Um sistema web para inspeção de conformidade em dispositivos IoT aplicados à saúde

Cesar Santos
Universidade Federal Rural de Pernambuco
Recife, Brasil
cesar.yuri@ufrpe.br

Ivonildo Pereira
Universidade Federal de Pernambuco
Recife, Brasil
ipgn@cin.ufpe.br

Matheus Frej
Universidade Federal de Pernambuco
Recife, Brasil
mflc@cin.ufpe.br

Waldemar Ferreira
Universidade Federal Rural de Pernambuco
Recife, Brasil
waldemar.ferreira@ufrpe.br

Sergio Soares
Universidade Federal de Pernambuco
Recife, Brasil
scbs@cin.ufpe.br

Resumo

Em dispositivos IoT aplicados à saúde (IoMT), a conformidade com leis de proteção de dados torna-se essencial devido ao tratamento de dados sensíveis e às exigências de segurança e privacidade. Este trabalho apresenta a evolução de uma ferramenta web de apoio à inspeção de conformidade previamente desenvolvida para sistemas gerais e soluções IoT, direcionando-a ao contexto de dispositivos IoMT. A solução foi desenvolvida considerando resultados de avaliações anteriores, além de regulamentações e práticas de segurança aplicáveis ao contexto de IoMT. O processo de evolução da ferramenta envolveu o levantamento de requisitos, a adaptação da checklist e a evolução da arquitetura do sistema. A avaliação foi conduzida por meio da análise de vulnerabilidades reportadas na literatura e de uma avaliação preliminar com especialistas. Os resultados indicam potencial da ferramenta para apoiar a identificação de não conformidades relacionadas à segurança, privacidade e proteção de dados em dispositivos IoMT.

Apresentação: https://doi.org/10.5281/zenodo.20367808

Palavras-chave

IoMT, Conformidade, Ferramenta Web, Proteção de Dados

1 Introdução

Com o avanço da Internet das Coisas (*Internet of Things* – IoT), dispositivos conectados passaram a ser amplamente utilizados na área da saúde, formando o ecossistema conhecido como *Internet of Medical Things* (IoMT) [19]. Esses dispositivos possibilitam monitoramento remoto de pacientes, coleta contínua de dados e integração entre sistemas médicos, contribuindo para melhorias no acompanhamento clínico e na qualidade dos serviços de saúde [28]. Entretanto, o uso crescente desses dispositivos também amplia preocupações relacionadas à segurança, privacidade e proteção de dados, especialmente devido ao tratamento de informações sensíveis e aos riscos de acesso não autorizado e comprometimento de dispositivos médicos conectados [3].

Nesse contexto, regulamentações como a *General Data Protection Regulation* (GDPR) [11] e a Lei Geral de Proteção de Dados (LGPD) [5] estabeleceram requisitos relacionados ao tratamento adequado de dados pessoais. Apesar disso, desenvolvedores ainda enfrentam dificuldades para adequar sistemas a essas regulamentações, principalmente devido à complexidade dos requisitos legais e à limitada adoção de ferramentas e abordagens práticas de apoio à conformidade [7]. Em dispositivos IoMT, esse cenário torna-se ainda mais desafiador devido às restrições computacionais presentes em muitos dispositivos médicos conectados [24].

Como forma de apoiar inspeções de conformidade, Mendes *et al.* [22] propuseram uma checklist para avaliação de sistemas computacionais quanto à adequação à LGPD. Posteriormente, Pereira *et al.* [23] estenderam a proposta para soluções IoT, incorporando requisitos relacionados à privacidade, segurança e conformidade em dispositivos conectados. Em seguida, Frej *et al.* [12] desenvolveram um sistema web para apoiar a utilização da checklist. Entretanto, as soluções existentes ainda não contemplam adequadamente particularidades de dispositivos IoMT. Diante desse cenário, este trabalho apresenta a evolução de uma ferramenta de inspeção de conformidade voltada ao contexto de dispositivos IoMT, incorporando uma nova checklist específica para dispositivos IoMT, adaptação dinâmica dos itens de inspeção conforme a categoria do dispositivo, reorganização do modelo de dados e associação automática dos itens de inspeção a princípios regulatórios.

A avaliação foi conduzida por meio da análise de vulnerabilidades reportadas na literatura e de uma avaliação preliminar com especialistas da área de tecnologia. Os resultados iniciais indicam potencial da ferramenta para apoiar a identificação de não conformidades relacionadas à segurança, privacidade e proteção de dados em dispositivos IoMT.

O artigo está estruturado da seguinte forma: a Seção 2 apresenta a fundamentação teórica. A Seção 3 discute os trabalhos relacionados. A Seção 4 apresenta as versões anteriores da ferramenta. A Seção 5 detalha o desenvolvimento e a evolução da ferramenta proposta. A Seção 6 apresenta a avaliação conduzida. A Seção 7 discute as ameaças à validade do estudo. Por fim, a Seção 8 apresenta as considerações finais e os trabalhos futuros.

2 Fundamentação Teórica

Esta seção apresenta conceitos relacionados à utilização de dispositivos conectados na área da saúde e aos aspectos regulatórios envolvidos na proteção de dados e privacidade.

2.1 IoT aplicada à saúde

A IoT consiste na interconexão de objetos físicos, dispositivos e sistemas por meio da Internet, permitindo comunicação, troca de dados e integração entre diferentes ambientes e aplicações [31]. Na área da saúde, dispositivos IoMT têm sido utilizados para oferecer serviços de saúde personalizados e inteligentes, contribuindo para a melhoria da qualidade de vida dos pacientes [18]. Entre suas aplicações, destacam-se o monitoramento remoto de pacientes, o acompanhamento contínuo de sinais vitais e o suporte à tomada de decisão médica por meio da análise de dados coletados por dispositivos conectados [28]. Nesse contexto, sensores, dispositivos vestíveis e implantáveis possibilitam a coleta e transmissão de informações médicas em tempo real, favorecendo respostas mais rápidas e maior eficiência nos serviços de saúde [20].

2.2 Desafios de conformidade regulatória em IoT

As leis de proteção de dados surgiram para estabelecer diretrizes para o tratamento adequado de dados pessoais, garantindo direitos relacionados à privacidade, segurança e transparência [33]. Com o avanço das tecnologias digitais e o aumento da coleta e compartilhamento de informações, diferentes países passaram a desenvolver regulamentações específicas para proteção de dados pessoais e sensíveis [14]. Entre as principais regulamentações destacam-se a *General Data Protection Regulation* (GDPR) [11], da União Europeia, considerada um dos principais marcos regulatórios da área, e a Lei Geral de Proteção de Dados (LGPD) [5], legislação brasileira inspirada em princípios da GDPR. Outras regulamentações relevantes incluem o *California Consumer Privacy Act* (CCPA) [6], nos Estados Unidos, e a *Privacy Act* australiana [2], consideradas neste trabalho por sua relevância internacional e diferentes abordagens relacionadas à proteção de dados pessoais.

Apesar da existência dessas regulamentações, sua compreensão e aplicação no desenvolvimento de software ainda representam desafios para engenheiros de software [27]. Entre as principais dificuldades estão a tradução de requisitos legais para soluções técnicas implementáveis [7, 21], a escassez de guias e ferramentas de apoio à conformidade [1, 26] e a ausência de padronização de técnicas e metodologias voltadas à adequação regulatória [10, 30]. Esses desafios tornam-se ainda mais críticos em dispositivos IoT médicos, que frequentemente operam com limitações de processamento, memória, armazenamento e energia [17, 34], dificultando a implementação de mecanismos robustos de segurança e privacidade. Além disso, esses dispositivos manipulam dados sensíveis e podem estar diretamente relacionados ao monitoramento e suporte à vida humana, fazendo com que falhas de segurança ou inadequações regulatórias comprometam tanto a privacidade quanto a segurança dos pacientes [32].

3 Trabalhos Relacionados

O estudo de Mendes *et al.* [22] propôs um checklist para avaliar a conformidade de sistemas computacionais com a LGPD, buscando aproximar os requisitos legais do contexto de desenvolvimento de software. Baseado nos princípios da GDPR, o autor desenvolveu uma abordagem inicial e avaliou sua aplicação em um sistema universitário. Posteriormente, Pereira *et al.* [25] expandiram a checklist para contemplar soluções IoT, incorporando requisitos específicos desse domínio e obtendo resultados promissores em avaliações realizadas em ambiente industrial. Em continuidade a essa linha de pesquisa, Frej *et al.* [12] desenvolveram uma ferramenta web para apoiar o processo de avaliação de conformidade, oferecendo funcionalidades que facilitam a inspeção e o gerenciamento dos resultados obtidos. Nosso trabalho busca dar continuidade a essas iniciativas, ampliando o suporte à conformidade para dispositivos IoMT, considerando requisitos específicos de segurança, privacidade e proteção de dados no contexto da saúde.

O trabalho de Cerqueira *et al.* [8] propôs a abordagem LGPD-Check, desenvolvida a partir de atividades como revisão bibliográfica, análise da legislação, entrevistas com especialistas e avaliação experimental da solução. A técnica organiza o processo de inspeção em diferentes perspectivas, contemplando a análise de requisitos de software, a avaliação de sistemas em execução e a verificação de práticas organizacionais relacionadas à proteção de dados. Os resultados apresentados pelos autores indicam que a abordagem foi capaz de auxiliar na identificação de não conformidades associadas aos princípios da LGPD em artefatos de software, além de demonstrar sua viabilidade em cenários reais de aplicação. Enquanto a LGPDCheck concentra-se na definição e validação de uma técnica de inspeção baseada em checklists, nossa proposta direciona-se ao contexto específico de dispositivos IoMT, disponibilizando uma plataforma web para apoiar a execução, organização e gerenciamento das verificações de conformidade.

No contexto da utilização de princípios regulatórios como apoio à conformidade em software, Rocha *et al.* [26] investigaram dificuldades enfrentadas por profissionais na implementação da LGPD, propondo um guia com técnicas e práticas para apoiar a conformidade em sistemas de software. Assim como esse trabalho, nossa proposta também utiliza princípios regulatórios como base estruturadora da solução. Entretanto, diferentemente de Rocha *et al.* [26], nossa abordagem é direcionada à inspeção de conformidade em dispositivos IoMT, incorporando requisitos de segurança, privacidade e análise de ameaças em ambientes de saúde.

Os trabalhos relacionados propõem checklists, técnicas de inspeção ou ferramentas de apoio à conformidade regulatória. Entretanto, nossa proposta diferencia-se por integrar uma checklist específica para dispositivos IoMT, adaptação dinâmica dos itens de inspeção e associação automática aos princípios regulatórios.

4 Ferramentas Anteriores de Apoio à Conformidade com a LGPD

Mendes *et al.* [22] propuseram um checklist para apoiar a verificação de conformidade de sistemas de software com a LGPD e a GDPR. A proposta foi construída a partir de uma Revisão Sistemática da Literatura e da análise de requisitos regulatórios relacionados à privacidade e proteção de dados.

Posteriormente, Pereira *et al.* [23] expandiram a checklist para o contexto de IoT, incorporando aspectos específicos desse domínio, como riscos associados à coleta contínua de dados, restrições computacionais e limitações de segurança dos dispositivos. Além disso, a versão estendida passou a incluir classificações de severidade e sugestões de mitigação para apoiar o processo de adequação à LGPD.

A versão inicial da ferramenta era baseada em planilhas eletrônicas, conforme ilustrado na Figura 1. Apesar de permitir a organização dos itens de inspeção, essa abordagem apresentava limitações relacionadas à flexibilidade, manutenção e evolução da solução.

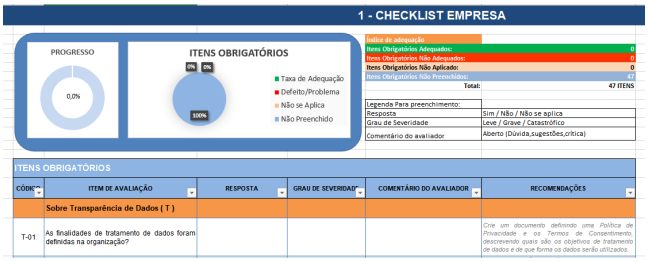

Figura 1: Visão da primeira versão do checklist no formato Excel.

Com o objetivo de superar as limitações da abordagem baseada em planilhas, Frej *et al.* [12] criaram uma versão web da checklist, incorporando funcionalidades como autenticação de usuários, armazenamento das avaliações realizadas, geração de relatórios em PDF, visualização gráfica dos resultados e filtragem dinâmica dos itens da checklist. A avaliação conduzida pelos autores indicou potencial da ferramenta para apoiar a identificação de lacunas de conformidade de forma mais prática e acessível.

Além disso, os autores identificaram oportunidades de evolução relacionadas à usabilidade, acessibilidade e expansão da ferramenta para outros contextos de aplicação. Neste trabalho, damos continuidade a essa linha de pesquisa ao evoluir a ferramenta para o contexto de dispositivos IoMT, incorporando adaptações relacionadas à segurança, privacidade e proteção de dados em dispositivos médicos conectados, bem como considerando comentários obtidos nas avaliações das versões anteriores da solução.

Em relação à versão anterior, esta nova versão introduz quatro evoluções: (i) desenvolvimento de uma nova checklist específica para dispositivos IoMT; (ii) adaptação dinâmica dos itens de inspeção conforme a categoria do dispositivo; (iii) reestruturação do modelo de dados para suportar diferentes categorias de dispositivos médicos; e (iv) associação automática dos itens da checklist aos princípios regulatórios de proteção de dados.

5 Desenvolvimento e evolução da ferramenta

Esta seção descreve a evolução da ferramenta proposta, incluindo modificações na arquitetura, reestruturação do modelo de dados, adaptação da checklist para dispositivos IoMT e melhorias de usabilidade implementadas. Também são apresentados o fluxo de utilização da ferramenta e aspectos relacionados à sua disponibilização.

5.1 Evolução da Arquitetura da Ferramenta

A arquitetura originalmente proposta por Frej *et al.* [12] foi mantida nesta nova versão da ferramenta, preservando a separação entre *frontend* e *backend*. O *frontend* permanece desenvolvido em React[1] e TypeScript[2], favorecendo modularização da interface, reutilização de componentes e evolução incremental das funcionalidades. O *backend* continua baseado em Express[3] e Prisma[4], permitindo organização dos casos de uso, persistência relacional e simplificação da comunicação com o banco de dados.

Embora a base arquitetural tenha sido preservada, foram realizadas modificações para adaptar a ferramenta ao contexto de dispositivos IoMT, ampliando sua flexibilidade de manutenção e evolução. Essas modificações incluíram melhorias na organização da aplicação, introdução de testes automatizados e aprimoramentos no fluxo de desenvolvimento.

O *backend* da aplicação passou a ser organizado em torno de casos de uso específicos, cada um seguindo um fluxo estruturado de desenvolvimento composto por implementação, testes unitários, testes integrados (*end-to-end*) e validação manual utilizando Postman. O processo de desenvolvimento foi gerenciado por meio do GitHub, utilizando *issues* e *branches* dedicadas para cada funcionalidade implementada. Essa organização contribuiu para maior rastreabilidade das alterações realizadas e tornou o processo de validação mais sistemático, uma vez que cada funcionalidade somente era incorporada ao sistema após a conclusão das etapas de teste e validação.

Além disso, o *backend* passou a centralizar a recuperação e organização dos dados utilizados pela checklist, reduzindo o acoplamento entre interface e persistência e facilitando futuras expansões da ferramenta.

5.2 Reestruturação do Modelo de Dados

A reestruturação do modelo de dados representa uma das principais modificações realizadas nesta nova versão da ferramenta. Na implementação anterior, a checklist era mantida parcialmente de forma estática no *frontend*, dificultando a manutenção, reutilização e expansão dos itens de avaliação. Além disso, a organização dos dados apresentava forte dependência da estrutura da interface, reduzindo a flexibilidade para adaptação a novos cenários regulatórios e novos tipos de dispositivos.

A checklist foi migrada para um modelo relacional persistido no banco de dados, permitindo o gerenciamento dinâmico dos itens de avaliação pelo *backend*. Essa mudança desacoplou os dados da interface e tornou a estrutura mais flexível.

Durante a adaptação da solução ao contexto de dispositivos IoMT, o modelo foi reorganizado para considerar características específicas de diferentes categorias de dispositivos médicos conectados. A ferramenta passou a utilizar três categorias principais de dispositivos: sensores, dispositivos vestíveis (*wearables*) e dispositivos implantáveis.

Cada item da checklist passou a ser associado a uma ou mais categorias de dispositivos, permitindo que diferentes conjuntos de perguntas fossem exibidos dinamicamente conforme o tipo de dispositivo selecionado pelo avaliador no início da inspeção. Dessa forma, perguntas específicas podem estar relacionadas apenas a dispositivos implantáveis, enquanto outras podem ser compartilhadas entre sensores e dispositivos vestíveis, por exemplo. Essa

[1] https://react.dev/

[2] https://www.typescriptlang.org/

[3] https://expressjs.com/

[4] https://www.prisma.io/

abordagem tornou o processo de avaliação mais contextualizado às limitações técnicas e aos riscos específicos de cada categoria de dispositivo. Além disso, a organização dinâmica dos itens reduziu redundâncias na estrutura da checklist e facilitou a reutilização de perguntas entre diferentes cenários de avaliação.

Outra modificação importante foi a substituição da associação baseada em legislações por uma abordagem centrada em princípios de proteção de dados e segurança. Os itens da checklist passaram a ser previamente relacionados a princípios como adequação, prevenção, segurança e responsabilização. Com isso, a ferramenta passou a consolidar automaticamente os resultados da avaliação considerando os princípios associados aos itens respondidos pelo usuário.

Mesmo com a simplificação estrutural, o modelo preservou informações essenciais da avaliação, incluindo resposta do avaliador, grau de severidade e comentários associados a cada item. Além disso, a nova estrutura manteve a flexibilidade necessária para inclusão futura de novos itens, princípios e categorias de dispositivos sem necessidade de alterações significativas na lógica da aplicação.

A Figura 2 apresenta o modelo entidade-relacionamento atualizado da ferramenta.

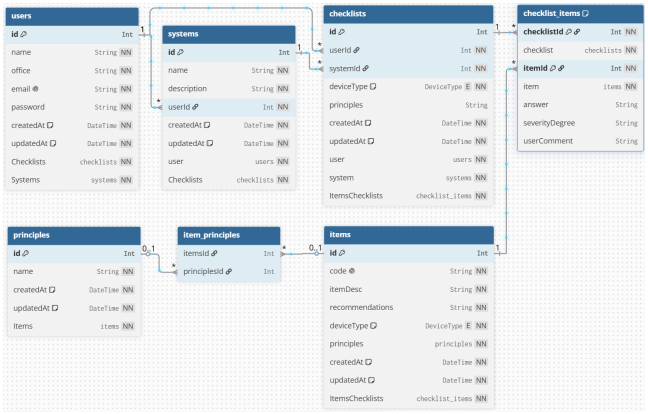

Figura 2: Diagrama entidade-relacionamento do banco de dados.

5.3 Adaptação da Checklist para Dispositivos IoMT

Além das modificações estruturais realizadas no modelo de dados, a checklist também foi adaptada para contemplar características específicas de dispositivos IoMT. Embora a ferramenta tenha evoluído a partir da versão anteriormente desenvolvida para soluções IoT, a checklist desta versão foi elaborada exclusivamente para o contexto de dispositivos IoMT, não reutilizando os itens das versões anteriores. Para sua construção, foi conduzida uma revisão da literatura com o objetivo de identificar requisitos de segurança, privacidade e proteção de dados, bem como vulnerabilidades recorrentes nesse domínio. Também foram analisadas regulamentações de proteção de dados aplicáveis e limitações técnicas desses dispositivos, como restrições de processamento, consumo de energia e disponibilidade contínua dos serviços médicos. Os estudos analisados permitiram extrair requisitos de segurança, vulnerabilidades e recomendações recorrentes para dispositivos IoMT. Requisitos semelhantes identificados em diferentes estudos foram agrupados e consolidados, dando origem aos itens da nova checklist. Cada item foi então associado às categorias de dispositivos e aos princípios regulatórios utilizados pela ferramenta.

Foram incorporados itens relacionados à utilização de mecanismos leves de criptografia, autenticação, atualização segura de *firmware*, controle de acesso, disponibilidade dos serviços e proteção de dados sensíveis dos pacientes. Além disso, a adaptação da checklist considerou riscos associados à comunicação entre dispositivos conectados, à integridade dos dados transmitidos e à privacidade das informações coletadas em ambientes de saúde.

Essas modificações permitiram tornar o processo de inspeção mais aderente às limitações técnicas e aos requisitos de segurança, privacidade e proteção de dados presentes no contexto de dispositivos IoMT.

5.4 Melhorias de Usabilidade

A ferramenta também passou por melhorias relacionadas à navegação e ao preenchimento da checklist durante o processo de inspeção. A interface foi reorganizada para tornar o fluxo de avaliação mais intuitivo, facilitando a visualização das perguntas e o acompanhamento do progresso da inspeção.

Além disso, o sistema mantém validações visuais para auxiliar o avaliador durante o preenchimento da checklist, destacando itens incompletos ou inconsistentes em vermelho. Também foram realizadas melhorias na organização das informações apresentadas ao usuário, buscando reduzir dificuldades durante o processo de avaliação.

Essas modificações contribuíram para tornar a utilização da ferramenta mais organizada e acessível durante as inspeções de conformidade.

5.5 Jornada do Usuário na Ferramenta

Ao acessar a ferramenta, o avaliador é inicialmente direcionado para uma página de instruções gerais, contendo orientações sobre o processo de inspeção e informações sobre os tipos de dispositivos suportados pela ferramenta. Nessa etapa, também são apresentados os objetivos da avaliação e recomendações relacionadas ao preenchimento da checklist, como pode ser observado na Figura 3.

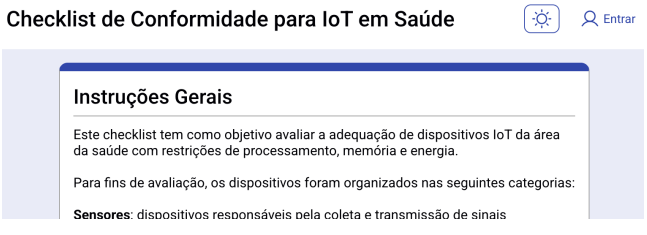

Figura 3: Página de instruções no sistema.

Para utilizar funcionalidades como armazenamento, edição e geração de relatórios das avaliações, o avaliador deve realizar autenticação na ferramenta. Após o login, é possível iniciar uma nova avaliação informando o nome do dispositivo ou sistema analisado e uma descrição do contexto da inspeção. Em seguida, o avaliador seleciona a categoria do dispositivo IoMT, podendo ser sensores, dispositivos vestíveis (*wearables*) ou implantáveis, permitindo que a ferramenta adapte dinamicamente os itens apresentados durante a inspeção, como ilustrado na Figura 4.

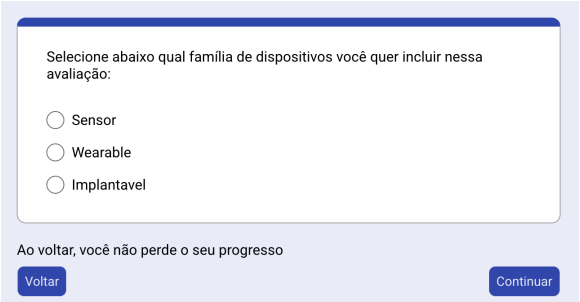

Figura 4: Seleção dos tipos de dispositivos.

Com base no tipo de dispositivo selecionado, o sistema recupera automaticamente perguntas específicas relacionadas à segurança, privacidade e proteção de dados, adaptando a checklist às características de cada categoria de dispositivo.

Em seguida, o avaliador responde aos itens da checklist, indicando se cada requisito está conforme, não conforme ou não se aplica. Para respostas negativas, a ferramenta exige o preenchimento do grau de severidade e de comentários adicionais. Ao final da inspeção, os resultados podem ser visualizados, editados e exportados em formato PDF (Figura 5).

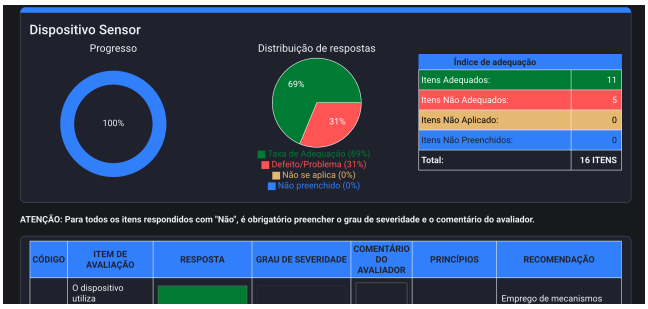

Figura 5: Exemplo de exibição gráfica dos resultados da avaliação.

5.6 Disponibilização da Ferramenta

Após a implementação das melhorias propostas, a ferramenta foi disponibilizada para utilização e testes em um servidor do Centro de Informática da Universidade Federal de Pernambuco (CIn-UFPE).

A aplicação foi implantada utilizando contêineres Docker[5], permitindo o empacotamento padronizado dos serviços da ferramenta e simplificando o processo de implantação, execução e manutenção da infraestrutura. A arquitetura implantada integra *frontend*, *backend* e banco de dados em ambiente containerizado, facilitando gerenciamento, atualização e escalabilidade dos serviços da aplicação.

Além disso, os repositórios do projeto permanecem disponíveis publicamente no GitHub, permitindo acesso ao código-fonte, reprodução da solução e evolução colaborativa da ferramenta. O repositório do *frontend* encontra-se disponível no GitHub[6], assim como o *backend*[7].

A ferramenta é disponibilizada como software de código aberto sob licença MIT.

6 Avaliação

Esta seção apresenta a avaliação da ferramenta proposta. Como se trata de uma primeira evolução da ferramenta para o contexto IoMT, a avaliação concentrou-se inicialmente na verificação exploratória da aplicabilidade da solução. O estudo foi conduzido em duas etapas: uma análise baseada em vulnerabilidades reportadas na literatura e uma avaliação preliminar com especialistas da área de tecnologia.

6.1 Avaliação baseada em cenários da literatura

A avaliação da ferramenta foi conduzida por meio da análise de vulnerabilidades e ameaças reportadas na literatura envolvendo dispositivos IoT aplicados à saúde. Para isso, foi adotada uma abordagem exploratória baseada em estudos previamente publicados, com o objetivo de verificar se a checklist proposta poderia auxiliar na identificação de problemas de segurança, privacidade e conformidade em cenários reais.

Foram selecionados seis estudos envolvendo sensores biomédicos, dispositivos vestíveis e implantáveis [4, 9, 13, 16, 29, 32]. Os trabalhos descrevem ameaças como comunicação insegura, falhas de autenticação, ataques de negação de serviço (DoS), vazamento de dados sensíveis, *spoofing* de sensores, reidentificação de usuários e comprometimento de *firmware*.

As vulnerabilidades identificadas foram relacionadas aos itens presentes na checklist proposta. O objetivo da avaliação não foi reproduzir experimentalmente os ataques, mas analisar se os mecanismos de segurança, privacidade e conformidade contemplados na checklist poderiam auxiliar na identificação de possíveis não conformidades. O artefato contendo a análise de cobertura foi disponibilizado publicamente[8].

A análise demonstrou que os itens da checklist estão alinhados a mecanismos frequentemente utilizados para mitigação dessas ameaças, especialmente em aspectos relacionados à criptografia de dados, autenticação, controle de acesso, gerenciamento seguro de chaves criptográficas, atualização segura de *firmware* e preservação da privacidade dos pacientes.

Como exemplo, um dos estudos analisados descreve ataques a bombas de infusão e bombas de insulina conectadas, nos quais comandos maliciosos poderiam comprometer a administração de

[5] https://www.docker.com/
[6] https://github.com/cesaryuri/LGPD-checklist-frontend
[7] https://github.com/cesaryuri/LGPD-checklist-api
[8] https://zenodo.org/records/20344670

medicamentos. Nesse cenário, a checklist auxiliaria na identificação de requisitos relacionados à autenticação, controle de acesso, integridade das comunicações e proteção criptográfica dos dados transmitidos.

6.2 Avaliação preliminar com especialistas

Como segunda etapa da avaliação, foi realizada uma avaliação preliminar com especialistas e profissionais da área de tecnologia. Participaram cinco profissionais com experiência em desenvolvimento, inspeção e segurança de sistemas.

Entre os participantes, três integram um núcleo de inovação em tecnologia da informação, comunicação e automação, sendo que dois já haviam participado de avaliações anteriores relacionadas à evolução da checklist proposta por Frej *et al.* [12] e do estudo conduzido por Pereira *et al.* [23]. A avaliação também contou com a participação de um engenheiro de testes de uma empresa multinacional de tecnologia e de um profissional de empresa privada que também participou da avaliação realizada no trabalho de Frej *et al.* [12].

A avaliação foi dividida em duas etapas. Na primeira, os participantes realizaram testes exploratórios na ferramenta, analisando aspectos de usabilidade, navegação, clareza das informações e fluxo de inspeção.

Ao final da avaliação, os participantes responderam a um questionário contendo questões objetivas e discursivas. As questões objetivas avaliaram as dimensões de facilidade de uso, utilidade percebida e intenção de uso da ferramenta, utilizando uma escala Likert de cinco pontos [15]. As questões discursivas permitiram aos participantes descrever funcionalidades consideradas relevantes, sugerir melhorias e compartilhar comentários sobre a experiência de utilização da ferramenta.

6.3 Resultados preliminares

Os resultados da avaliação indicaram uma percepção positiva dos participantes em relação à ferramenta. Na dimensão de facilidade de uso, todos os participantes responderam "Concordo Totalmente". Em relação à utilidade percebida, quatro participantes responderam "Concordo Totalmente", enquanto um respondeu "Concordo Parcialmente". Da mesma forma, na dimensão de intenção de uso da ferramenta em processos de inspeção e avaliação de conformidade, quatro participantes demonstraram concordância total e um concordância parcial.

Além das respostas objetivas, os participantes forneceram comentários qualitativos sobre a utilização da ferramenta. Entre os aspectos positivos destacados, apontaram que as perguntas da checklist são diretas e objetivas, além de considerarem a interface clara e de fácil compreensão durante o processo de inspeção.

Também foram identificadas oportunidades de melhoria relacionadas principalmente à experiência de uso em dispositivos móveis. Alguns participantes relataram dificuldades de navegação e adaptação da interface em determinados modelos de celulares, indicando a necessidade de aprimoramentos na responsividade da ferramenta. Nos testes realizados em computadores, não foram relatados problemas de utilização.

Os participantes também sugeriram melhorias na interface visual e a inclusão de mecanismos adicionais de apoio à interpretação da legislação, como recursos inteligentes de assistência ao usuário.

Além dos comentários relacionados à usabilidade, um dos participantes apresentou uma proposta de refinamento da interface, incluindo uma prototipação com melhorias na organização dos componentes e na adaptação da navegação para dispositivos móveis. Segundo o participante, essas alterações tornam o fluxo de inspeção mais intuitivo e adequado ao contexto de auditorias de segurança.

7 Ameaças à Validade

Este trabalho apresenta algumas limitações. A avaliação preliminar foi conduzida com um número reduzido de participantes, o que limita a generalização dos resultados obtidos. Além disso, os participantes possuíam experiência na área de tecnologia, não incluindo profissionais da área da saúde, o que limita a extrapolação dos resultados para o contexto clínico. A análise da ferramenta também foi baseada em cenários e vulnerabilidades reportadas na literatura, sem a realização de avaliações em ambientes reais envolvendo dispositivos IoMT ou contextos hospitalares.

Apesar das limitações, os resultados preliminares indicam potencial da solução para apoiar inspeções de conformidade.

8 Considerações Finais

Este trabalho apresentou a evolução de uma ferramenta web para apoio à inspeção de conformidade em dispositivos IoMT. A solução proposta expandiu versões anteriores da checklist de conformidade com a LGPD, incorporando adaptações voltadas ao contexto de dispositivos IoMT e incluindo requisitos relacionados à segurança, privacidade e proteção de dados.

Entre as principais contribuições, destacam-se a reestruturação da arquitetura da ferramenta, a adaptação dinâmica da checklist conforme o tipo de dispositivo avaliado e a associação dos itens de inspeção a princípios regulatórios de proteção de dados.

A avaliação conduzida com base em cenários da literatura e com especialistas da área de tecnologia indicou resultados preliminares positivos quanto à utilidade e aplicabilidade da ferramenta. Além disso, os participantes forneceram sugestões relevantes para evolução da solução.

Como trabalhos futuros, pretende-se ampliar a avaliação da ferramenta em ambientes reais, envolvendo dispositivos IoMT e profissionais da área da saúde. Nessas avaliações, serão investigados aspectos relacionados à eficácia da ferramenta na condução de inspeções de conformidade. Além disso, pretende-se expandir a checklist para contemplar um maior número de tipos de dispositivos IoMT.

Disponibilidade de Artefatos

Os artefatos desenvolvidos durante este trabalho estão disponíveis abertamente em: https://doi.org/10.5281/zenodo.20368220

Agradecimentos

Este trabalho é parcialmente apoiado pelo INES.IA (www.ines.org.br), CNPq processo 408817/2024-0. Sergio Soares é parcialmente apoiado pelo CNPq, processo 306000/2022-9.

Referências

[1] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. 2021. I'm all ears! Listening to software developers on putting GDPR principles into software development practice. *Personal and Ubiquitous Computing* 25, 5 (2021), 879–892.

[2] Australian Government. 1988. Privacy Act 1988. https://www.legislation.gov.au/Details/C2018C00215 Accessed: 2024-09-11.

[3] Marc Jayson Baucas, Petros Spachos, and Stefano Gregori. 2023. Private blockchain-based wireless body area network platform for wearable Internet of Thing devices in healthcare. In *ICC 2023-IEEE International Conference on Communications*. IEEE, IEEE, Piscataway, NJ, USA, 6181–6186.

[4] Vimal Bibhu, Anand Kumar Shukla, Basu Dev Shivahare, Jatinder Kaur, Mohd Shukri, Ab Yajid Johar MGM, Ayham Sameer Faaq, Mohammed Kareem AlShujairi, and Shatrudhan Pandey. 2024. Analysis of security and privacy challenges of smart health and sensing systems. *Results in Engineering* 24 (2024), 103466.

[5] Brasil. 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 24 de abril de 2024.

[6] California State Legislature. 2018. California Consumer Privacy Act of 2018 (CCPA). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375,2018 Accessed: 2024-09-11.

[7] E.D. Canedo, A.T.S. Calazans, and I.N. et al. Bandeira. 2022. Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requirements Engineering* 27 (2022), 545–567.

[8] Diego André Cerqueira, Rafael Maiani de Mello, Jéssica Soares da Costa, and Guilherme Horta Travassos. 2025. Experimental evaluation of a checklist-based inspection technique to verify the compliance of software systems with the brazilian general data protection law. *Empirical Software Engineering* 30, 5 (2025), 122.

[9] Ge Chu, Farah Al-Shareefi, Haoyu Wu, Yongle Hu, and Shiping Yan. 2024. Penetration Testing for Securing IoT-Enabled Healthcare Systems: A Focus on Wearable Devices and Remote Surgery. In *2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. IEEE, IEEE, Piscataway, NJ, USA, 5944–5951.

[10] Edna Dias Canedo, Angelica Toffano Seidel Calazans, Eloisa Toffano Seidel Masson, Pedro Henrique Teixeira Costa, and Fernanda Lima. 2020. Perceptions of ICT practitioners regarding software privacy. *Entropy* 22, 4 (2020), 429.

[11] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation). Disponível em: https://gdpr-info.eu/. https://gdpr-info.eu/ Acesso em: 24 de abril de 2024.

[12] Matheus Frej, Ivonildo Pereira, Waldemar Ferreira, and Sergio Soares. 2024. Um sistema web para auxiliar soluções na conformidade com a LGPD. In *Simpósio Brasileiro de Engenharia de Software (SBES)*. SBC, Sociedade Brasileira de Computação, Porto Alegre, RS, Brasil, 713–719.

[13] Rakibul Hasan, Md Al Amin, Sheikh Dobir Hossain, and Md Ibrahim Abdullah. 2023. Protecting Data Confidentiality and Assuring Integrity, and Preventing Rogue Devices in Medical Body Area Network. In *2023 5th International Conference on Sustainable Technologies for Industry 5.0 (STI)*. IEEE, IEEE, Piscataway, NJ, USA, 1–6.

[14] Lars Hornuf, Sonja Mangold, and Yayun Yang. 2023. Data protection law in Germany, the United States, and China. In *Data privacy and crowdsourcing: A comparison of selected problems in China, Germany and the United States*. Springer, Cham, 19–79.

[15] Ankur Joshi, Saket Kale, Satish Chandel, and D Kumar Pal. 2015. Likert scale: Explored and explained. *British journal of applied science & technology* 7, 4 (2015), 396–403.

[16] Théo Jourdan, Antoine Boutet, Amine Bahi, and Carole Frindel. 2020. Privacy-Preserving IoT framework for activity recognition in personal healthcare monitoring. *ACM Transactions on Computing for Healthcare* 2, 1 (2020), 1–22.

[17] Sivanarayani M Karunarathne, Neetesh Saxena, and Muhammad Khurram Khan. 2021. Security and privacy in IoT smart healthcare. *IEEE Internet Computing* 25, 4 (2021), 37–48.

[18] Mostafa Haghi Kashani, Mona Madanipour, Mohammad Nikravan, Parvaneh Asghari, and Ebrahim Mahdipour. 2021. A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications* 192 (2021), 103164.

[19] Chunyan Li, Jiaji Wang, Shuihua Wang, and Yudong Zhang. 2024. A review of IoT applications in healthcare. *Neurocomputing* 565 (2024), 127017.

[20] Zhao-xia Lu, Peng Qian, Dan Bi, Zhe-wei Ye, Xuan He, Yu-hong Zhao, Lei Su, Siliang Li, and Zheng-long Zhu. 2021. Application of AI and IoT in clinical medicine: summary and challenges. *Current medical science* 41, 6 (2021), 1134–1150.

[21] Pedro Machado, Jéssyka Vilela, Mariana Peixoto, and Carla Silva. 2023. A systematic study on the impact of GDPR compliance on Organizations. In *Proceedings of the XIX Brazilian Symposium on Information Systems*. SBC, Maceió, Brazil, 435–442.

[22] João Mendes, Davi Viana, and Luis Rivero. 2021. Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In *Proceedings of the XXXV Brazilian Symposium on Software Engineering*. ACM, Porto Alegre, RS, Brasil, 263–268.

[23] Ivonildo Pereira Gomes Neto, João Mendes, Waldemar Ferreira, Luis Rivero, Davi Viana, and Sergio Soares. 2024. An LGPD Compliance Inspection Checklist to Assess IoT Solutions. In *Companion Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering*. ACM, New York, NY, USA, 340–350. doi:10.1145/3663529.3663853

[24] Kruthika Paulraj, Nisha Soms, S David Samuel Azariya, Vidhushavarshini Sureshkumar, et al. 2023. Smart healthcare monitoring system: Integrating IoT, deep learning, and XGBoost for real-time patient diagnosis. In *2023 OITS International Conference on Information Technology (OCIT)*. IEEE, IEEE, Piscataway, NJ, USA, 708–713.

[25] Ivonildo Pereira, João Mendes, Davi Viana, Luis Rivero, Waldemar Ferreira, and Sergio Soares. 2022. Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal. In *Trilha da Indústria - Congresso Brasileiro de Software: Teoria e Prática (CBSOFT), 13*. SBC, Uberlândia, Brazil, 28–31. doi:10.5753/cbsoft_estendido.2022.226679

[26] Lucas Dalle Rocha, Geovana Ramos Sousa Silva, and Edna Dias Canedo. 2023. Privacy compliance in software development: A guide to implementing the LGPD principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. ACM, New York, NY, USA, 1352–1361.

[27] Pattaraporn Sangaroonsilp, Hoa Khanh Dam, Morakot Choetkiertikul, Chaiyong Ragkhitwetsagul, and Aditya Ghose. 2023. A taxonomy for mining and classifying privacy requirements in issue reports. *Information and Software Technology* 157 (2023), 107162.

[28] Jahanzeb Shahid, Rizwan Ahmad, Adnan K Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M Almuhaideb. 2022. Data protection and privacy of the internet of healthcare things (IoHTs). *Applied sciences* 12, 4 (2022), 1927.

[29] Anastasiia Strielkina, Oleg Illiashenko, Marina Zhydenko, and Dmytro Uzun. 2018. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, IEEE, Piscataway, NJ, USA, 67–73.

[30] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–15.

[31] Bedir Tekinerdogan, Ömer Köksal, and Turgay Çelik. 2023. System architecture design of IoT-based smart cities. *Applied Sciences* 13, 7 (2023), 4173.

[32] Geethapriya Thamilarasu, Adedayo Odesile, and Andrew Hoang. 2020. An intrusion detection system for internet of medical things. *IEEe Access* 8 (2020), 181560–181576.

[33] Philip Andreas Weber, Nan Zhang, and Haiming Wu. 2020. A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research* 20, 3 (2020), 565–587.

[34] Jori Winderickx, Pierre Bellier, Patrick Duflot, and Nele Mentens. 2021. Communication and security trade-offs for battery-powered devices: a case study on wearable medical sensor systems. *Ieee Access* 9 (2021), 67466–67476.