to Market Deployment, IERC Cluster Book*, 2014. Citado na página 11.

PARK, J. et al. A secure patient information transfer method through delegated authorization. In: IEEE. *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. [S.l.], 2016. p. 56–60. Citado 2 vezes nas páginas 25 e 34.

PESSOA, C. R. M. et al. A internet das coisas: Conceitos aplicações, desafios e tendências. In: *13th International Conference on Information Systems and Technology Management–Contecsi, June*. [S.l.: s.n.], 2016. Citado na página 12.

PINHEIRO, P. P. *Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD*. [S.l.]: Saraiva Educação SA, 2020. Citado na página 24.

PORTELA, C.; VASCONCELOS, A.; OLIVEIRA, S. R. B. Um modelo iterativo para o ensino de engenharia de software baseado em abordagens focadas no aluno. In: *Brazilian Symposium on Computers in Education (Simpósio Brasileiro de Informática na Educação-SBIE)*. [S.l.: s.n.], 2017. v. 28, n. 1, p. 304. Citado na página 15.

PRESSMAN, R.; MAXIM, B. *Engenharia de Software-8ª Edição*. [S.l.]: McGraw Hill Brasil, 2016. Citado 6 vezes nas páginas 16, 17, 41, 45, 46 e 47.

QUSA, H. et al. Secure smart home using open security intelligence systems. In: IEEE. *2019 Sixth HCT Information Technology Trends (ITT)*. [S.l.], 2019. p. 12–17. Citado na página 20.

RAMACHANDRAN, M. Software security requirements management as an emerging cloud computing service. *International Journal of Information Management*, Elsevier, v. 36, n. 4, p. 580–590, 2016. Citado 3 vezes nas páginas 18, 19 e 40.

REHMAN, T. ur; KHAN, M. N. A.; RIAZ, N. Analysis of requirement engineering processes, tools/techniques and methodologies. *International Journal of Information Technology and Computer Science (IJITCS)*, v. 5, n. 3, p. 40, 2013. Citado na página 16.

RGHIOUI, A. et al. Protecting e-healthcare data privacy for internet of things based wireless body area network. *Research Journal of Applied Sciences, Engineering and Technology*, Maxwell Science Publishing, v. 9, n. 10, p. 876–885, 2015. Citado 2 vezes nas páginas 11 e 25.

RIOS, R.; FERNANDEZ-GAGO, C.; LOPEZ, J. Modelling privacy-aware trust negotiations. *Computers & Security*, Elsevier, v. 77, p. 773–789, 2018. Citado na página 40.

RIZK, D.; RIZK, R.; HSU, S. Applied layered-security model to iomt. In: IEEE. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. [S.l.], 2019. p. 227–227. Citado na página 26.

SALEEM, W. Y. B.; ALI, H.; ALSALLOOM, N. A framework for securing ehr management in the era of internet of things. In: IEEE. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. [S.l.], 2020. p. 1–5. Citado na página 25.

SANTOS, B. P. et al. Internet das coisas: da teoriaa prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos*, 2016. Citado na página 46.

SEDELMAIER, Y.; LANDES, D. Software engineering body of skills (swebos). In: IEEE. *2014 IEEE Global Engineering Education Conference (EDUCON)*. [S.l.], 2014. p. 395–401. Citado na página 15.

SEQUEIROS, J. B. et al. Attack and system modeling applied to iot, cloud, and mobile ecosystems: embedding security by design. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 53, n. 2, p. 1–32, 2020. Citado 2 vezes nas páginas 17 e 40.

SOMMERVILLE, I. Engenharia de software-8ª ediçao (2007). *Ed Person Education*, 2011. Citado 3 vezes nas páginas 16, 19 e 46.

TEFFÉ, C. S. de; VIOLA, M. Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. *Civilistica. com*, v. 9, n. 1, p. 1–38, 2020. Citado na página 24.

VEGENDLA, A. et al. A systematic mapping study on requirements engineering in software ecosystems. *Journal of Information Technology Research (JITR)*, IGI Global, v. 11, n. 1, p. 49–69, 2018. Citado na página 16.

VIEIRA, A. M. C. D. A. et al. Aplicação de técnicas de engenharia de software no desenvolvimento de um sistema para análise de matrizes químicas por meio de imagem digital. Universidade Federal do Amazonas, 2015. Citado na página 17.

WILLIAMS, P. A.; MCCAULEY, V. Always connected: The security challenges of the healthcare internet of things. In: IEEE. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. [S.l.], 2016. p. 30–35. Citado 2 vezes nas páginas 11 e 34.

YIĞIT, B. et al. Cost-aware securing of iot systems using attack graphs. *Ad Hoc Networks*, Elsevier, v. 86, p. 23–35, 2019. Citado na página 25.

ZOUKA, H. A. E. An authentication scheme for wireless healthcare monitoring sensor network. In: IEEE. *2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT)*. [S.l.], 2017. p. 68–73. Citado 2 vezes nas páginas 26 e 34.

ZOWGHI, D.; COULIN, C. Requirements elicitation: A survey of techniques, approaches, and tools. In: *Engineering and managing software requirements*. [S.l.]: Springer, 2005. p. 19–46. Citado na página 45.

Apêndices

APÊNDICE A – Projetos com Adm.R

Sistema ULTRALAB

Documento dos Requisitos e Projeto

Versão 1.0

Alex

Breno

Carlos

Douglas

Everton

Fernando

Gabriel

Hugo

Igor

Profa. M.ª Maiane de Castro Santos

Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

Histórico de Alterações

Data	Versão	Descrição	Autor(es)
05/04/22	1.0	Criação e preenchimento do documento	Anderson Costa Breno Barroso Guilherme Santos Manoel Moreira Marcus Melo Naldo Batista Natanael Nascimento Vitor Tiburtino Welison Santos

Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

Sumário

Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

1. Introdução

Este documento apresenta uma visão geral da criação do projeto de software baseado em sistema que rode pesquisas para o Laboratório XYZ.

1.1 Declaração de necessidade e viabilidade

Vendo a necessidade de monitorar as dores dos pacientes ao longo do tratamento e que muito dos pacientes acabavam esquecendo de tomar os remédios nas horas corretas, será desenvolvido um sistema de pesquisa e registro, com foco em obter informações acerca do grau de dor que os participantes sentem após ingerirem uma droga que está sendo testada com efeito anestésico.

1.2 Descrição do ambiente

Sensor de presença: Mini Sensor de Movimento e Presença PIR HC-SR505

Raspberry PI 2 Zero 2 W

Fonte de alimentação: 5V 10000mA / Rede elétrica 5V(USB)

Corrente bateria: 10A

Corrente Raspberry: 0,58A(estresse), 0,28(estática)

Corrente sensor: 0,02A(estático)

Consumo energético:

- Configuração normal(raspberry) e sob estresse:
  10A / ~0,6A = ~16,7h (duração da bateria)

  Obs.: Na prática, perde-se parte da energia. Por isso, deve-se estimar uma redução na duração. No exemplo, estimamos que a bateria dure apenas 90% do tempo calculado, ou seja, 3,6 horas. A estimativa da redução do tempo de duração é feita com base nas curvas de descarga da bateria, fornecidas pelo fabricante. Então: ~15h de autonomia.

- Configuração normal(sem estresse):
  10A / ~0,3A = ~33,3h (duração da bateria)
  Com a estimativa de 90% da bateria, temos: ~30h

Configurações ainda podem ser feitas nos raspberry para que ele consuma menos bateria e atinja uma duração ainda maior.

https://picockpit.com/raspberry-pi/raspberry-pi-zero-2-battery/

2. Descrição Geral do Sistema

Esta seção tem como objetivo descrever de forma geral o sistema, o escopo e as principais funções. A descrição geral do sistema deve abranger os itens a seguir.

Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

2.1 Descrição do problema

O Laboratório XYZ deseja fazer um sistema que permita aos participantes de uma pesquisa, com duração de uma semana, o registro de informações acerca do grau de dor que sentem após ingerirem uma droga que está sendo testada com efeito anestésico, os participantes serão divididos em dois grupos e irão ingerir a droga 2x ao dia, a cada 12 horas durante uma semana, um grupo recebe a droga A (placebo) e o outro recebe a droga B, o sistema deve armazenar dados fornecidos pelos pacientes, droga ingerida (A ou B), grau de dor no início do tratamento e no final (numa escala de 0 a 100 - 0 = nenhuma dor; 100 = dor extrema). O sistema deve calcular a diferença entre os valores obtidos no final e no início do tratamento

para ambas drogas e calcular as médias dessas diferenças. Os participantes recebem login (só podem fazer um único registro referente a dor inicial, e outro referente a dor final, uma vez registrado não pode ser modificado). Informações como média, e visualização de todos registros serão protegidos para quem tiver credenciamento específico. Para lembrarem de ingerirem a droga na hora determinada vão receber um porta medicamentos com sensor que verifique a presença da droga capaz de alertá-los sobre a necessidade de ingeri-la e de registrar grau de dor inicial, ao final do tratamento, outro dispositivo irá alertar sobre registrar o grau de dor final.

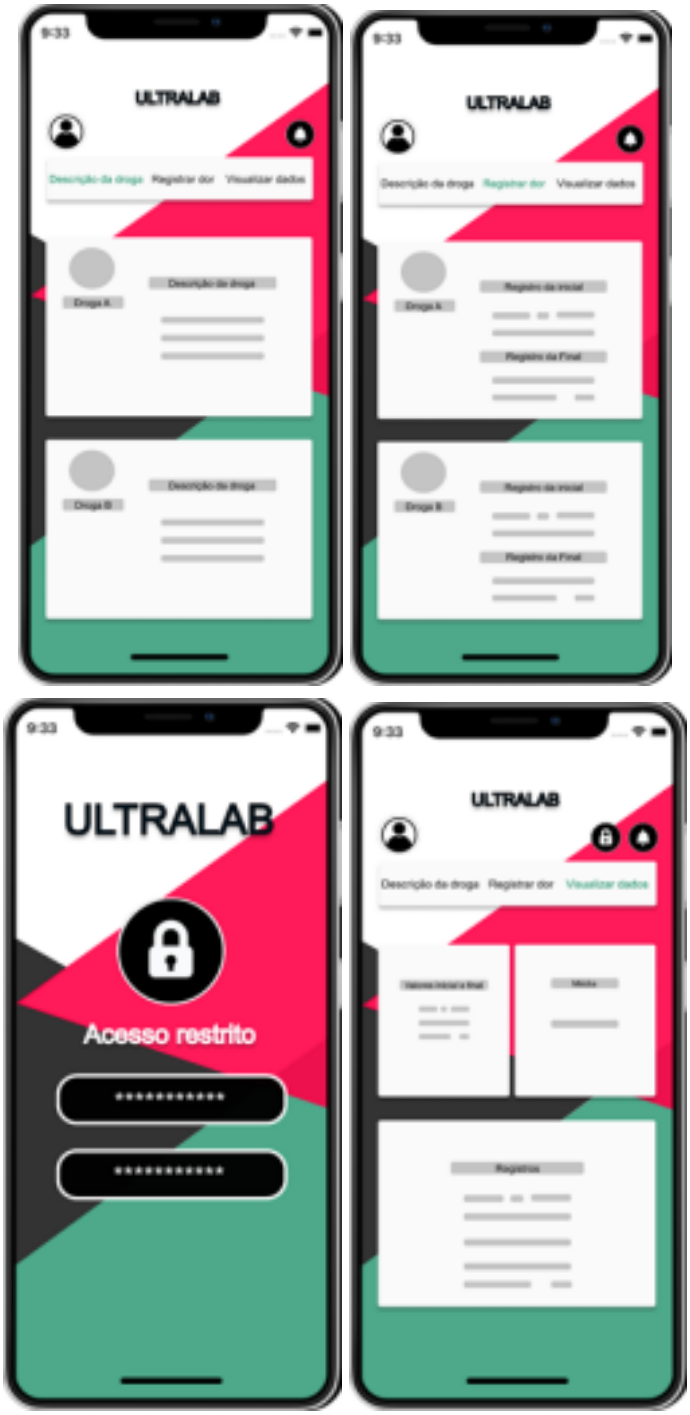
2.2 Principais s*takeholders* e usuários

Papel	**Responsabilidades**	***Stakeholders***
Participante	Indicar o grau da dor inicial e final	Paciente
Sistema	Calcular a diferença entre os valores obtidos	Sistema
Sensor de presença	Verificar a presença da droga	
Sensor de alarme	Avisar o horário de aplicação das drogas	
Pesquisador	Mapear os resultados	Farmacêutico

2.3 Estórias dos usuários

Nº	**Como…**	**Eu gostaria de…**	**pois eu quero…**
1	Participante	participar da pesquisa	contribuir com o estudo
2	Pesquisador	analisar as informações	entender como as drogas se comportamnos pacientes

2.4 Protótipo de Telas



Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

2.5 Documento de Visão

Quadro 1 – Modelo do Documento de Visão.

<table>
<tr><th colspan="2">Modelo do Documento de Visão</th></tr>
<tr><td>Nome do Produto: Sistema ULTRALAB</td><td>Público-alvo: Pesquisadores; Participantes de uma pesquisa;</td></tr>
<tr><td>Condições Gerais de Satisfação (Critérios para aceitação):
Entregar a primeira versão do software com todas as necessidades básicas do cliente supridas, ou seja, apenas com os requisitos em status de essencial.</td><td rowspan="2">Características-chave:

Praticidade e facilidade na coleta de dados relacionados aos níveis de dor de um paciente durante um tratamento;
Agendamento dos horários dos remédios;
Lembrete automático para tomar o remédio;</td></tr>
<tr><td>Premissas, Riscos e Impedimentos:
Premissas: O sistema será mobile; o sistema deverá ser preparado e configurado antes do lançamento;

Riscos: Algum discente trancar a disciplina;

Impedimentos: não identificado até o momento;</td></tr>
<tr><td>Expectativas de Prazo: 6 meses</td><td>Expectativas de Custo: Sem custos.</td></tr>
<tr><td>Elaborado por:
Anderson Costa
Breno Barroso
Guilherme Santos
Manoel Moreira</td><td>Aprovado por (Dono do Produto):
Maiane de Castro Santos</td></tr>
</table>

3. Requisitos do Sistema

3.1 Requisitos Funcionais

Identificação	Descrição	Classificação (Importante, Essencial ou Desejável)	Atores
RF001	O sistema deve registrar qual foi a droga ingerida	Essencial	Sistema
RF002	O sistema deve registrar qual o grau da dor inicial que o participante sente(escala 0-100)	Essencial	Sistema
RF003	O sistema deve registrar qual o grau da dor final que o paciente sente(escala 0-100)	Essencial	Sistema
RF005	O sistema deve permitir cadastrar nome, endereço, contato, rg, cpf e anamnese de cada participante	Essencial	Sistema
RF005	Deverá fornecer um login para o participante inserir informações no sistema	Essencial	Farmacêutico

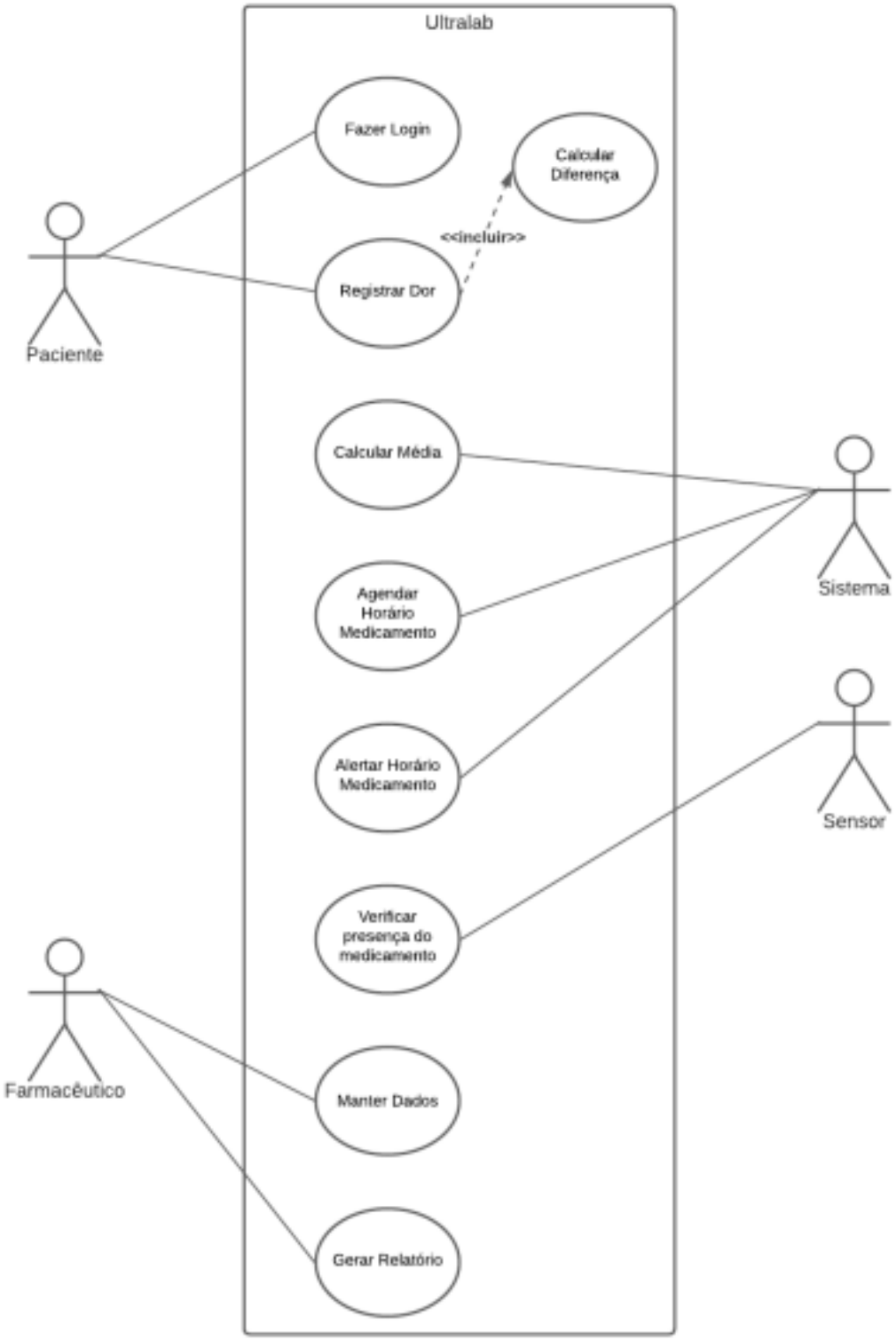
RF006	O sistema deve gerar cálculo de média e diferença para usuários com credenciamento específico	Essencial	Sistema
RF007	O sistema deve exibir todos os usuários somente para usuários com credenciamento específico	Importante	Sistema
RF008	O sistema deve verificar a presença da droga no porta medicamentos com sensor	Importante	Sistema
RF009	O sistema deve alertar ao participante sobre a necessidade de ingerir a droga	Essencial	Sistema
RF010	O sistema deve alertar ao participante de inserir as informações sobre o grau da dor	Essencial	Sistema

3.2 Requisitos Não-Funcionais

Identificação	**Descrição**	**Classificação (Importante, Essencial ou Desejável)**	**Tipo**
RNF001	O sistema deve prover controle de acesso	Essencial	Segurança
RNF002	O usuário deverá inserir somente um único registro de dor no início e outro registro ao final do tratamento	Essencial	Confiabilidade
RNF003	O sistema deve restringir o acesso às informações de todos os registros a uma credencial específica	Essencial	Segurança

RNF004	O sistema deve garantir que os dados dos sensores sejam salvos ao descarregar um dos sensores	Essencial	Desempenho Restrição de Hardware
RNF005	O sensor deverá conter duas baterias para o caso de uma apresentar falha.	Importante	Segurança
RNF006	O sistema deverá impedir o usuário de alterar o grau de dor uma vez que for inserido	Essencial	
RNF007	O tratamento dos dados utilizará padrões exigidos pela Lei Geral de Proteção de Dados	Essencial	Segurança
RNF008	O sistema deve realizar *backup's* diariamente de modo a manter cópias dos dados armazenados para o caso haver falhas do sistema.	Importante	Confiabilidade
RNF009	O sistema deverá apresentar um guia rápido de como utilizar o aplicativo durante a realização da pesquisa	Importante	Usabilidade
RNF010	O sistema deverá utilizar apenas soluções open-source	Importante	Restrição de software

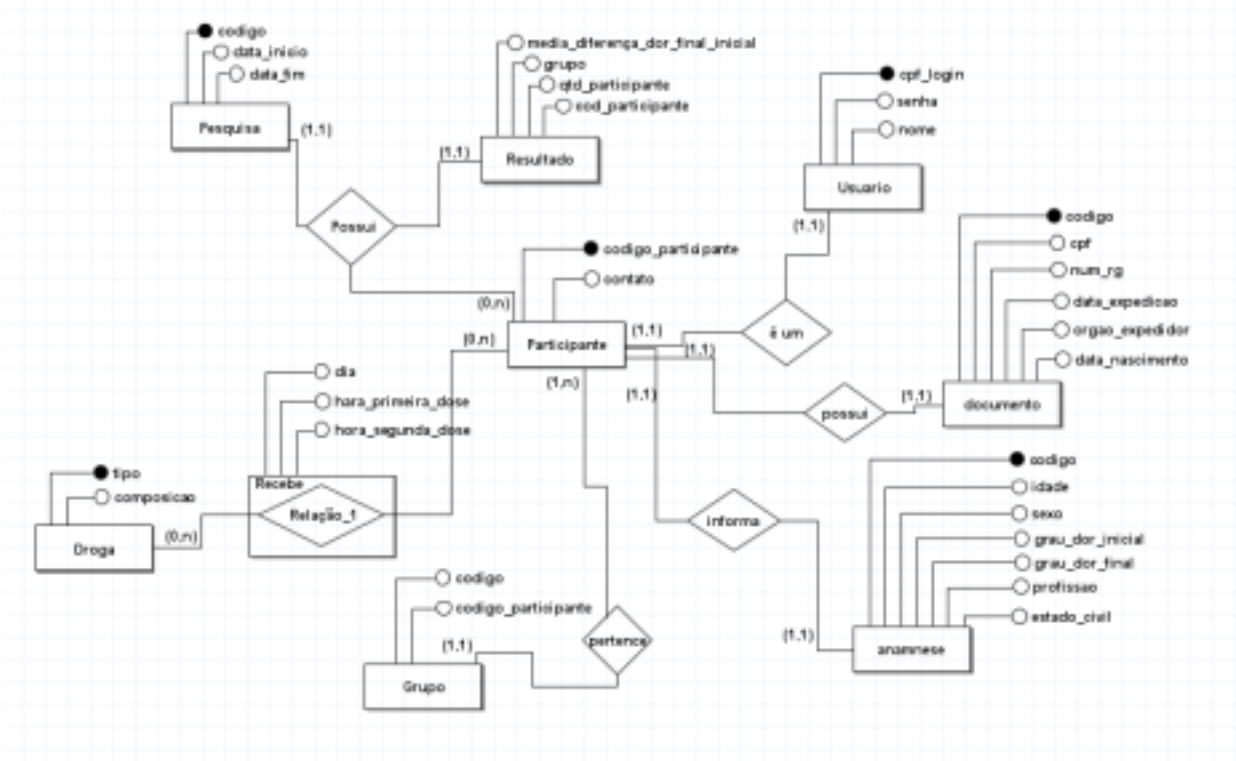
4. Diagrama de *Use Case*



Sistema ULTRALAB	Sistemas de Apoio à Decisão
Documento dos Requisitos, Projeto e Arquitetura	Versão 1.0

5. Representação da arquitetura

5.1 Visão dos Dados - Modelo Conceitual



Referências

https://picockpit.com/raspberry-pi/raspberry-pi-zero-2-battery/

https://www.sta-eletronica.com.br/artigos/baterias-em-geral/informacoes-basicas/como-calcul
ar-quanto-dura-uma-bateria#:~:text=Por%20exemplo%2C%20se%20temos%20uma,0%2C5A%20%3D%204%20horas.&text=Tempo%20de%20dura%C3%A7%C3%A3o%20%3D%202Ah%20%2F%204A%20%3D%200%2C5%20horas

https://www.tomshardware.com/reviews/raspberry-pi-zero-2-w-revi

SOMMERVILLE, Ian. Engenharia de software. 8ª ed. São Paulo: Pearson Addison-Wesley, 2007.

PRESSMAN, Roger S. Engenharia de software. 7ª ed. Porto Alegre: Bookman, 2011

Rede de Hospitais FICTÍCIA

PRONTIOT
Documento de Arquitetura e Projeto

Versão 1.0

[Autor(es)]
Alan
Alisson
Bruno
Caio
Daniel
Davi
Eduarda
Felipe
Gustavo

Rede de Hospitais FICTÍCIA

SAD/2021-

2

Sistema <Nome do Sistema> Engenharia de Software II
Documento dos Requisitos, Arquitetura e Projeto Versão x.x

Histórico de Alterações

Data	Versão	Descrição	Autor(es)
07/04/22	*1.0*	*Elaboração do documento*	*Todos do grupo 1*

Sumário

Sistema PRONTIOT Sistemas de Apoio à Decisão

Documento dos Requisitos, Arquitetura e Projeto Versão 1.0

1. Introdução

A rede de hospitais FICTÍCIA realiza milhares de atendimentos em seus hospitais, mas os dados de seus prontuários, em alguns casos, ainda não são informatizados e quando são estão completamente desorganizados, sem controle e acesso facilitados.

1.1 Finalidade

A rede de FICTÍCIA solicitou o desenvolvimento de um sistema que permita o acesso ao prontuário dos pacientes de forma informatizada. Este sistema deve trazer eficiência e segurança aos atendimentos realizados.

1.2 Escopo

Ideia geral do projeto: Informatizar o acesso aos prontuários dos pacientes e torná-los disponíveis com facilidade para médicos, enfermeiros e emergencistas tanto em computadores quanto em dispositivos móveis.

Ponto central: Prontuários acessíveis 24h e coleta automática dos dados vitais do paciente(sensores de frequência cardíaca, temperatura corporal, índice de glicose, saturação de oxigênio, etc).

1.3 Definições, Acrônimos e Abreviações

1.3.1 Definições

Abordagem de modelagem a ser utilizada: Orientada a objeto

Forma de levantamento de requisitos: Entrevistas e validações com stakeholders

1.3.2 Acrônimos e Abreviações

A correta interpretação deste documento exige o conhecimento de algumas convenções e termos específicos e abreviações, que são descritos a seguir (em ordem alfabética). API – application programming interface

Broker – Servidor que recebe e envia dados para os sensores e dispositivos

Java – linguagem computacional

MQTT – Message Queuing Telemetry Transport – Protocolo de comunicação para sensores e pequenos dispositivos

SGBD – Sistema de Gerenciamento de Banco de Dados

SQL – linguagem para bancos de dados

Stakeholders – partes interessadas

IOT – Internet of things (Internet das coisas)

OWASP – Open Web Application Security Project (Projeto Aberto de Segurança em Aplicações Web)

1.4 Referências

PRESSMAN, R. S. MAXIM, B. R. Engenharia de Software. 8ª Ed. Porto Alegre. AMGH Editora, 2016.

SOMMERVILLE, I. Engenharia de Software. Tradução de Luiz Cláudio Queiroz. 10ª Ed. São Paulo. Pearson Education do Brasil, 2018.

PROJECTS. OWASP, 2022. Disponível em: <https://owasp.org/projects/>. Acesso em: 02 de abr. de 2022.

MQTT: The Standard for IoT Messaging. MQTT, 2022. Disponível em: <https://mqtt.org/>. Acesso em: 04 de abr. de 2022.

PostgreSQL: The World's Most Advanced Open Source Relational Database. POSTGRESS.ORG, 2022. Disponível em: <hhttps://www.postgresql.org/>. Acesso em: 03 de abr. de 2022.

MANCINI, Mônica Internet das Coisas: História, Conceitos, Aplicações e Desafios. Fevereiro/ 2017. DIsponível em: <https://www.researchgate.net/publication/326065859_Internet_das_Coisas_Historia_Conceitos_Aplicacoes_e_Desafios>. Acesso em: 02 de abr. de 2022.

1.5 Visão Geral

Serão apresentados nos próximos tópicos os elementos da arquitetura deste software: A Representação Arquitetural que descreve qual é a arquitetura de software só sistema e sua representação, Metas e Restrições da Arquitetura que descreve os requisitos e objetivos do software que influenciam a arquitetura, Visão de Casos de Uso que lista os casos de uso principais do software assim como sua representação, Visão Lógica que descreve as partes significativas do ponto de vista da arquitetura do modelo de design, como sua divisão em subsistemas e pacotes, Visão de Processos que descreve a decomposição do sistema em processos leves e processos pesados, Visão de Implantação que descreve uma ou mais configurações da rede física na qual o software é implantado e executado, Visão de Implementação que descreve a estrutura geral do modelo de implementação, a divisão do software em camadas e os subsistemas no modelo de implementação e todos os componentes significativos do ponto de vista da arquitetura, Visão de Dados que descreve a perspectiva de armazenamento de dados persistentes do sistema, Tamanho e Desempenho que descreve a perspectiva de armazenamento de dados persistentes do sistema e Qualidade que é uma descrição de como a arquitetura do software contribui para todos os recursos (exceto a funcionalidade) do sistema.

2. Representação Arquitetural

O sistema é composto por diversos módulos, onde cada um será responsável por uma funcionalidade específica dentro do sistema. O módulo principal consiste do agregador de funcionalidades que somente permite o acesso após a realização de login por parte do usuário, sendo que essa autenticação vai liberar para o usuário, somente as funcionalidades que estão disponíveis para o nível de acesso do mesmo. Entretanto, existem funcionalidades cujo funcionamento não dependerão diretamente do usuário, uma vez que o sistema estará integrado com equipamentos/sensores que transmitirão dados vitais sobre o paciente, vinculando os dados obtidos pelos sensores ao prontuário do paciente. Os usuários não terão acesso a editar nem a excluir as informações de saúde previamente

inseridas no sistema. O sistema pode ser utilizado fora do ambiente hospitalar (numa ambulância ou em visita domiciliar, por exemplo), com o uso de sensores portáteis com essa finalidade, e de dispositivos móveis para acesso ao prontuário do paciente.

Será definida hierarquicamente, a estrutura do sistema, onde teremos uma parte do sistema que será composta por APIs de acesso aos dados dos sensores (que utilizarão o protocolo MQTT para comunicação com o servidor de dados de IoT); APIs de acesso a sistemas terceiros, como o ConectSUS, para obtenção de dados de saúde como vacinas, medicamentos de uso contínuo, etc; e APIs de inserção e visualização de dados dos prontuários dos pacientes. nenhuma parte do sistema terá acesso direto aos dados, tendo em vista a garantia da segurança dos dados de saúde das pessoas atendidas. Para que este ponto seja atingido, durante as fases de desenvolvimento do sistema, serão observados os princípios definidos pela OWASP como sendo as melhores práticas no desenvolvimento seguro de software.

3. Metas e Restrições da Arquitetura

3.1 Requisitos Funcionais

Identificação	**Descrição**	**Classificação (Importante, Essencial ou Desejável)** **Gerência ou Área ou Setor e Atores envolvidos**
RF01	O sistema deve possuir diferentes níveis de controle de acesso aos dados do prontuário.	Essencial
RF02	O sistema deve possuir um monitor de eventos e atividades para garantir integridade dos dados, considerando soluções de anonimização dos dados do usuário.	Importante
RF03	O sistema deve se integrar de forma segura ao ConectSus para obtenção de dados de vacinação do paciente	Desejável
RF04	O sistema deve possuir uma tela de login, pedindo email e senha, para realizar a autenticação no sistema.	Essencial Todos

RF05	O sistema deve possuir uma tela de detalhes do prontuário, que deve: - Exibir os dados captados pelos sensores em tempo real: Temperatura corporal, frequência cardíaca e nível de glicose.	Essencial	médico, enfermeiro, emergencista

	- Exibir um histórico dos dados captados pelos sensores, permitindo filtragem por tipo de dado. - Exibir dados anteriormente exibidos na listagem: Nome, CPF, idade, urgência de atendimento, categoria do problema e sexo. - Exibir o motivo da consulta, presença de alergias, histórico de vacinação e medicamentos, procedimentos realizados (cirurgias, por exemplo), necessidade de insulina, solicitações de exames e resultados. - Essa tela deve ser acessada a partir da listagem.		
RF06	O sistema deve permitir o cadastro de pacientes	Essencial	enfermeiro, emergencista
RF07	"O sistema deve possuir uma listagem dos prontuários dos pacientes: - Devem ser exibidos os dados: Nome, CPF, idade, urgência de atendimento, categoria do problema do paciente, sexo e data de criação. - Filtragem e ordenação por Nome, CPF, idade, urgência de atendimento, categoria do problema do paciente, sexo e data de criação.	Essencial	médico, enfermeiro, emergencista

	- A ordenação padrão deve ser por urgência de atendimento."	
RF08	O sistema deve possuir uma tela de cadastro de prontuário, que deve: - Permitir o cadastro dos dados do paciente, os mesmos exibidos na tela de detalhes, com exceção dos dados de monitoramento em tempo real. - Essa tela deve ser acessada a partir da listagem. - Ao digitar o CPF, deve ser consultado na base de dados se algum cadastro com esse CPF já existe. - Se existir, os dados devem ser preenchidos automaticamente. - Senão, ao final do cadastro desse prontuário, o usuário deverá ser cadastrado com os dados.	Essencial médico, enfermeiro, emergencista

	- Nenhum atendimento pode ser excluído, ficando os dados sempre presentes no histórico do paciente.	
RF09	O sistema permitirá a classificação do Paciente de acordo com seu grau de risco à saúde, e este grau de risco será definido pelo usuário	Essencial médico, enfermeiro, emergencista
RF10	O Sistema deve permitir a alteração da classificação do Paciente, alterando a cor do Paciente a medida que o mesmo melhore ou piore.	Importante médico, enfermeiro, emergencista
RF11	O sistema deve guardar dados da sessão	Essencial Todos

3.2 Requisitos Não Funcionais

Identificação	Descrição	Classificação (Importante, Essencial ou Desejável)	Gerência ou Área ou Setor e Atores envolvidos
RNF01	A consulta de dados dos pacientes e prontuários poderá ser mobile ou web	Essencial	
RNF02	O cadastro e edição de dados pessoais de usuários e pacientes será exclusivamente web	Essencial	
RNF03	O sistema receberá dados de sensores sem a necessidade de inserir os dados manualmente, serão capturados pelos sensores e enviados em tempo real ao sistema (temperatura corporal, de monitoramento cardíaco, índice glicêmico, saturação de oxigênio, etc)	Essencial	
RNF04 RNF05	Os graus de riscos devem ser classificados por cor (A cor vermelha indica atendimento imediato; os casos urgentes recebem a cor amarela ,cores verde e azul representam casos de menor gravidade) Os dados deverão estar em servidores redundantes, visto que, são dados vitais de pacientes e seus históricos serão mantidos permanentemente.	Essencial Essencial	

RNF06	Uma API ficará responsável por coletar os dados no Broker MQTT e os armazenará na unidade de	Essencial	

	persistência, além de disponibilizá-los para consulta via WEB e Mobile.	
RNF07	O sistema deverá estar em servidores de alta disponibilidade.	Essencial
RNF08	O desenvolvimento do sistema deve adotar controles preventivos de segurança e autenticidade seguindo diretrizes da OWASP	Importante
RNF09	O sistema ficará disponível 24 h por dia	Essencial
RNF10	O protocolo de comunicação IOT utilizado para comunicação entre os sensores e o software é o MQTT	Importante
RNF11	Os dados coletados pelos sensores serão gerenciados por um Broker MQTT que será implementado em um servidor AWS	Importante
RNF12	O sistema e os dados serão armazenados em 3 servidores AWS clusterizados e gerenciados a partir de um Balanceador de Cargas	Essencial

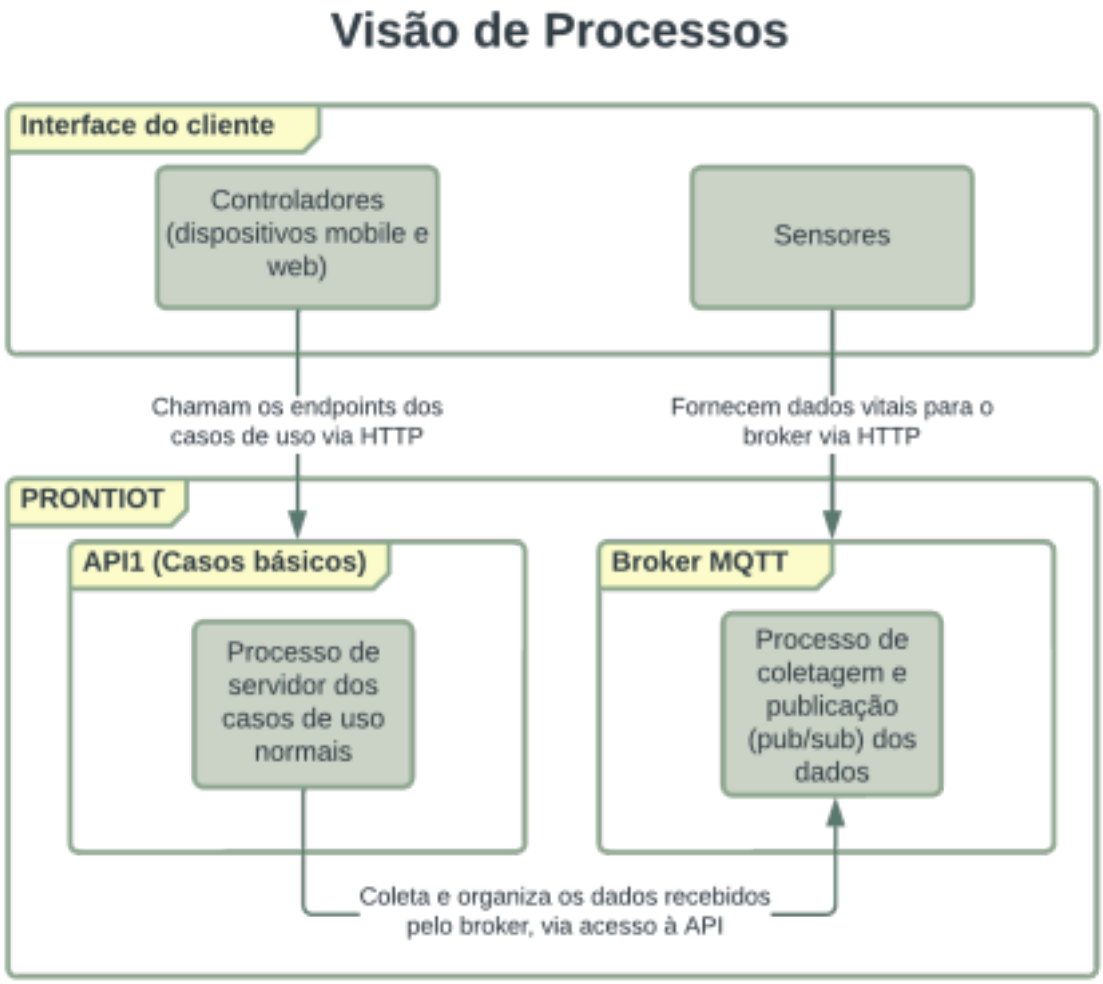
4. Visão de Casos de Uso

Na rede de hospital FICTÍCIA há a necessidade de ter um sistema informatizado para ter acesso ao prontuário dos cidadãos, na realização do atendimento são captados os dados do paciente verificando se o mesmo já (possui) (se disponibiliza de) um cadastro, realizado esse primeiro contato prévio de cadastro do prontuário, o paciente passará por uma triagem para classificar o grau de risco do seu atendimento sendo elas: Vermelha (Risco Alto), Amarela (Risco Intermediário) e Azul e Verde (Risco Baixo). Posteriormente no atendimento já com os profissionais de saúde onde será analisado o histórico do paciente, o sistema também permitirá a integração de dispositivos com médicos, enfermeiros e emergencistas, ocorrendo troca de informações em relação ao paciente. Gerando uma maior eficiência para os profissionais resolverem problemas, caso o paciente que esteja na rede hospitalar e baixe o nível de glicose para 50 mg/dl, o sistema que estará monitorando através de sensor corporal portátil que mede, em intervalos regulares e de forma automática. O sistema também contará com o monitoramento da frequência cardíaca do paciente, no qual pode ser realizada por duas soluções: um relógio esportivo com um monitor de frequência cardíaca baseada no pulso ou uma braçadeira com sensor óptico de frequência cardíaca, onde ambos utiliza luzes de LED e um detector para medir as mudanças dos vasos sanguíneos e transformando em medidas.

5. Visão Lógica

A arquitetura será dividida em 5 (quatro) camadas: uma responsável pelo gestão e armazenamento dos dados, uma responsável pela interface com o usuário contemplando os diferentes tipos de plataforma, seus protocolos, uma camada responsável pela comunicação entre os dispositivos IOT, uma camada responsável por implementar as regras de negócio e a última responsável pela integração entre todas as outras camadas.

6. Visão de Processos



7. Visão de Implantação

A API será implantada na Amazon Web Services (AWS) mais precisamente numa instância do tipo t3.large que será utilizada como balanceador de carga, como os dados do sistema devem ser redundantes para assim evitar que o sistema fique indisponível, serão utilizadas três instâncias r6gd.metal, cada uma com 64 núcleos de processamento AWS Graviton2, 512GB de memória RAM e dois SSDs de 1.9TB cada e largura de banda de rede de 25Gbps. Cada instância r6gd.metal terá um banco de dados PostgreSQL para armazenamento e serão responsáveis por duplicar os dados entre si para que haja uniformidade. Vale lembrar que cada máquina citada anteriormente deve estar geograficamente distribuída para minimizar os riscos de indisponibilidade do sistema. O valor total mensal aproximado para manter essa infraestrutura é de 7.500,00 dólares americanos.

Serão necessários sensores utilizados no processo de triagem de pacientes, como por exemplo: sensor de saturação, sensor de frequência cardíaca, temperatura, etc. Estes sensores utilizarão o protocolo HTTP para comunicação com um Broker MQTT para enviar os dados do paciente e a API consumirá os dados recebidos pelo broker para assim registrá-los em banco de dados.

Abaixo segue uma visão simplificada da implantação e comunicação entre componentes do projeto.

8. Visão de Implementação

8.1 Visão Geral

O sistema será dividido entre backend e frontend. O backend trata-se de uma aplicação que rodará em um servidor web e que realizará as operações e persistência de dados do sistema. O backend disponibilizará seus serviços via HTTP a partir de endpoints específicos. O frontend trata-se de uma parte do sistema que rodará no dispositivo do usuário, provendo uma interface para que o mesmo possa visualizar os dados e realizar operações, que serão feitas a partir de requisições HTTP para a API. No caso do sistema atual, haverá dois frontends, um para dispositivos web e outro para mobile, de forma que ambos consomem a mesma API.

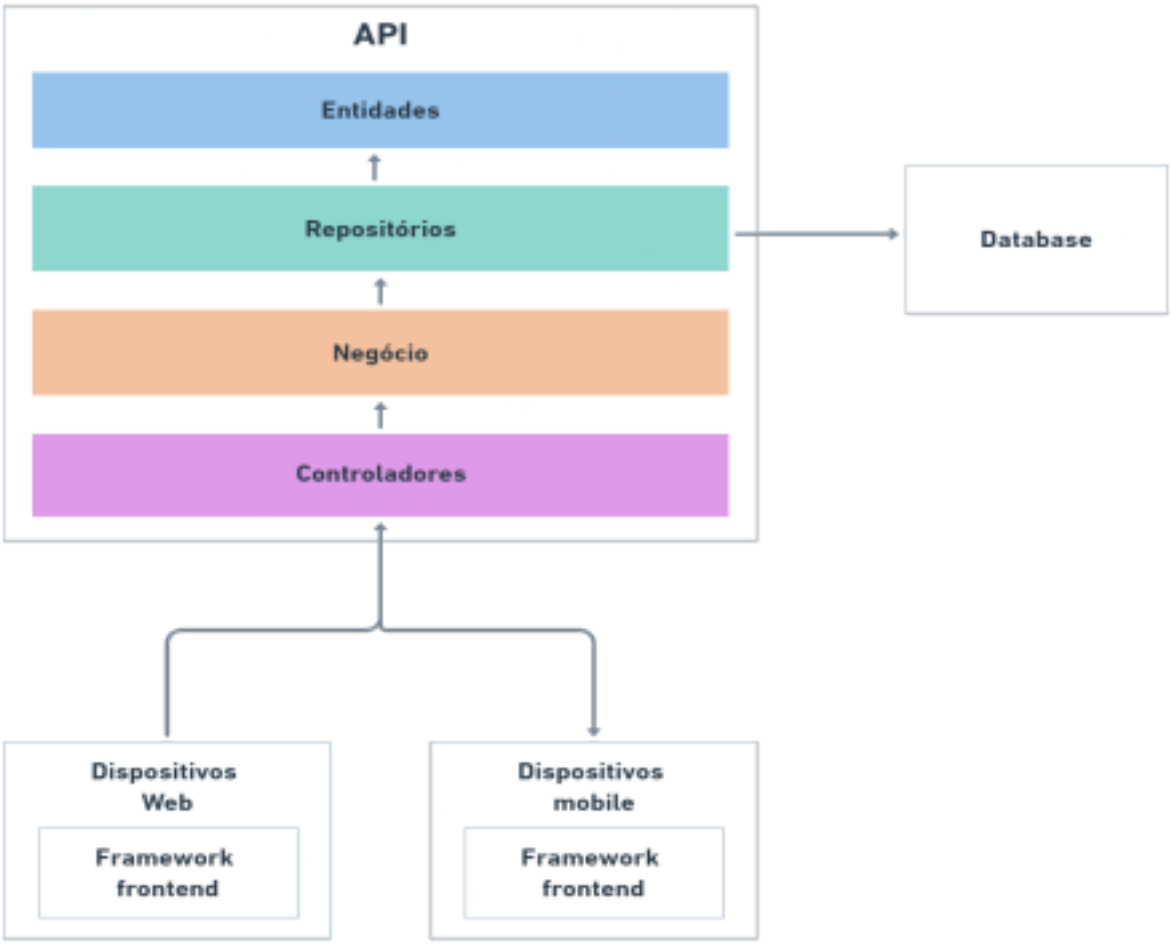
A API será construída com uma arquitetura em camadas: Camada de Modelos, Camada de Repositórios (Acesso e persistência de dados), Camada de Negócio e Camada de Controladores. As camadas obedecem uma hierarquia, de forma que elas só conhecem camadas diretamente acima ou diretamente abaixo da posição delas na mesma.

8.2 Camadas

- Camada de Modelos: Nessa camada estão contidas as modelagens das entidades do negócio em questão, por exemplo: Paciente, Usuário, Prontuário, Atendimento, etc.
- Camada de Repositórios: Nessa camada estão contidas entidades responsáveis pelo acesso a camada de dados, realizando diversas operações como, por exemplo, leitura e persistência de dados.
- Camada de Negócio: Nessa camada estão contidas as entidades responsáveis por modelar a lógica do negócio, por exemplo: Login, geração de token, cadastro de pacientes, etc.
- Camada de Controladores: Nessa camada estão contidas as entidades responsáveis pela comunicação entre os dispositivos externos e a camada de negócio, por exemplo: Navegadores, dispositivos móveis via HTTP, comunicação em tempo real com WebSockets.

8.3 Diagrama de componentes

Abaixo segue um diagrama da visão de implementação do sistema:



9. Visão de Dados

Nossa aplicação guarda alguns grupos de informações persistentes relacionadas ao paciente, ao usuário e de procedimentos realizados sobre o paciente.

- Paciente:

  ◆◆ A respeito do paciente nós guardamos os principais dados cadastrais e algumas necessidades, como se ele é alérgico ou precisa de insulina e o campo observação para dados extras como por exemplo lista as alergias ● Usuário

  ◆◆ Para o usuário nós guardamos os principais dados cadastrais, o tipo de usuário (Médicos, enfermeiros e emergencista) e uma senha para a realização de login com cpf.

- Exames

◆◆ Com os exames nós guardamos apenas o nome, e o paciente no qual foi realizado. Assim é possível através do paciente recuperar todos os exames e resultados.

● Atendimento

�� O mesmo acontece para o atendimento, onde podemos resgatar as informações dos atendimentos realizados ao paciente e o responsável pelo atendimento.

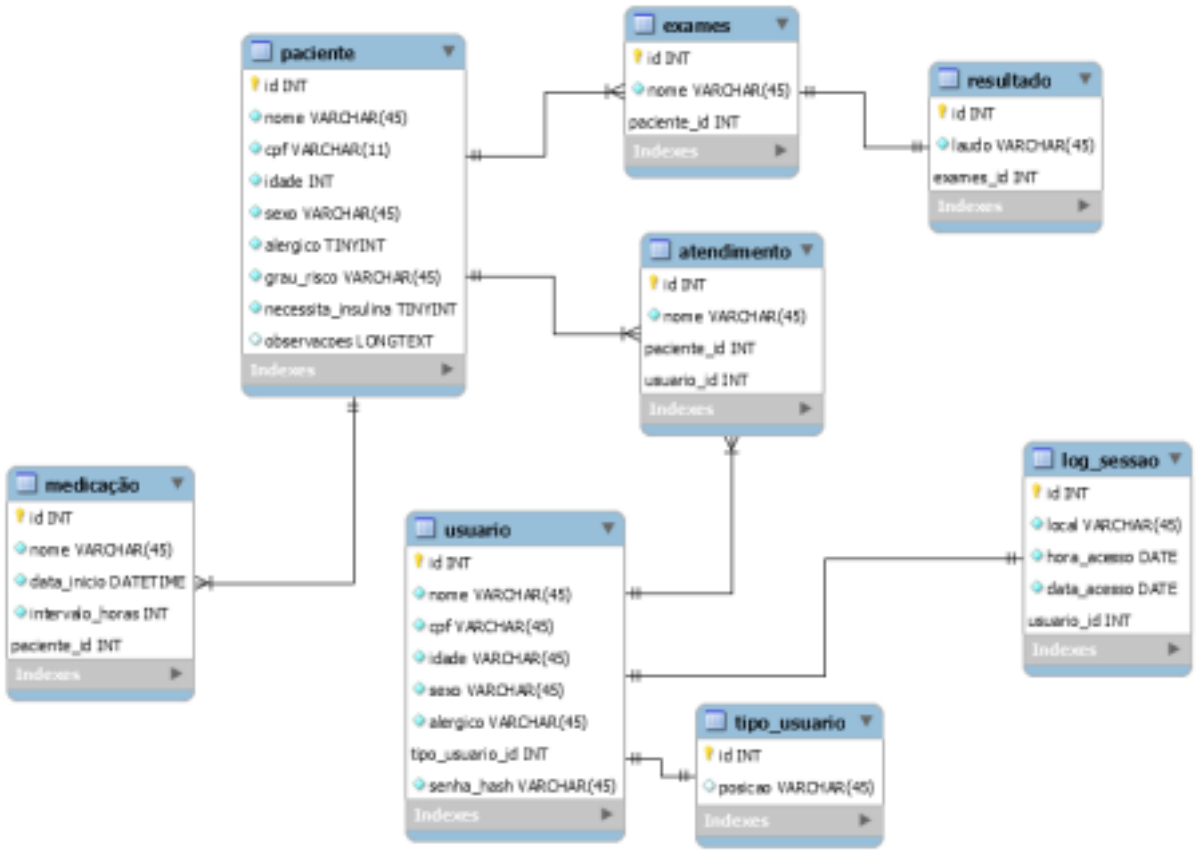
● Medicação

�� Com a medicação é possível manter um registro de todos os medicamentos cadastrados para o paciente, como a data de início do medicamento e o intervalo em horas de determinada medicação.

● Log

�� Por fim, mantemos também registrado o log de usuários, quem acessou, onde e em que local

Abaixo segue um diagrama da visão de dados persistente do sistema



Sistema PRONTIOT Sistemas de Apoio à Decisão
Documento dos Requisitos, Arquitetura e Projeto Versão 1.0

10. Tamanho e Desempenho

Diante das necessidades de um sistema de alta disponibilidade, alto desempenho e alta confiabilidade, não é uma tarefa fácil dimensionar com precisão as reais exigências de infraestrutura. Sendo assim, a solução arquitetural precisa prover um sistema com capacidade de escalabilidade, com baixo acoplamento entre as partes e alta capacidade de replicação.

Pensando em termos de escalabilidade, o sistema foi projetado a partir de infraestrutura em nuvem (Amazon AWS), que traz a flexibilidade de expandir ou diminuir a quantidade de recursos de hardware disponíveis em um modelo de pagamento por uso (pay-as-you-go). Dentro desse modelo há possibilidade tanto de escalabilidade vertical, o foco inicial, com máquinas de alto desempenho, tanto de escalabilidade horizontal, replicando instâncias da aplicação, através de contêineres e da distribuição de carga (load balancer).

A partir dos requisitos de alta confiabilidade e disponibilidade, uma arquitetura voltada para a nuvem possibilita ter mecanismos de backup e recuperação para casos de falha na infraestrutura, sendo possível até mesmo configurar instâncias de componentes reservas em diferentes data-centers, para múltiplas regiões, de forma automatizada. Dentro dos componentes internos do sistema, é possível ao longo do desenvolvimento adotar estratégias de resiliência, como Circuit-Breaker.

Todos os conceitos e estratégias mencionadas, dependem do fator monitoramento, só é possível dimensionar custos, obter flexibilidade no aumento ou na diminuição de desempenho ou armazenamento sob demanda, a partir da observação da demanda e de como os recursos estão sendo distribuídos. De forma macro, a AWS fornece o serviço CloudWatch para monitoramento da infraestrutura, ideal para as necessidades do projeto. De forma micro, diversas ações como benchmark, cache, testes de carga e logging permitem dimensionar as necessidades de dentro da aplicação.

11. Qualidade

Considerando toda a conjectura do projeto, desde sua finalidade, seus stakeholders e escopo definidos, é de suma importância alinhar adequadamente, a arquitetura de software com os requisitos mínimos para entregar um projeto confiável, seguro, estável, em suas plataformas, garantindo usabilidade para os usuários.

11.1 Portabilidade

Pela necessidade do sistema estar atuante 24h por dia, é necessário que ele esteja acessível em qualquer lugar. Diante disso, o sistema possui a capacidade de interação multiplataforma, utilizando versões mobile e WEB. Isso se deve graças a sua arquitetura de Camadas, que faz a comunicação entre os dispositivos, utilizando WebSockets e protocolos HTTP.

11.2 Confiabilidade

Pelo fato da característica de API ter a separação cliente / servidor, há muito mais facilidade durante o desenvolvimento da aplicação. Como cada requisição é feita de maneira única e independente, é possível mudar uma requisição para outro DNS, sem que isso interfira na aplicação.

Em outras palavras, a API permite que a aplicação acesse banco de dados de diferentes

servidores, o que muitas vezes é importante para o desenvolvimento em grandes aplicações. Portanto, sua utilização garante mais visibilidade e confiabilidade ao utilizar esses recursos.

11.3 Extensibilidade

Inicialmente, não há previsão para extensões do projeto. Contudo, devido sua Arquitetura ser baseada em API's e Camadas realizados em softwares de alta disponibilidade é possível, futuramente, expandir ou alterar sua comunicação com outras ferramentas. Como clientes e servidores são separados, um produto pode ser dimensionado por uma equipe de desenvolvedores sem muitos problemas.

Além disso, é mais fácil integrar a API a outros sites sem refatorar a infraestrutura do mesmo. Isso permite que os desenvolvedores trabalhem mais rápido em vez de perder tempo retrabalhando um site do zero. Como alternativa, eles podem simplesmente adicionar funcionalidade extra.

11.4 Segurança e Privacidade

O projeto visa seguir os preceitos da OWASP, utilizando técnicas de segurança, parametrizando consultas, validando todas as entradas, implementando controles de identidade, autenticação e acesso, protegendo os dados, usufruindo da arquitetura de Camadas da API, que usam HTTP e suportam criptografia Transport Layer Security (TLS) . TLS é um padrão que mantém a privacidade de uma conexão com a Internet e verifica se os dados enviados entre dois sistemas (um servidor e um servidor ou um servidor e um cliente) estão criptografados e não modificados. Isso significa que se um agente não autorizado que tenta expor as informações do software não pode ler seus dados nem modificá-los.

Sistema MPM

Documento de Requisitos, Arquitetura e Projeto

Versão 1.0

Documento de Especificação de Requisitos

Equipe 3

Antonio, Arthur, Marcos, Luiza, Pedro, Raiane, Ricardo

Profº Gilton Jose Ferreira da Silva

Profª Maiane de Castro Santos

Sistemas de Apoio à Decisão/2021-2

Histórico de Alterações

Data	Versão	Descrição	Autor(es)
05/04/2022	*1.0*	*Criação do documento*	*Equipe 3*
07/04/2022	*1.0*	*Definição de objetivos*	*Equipe 3*
12/04/2022	*1.0*	*Inclusão de Requisitos*	*Equipe 3*
13/04/2022	*1.0*	*Definição de Arquitetura*	*Equipe 3*
19/04/2022	*1.0*	*Ajustes Finais*	*Equipe 3*

Sumário

1. Introdução

O Laboratório XYZ deseja monitorar a participação das pessoas e o grau de dor no estudo da eficiência de uma medicação com efeito analgésico que está sendo testada.

1.1 Objetivo do projeto

Um sistema que permita aos participantes da pesquisa o registro de informações acerca do grau de dor que sentem após ingerirem uma droga que está sendo testada, o sistema teria capacidade de armazenar dados fornecidos pelos pacientes como droga ingerida (A ou B), grau de dor no início do tratamento e no final, além de alerta para lembrar o paciente de ingerir o medicamento no horário apropriado.

A mensuração da dor é um desafio, já que a dor é subjetiva e é influenciada por diversos fatores, desde culturais, emocionais e ambientais. Existem diversas abordagens multidimensionais na avaliação da dor, as abordagens podem incluir a duração da dor, a intensidade e localização por exemplo. Decidimos utilizar um Protocolo de Gerenciamento da Dor Orientado por Intensidade do tipo EVN (escala visual numérica) que varia de zero (ausência de dor) 1 a 3 (dor leve), 4 a 7 (dor moderada), 8 a 10 (dor intensa) onde o participante do experimento visualiza uma escala e localiza espacialmente a intensidade da dor que sente no momento. O sistema então permite o acompanhamento do aumento ou diminuição do grau da dor pela média, mas também classifica por intensidade (leve,moderada e intensa).

1.2 Glossário, convenções, termos e abreviações

EVN - Escala Visual Numérica

2. Descrição Geral do Sistema

Até estar disponível para os pacientes, todo medicamento passa por um longo e custoso processo de pesquisa e desenvolvimento. Das primeiras atividades relacionadas à descoberta de um princípio ativo até o início da comercialização, a produção de um novo medicamento compreende diferentes etapas.

2.1 Descrição do problema

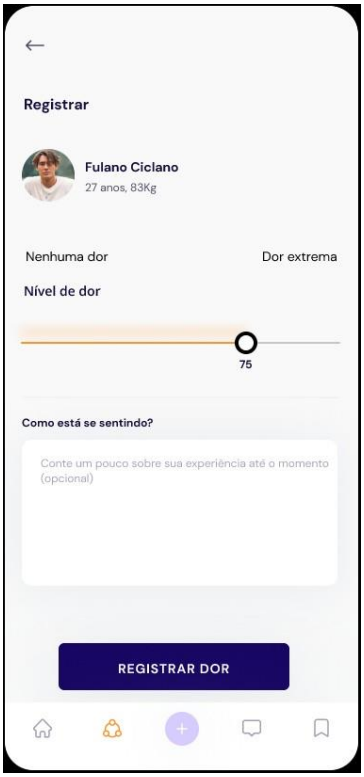
O potencial medicamento deve seguir, então, para os testes pré-clínicos laboratoriais (in vitro) e em animais (in vivo), com objetivo de determinar se ele é seguro para ser testado em humanos. O dossiê de pesquisa é apresentado aos órgãos regulatórios e aos comitês de ética em pesquisa, que aprovam se o novo medicamento pode ser testado em pessoas. E finalmente o medicamento é testado em grupos de pessoas para definição de:

- Qual a maior dose possível e tolerada.
- Qual a menor dose que surte efeito.
- Qual será a relação entre frequência e dosagem.
- Qual a efetividade da droga em relação a outros tratamentos, incluindo o placebo.
- Quais efeitos adversos e contraindicações.

2.2 Principais s*takeholders* e usuários

Papel	Responsabilidades	*Nome*
Pesquisadores	Conferir Métricas Adquiridas	Administrador
Participantes	Usar o Sistema para Registro de Métricas	Usuário

2.3 Protótipos de Telas e Relatórios



3. Requisitos do Sistema

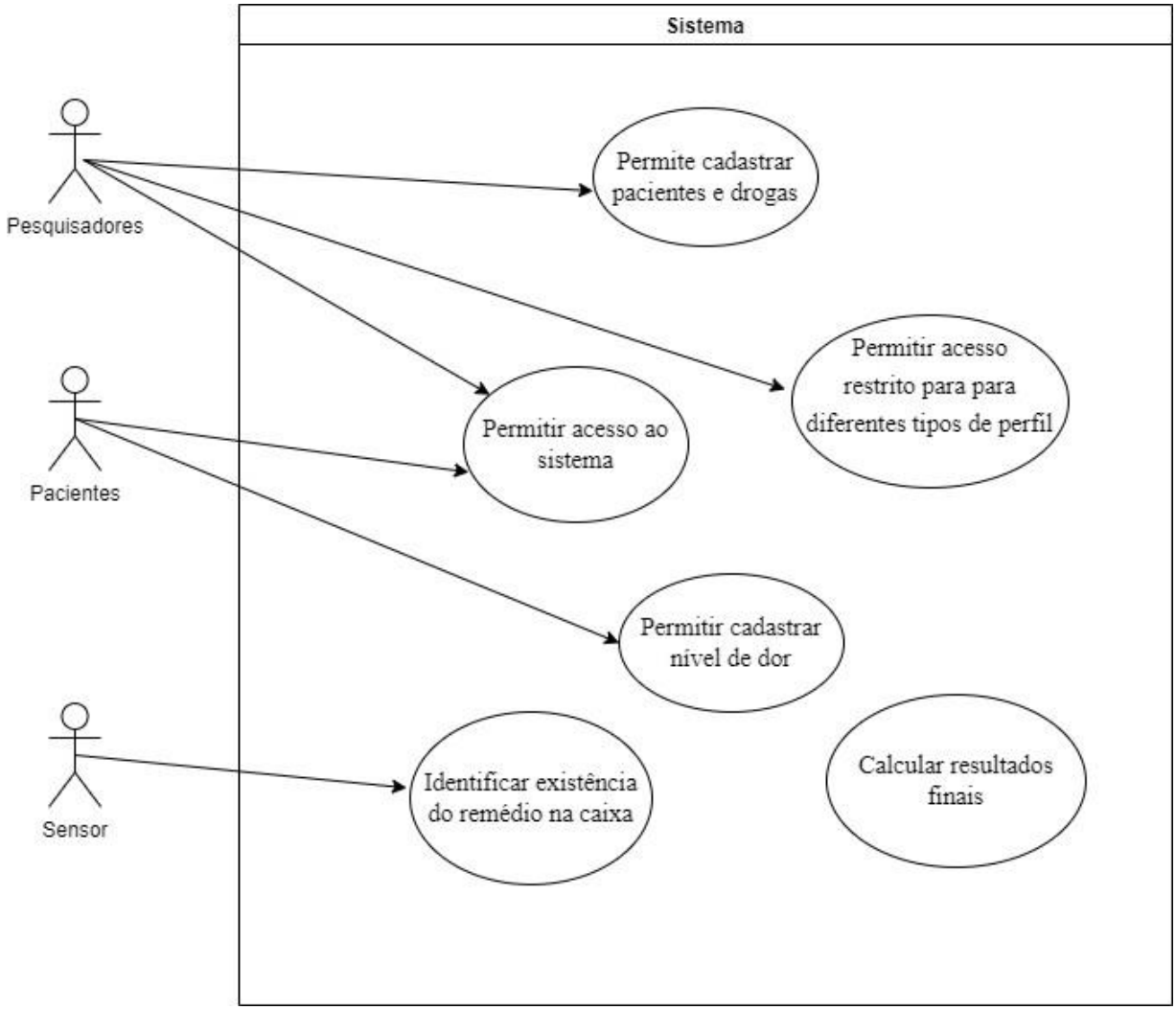
3.1 Requisitos Funcionais

Identificação	Descrição	Classificação (Importante, Essencial ou Desejável)	Gerência ou Área ou Setor e Atores envolvidos
RF01	Permitir acesso ao sistema	Essencial	Participantes, Pesquisadores
RF02	Permitir cadastrar nível de dor	Essencial	Participantes
RF03	Permitir acesso restrito para para diferentes tipos de perfil	Essencial	Pesquisadores
RF04	Permite cadastrar pacientes e drogas	Essencial	Pesquisadores
RF05	Identificar existência do remédio na caixa	Essencial	Sensor
RF06	Um relatório dos resultados deve ser fornecido após o final do experimento	Essencial	Sistema

3.2 Requisitos Não-Funcionais

Identificação	Descrição	Classificação (Importante, Essencial ou Desejável)	Tipo
RNF001	O usuário deve estar apto a utilizar todo o sistema após 1 hora de treinamento	Importante	Usabilidade
RNF002	O aplicativo deve ser compatível com Android e IOS	Importante	Portabilidade
RNF003	O sistema deve estar disponível 99% do tempo	Essencial	Confiabilidade
RNF004	O sistema deve se comunicar por bluetooth	Essencial	Interoperabilidade
RNF005	O app do sistema deve ser desenvolvido com as tecnologia Dart e Flutter	Desejável	Implementação
RNF006	O sistema não apresentará aos usuários quaisquer dados de cunho privativo	Essencial	Ético
RNF007	O sistema deve gerar relatórios no formato xlsx (excel)	Desejável	Padrão

4. Diagrama de *Use Case*



5. Representação da Arquitetura

Esta seção descreve a arquitetura adotada para desenvolvimento do sistema de software projetado, considerando as restrições técnicas, débito técnico de arquitetura e os atributos de qualidade assumidos para o projeto.

5.1 Arquitetura de software escolhida

No design da arquitetura houve algumas decisões de projeto que definem a arquitetura final. Além disso, algumas alternativas foram exploradas, porém descartadas. A seguir são descritas hipóteses, restrições, resultados de análises e experiências significativas para a arquitetura.

API para comunicação: O projeto se trata de uma aplicação para dispositivos móveis, portanto a decisão de como comunicar a aplicação com o banco de dados se apresenta em duas possibilidades: comunicação direta entre a aplicação e o banco que, após análise, se mostrou pouco seguro e uma prática incomum no desenvolvimento de

aplicações. A outra alternativa é construir uma API Rest para acessar a informação do banco de dados concentrando a lógica de negócio dentro da API, obtemos assim uma escalabilidade maior, e caso se faça necessária a migração da aplicação para outra plataforma, o código e as regras do negócio estarão concentrados em um único ponto.

Arquitetura híbrida: Com o uso de uma API e, consequentemente, a separação da aplicação em componentes, a arquitetura deve ser híbrida, em camadas no lado do servidor com tratamento de requisições feitas pela interface.

6. Referências

1. COLLINS, Sally L.; MOORE, R. Andrew; MCQUAY, Henry J. The visual analogue pain intensity scale: what is moderate pain in millimetres?. **Pain**, v. 72, n. 1-2, p. 95-97, 1997.
2. NAIME, Fauzia F. **Manual de tratamento da dor**. Editora Manole, 2013.
3. MELZACK, Ronald; CASEY, Kenneth L. Sensory, motivational, and central control determinants of pain: a new conceptual model. **The skin senses**, v. 1, p. 423-43, 1968.

Levantamento de Requisitos para Internet das Coisas com Foco em Segurança: Teoria e Prática

Equipe: Lucas e Mateus

Orientador(a): Maiane Castro

LOADING

Índice

Estudo de caso

Uma rede de hospitais solicitou o desenvolvimento de um sistema que permita o acesso à prontuário dos cidadãos de forma informatizada, o sistema a ser desenvolvido deve trazer eficiência e segurança aos atendimentos realizados, é esperado que o sistema permita armazenamento de dados do paciente, nome, CPF, idade, sexo, presença de alergias, motivo da consulta, histórico de vacinação e medicamentos, procedimentos realizados, necessidade de insulina solicitações de exames e resultados, deve ser conectado à sensor de temperatura corporal, de monitoramento cardíaco e de glicose, permitindo captura e armazenamento automático dos dados obtidos, além de funcionar em dispositivos móveis 24h por dia, permitindo que o profissional realize atendimento fora do ambiente hospitalar. Médicos, enfermeiros e emergencista que possuam autenticação necessária podem consultar ou/e incluir novo atendimento nunca modificar, os mesmos ainda devem classificar o paciente por grau de risco (A cor vermelha indica atendimento imediato; os casos urgentes recebem a cor amarela ,cores verde e azul representam casos de menor gravidade.informações como usuário, data, hora e local do último acesso deve ser registradas, alguns tipos de dados como doenças venéreas possuem chave especial estando disponíveis apenas para categoria específica. O prontuário do paciente pode ser acessado a partir do seu nome ou CPF.

Levantamento de custos Materiais

- Fonte de alimentação
- Microcontrolador
- Sensor de temperatura IR
- Sensor de monitoramento cardíaco
- Medidor de glicose
- Módulo GSM
- Considerações finais

Sobre os materiais

A seguir temos os materiais necessários para monitoramento de temperatura de um paciente. A análise foi realizada baseada em uso perto ou distante da residência. Portanto, utilizamos um módulo GSM para enviar dados a uma plataforma de IoT mesmo em lugares sem acesso Wi-Fi.

O GSM (Global System for Mobile Comunication (ou Sistema Global para Comunicação Móvel) é uma tecnologia utilizada em aparelhos móveis para conexão destes à Internet.

Para um uso mais confortável, damos preferência a materiais pequenos e leves.
O microcntrolador recebe medições de leitura do sensor infravermelho e monitoramento cardíaco e os envia ao banco de dados do site com suporte IoT ThingSpeak.

Fonte de alimentação

Baterias

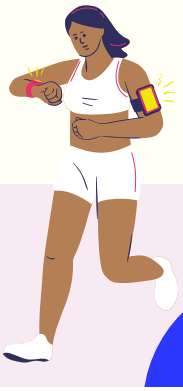
3.7v
2000mAh

Controlador de carga

7,4V e 8,4V
5000mA

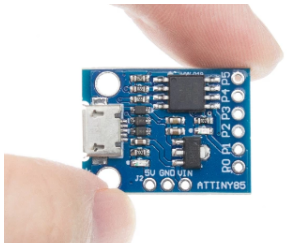
Adaptador AC/DC

7,5V
2500mAh



Obs.: o controlador de carga deve ficar na parte externa, sendo conectado no momento de de carga com plug e fonte específicos. Isto torna o aparelho de monitoramento mais compacto.

Microcontrolador

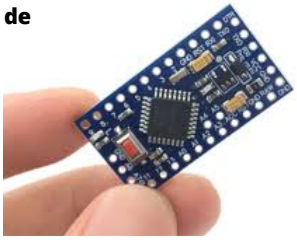


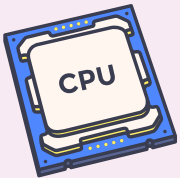
ATTiny85 é um processador de 8-Bits da ATMEL. Possui 8k programáveis, 6 linhas de entrada e saída para propósito geral e 4 canais de 10 bits com conversor analógico digital. Roda em até 20MHz com cristal externo podendo ser programado no circuito via SPI

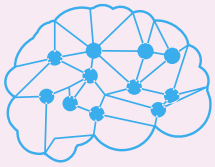
Alimentação Externa: 7 a 12v (seleção automática).

O Arduino Pro Mini é uma placa de microcontrolador baseado no ATmega328P

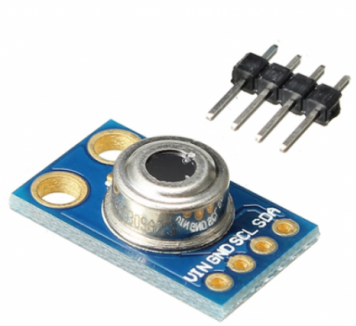
Possui a versão 5Vc de 16MHz e 3,3V de 8Mhz







Sensor de temperatura



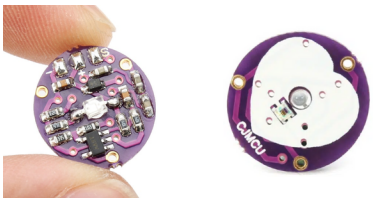
Especificações:

- Sensor de temperatura IR infravermelho
- Controlador MLX90614 (Datasheet MLX90614)
- Saída com resolução de 10-bit PWM
- Faixa de temperatura ambiente: -40 a 125°C
- Faixa de temperatura para objetos: -70 a 380°C
- Precisão: ±0,5°C
- Tensão de operação: 3VDC
- Dimensões: 17 x 11,5 x 6 mm

Sensor de frequência cardíaca

O Sensor de Frequência Cardíaca Oxímetro MAX30102 é um fotodetector, composto por 2 LEDs e circuitos que detectam batimentos cardíacos e medem indiretamente a quantidade de oxigênio no sangue.
Alimentação: 5V

X



O sensor de pulso monitor cardíaco efetua a leitura das batidas do coração usando um sensor óptico amplificado, e envia esses dados para o microcontrolador como o Arduino através de um único pino de sinal.

Tensão de operação: 3 ou 5VDC
Aprox. o dobro do preço

FreeStyle Libre

FreeStyle Libre é indicado para medir os níveis de glicose do líquido intersticial em pessoas (com 4 anos de idade ou mais) com diabetes mellitus, incluindo gestantes.

Leitor de glicose por sensor, sem picadas e sem dores.
Sensor aplicado na parte superior do braço.
Leitura da glicose por scanner, via leitor ou smartphone compatível.
Obtenha dados atualizados da glicose e histórico glicêmico.
O sensor dura até 14 dias.

Módulo GSM e
Chip M2M (telemetria)

O Módulo **SIM800L** é utilizado para comunicação via dados GSM/ GPRS, necessita de um chip de operadora de telefonia móvel para comunicação

O chip utilizado é um especifíco para soluções para o mercado M2M / **IoT.** Utilizar um chip específico fornecido pela operadora evita bloqueios na linha, portanto, falha no fornecimeto dos dados.

Tensão de trabalho: 3,6V-4,2V

Módulo GSM e Chip M2M (telemetria)

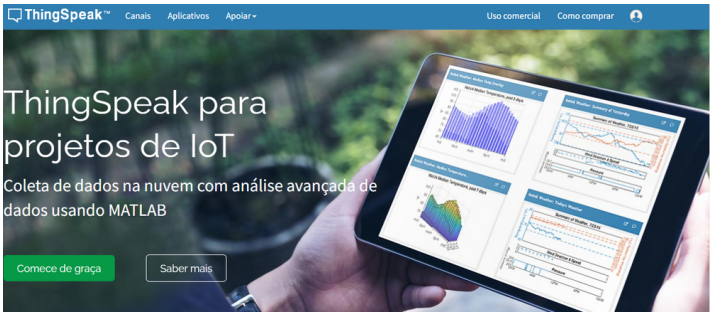
CONECTIVIDADE E GESTÃO M2M Início Conheça Benefícios Passo a passo Serviços Kite Platform Dúvidas

Escolha o melhor plano para sua empresa

20 MB	50 MB	100 MB
R$ 6,90 unidade/mês	R$ 9,90 unidade/mês	R$ 11,90 unidade/mês
Solicite	Solicite	Solicite

ThingSpeak

O ThingSpeak é um serviço de plataforma de análise de IoT que permite agregar, visualizar e analisar fluxos de dados ao vivo na nuvem. Você pode enviar dados para o ThingSpeak de seus dispositivos, criar visualização instantânea de dados ao vivo e enviar alertas.



Considerações parciais

Mostramos alguns detalhes do sistema de monitoramento de temperatura corpórea, monitoramento cardíaco e glicose. Algo que pode ser ampliado e verificado com mais detalhes as tecnologias disponíveis no mercado para tal aplicação.
O passo seguinte é a análise da plataforma *ThingSpeak IoT* para salvar os dadosenviados via GSM pelo microcontrolador.

Orçamento do material

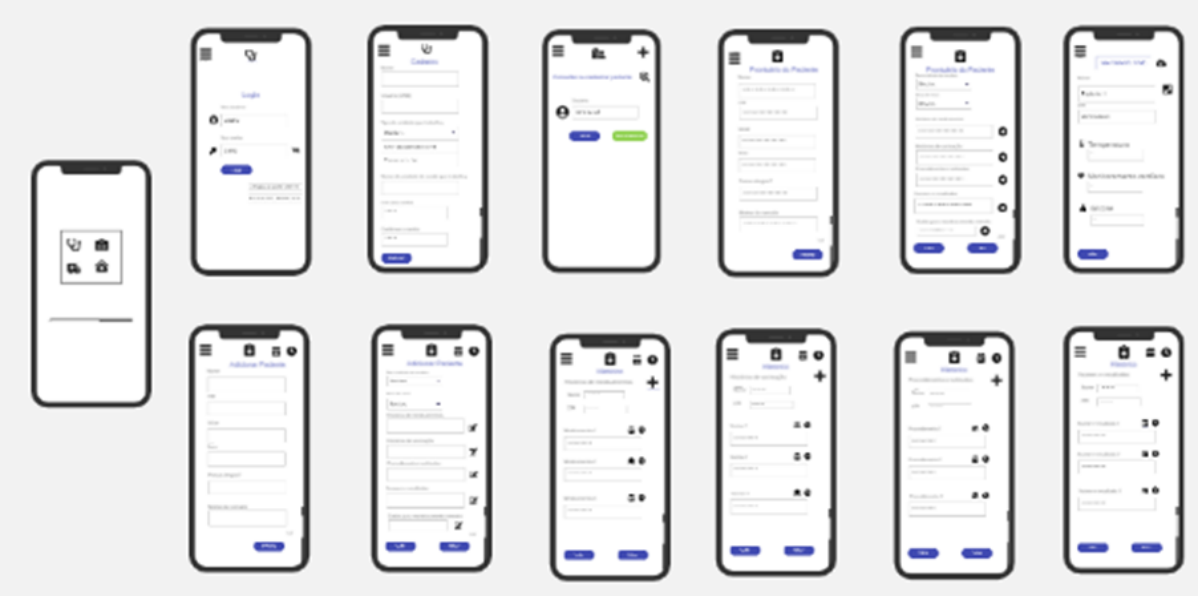
Planilha

CUSTOS VARIÁVEIS DIRETOS SOBRE O SERVIÇO PRESTADO			
CUSTOS COM MATERIAIS			
Componente	Quantidade	Preço (unidade)	Total
Bateria 3.7 V/2000mAh	2	R$ 27,00	R$ 54,00
Controlador de carga	1	R$ 18,00	R$ 18,00
Fonte (adaptador AC/DC) 5V/3000mA	1	R$ 35,00	R$ 35,00
Arduino pro mini	1	R$ 30,00	R$ 30,00
Sensor de temperatura IR MLX90614	1	R$ 79,00	R$ 79,00
Sensor de Frequência Cardíaca Oxímetro MAX30102	1	R$ 36,00	R$ 36,00
FreeStyle Libre	1	R$ 290,00	R$ 290,00
Módulo GSM SIM800L	1	R$ 50,00	R$ 50,00
Chip M2M	1	R$ 10,00	R$ 10,00
SUBTOTAL	**5**	**R$ 575,00**	**R$ 602,00**

CUSTOS DE SERVIÇOS		
Serviço Operadora chip M2M (mensal)	R$	11,90
SUBTOTAL	**R$**	**11,90**

TOTAL DE CUSTOS DIRETOS DO SERVIÇO	**R$**	**613,90**

Prototipagem



Tela inicial e login

Tela inicial do sistema na versão mobile.

Tela para o profissional de saúde fazer o login, ou seja, apenas pessoas autorizadas podem logar.
O usuário pode ser o cadastro do CRM (Conselho Regional de Medicina) válido ou algo similar que comprove cargo na área saúde.

Caso seja um novo usuário É necessário clicar em cadastre-se.

Para recuperar a senha

Cadastro de profissional e paciente

Ao clicar em "cadastre-se", o novo usuário é redirecionado para essa tela onde é solicitado os dados pesssoais e referente à unidade de atuação.

Também é solicitado o usuário e senha para login nos acessos seguintes.

Caso seja um novo atendimento, o profissional deve cadastrar o paciente.

O profissional de saúde ver o prontuário do paciente uando o nome completo ou CPF (Cadastro de Pessoa Física).

Prontuário de paciente

No protuário do paciente deve ter: nome completo, CPF, idade, sexo, se possui alergias, motivo da consulta, necessidade de insulina, grau de risco, histórico de medicamentos, histórico de vacinas, procedimentos realizados, exames e resultados.

Algumas opções possui uma seta que redireciona para mostrar o histórico e monitoramento do paciente.

Dados para identificação do paciente

O contato do paciente fica disponível para eventuais consultas.

O monitoramento remoto exibe dados de temperatura, monitoramento cardíaco e glicose.

Cadastro de paciente e históricos

Os dados do paciente devem ser inseridos. Semelhante ao que aocntece nos protuários físicos.

Ao clicar no icone de editar, abre uma tela para inserir históricos e comunicação do sistema IoT (ThingSpeak) que armazena os dados de monitoramento que fica com o paciente.

Histórico de medicamentos ministrados a pacientes.

Identificação do paciente

Medicamento , data e hora.

Habilita após inserir o conteúdo no campo referente ao medicamento.

Continuação: históricos

Históricos


Histórico de exames e resultados de exames.
Histórico
Exames e resultados
Nome
CPF
Identificação do paciente
Exame e resultado 1
Exame e resultado 2
Exame e resultado 3
Exame e resultado , data e hora de registro.
Voltar
Salvar
Habilita após inserir o conteúdo no campo referente ao Exame e resultado.

Ivanildo Nascimento
Matheus Cavalcante

ivanildosts369@gmail.com

jmatheusoc269@gmail.com

APÊNDICE B – Projetos sem Adm.R

Aluno: João, Júnior, Lara e Luan

1. Requisitos funcionais (casos de uso)

[RF001] Cadastrar paciente

Descrição do caso de uso: Este caso de uso permite que os usuários cadastrem um paciente.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O usuário precisa de privilégio para cadastrar um novo paciente.

Saídas e pós-condição: Um novo paciente é cadastrado no sistema.

[RF002] Armazenar dados dos Pacientes

Descrição do caso de uso: Esse caso de uso permite que os dados dos pacientes sejam armazenados no sistema.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: Os dados dos pacientes devem ser cadastrados no sistema.

Saídas e pós-condição: Os dados do paciente serão armazenados no sistema.

[RF003] Conectar a equipamentos de monitoramento

Descrição do caso de uso: Este caso de uso permite que o sistema possa se conectar com os sistemas dos equipamentos de monitoramento da saúde do paciente.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O sistema deverá interagir com os equipamentos.

Saídas e pós-condição: Sistemas conectados.

[RF004] Capturar dados dos equipamentos conectados

Descrição do caso de uso: Este caso de uso permitir que os sistemas capturem dados obtidos pelos equipamentos a ele conectado.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O equipamento deve estar conectado ao sistema.

Saídas e pós-condição: Os dados são capturados automaticamente.

[RF005] Armazenar dados obtidos pelos equipamentos

Descrição do caso de uso: Este caso de uso é usado quando o sistema capturar dados dos equipamentos.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O sistema deverá estar conectado aos equipamentos monitoramento e os dados devem serem capturados.

Saídas e pós-condição: Os dados capturados serão armazenados no sistema.

[RF006] incluir atendimentos

Descrição do caso de uso: Este caso de uso permite que os médicos, enfermeiros e emergencistas, incluam novos atendimentos no sistema.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O sistema só deve permitir que um novo atendimento possa ser incluído por médicos, enfermeiros e emergencistas autenticados.

Saídas e pós-condição: Um novo atendimento será incluído no sistema.

[RF007] Consultar atendimentos

Descrição do caso de uso: Este caso de uso permite que os médicos consultem os atendimentos cadastrados no sistema.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O atendimento deverá estar cadastrado no sistema.

Saídas e pós-condição: O sistema apresenta o atendimento solicitado para consulta.

[RF008] Consultar Prontuários

Descrição do caso de uso: Este caso de uso permite que os usuários do sistema acessem os prontuários dos pacientes.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O usuário deverá pesquisar o portuário pelo CPF do paciente cadastrado no sistema.

Saídas e pós-condição: O sistema mostrará o prontuário solicitado.

[RF009] Registrar informações de acesso ao sistema

Descrição do caso de uso: Este caso de uso permite ao usuário o sistema possar armazenar dados de acesso ao sistema como usuário, data, hora e local de acesso ao sistema.

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O Sistema deverá armazenar esses dados a cada acesso.

Saídas e pós-condição: Dados Registrados.

[RF010] Credenciamento de Acesso ao Sistema

Descrição do caso de uso: Este caso de uso permite cada usuário faça login ao sistema a partir das credenciais de acesso para cada tipo de usuário,

Prioridade: ■ Essencial □ Importante □ Desejável

Entradas e pré-condições: O usuário deverá fazer o login no sistema adicionando a senha de acesso.

Saídas e pós-condição: O usuário será logado ao sistema.

2. Requisitos não-funcionais

[RNF001] Eficiência

Embora não seja um requisito funcional ao sistema, deve ser considerada por corresponder a um fator de qualidade de software.

[RNF002] Segurança

O sistema deve fornecer mecanismos de segurança, autenticação e backup, o sistema nunca deve permitir que os médicos, enfermeiros e emergencista modifique os dados de atendimentos já cadastrado no sistema.

[RNF003] Disponibilidade

O Sistema deverá funcionar em dispositivos móveis 24 horas por dia.

APÊNDICE C – Termo de Consentimento Livre e Esclarecido (T.C.L.E.)

Esse curso tem como finalidade auxiliar no processo de validação da pesquisa Levantamento de Requisitos em Dispositivos de Internet das Coisas da Saúde com Ênfase em Segurança da Informação. Ao participar deste estudo a(o) Sra. (Sr.) irá colaborar com os orientadores: Prof. Dr. Admilson de Ribamar Lima Ribeiro, Prof. Dr. Gilton José Ferreira da Silva e a discente Maiane de Castro Santos na criação de um modelo de desenvolvimento de aplicações de Internet das Coisas que será desenvolvido durante a pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação – PROCC da Universidade Federal de Sergipe - UFS da discente Maiane de Castro Santos. A(O) Sra. (Sr.) tem liberdade de se recusar a participar e ainda se recusar a continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo. Sempre que quiser poderá pedir mais informações sobre a pesquisa por meio do e-mail maianecs@dcomp.ufs.br. Todas as informações coletadas neste estudo serão tratadas como confidenciais. Somente o aluno e orientadores terão conhecimento dos dados e em nenhum momento serão divulgadas informações que os identifique de maneira individual. Ao participar desta pesquisa a Sra. (Sr.) não terá nenhum benefício direto nem prejuízos.

APÊNDICE D – Casos

ESTUDO DE CASO 1

Uma rede de hospitais solicitou o desenvolvimento de um sistema capaz de permitir o acesso ao prontuário dos cidadãos de forma informatizada. O sistema a ser desenvolvido, deverá trazer eficiência e segurança aos atendimentos realizados. É esperado que o sistema armazene os dados do paciente: nome, CPF, idade, sexo, presença de alergias, motivo da consulta, histórico de vacinação e medicamentos, procedimentos realizados, necessidade de insulina, solicitações de exames e resultados. tal sistema deve ser conectado a sensor de temperatura corporal, de monitoramento cardíaco e de glicose, permitindo captura e armazenamento automático dos dados obtidos, além de funcionar em dispositivos móveis 24h por dia, permitindo que o profissional realize atendimento dentro e fora do ambiente hospitalar. Médicos, enfermeiros e emergencistas que possuam autenticação necessária, podem consultar ou/e incluir novo atendimento, nunca modificar. Os mesmos ainda devem classificar o paciente por grau de risco (a cor vermelha indica atendimento imediato; os casos urgentes recebem a cor amarela; cores verde e azul representam casos de menor gravidade). Informações como: usuário, data, hora e local do último acesso devem ser registradas e alguns tipos de dados como doenças venéreas possuem chave especial estando disponíveis apenas para a categoria específica. O prontuário do paciente pode ser acessado a partir do seu nome ou CPF.

ESTUDO DE CASO 2

O Laboratório XYZ deseja fazer um sistema capaz de permitir aos participantes de uma pesquisa (com duração de uma semana). O registro de informações acerca do grau de dor que sentem após ingerirem uma droga que está sendo testada com efeito analgésico. Os participantes serão divididos em dois grupos e irão ingerir a droga 2x ao dia de 12 em 12 horas. um grupo recebe a droga A (placebo) e o outro recebe a droga B(anti inflamatório); o sistema deve armazenar dados fornecidos pelos pacientes, droga ingerida (A ou B), grau de dor no início do tratamento e no final (numa escala de 0 a 100 - 0 = nenhuma dor; 100 = dor extrema); o sistema deve calcular a diferença entre os valores obtidos no final e no início do tratamento para ambas drogas e calcular as médias dessas diferenças; os participantes recebem login (só podem fazer um único registro referente a dor inicial, e outro referente a dor final, uma vez registrado não pode ser modificado). Informações como média, e visualização de todos registros serão protegidos para quem tiver credenciamento específico. Para lembrarem de ingerir a droga na hora determinada, os pacientes participantes deverão receber um porta medicamentos com sensor que verifique a presença da droga, e seja capaz de alertá-los sobre a necessidade de ingerí-la e de registrar o grau de dor inicial e final.

APÊNDICE E – Framework - Adm.R

Adm.R

Framework conceitual desenvolvido por Maiane de Castro Santos sob orientações de Gilton José Ferreira da Silva e Admilson Ribamar Lima Ribeiro do departamento de computação da UFS a fim de auxiliar no levantamento de requisitos para IoT na tentativa de prover que o sistema funcione como esperado minimizando falhas de Segurança.

→ Declaração de necessidade e viabilidade

Identifique o problema e como esse sistema ajudaria na resolução deste (o que deve ser construído, o que está sendo resolvido);
o domínio do sistema (casa inteligente, saúde, lazer, etc.);
os atores (dispositivos físicos, atores humanos,etc.);
o que o sistema deve fazer;
tipos de dados coletados.

→ Definição de stakeholders

Nomeie e caracterize qualquer pessoa envolvida;
pergunte aos envolvidos identificados sobre a necessidade de contatar mais alguém;
Estabeleça restrições aos perfis de acesso esperados, quanto a hierarquia de profissionais de saúde ou familiares do paciente.
verifique se todos os envolvidos estão de acordo com as necessidades declaradas anteriormente caso contrário, identifique as novas necessidades.

→ Descrição do ambiente

Defina processador, memória, unidades de comunicação(protocolos, padrões, normas, etc.), fonte de energia (baterias, energia solar, etc.), unidades de sensores e atuadores.

→ Definição de requisitos e restrições

Identifique serviço que o sistema deve fornecer, como o sistema deve reagir a entradas específicas de dados e como deve se comportar em determinadas situações (Requisitos Funcionais);
Identifique características do sistema relacionadas a usabilidade, confiabilidade, segurança, desempenho esperado e restrições de hardware e software - (Requisitos não Funcionais);
Identifique eventuais riscos e aponte meios de gerenciar esses riscos (Requisitos de Segurança).
Indique orçamento estimado.(custo e tempo)

→ Cenário de utilização

Crie um conjunto de cenários que identifique um roteiro de uso para o sistema, evidenciando situações com necessidade de segurança. (casos de uso, diagramas de sequência, de classes, de objetos, mapas e fluxogramas de processo);
Identifique cenários específicos para diferentes condições/ restrições de saúde, características das instalações físicas e de conectividade das instalações hospitalares ou residenciais.

→ Sugestão de artefatos

Interação com os stakeholders por meio da observação e de entrevista, e utilização de cenários e protótipos pode ajudar stakeholders compreenderem o sistema.
Algumas ferramentas de apoio: modelo 4+1 e template de arquitetura de software.

Referências

Pressman 8ª ed (2016)
Santos (2016)
Sommerville 9º ed(2011)
Zowgui e Coulin (2005)

APÊNDICE F – Questionário 1

Formulário de Caracterização do Participante

Esse formulário será utilizado para compreender seu grau de familiaridade com relação à Engenharia de software, Segurança da Informação e Internet das Coisas.

*Obrigatório

1. Nome completo (Conforme Sigaa): *

_____

2. Número da matricula:

_____

3. Curso: *

_____

4. Qual sua experiência com Engenharia de Software? *

Marcar apenas uma oval.

- ◯ Ótima, trabalho na área
- ◯ Muito Boa, já trabalhei em projetos industriais
- ◯ Boa, pratiquei em projetos em sala de aula
- ◯ Razoável, estudei somente em aula ou livro
- ◯ Nenhuma atuação na área

5. Qual seu nível de conhecimento acerca de Segurança da Informação? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

6. Como você avalia seu conhecimento sobre levantamento de requisitos? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

7. Você utiliza ou já utilizou alguma técnica para Levantamento/Engenharia de Requisitos, se sim qual? *

_____

_____

_____

_____

8. Sobre Internet das Coisas (IoT), como você avalia seu conhecimento? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

9. Em que grau você está no desenvolvimento de sistemas para IoT? *

Marcar apenas uma oval.

- ◯ Avançado
- ◯ Fluente
- ◯ Intermediário
- ◯ Básico
- ◯ Nenhum

APÊNDICE G – Formulário de Inscrição

Formulário de inscrição

*Obrigatório

1. Esse curso tem como finalidade auxiliar no processo de validação da pesquisa Levantamento de Requisitos em Dispositivos de Internet das Coisas da Saúde com Ênfase em Segurança da Informação. Ao participar deste estudo a(o) Sra. (Sr.) irá colaborar com os orientadores: Prof. Dr. Admilson de Ribamar Lima Ribeiro, Prof. Dr. Gilton José Ferreira da Silva e a discente Maiane de Castro Santos na criação de um modelo de desenvolvimento de aplicações de Internet das Coisas que será desenvolvido durante a pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação – PROCC da Universidade Federal de Sergipe - UFS da discente Maiane de Castro Santos. A(O) Sra. (Sr.) tem liberdade de se recusar a participar e ainda se recusar a continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo. Sempre que quiser poderá pedir mais informações sobre a pesquisa por meio do e-mail maianecs@dcomp.ufs.br. Todas as informações coletadas neste estudo serão tratadas como confidenciais. Somente o aluno e orientadores terão conhecimento dos dados e em nenhum momento serão divulgadas informações que os identifique de maneira individual. Ao participar desta pesquisa a Sra. (Sr.) não terá nenhum benefício direto nem prejuízos.
   Li e concordo com o Termo de Consentimento Livre e Esclarecido

   Marcar apenas uma oval.

   ◯ Sim
   ◯ Não

   Questionário

2. Nome completo: *

   _____
   _____
   _____
   _____
   _____

3. E-mail: *

4. Curso: *

5. Por favor, indique qual o maior nível de formação você tem atualmente *

Marcar apenas uma oval.

- ◯ Técnico
- ◯ Graduação
- ◯ Mestrado
- ◯ Doutorado
- ◯ Outro: _____

6. Qual sua experiência com Engenharia de Software - ES? *

Marcar apenas uma oval.

- ◯ Ótima, trabalho na área
- ◯ Muito boa, já trabalhei em projetos industriais
- ◯ Boa, pratiquei em projetos em sala de aula
- ◯ Razoável, estudei somente em aula ou livro
- ◯ Nenhuma atuação na área

7. Qual seu nível de conhecimento acerca de Segurança da Informação? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

8. Como você avalia seu conhecimento sobre Levantamento de Requisitos? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito Ruim

9. Você utiliza ou já utilizou alguma técnica para Levantamento/Engenharia de Requisitos, se sim qual? *

_____

_____

_____

_____

_____

10. Sobre Internet das Coisas (Internet of Things - IoT), como você avalia seu conhecimento? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

11. Como avalia seu conhecimento sobre desenvolvimento de Tecnologia para a área da Saúde? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

12. Como você avalia seu conhecimento sobre IoT na Saúde? *

Marcar apenas uma oval.

- ◯ Muito bom
- ◯ Bom
- ◯ Mediano
- ◯ Ruim
- ◯ Muito ruim

13. Em que grau você está no desenvolvimento de sistemas para IoT? *

Marcar apenas uma oval.

- ◯ Avançado
- ◯ Fluente
- ◯ Intermediário
- ◯ Nenhum

Acesse esse link para entrar no nosso grupo no Telegram: https://t.me/+mLIbu8spsQowNTQx

Ou se preferir acesse o QR CODE para entrar no nosso grupo no Telegram:

APÊNDICE H – Formulário Pós uso do Adm.R

Formulário pós uso do Framework Adm. R

*Obrigatório

1. 1.Como você classifica o grau de dificuldade durante o uso do Adm. R *

   Marque todas que se aplicam.

   - [ ] Muito fácil
   - [ ] Fácil
   - [ ] Mediano
   - [ ] Difícil
   - [ ] Muito difícil

2. 2.Você acredita que a utilização do Adm. R facilita a elicitação de requisitos em projetos de dispositivos de Internet das Coisas? *

   Marque todas que se aplicam.

   - [ ] Totalmente
   - [ ] Boa parte das vezes
   - [ ] Não

3. 3. Você acredita que a utilização do Adm. R reduz o tempo de atividade de elicitação de requisitos se comparada a não utilização dele? *

   _____

   _____

   _____

4. 4. Como o Adm.R auxiliou você a levantar requisitos? *

Marque todas que se aplicam.

- [ ] Bom. Talvez não tivesse identificado alguns requisitos se não tivesse utilizado
- [ ] Neutro. Encontraria os mesmos requisitos se não tivesse utilizado
- [ ] Ruim. O meu desempenho teria sido melhor se eu não tivesse utilizado

5. 5. Você acredita que o uso do Adm. R influencia de alguma forma na segurança * de dispositivos IoT?

Marque todas que se aplicam.

- [ ] Sim
- [ ] Talvez
- [ ] Não

6. 6. Você sentiu a necessidade de algum artefato adicional no Adm. R *

7. Registre sua opinião a respeito do Adm. R

7. Pontos positivos do Adm. R *

8. Pontos negativos do Adm. R *