UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

IVONILDO PEREIRA GOMES NETO

Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT

Recife

2022

IVONILDO PEREIRA GOMES NETO

Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT

Trabalho apresentado ao Programa de mestrado acadêmico do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da computação.

Área de Concentração: Engenharia de software e linguagens de programação.

Orientador (a): Sérgio Castelo Branco Soares

Coorientador (a): Waldemar Pires Ferreira Neto

Recife

2022

Catalogação na fonte
Bibliotecária Nataly Soares Leite Moro, CRB4-1722

G633e Gomes Neto, Ivonildo Pereira
Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT / Ivonildo Pereira Gomes Neto. – 2022.
109 f.: il., fig.

Orientador: Sérgio Castelo Branco Soares.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2022.
Inclui referências e apêndices.

1. Engenharia de software e linguagens de programação. 2. LGPD. 3. IoT. 4. Checklist de inspeção. I. Soares, Sérgio Castelo Branco (orientador). II. Título

005.1 CDD (23. ed.) UFPE - CCEN 2022 – 104

Ivonildo Pereira Gomes Neto

“Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT”

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Engenharia de Software e Linguagens de Programação.

Aprovado em: 15/03/2022.

BANCA EXAMINADORA

_____

Prof. Dr. Kiev Santos da Gama
Centro de Informática/UFPE

_____

Prof. Dr. Luis Jorge Enrique Rivero Cabrejos
Departamento de Informática/UFMA

_____

Prof. Dr. Sérgio Castelo Branco Soares
Centro de Informática/UFPE
(**Orientador**)

AGRADECIMENTOS

Primeiramente agradeço a Deus pela saúde e a realização de mais um sonho.

Agradeço aos meus orientadores, Sérgio Soares e Waldemar Neto, por todo ensinamento e paciência durante todo esse processo de aprendizagem, resultando no meu crescimento acadêmico e profissional. Sinto uma imensa satisfação em ter recebido a oportunidade de trabalhar com eles.

Agradeço também a minha família que sempre me incentivou e me apoiou em todos os momentos da minha vida.

Quero agradecer também a um grande amigo, Matheus Barbosa, por todo apoio durante toda essa trajetória.

Agradeço também a Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), pelo suporte financeiro através da bolsa de mestrado.

RESUMO

Com os atuais avanços digitais, a sociedade torna-se mais dependente da tecnologia. Para acompanhar estes avanços, o investimento na segurança das informações passa a ser cada vez mais necessário. Isto não é diferente para no contexto da IoT (do inglês, *Internet of things*), pois ela traz diversos benefícios para o cotidiano tanto de pessoas como empresas, pois diversos projetos na IoT tratam diversos dados pessoais. Diante disso, se faz necessária certa proteção de informações relacionadas. No Brasil, a Lei Geral de Proteção dos Dados (LGPD) legisla sobre a gestão da segurança da informação. Este trabalho visa propor um mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas de IoT. Inicialmente, identificamos trabalhos sobre o impacto da LGPD no desenvolvimento de soluções brasileiras de IoT. Foi realizada uma revisão sistemática da literatura (RSL) para identificar artigos relevantes. Posteriormente, estendemos um checklist de inspeção proposto para avaliar sistemas de software em relação à conformidade com a LGPD. Nossa extensão incluiu atributos para avaliar soluções de IoT. A avaliação ocorreu em uma instituição privada ligada à inovação industrial. Consideramos que esse é o perfil do público-alvo do mecanismo proposto. A avaliação foi conduzida como um estudo de caso onde, após inspeção de possíveis falhas de segurança no sistema da empresa, foi aplicado um questionário de pós-inspeção com o mecanismo proposto. Este questionário avaliou a facilidade em usá-lo e a intenção dos participantes em utilizá-lo em outros sistemas. Por fim, ocorreu um grupo focal, onde foram discutidos benefícios, pontos críticos e melhorias aplicáveis ao *checklist*. Foram apresentadas opiniões positivas sobre o uso do mecanismo proposto. Os participantes conseguiram utilizá-lo sem grandes problemas. Além disso, foi possível encontrar defeitos de segurança nos sistemas. Os participantes consideraram o mecanismo como de grande utilidade para guiar os profissionais nas soluções dos defeitos encontrados. Conclui-se que o mecanismo proposto é capaz de auxiliar profissionais na averiguação de adequação à LGPD em projetos que envolvem IoT à LGPD. O estudo foi realizado em uma instituição específica, identificando defeitos reais de uma empresa. No entanto, os resultados não podem ser generalizados. É necessário replicações do estudo para identificar se esses resultados se aplicam a outras empresas.

Palavras-chaves: LGPD; IoT; checklist de inspeção.

ABSTRACT

With the current digital advances, society has become more dependent on technology. To keep up with these advances, investment in information security becomes increasingly necessary. This is no different in the context of the IoT (Internet of things), as it brings several benefits to the daily lives of both people and companies, as several IoT projects deal with different personal data. Given this, some protection of related information is necessary. The General Data Protection Law (Lei Geral de Proteção dos Dados - LGPD) legislates information security management in Brazil. This work aims to propose a mechanism to verify the adequacy of the LGPD considering the specific characteristics of IoT. Initially, we identified works on the impact of LGPD on the development of Brazilian IoT solutions. A systematic literature review (SRL) was performed to identify relevant articles. Subsequently, we extended a proposed inspection checklist to assess software systems for LGPD compliance. Our extension included attributes for evaluating IoT solutions. The evaluation took place in a private institution linked to industrial innovation. We consider this to be the target audience profile of the proposed mechanism. The review was conducted as a case study where, after inspection of possible security flaws in the company's system, a post-inspection questionnaire was applied with the proposed mechanism. This questionnaire evaluated the ease of using it and the participants' intention to use it in other systems. Finally, a focus group took place, where benefits, critical points, and improvements applicable to the checklist were discussed. Positive opinions were presented on the use of the proposed mechanism. The participants were able to use it without considerable problems. In addition, it was possible to find security defects in the systems. Participants considered the mechanism very useful to guide professionals in solving the defects found. It is concluded that the proposed mechanism can assist professionals in verifying the adequacy of the LGPD in projects that involve IoT to the LGPD. The study was carried out in a specific institution, identifying actual defects of a company. However, the results cannot be generalized. The study's replication is needed to determine whether these results apply to other companies.

Keywords: LGPD; IoT; inspection checklist.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A tecnologia está em constante crescimento, progressivamente as atividades passam a se tornar mais dependentes da modernização tecnológica. Dentre essas modernizações, uma que vem sendo discutida amplamente se refere ao termo *Internet of Things* (IoT), ou "Internet das Coisas". Garg e Dave (GARG; DAVE, 2019) relatam que a IoT estabelece conexões entre os dispositivos de computador que são utilizados através da Internet, possibilitando o envio e recebimento de dados. A IoT é capaz de interligar o mundo físico ao mundo digital, essa interação é feita através de sensores e atuadores, coletando informações que em seguida são armazenadas e processadas. Ao mesmo tempo, a IoT está cada vez mais presente no nosso cotidiano, ao ponto de estarmos nos tornando cada vez mais dependentes dela.

Existem aplicações IoT em diversas áreas como na residência, agricultura, medicina, comunicação sem fio, dentre outros (VARDHINI et al., 2019). Um exemplo de IoT na residência: se uma determinada pessoa estiver viajando e por acaso esquecer o ferro de passar ligado. Ela poderá desligá-lo à distância através de seu dispositivo móvel, sem a necessidade de voltar até a sua casa para realizar esse procedimento. Outro exemplo, essa pessoa será capaz de deixar o seu café da manhã programado para ficar pronto no horário que acordar. Um exemplo bastante utilizado no cotidiano são os *smartwatches*, os relógios inteligentes, que possuem funções extras como contador de passos, monitoramento cardíaco, além de mostrar as horas.

Em uma época onde a informação é muito valiosa, estes equipamentos IoT vêm recolhendo dados pessoais e realizando os tratamentos sobre eles. Desta forma, é de suma importância que haja uma certa proteção dessas informações. De forma que diversas iniciativas vêm investindo cada vez mais na segurança da informação (ANGST et al., 2017).

Na busca de proteção das informações pessoais, ocorreu nos últimos anos o surgimento de leis com o intuito de proteger os dados pessoais (WACHTER, 2018). No Brasil, a Lei Federal nº 13.709/2018 conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) refere-se ao tratamento de informações que apresentam relação com os dados pessoais, podendo ser de pessoa física ou jurídica. Essa regulamentação traz grandes benefícios, permitindo uma maior segurança dos dados pessoais, e o não cumprimento da lei é arrecadado em penalidades (PINHEIRO, 2020). Diante disso, é necessário que todas as empresas brasileiras que trabalham com dados pessoais, estejam em conformidade com a LGPD. Sem que houvesse uma regulamentação, seria mais fácil o uso indevido de dados pessoais e um excesso de coleta e

processamento de dados além do necessário, podendo causar transtornos para os indivíduos que tiveram seus dados pessoais coletados. (SOUZA et al., 2020).

As leis de proteção de dados (incluindo a LGPD) impactam fortemente aplicações que fazem uso de equipamentos IoT (OLIVEIRA et al., 2019). Isso se deve ao fato destes equipamentos poderem acessar dados sensíveis, dessa forma sendo necessários mecanismos de proteção para os dispositivos. Proteger as informações de acordo com os fundamentos e os princípios previstos na LGPD é um grande desafio. Este desafio é ainda maior quando se refere a proteger dados que são acessados por dispositivos IoT. Especialmente pelo fato da LGPD não possuir definições técnicas em relação às formas de proteção de tais equipamentos. A lei faz referência a boas práticas, deixando por conta do responsável pelo controle dos dados definir mecanismos para fazer com que os dados acessados pelos equipamentos sejam protegidos.

Inicialmente foi realizado um estudo exploratório com o intuito de identificar artigos que abordavam métodos utilizados por empresas para verificar a conformidade com a LGPD. Simultaneamente, fizemos uma pesquisa sobre artigos que abordam métodos para proteção dos dispositivos IoT. O estudo exploratório aconteceu em duas bases de dados, IEEE e ACM. A pesquisa aconteceu com as palavras chaves: IoT, LGPD, *security*, *company* e sinônimos. Nesta pesquisa preliminar focamos especialmente nas seções: objetivos, resumo do artigo e os trabalhos futuros. Enquanto a pesquisa exploratória sobre os temas relevantes para esta pesquisa, houve reuniões com profissionais de um instituto de inovação privado que trabalham com IoT com o objetivo de entender possíveis problemas. Estes profissionais mostraram-se bastante receptivos no tocante à temática da pesquisa e sugerindo a criação de um mecanismo de inspeção que avaliasse se a empresa estava em conformidade com a LGPD. Em particular, os profissionais reforçaram limitações em encontrar métodos de proteção dos dispositivos IoT. Neste contexto, um dos artigos da pesquisa exploratória se destacou, Mendes et al. (MENDES; VIANA; RIVERO, 2021). Neste artigo, os autores desenvolveram um mecanismo de inspeção para avaliar os sistemas de softwares em relação a aderência a LGPD. Visando enriquecer o resultado desta pesquisa como um todo, realizamos uma parceria com os autores do estudo Mendes et al. (MENDES; VIANA; RIVERO, 2021). Os autores relataram que estavam trabalhando na segunda versão do mecanismo de inspeção. Diante disso, foi realizado o alinhamento das pesquisas e uma parceria entre pesquisadores da UFPE e da UFMA.

1.1 OBJETIVOS

Considerando o que foi discutido na seção anterior, percebe-se a necessidade de investigar maneiras de auxiliar projetos que envolvem dispositivos IoT de forma que os tratamentos e manipulações sobre informações que são realizadas por estes dispositivos estejam feitas em conformidade com a LGPD. Diante disso, este estudo tem como objetivo propor um mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT.

Visando o objetivo apresentado, foram propostas duas perguntas de pesquisa que uma vez respondidas alcançam nosso objetivo geral:

Q1. Como propor um *checklist* de inspeção de soluções computacionais específicas de IoT frente a LGPD?

Q2. O *checklist* proposto ajuda na identificação de problemas em relação à soluções computacionais específicas de IoT frente a LGPD?

1.2 ESTRUTURA DA DISSERTAÇÃO

- Capítulo 2 tem como objetivo apresentar a fundamentação teórica que teve como base para a realização deste trabalho.
- Capítulo 3 descreve o processo para concepção do mecanismo de inspeção para aderência de sistemas à LGPD. Posteriormente, apresenta a atualização da revisão sistemática sobre LGPD focando somente em IoT. Em seguida apresenta a extensão proposta considerando os trabalhos específicos para auxiliar a averiguação de adequação à LGPD, considerando as características específicas com IoT. É apresentado o procedimento de coleta e análise dos dados, elaboração do mecanismo de averiguação da conformidade de projeto que envolve IoT.
- Capítulo 4 apresenta os resultados da avaliação do mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT. Apresentando os resultados do questionário para identificar a viabilidade do mecanismo de inspeção proposto em termos de utilidade, facilidade e intenção de uso. Também apresenta os resultados da análise das discrepâncias das respostas dos participantes e os resultados de um grupo focal com os participantes debatendo as discrepâncias das respostas.

- Capítulo 5 tem o objetivo de apresentar as conclusões atingidas por este estudo. Posteriormente, descreve as limitações e ameaças a validade. Em seguida, é apresentado os trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma visão geral dos principais conceitos sobre a LGPD e a IoT. Também apresenta problemas de segurança e vulnerabilidades dos dispositivos IoT, com ênfase em aspectos importantes para uma melhor compreensão do problema abordado nesta dissertação. A Seção 2.1 apresenta um breve resumo do surgimento da LGPD. Na Seção 2.2, são apresentadas algumas relações preliminares entre a LGPD e os dispositivos IoT. A seção 2.3 aborda algumas das boas práticas de segurança incluídas na LGPD. Seção 2.4 descreve os conceitos mais relevantes sobre IoT que são tratados nesta pesquisa. Na seção 2.5 apresenta problemas de segurança na internet. Por fim, na seção 2.6 são apresentados e discutidos os trabalhos relacionados.

2.1 SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

As leis de proteção de dados tornaram-se um assunto popular nos últimos anos, apesar de se tratar de debate discutido há décadas.

Desde a década de 70 até os dias atuais, houve mudanças significativas. Leis que tinham o intuito de proteger os dados tornaram-se antiquadas visto o grande avanço dos centros que realizavam os processamentos dos dados, tornando assim ineficiente a maneira como os órgãos públicos trabalhavam com autorizações e acompanhamentos detalhados (DONEDA, 2011).

No ano de 2012 surgiu a *General Data Protection Regulation* - (GDPR), entrando em vigor apenas no ano de 2018. A GDPR é um dos regulamentos de proteção de dados mais rigorosos em relação às leis da União Europeia, tendo como objetivo a proteção dos dados pessoais (GOBEO; FOWLER; BUCHANAN, 2020). A GDPR é responsável por realizar o tratamento de dados da União Europeia, o que foi um grande incentivo para diversos países, principalmente aqueles que pretendiam vincular-se comercialmente com a União Europeia, sendo necessário possuir regulamentações semelhantes, caso contrário, operações econômicas seriam canceladas (PINHEIRO, 2020). Diversos países criaram suas leis de proteção de dados inspirados na GDPR, inclusive o Brasil.

No Brasil, A LGPD Lei n. 13.709/2018, foi aprovada em agosto de 2018 e entrou em vigor em agosto de 2020. É a lei brasileira que através de suas regulamentações, impõe regras para o tratamento de dados pessoais, podendo ser por pessoa física ou jurídica e abrangendo tanto

as instituições públicas como as privadas (PINHEIRO, 2020). Com a criação da LGPD, o Brasil faz parte de um conjunto com mais de 120 países que desenvolveram leis para proteção dos dados (CHAGAS; BIAZOTTO, 2021).

A privacidade dos dados pessoais, trata-se de direito constitucional, desde as Leis 12.965/2014 que tinha o objetivo de realizar o regulamento de uso da internet no Brasil e a Lei 8.078/1990 com propósito da proteção aos direitos do consumidor (GARCIA et al., 2020). Comparando a LGPD com essas duas leis citadas anteriormente, destaca-se que a Lei 12.965/2014 tem suas normas com o foco nos direitos e deveres das pessoas na internet, enquanto a LGPD faz uma aplicação na segurança da privacidade dos dados, sendo mais específica, com suas normas em todo processamento de dados, protegendo também a privacidade das pessoas que não estão conectadas à internet. De acordo com o trabalho de Follone e Filho (FOLLONE; FILHO, 2020) a Lei 12.965/2014 está concentrada no consumidor e fornecedor em relação ao mercado econômico. Enquanto a LGPD se concentra na relação entre os dados pessoais dos titulares em relação ao controlador desses dados, outras leis de privacidade também foram implementadas, como a Constituição Federal, a Lei de Acesso à Informação, a Lei do Habeas Data e o Decreto do Comércio Eletrônico (GARCIA et al., 2020).

A LGPD impacta diretamente às empresas em diversos setores, um exemplo é a folha de pagamento que possui dados pessoais, sendo necessário as empresas certificar-se de que estão seguindo os fundamentos e princípios propostos pela lei. O não cumprimento dessas determinações poderá acarretar em multas.

A LGPD através dos seus fundamentos e princípios conduz as empresas a realizar o tratamento e proteção de dados, porém, seguir essas normas não garante que a empresa esteja totalmente protegida e não poderá ocorrer vazamento de dados. Mas estando em aderência com a LGPD, se por acaso ocorrer um vazamento de dados, a punição recebida pela empresa será mais leve (CHAGAS; BIAZOTTO, 2021).

2.2 RELAÇÃO ENTRE AS LEIS DE PROTEÇÃO DE DADOS E OS DISPOSITIVOS IOT

Dispositivos IoT são capazes de realizar a coleta de diversos dados do usuário, como nome, CPF e dados de cartão de crédito. Os dispositivos IoT também são capazes de coletar dados do ambiente onde estiverem alocados, como temperatura. Os dados coletados nesses equipamentos podem ser enviados para desconhecidos, sem permissão do usuário, se este define seus dispositivos portáteis para modo de transmissão. Poderá ser conectado em outros equipa-

mentos que estiverem em alcance para estabelecerem uma conexão, podem enviar solicitações inseguras e oferecer acesso aos dados pessoais.

Possuir uma proteção eficaz que os dispositivos possam suportar é uma grande preocupação, principalmente porque os dados pessoais estão contidos nesses equipamentos e os usuários querem um nível alto de proteção que seja eficaz para proteção dos seus dados (BARATI et al., 2020). Ainda de acordo com o autor, as leis de proteção de dados surgem com fundamentos para fornecer o direito da privacidade dos dados das pessoas, não permitindo que as empresas que realizam os tratamentos de dados forneçam informações pessoais para outras empresas sem a permissão dos titulares desses dados. Dessa forma, antes da realização do processamento de dados, leis de proteção de dados como a LGPD pedem o consentimento dos usuários, sendo legalmente proibidos de realizar qualquer coleta de dados sem autorização e dando aos usuários pleno direito de manipular seus dados por meio desses dispositivos inteligentes. Ou através de outros meios eletrônicos que tenham conectividade com esses dispositivos, permitindo que os usuários acessem seus dados.

De acordo com Oliveira et al. (OLIVEIRA et al., 2019), as leis de proteção de dados impactam os dispositivos IoT, porque é necessário criar mecanismos de proteção para estes dispositivos. Não é apenas seguir todos os procedimentos formais, como por exemplo: seguir todas as etapas de consentimento do titular de dados. É preciso proteger todo o ambiente contra possíveis invasões à privacidade de dados. Se, após a coleta dos dados em um dispositivo, os dados forem enviados para um local onde serão utilizados diversos mecanismos de segurança, o sistema está visualmente protegido. Porém, se o equipamento estiver comprometido e enviando cópia dos dados para outro destino indevidamente, contém vazamentos de dados. Diante disso, é importante realizar uma análise minuciosamente para proteger o equipamento.

A LGPD não possui definições técnicas em relação à proteção dos equipamentos, mas essa lei faz referência a boas práticas de segurança, deixando por conta do responsável pelo controle dos dados criar mecanismos para proteger os equipamentos. Os responsáveis pelo tratamento de dados poderão: criar as normas de segurança; desenvolver os padrões técnicos; criar métodos educativos para seus funcionários; criar métodos de supervisão do tratamento de dados, entre outros procedimentos técnicos e administrativos que podem ser realizados pelo responsável pelos dados a estarem em concordância com a LGPD.

Diferente dos *smartphones* atuais que possuem interface gráfica para o usuário, facilitando a interação e compreensão do funcionamento, alguns dispositivos IoT não possuem interface, apenas sons e luzes, o que dificulta entender qual coleta de dados o dispositivo está fazendo

ou como essas informações serão usadas (URQUHART; LODGE; CRABTREE, 2019). Dispositivos IoT sem interface gráfica necessitam do consentimento do usuário para estar em conformidade com a lei brasileira. Conectar este dispositivo com outro equipamento, como o celular, pode ser uma alternativa para facilitar que o usuário assine o consentimento. A LGPD deixa claro que o consentimento deve ser fornecido através de uma escrita compreensível, não contendo nenhum conteúdo enganoso ou que incite o titular dos dados ao erro, conhecido como "vício de consentimento".

2.3 LGPD E SUAS BOAS PRÁTICAS DE SEGURANÇA

Há anos recomenda-se a criação e uso de boas práticas de segurança de dados, no entanto poucas organizações aderiram às recomendações, visto que as empresas devem fazer investimentos financeiros, em recursos humanos e tecnológicos (POHLMANN, 2020). Após a criação da LGPD, será necessário que as organizações implementem boas práticas, o não cumprimento poderá acarretar em problemas, como o recebimento de multas (CHAGAS; BIAZOTTO, 2021).

Os responsáveis por realizar o tratamento dos dados são responsáveis pela criação dos métodos de segurança, atribuindo técnicas para proteger os dados pessoais contra qualquer acesso indevido e qualquer outro tipo de vazamento de dados ou alteração. Diante disso, para uma empresa está adequada, é necessário investir na segurança técnica, visto que se empresa estiver aparentemente adequada a LGPD mas com problemas internos de segurança e acabar ocorrendo vazamento de dados, a empresa poderá se prejudicar judicialmente, além de afetar os usuários que tiveram seus dados vazados. Se por acaso ocorrer algum incidente de segurança, que possa causar danos ou risco aos titulares, como o vazamento dos dados pessoais, a empresa deve comunicar a autoridade nacional e ao titular, descrevendo o incidente, especificando quais dados foram vazados, quais medidas técnicas de segurança estavam sendo utilizadas e também as medidas que a empresa realizará. Com isso, todo esse procedimento entrará em consideração na apuração do vazamento de dados, podendo assim identificar qual foi a causa e se a empresa foi declarada culpada poderá receber penalizações.

2.4 INTERNET OF THINGS - IOT

O termo IoT é utilizado para representar objetos físicos que conseguem interagir entre eles através da *internet*. Ashton et al. (ASHTON et al., 2009) em uma apresentação na Procter &

Gamble (P&G), pronunciou pela primeira vez o termo "*Internet of Things*" (IoT), em 1999. Unindo a ideia entre a *Radio Frequency Identification* (RFID) com a cadeia de suprimentos da P&G.

A recomendação ITU-T Y.2060 descreve internet das coisas como uma infraestrutura mundial que fornece serviços para a sociedade ao conectar as "coisas" (a parte física e a virtual) e que estão em constante evolução. A IoT tem a habilidade de tornar dispositivos comuns em dispositivos inteligentes, tendo a capacidade de se comunicarem com outros dispositivos comuns através da rede e tomarem decisões por conta própria (AL-FUQAHA et al., 2015).

Para Atzori et al. (ATZORI; IERA; MORABITO, 2010) a internet das coisas é a junção em parte desses três termos:

- **Conduzindo a internet** – Conduzindo a internet, está relacionado a IPSO (*IP for Smart Objects*). Alliance foi uma organização formada por 25 empresas no ano de 2008. Organização de comunicação responsável por proporcionar o protocolo capaz de conectar objetos inteligentes (GERSHENFELD; KRIKORIAN; COHEN, 2004).

- **Conduzindo as coisas** – As "coisas" são os objetos eletrônicos comuns. Quando foi estabelecido o primeiro conceito de IoT, as coisas eram identificadas como objetos comuns, como: etiquetas de identificação por radiofrequência (RFID) (PRESSER; GLUHAK, 2009).

- **Conduzindo a semântica** – A semântica está relacionada aos desafios das organizações dos dados criados pelos sistemas IoT, visto que os dispositivos IoT produzem bastante informações sem organização, este problema pode ser solucionado através de tecnologias semânticas (TOMA; SIMPERL; HENCH, 2009).

Os equipamentos IoT podem se conectar na internet através de tecnologias como WI-FI e bluetooth, desta forma, permitindo o acesso remoto a computadores que podem estar em outro ambiente e controlar esses equipamentos através do acesso a internet. Todo equipamento conectado à internet pode ser manuseado e controlado a distância.

Wazid et al. (WAZID et al., 2019) relata sobre os resultados de um relatório, onde foi publicado que os dispositivos IoT no geral, alcançarão a um trilhão de dispositivos conectados até o ano de 2025, no artigo de Chen et al. (CHEN et al., 2020), é mencionado que o relatório do McKinsey Global Institute, relatada a mesma visão para 2025. Quadro 1 apresenta o aumento no número de dispositivos ao longo das décadas.

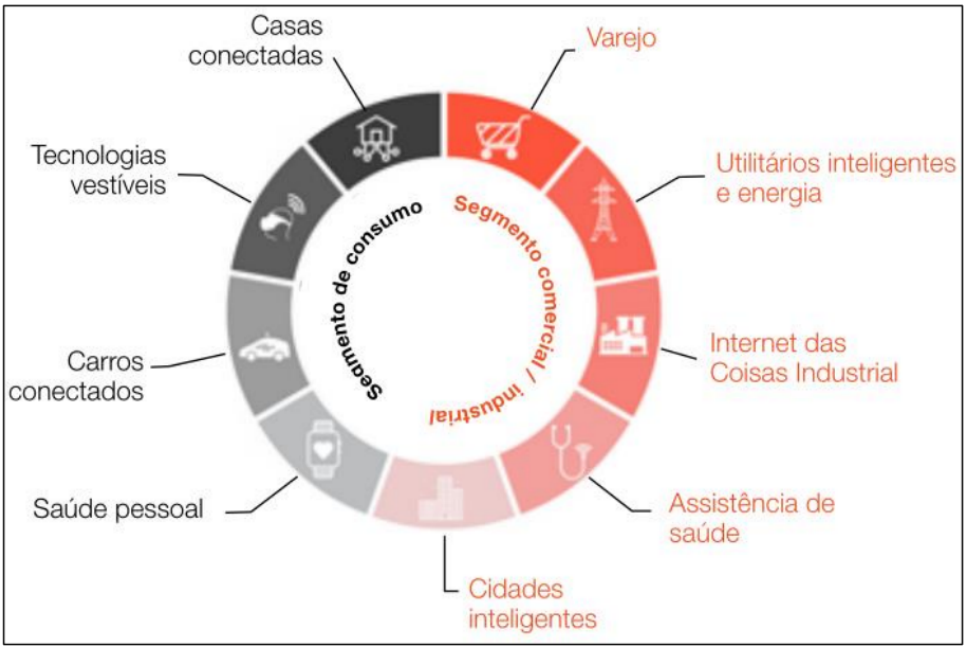
Quadro 1 – Estimativa da quantidade de dispositivos.

Ano	Números dos dispositivos conectados
1990	3 milhões
1999	9 milhões
2010	1 bilhão
2013	9 bilhões
2025	1 trilhão

Fonte: Adaptado de (KHANDELWAL, 2019a).

A IoT traz diversos benefícios, facilitando a vida das pessoas em diversas áreas, como na indústria, na saúde (hospitais, clínicas, equipamentos monitoramento pessoal), acompanhamento ambiental, automação residencial, e mobilidade urbana (MENEGHELLO et al., 2019). Figura 1 demonstra a aplicações IoT em diversificadas áreas da sociedade.

Figura 1 – Aplicações IoT



Fonte: (LEITE, 2019).

A IoT através das trocas de informações entre os equipamentos, consegue automatizar os processos, tomando decisões que poderiam ser bem mais burocráticas se dependesse da intervenção de um humano (LEITE, 2019). Por exemplo, na área da produção alimentar através da agricultura, para ocorrer uma boa produtividade pode ser utilizado dispositivos IoT para monitoramento da umidade do solo e previsão do tempo, com o intuito de identificar qual

o melhor momento e localidades para realizar a irrigação. Desta forma, os dispositivos são capazes de realizarem as decisões (PEREIRA, 2020).

Na área industrial, altos investimentos são feitos e os componentes eletrônicos estão trabalhando 24 horas por dia, melhorando a produtividade, os processos internos automatizados, podendo diminuir o índice de erros nas operações, e reduzindo custos. De acordo com Lohan et al. (LOHAN et al., 2018), os dispositivos IoT estão sempre evoluindo a indústria, surgindo mais tecnologias que conseguem automatizar os processos, como drones e robôs de fábrica. A indústria desenvolve soluções IoT para todas as áreas onde podem ser aplicáveis.

Na saúde, equipamentos inteligentes conseguem proporcionar a coleta de informações de forma confiável, não necessitando de um profissional da área para realizar o processo. Também são capazes de realizar monitoramento de pacientes (GOMES, 2019).

Nas cidades inteligentes, os autores Barrionuevo et al. (BARRIONUEVO; BERRONE; RICART, 2012), Kourtit et al. (KOURTIT; NIJKAMP; ARRIBAS, 2012) e Zygiaris (ZYGIARIS, 2013) relatam que são conhecidas pela inclusão da infraestrutura digital em diversas áreas, como por exemplo no desenvolvimento urbano, sustentabilidade ambiental e inclusão social. Existem diversas aplicações relacionadas com as cidades inteligentes, e muitas plataformas a serem desenvolvidas (BARANAUSKAS; SOUZA; PEREIRA, 2012).

2.4.1 Privacidade do usuário de IoT

Os dispositivos IoT são capazes de realizar a coleta de diversas informações, como os dispositivos pessoais que conseguem coletar batimentos cardíacos, pressão arterial e demais informações do usuário (YANG; FORTE; TEHRANIPOOR, 2015). Para exemplificar a gravidade do risco que as pessoas podem sofrer quando um equipamento é invadido, se um equipamento voltado para o gerenciamento de medicamentos em humano for comprometido, poderá ser uma grande ameaça a vida do usuário, o invasor poderá alterar o equipamento, como por exemplo a modificação de dosagem de uma bomba de insulina (GUO et al., 2016).

O risco de vazamento de dados, não está ligado apenas aos dados pessoais, é de grande importância a proteção de qualquer informação que envolva o usuário, um exemplo pode ser dado através de um sistema de automação residencial, onde existem sistemas que oferecem algumas funcionalidades, através de sensores de luzes para identificar se possui alguém naquela localidade. Se um sistema desse é invadido, o sujeito mal intencionado que causou essa invasão poderá criar uma análise do usuário, identificando todos os hábitos (WURM et al., 2016).

2.4.2 Desafio dos dispositivos restritos

Um dos grandes desafios dos equipamentos IoT é a segurança dos dispositivos com restrições em memória e processamento, esses dispositivos não conseguem utilizar mecanismos de proteção com grande eficiência, visto que são dispositivos de pequeno porte. Com isso, devem ser analisados minuciosamente os recursos dos equipamentos e criar mecanismos de proteção para cada situação específica.

Bormann et al. (BORMANN; ERSUE; KERANEN, 2014) classifica os dispositivos restritos, os definem em três classes, sendo elas: 0,1,2. A classe 0 contém uma maior restrição e é a que possui o maior desafio em relação à segurança. Essa classe está relacionada a sensores, sendo dispositivos com tão pouco poder de processamento e pouca memória que geralmente não conseguem fazer conexões seguras com a internet. A classe 1, possui restrição alta, mas conseguem utilizar protocolos específicos para equipamentos restritos, como o protocolo CoAP. A classe 2, possui menor restrição, contém mais capacidade de processamento, conseguindo utilizar pilhas de protocolos idênticas às que são usadas em equipamentos como servidores e notebooks.

2.5 PROBLEMAS DE SEGURANÇA

É importante entender os perigos que se escondem na internet. É fato que a internet traz benefícios imensuráveis, facilitando a vida do ser humano. Entretanto, o sistema não é perfeito e apresenta falhas. Do mesmo modo que existem programas que aproximam as pessoas ou fazem a segurança dos seus dados, por assim dizer, também existem programas maliciosos que prejudicam os dados dos usuários. Vivemos em uma era onde a informação vale muito, diante disso é necessário identificar quando algo não é confiável, e assim obter maiores proteções (KHASHIROVA et al., 2021). Diante disso, neste capítulo será apresentado sobre o impacto dos problemas de segurança, destacando os principais mecanismos responsáveis por vazamento de dados.

2.5.1 Vazamento de dados

O termo vazamento de dados ou "perda de dados", significa que dados foram divulgados sem autorização (ALNEYADI; SITHIRASENAN; MUTHUKKUMARASAMY, 2016). Podendo aconte-

cer intencionalmente ou acidentalmente (HUANG et al., 2018).

O vazamento de dados cada vez mais está sendo expandido, causando uma grande ameaça à segurança das informações empresariais e pessoais (GARG; DAVE, 2019). Ao ocorrer vazamento de dados de uma empresa, poderá acontecer o comprometimento de dados confidenciais, como projetos em andamento, segredos comerciais e os perfis dos clientes. Clientes podem ser afetados quando ocorre o vazamento dos seus dados, porém é difícil identificar a quantidade de prejudicados e qual a gravidade do vazamento desses dados, porque podem utilizar os dados de diferentes maneiras (ALNEYADI; SITHIRASENAN; MUTHUKKUMARASAMY, 2016).

Os cidadãos ao firmar um serviço ou compra com uma determinada empresa, fornecem os seus dados pessoais, como e-mail, nome completo, RG, CPF e dados de cartão de crédito. A segurança desses dados pessoais devem ser prioridade para as empresas. Quando ocorre vazamento de dados em uma empresa, o conceito dela diminui, podendo perder valor de mercado (MACHADO et al., 2019). Ocorrerá insatisfação dos clientes, além das pessoas não fornecerem confiança na empresa. Além disso, o mais prejudicado é o cliente, pois ao ter seus dados divulgados, pode ser vítima de diversos golpes, como por exemplo, utilizarem seu cartão de crédito para compras indevidas.

O vazamento de dados de uma empresa pode ser algo catastrófico, sendo expostas informações de muitas pessoas, é um grande risco aos titulares dos dados, podendo causar transtornos e prejuízos. Um exemplo foi o ocorrido em 2019, quando aconteceu o vazamento de dados de 2,4 milhões de usuários, após os dados de uma empresa que trabalham com gerenciamento de senhas serem comprometidas, ocorreu o vazamento de muitas informações, como nome dos usuários, endereço do IP de suas máquinas e seus e-mails (PARENT, 2019).

São diferentes os setores no qual indivíduos mal intencionados realizam invasões para recolherem dados pessoais, como na área da saúde, em setores de hospitais, laboratórios, no qual contém muitos dados pessoais e são os principais alvos, porque essas informações podem ser vendidas na *dark web* com mais facilidade (RILEY, 2019).

Um vazamento ocorrido no Brasil, mais especificamente no Rio Grande do Sul, foi no sistema do Detran (Departamento Estadual de Trânsito) onde foram vazados dados dos registros de Carteira Nacional de Habilitação (CNH) de 70 milhões de pessoas. Sendo possível o acesso indevido de dados como, número da CNH, RG, placa do veículo e multas (BRASILINE, 2019).

Na área de restaurante, um caso que gerou repercussão foi o caso dos 103 restaurantes da franquia Checkers and Rally's que continham um *malware* recolhendo os dados de cartão

de créditos dos clientes, esse software malicioso só foi descoberto após três anos recolhendo dados pessoais dos clientes (KHANDELWAL, 2019b).

Quando ocorre vazamento de dados de cartão de crédito, é difícil identificar qual organização foi responsável pelo vazamento dessas informações, visto que as pessoas utilizam cartões de crédito em diversos serviços e a responsabilidade da proteção dessas informações é da organização que está realizando o tratamento desses dados.

2.5.2 *Malware*

Malware ou *software* malicioso é um programa tecnológico que tem a intenção de prejudicar um sistema, é uma grande ameaça à segurança dos equipamentos conectados a internet (POONIA; SINGH, 2014). De acordo com Chandramohan e Tan (CHANDRAMOHAN; TAN, 2012) é um dos maiores problemas contra a segurança nas redes de internet. São inúmeros métodos de ataques utilizando *softwares* maliciosos, a grande preocupação antes era apenas com computadores, mas com o passar do tempo, os dispositivos também se tornaram alvos dos cibercriminosos, visto o grande crescimento dos dispositivos IoT e a rápida evolução dos seus sistemas, onde muitas pessoas mal intencionadas desenvolvem diversos mecanismos com o intuito de invadir essa tecnologia. Esses ataques aos sistemas IoT, podem causar grandes prejuízos, como roubos de informações e alteração aos dados (WAZID et al., 2019).

Diante desse grande avanço dos dispositivos IoT, os cibercriminosos começaram a investigar os dispositivos IoT para fins ilícitos. Um grande problema é que na criação de *firmware* utilizados em diversos dispositivos IoT, não foram levadas em consideração as boas práticas de segurança dos desenvolvedores experientes, com isso, diversos ataques ocorreram nas diversificadas plataformas de IoT (VIGNAU; KHOURY; HALLé, 2019). É de grande importância a detecção dos *softwares* maliciosos o mais rapidamente possível. Conseguir identificar um *malware* é um processo árduo, à medida que os criadores são cada vez mais experientes e desenvolvem cada vez mais métodos que tornam difícil encontrar os programas maliciosos (SARACINO et al., 2018).

O *malware* deve ser detectado o mais cedo possível, antes de causar qualquer dano ao sistema em diversos ambientes, como por exemplo, na indústria, podendo ter prejuízos significativos, como perda de dados que acarretará em perdas financeiras e perda de informações importantes da indústria (MANSFIELD-DEVINE, 2012).

Uma solução para a detecção de *malware*, é a utilização de *softwares* anti *malware*. Para os sistemas operacionais como windows, IoS, entre outros. Possuir um *software* contra *malware*

não é um problema, diferentemente dos sistemas que possuem poucos recursos, desta forma é um grande desafio encontrar *malwares* em um período limitado de tempo (SHARMEEN et al., 2018). As empresas que trabalham com antivírus, combatem uma enorme quantidade de *malware* cotidianamente (POONIA; SINGH, 2014). Além da detecção por antivírus, em alguns casos o usuário é capaz de perceber os sintomas dos programas maliciosos, como por exemplo: aparecimento de arquivos incomuns, mudança nas configurações do dispositivo, dentre outros comportamentos diferentes, como envio de mensagens automáticas que não deveriam ter sido enviadas (WU et al., 2014) (BOCHIE et al., 2020) (ZHOU; YU, 2018). Porém, o *malware* pode não apresentar nenhum tipo de sintoma e realizar crimes sem demonstrar rastros facilmente visíveis.

O trabalho de Vignau et al. (VIGNAU; KHOURY; HALLé, 2019) apresenta a classificação de *malwares* para IoT, essa pesquisa selecionou através da literatura *malwares* mais prejudiciais aos ambientes IoT, o autor classificou em 15 tipos de *malwares*, sendo eles:

1. Capacidades de negação de serviço – Utiliza diferenciadas técnicas para impedir o funcionamento normal, causando uma negação do serviço. Também é possível destruir fisicamente o equipamento, pode ocorrer eliminando o *firmware* do dispositivo ou causando um sobrecarregamento.

2. Roubo de dados – Os *malwares* também objetivam realizar roubo de dados, infectando o dispositivo e direcionando os dados para o cibercriminoso responsável pelo *malware*.

3. Exploração de endpoint – Esse método é uma forma de invadir outros dispositivos que estejam conectados com um dispositivo IoT que está comprometido por causa da invasão. Esse método pode ser realizado através de vulnerabilidade de um dispositivo ou através de interceptação ilegal na comunicação da rede.

4. Espionagem Industrial – Esse *malware* tem o intuito de conseguir acesso das plantas industriais, inclusive, é capaz de conseguir controlar os dispositivos e identificar sua localização exata. Também é possível encobrir o tráfego malicioso durante a extração de dados.

5. Exploração – Utilização de variadas técnicas para conseguir acesso a dispositivos, um exemplo é a técnica de ataque por força bruta, é uma maneira de conseguir acesso privilegiado através de inúmeras tentativas.

6. Arquitetura Alvo – Certos *Malwares* são projetados para invadir uma determinada arquitetura, beneficiando de falhas que não foram reparadas. Existem *Malwares* criados com o objetivo de conseguir acesso aos dispositivos IoT através de vulnerabilidades que não foram consertadas.

7. Métodos de escaneamento – É utilizado através de *botnets*, são variadas maneiras para realizar um escaneamento na internet com o intuito de identificar novos alvos e infectá-los com o *malware*.

8. Arquitetura de *botnet* – Categorizam as arquiteturas dos *botnets* em três, sendo elas: i) arquitetura centralizada, no qual um servidor se comunica com os *bots*; ii) arquitetura P2P, no qual não existe um servidor centralizado, os *botnets* utilizam os protocolos P2P, que foram criados através do protocolo uTorrent ou através do protocolo *BitTorrent*.

9. Recursos de anti-detecção – Os *malwares* fazem a exclusão dos processos legítimos e aplicam os nomes dos processos legítimos aos novos processos, dessa forma dificultando a sua identificação, desse modo, conseguindo impedir que o *malware* seja apagado com facilidade.

10. Recursos que aumentam a eficiência – Diversos *malwares* são aptos a monopolizar dispositivos, evitando outras infecções e também são capazes de utilizar recursos para os dispositivos não conseguirem reiniciar. Desta forma, sendo o único *malware* a conseguir controlar ilegalmente o dispositivo invadido.

11. Algoritmo de geração de Domínio – São *malwares* que objetivam utilizar algoritmos de geração de domínios para atrapalhar as ações de segurança, impossibilitando as atividades dos servidores.

12. Modularidade do código – Existem *malwares* que quando atualizados recebem novos recursos, podendo realizar ataques de diferentes formas.

13. Varredura de vítima – Os *malwares* possuem habilidade de conferir as arquiteturas dos equipamentos que pretendem conseguir acesso, com o intuito de infectar diversos equipamentos simultaneamente, remetendo variantes dos binários para cada alvo.

14. Evasão da virtualização – Esse *malware* consegue identificar um ambiente virtualizado e se estiver atuando neste ambiente virtualizado, ele se exclui, juntamente com os seus

sistemas de arquivos, dificultando que os profissionais de segurança consigam estudar o código deste *malware*.

15. Mineração de criptografia – Os dispositivos infectados com esse *malware* ficam minerando criptomoedas, é uma ameaça que está em crescimento nos sistemas IoT. Antes essa ameaça estava apenas direcionada para computadores, mas a partir de 2014 foi identificado em dispositivos IoT.

Além desses *malwares*, existem incontáveis *softwares* maliciosos, visto que a qualquer momento desenvolvedores podem criar novos *malwares* ou adaptar os antigos para realização dos seus crimes.

2.5.3 Engenharia social

A engenharia social é um dos meios mais utilizados de obtenção de informações sigilosas e importantes. Isso porque explora com muita sofisticação as falhas de segurança dos humanos. É qualquer método usado para enganar ou explorar a confiança das pessoas para a obtenção de informações sigilosas e importantes. Muitos cibercriminosos atingem seus objetivos através de técnicas de engenharia social. E tudo porque o humano é um ser que, ao contrário dos computadores, é constantemente afetado por aspectos emocionais. A melhor arma contra a engenharia social é a informação. De nada adianta as pessoas usarem sistemas ultra-protegidos se não tiverem ciência dos golpes que podem sofrer. O grande problema é que muitos internautas, independente da idade, estão dando seus primeiros passos na internet e não têm noção dos perigos existentes nela. Muitos ficam maravilhados com a grande rede e tendem a acreditar em tudo que lêem nesse meio (ALVES, 2010).

2.5.4 Vulnerabilidade IoT

Com o avanço exponencial dos dispositivos, a tecnologia ganha mais popularidade, sendo utilizado em diversas áreas e coletando milhares de dados pessoais, consequentemente muitos sujeitos mal intencionados exploram essa tecnologia para conseguir benefícios ilícitos (DHILLON; KALRA, 2017). Atamli e Martin (ATAMLI; MARTIN, 2014) realiza uma classificação dos principais responsáveis pelas ações de má intenção em relação aos sistemas IoT:

1. O usuário maldoso é o dono de um dispositivo IoT, utilizando mecanismo para ter acesso indevido a partes que usuário não possui permissão. Tendo o intuito coletar informações dos fabricantes, podendo utilizar essas informações para benefícios próprios ou vender para terceiros.

2. O invasor externo é aquele que não tem nenhuma permissão de acesso, mas cria mecanismos para invadir e conseguir acesso ao sistema ou equipamento, podendo ter muitas finalidades com seus resultados da invasão, como por exemplo, conseguir acessos aos dados.

3. O fabricante mal intencionado é o oposto do usuário maldoso, no qual ele deseja obter informações do fornecedor, neste caso o fornecedor que deseja os dados do usuário. Com isso, o fabricante mal intencionado pode utilizar de mecanismos para ter acesso a privacidade do usuário através de suas informações ou até mesmo utilizar as informações para tentar invadir outros dispositivos de outras marcas utilizado pelo usuário.

A IoT apresenta muitos desafios de segurança, além de possuir os problemas de segurança da internet, também possui novos problemas específicos de IoT (FURFARO et al., 2017). De acordo com Tekeoglu e Tosun (TEKEOGLU; TOSUN, 2016) é um grande desafio conseguir resolver esses problemas de segurança, porque são diversos dispositivos possuindo uma grande diferença estrutural. Não é possível elencar todas as vulnerabilidades dos dispositivos, visto que a literatura apresenta uma grande quantidade de vulnerabilidades, além disso, sempre surgem novos problemas de segurança, tornando-se incontáveis as vulnerabilidades exigidas. Com isso, destaca-se algumas vulnerabilidades:

1. Criptografia inadequada – A criptografia é capaz de proteger a informação através de métodos, impossibilitando acesso não autorizado, sendo de grande importância a proteção desses dados no ambiente IoT. Dispositivos com pouco poder computacional possuem dificuldades na eficiência e eficácia de métodos de proteção, podendo ser mais fácil que um invasor consiga passar por esses métodos e conseguir acesso ao dispositivo de forma inadequada (NESHENKO et al., 2019).

2. Energia – Para o funcionamento do dispositivo é necessário uma fonte de energia, que geralmente é através de uma bateria de difícil substituição. Se faz necessário mecanismo para geração de energia como energias sustentáveis, e a realização de um gerenciamento

de energia (LEITE, 2019). Um exemplo de ataque relacionado a energia do dispositivo é o ataque "vampiro", esse ataque tem como objetivo consumir os recursos da rede, sendo capaz de drenar a energia, causando uma indisponibilidade nos dispositivos (PATEL; SONI, 2015).

3. Portas abertas desnecessárias – Se o dispositivo possui portas abertas que não são necessárias, torna-se um grande risco, diante disso, todas as funcionalidades que não forem necessárias deverão ser desativadas (SACHIDANANDA et al., 2017). Em casos de portas físicas desnecessárias, essas também devem ser desativadas (GOMES, 2019).

4. Adulteração física – Dispositivos IoT poderão sofrer alterações fisicamente se algum invasor tiver acesso a ele, sendo possível colocar a instalação de algum programa malicioso através de portas visíveis e de fácil acesso (YANG; FORTE; TEHRANIPOOR, 2015).

5. Autenticação inadequada – Os dispositivos que possuem restrições como pouco poder computacional é um desafio para a realização de autenticação, com isso, um criminoso cibernético poderá ser capaz de procurar autenticações ineficientes, criando mecanismo para ter acesso indevido ao dispositivo (NESHENKO et al., 2019).

2.6 TRABALHOS RELACIONADOS

Os trabalhos relacionados a seguir estão divididos em duas Seções, a subseção 2.6.1 apresenta instrumentos em relação a LGPD. De acordo com Raposo et al. (RAPÔSO et al., 2019) existem poucos trabalhos na literatura específicos em realizar uma análise minuciosa da LGPD, o trabalho de Mendes et al. (MENDES; VIANA; RIVERO, 2021) complementa que além da escassez de trabalhos da LGPD, menor é a quantidade relacionada a atributos de qualidade da lei. E trabalhos sobre a LGPD relacionados a segurança em IoT é bem mais específico, consequentemente possuindo menos trabalhos acadêmicos nessa área. Com isso, não foram identificados trabalhos relacionados ao objetivo deste estudo, mas foram identificados trabalhos relacionados ao contexto deste estudo.

Na subseção 2.6.2 que apresenta trabalhos relacionados a boas práticas de segurança para os dispositivos IoT, onde através de um manual os avaliadores consigam identificar problemas de segurança nos equipamentos, sendo semelhante a esta pesquisa que também realiza uma lista de segurança.

2.6.1 Instrumentos de software em relação a LGPD

O trabalho de Mendes et al. (MENDES; VIANA; RIVERO, 2021) desenvolveu e avaliou um *checklist* de inspeção que visa avaliar os sistemas de *softwares* computacionais a estarem em conformidade com a LGPD. Os autores realizaram um mapeamento sistemático da literatura com o intuito de identificar trabalhos acadêmicos com descrições e interpretações de autores sobre a LGPD e métodos para os sistemas computacionais ficarem em conformidade com a LGPD. Mencionaram os poucos trabalhos encontrados em relação a LGPD, diante disso, expandiram a busca para identificar trabalhos da GDPR, como complemento do estudo. Através do mapeamento sistemático dos autores, não foi encontrado nenhum *checklist* com o mesmo propósito, acreditando assim, ser o primeiro instrumento de avaliação de sistemas através de um *checklist* em relação a LGPD. O desenvolvimento do *checklist* foi baseado através de atributos de qualidade, onde descrevem os fundamentos e princípios da lei, esses atributos foram extraídos de artigos relacionados da LGPD, GDPR e também foram extraídos diretamente da própria lei brasileira de proteção de dados, a lei 13.709/2018. Para avaliar o instrumento proposto, utilizaram um sistema de uma Instituição Federal de ensino. Como resultados obtiveram que o *checklist* proposto é capaz de identificar problemas nos sistemas de *software* em relação a adequação da LGPD.

O trabalho de Camelo (CAMELO, 2022) desenvolveu um guia de privacidade e um catálogo de padrões de privacidade para conduzir analistas de requisitos a descrever os requisitos de privacidade em relação à aderência à LGPD. O guia de privacidade foi criado a partir de resultados de uma entrevista exploratória com analistas de requisitos, onde identificaram a importância de um método para auxiliar na condução das especificações de requisitos em relação a LGPD que seja de fácil manuseio, visto a necessidade dos analistas em realizar a interpretação da LGPD. Para avaliação do guia de privacidade, utilizaram um *survey* com 18 participantes, com o intuito de identificar a utilidade e facilidade do guia proposto. Os resultados mostraram que o guia de privacidade é capaz de auxiliar os analistas de requisitos, além de ser um método rápido e simples de especificar os requisitos de privacidade em relação a aderência a LGPD.

2.6.2 Boas práticas de segurança

Gomes (GOMES, 2019) desenvolveu um manual de regras de boas práticas para elaboração de dispositivos IoT específicos na área da saúde, com o intuito dos profissionais responsáveis pela escolha dos equipamentos realizarem uma análise para identificar quais dispositivos são mais adequados para utilização nas unidades de saúde, levando em consideração a segurança dos equipamentos. Para o desenvolvimento do manual de regras de boas práticas, o autor realizou pesquisas das principais ameaças aos dispositivos IoT, com o propósito de identificar quais as maneiras de realizar a invasão nos dispositivos, para assim obter informações de como pode ser realizada a proteção necessária. O autor também analisou alguns equipamentos utilizados nas unidades de saúde, tendo o objetivo identificar quais as vulnerabilidades encontradas nos equipamentos.

O trabalho de Medeiros et al. (MEDEIROS et al., 2017) desenvolveu um guia de boas práticas para a proteção dos dispositivos IoT, esse guia de boas práticas possui a finalidade de detectar problemas de segurança para proteger os dados pessoais e organizacionais. Este guia pode ser utilizado pelos desenvolvedores de sistemas, fabricantes IoT e também pelos usuários. O guia é dividido entre duas partes, a parte do fabricante e a parte do desenvolvedor e usuário. Contendo as categorias: Segurança da Informação; Acesso de usuário e credenciais; Privacidade, divulgação e transparência; e Notificação a usuários. Para avaliação do guia de boas práticas de segurança dos dispositivos, foi realizado com uma empresa nacional de seguros, onde apresentou problemas de segurança e pontos de melhorias. A autora destaca a importância dos usuários seguirem boas práticas de segurança, porque geralmente são os usuários que possuem maior chances de se prejudicarem em relação a segurança dos seus dados, principalmente porque muitos usuários não possuem conhecimentos suficientes sobre segurança computacional. O guia de privacidade proposto pela autora tem benefícios como: conscientizar os usuários da importância dos sistemas atualizados, dos riscos que podem correr e métodos de prevenção para segurança.

Leite (LEITE, 2019) adaptou um manual de regras de boas práticas de proteção para os dispositivos IoT que foi desenvolvida pela empresa Cloud Security Alliance - CSA, o autor acrescentou recomendações de seguranças de especialistas da área da segurança da informação, também abordou sobre problemas de segurança dos dispositivos IoT em relação às vulnerabilidades e ameaças que os dispositivos podem receber. Primeiramente o autor realizou uma pesquisa para identificar vulnerabilidades no sistemas IoT, analisando métodos de invasão

e classificando os tipos de ataques. Também foram destacados métodos de proteção para o ambiente IoT. O autor apresentou acontecimentos reais de problemas de segurança e relatou sobre a grande vulnerabilidade presentes nos dispositivos IoT e o grande desafio dos fabricantes e desenvolvedores em criar mecanismos de proteção para os equipamentos inteligentes, visto a imensa quantidade de problemas de segurança.

2.7 RESUMO DO CAPÍTULO

Esse capítulo apresentou a fundamentação teórica deste trabalho, descrevendo sobre as leis de proteção de dados, apresentando a relação da LGPD com os dispositivos IoT. Posteriormente foi apresentado conceitos de IoT, os problemas de segurança, apresentando as vulnerabilidades dos equipamentos IoT. Por fim, apresentou os trabalhos relacionados.

3 MECANISMOS DE VERIFICAÇÃO DA ADEQUAÇÃO À LGPD

Este capítulo apresenta todo o processo de proposição do mecanismo de verificação da aderência de soluções de IoT em relação a LGPD. O mecanismo proposto é um *checklists* com o intuito identificar a aderência dos sistemas em relação a LGPD. Como apresentado na introdução, já havia sido proposto um *checklist* preliminar para auxiliar a averiguação de adequação de sistemas em geral à LGPD. Desta forma, nosso trabalho consiste em uma extensão a este *checklist*, considerando somente as características específicas de IoT. Seção 3.1 detalha a versão preliminar do *checklist* geral de adequação a LGPD. Seção 3.2 expõe um *update* realizado em uma revisão sistemática da literatura sobre adequação à LGPD. Seção 3.3 descreve uma segunda versão do *checklists*, onde foi proposta formas de extensão do *checklist*. Por fim, Seção 3.4, mostra nosso *checklist* específico para IoT.

3.1 VISÃO PRELIMINAR DO *CHECKLIST* GERAL DE ADEQUAÇÃO À LGPD

O trabalho de Mendes et al. (MENDES; VIANA; RIVERO, 2021) desenvolveu a primeira versão do *checklist* de inspeção com o objetivo de avaliar se os sistemas de *softwares* estão em conformidade em relação à LGPD. Em princípio, o público alvo desta primeira versão são desenvolvedores de *software* que não possuem acesso a recursos legais para verificação dos fundamentos legais nos sistemas.

Para o desenvolvimento do *checklist* os autores inicialmente realizaram uma RSL com a finalidade de encontrar atributos de qualidade e métodos para avaliar a conformidade de sistemas em relação a LGPD. Após isso, extraíram os atributos de qualidade diretamente da lei, de artigos relacionados a LGPD, de artigos referentes aos sistemas computacionais em relação a LGPD e para complemento, artigos relacionados a GDPR. Posteriormente, foram categorizados os atributos e selecionadas as melhores descrições que consequentemente foram transformadas em perguntas de acordo com o propósito de um *checklist*.

Esta versão do *checklists* possui 52 itens sendo categorizados em cinco partes:

- **Transparência**: É a responsabilização do controlador de dados em fornecer informações verdadeiras, fáceis e acessíveis para os titulares de dados.
- **Segurança**: São as medidas de proteção que a organização deve possuir para proteger os dados pessoais.

- **Consentimento**: É a permissão que o titular de dados fornece para a realização do tratamento dos seus dados pessoais.
- **Responsabilidade**: São os métodos que o controlador de dados deve possuir para comprovar a aderência aos fundamentos e princípios da lei.
- **Direitos dos titulares**: É o direito que o titular possui em relação aos seus dados pessoais, como por exemplo, acessar e atualizar seus dados pessoais.

Quadro 2 apresenta como exemplo simplificado sete itens do *checklist* (A versão completa está disponível no Apêndice D. Cada item é apresentado com as informações detalhadas das 5 colunas. A primeira é a categoria, representando um código através das iniciais das categorias, onde **TR01** representa o primeiro item da categoria transparência. A coluna seguinte apresenta a pergunta para identificar a aderências dos sistemas de *software* em relação a LGPD. As últimas três colunas representam de onde os atributos foram extraídos para criação dos itens. Onde a **LEI** significa a análise da LGPD (13.709/2018). A coluna **LGPD** significa os atributos que foram extraídos da literatura referente à lei LGPD e a coluna **GDPR**, significa os atributos que foram extraídos da literatura referente à lei GDPR.

Quadro 2 – Trecho da versão preliminar do *checklist*.

Cat	Itens	LEI	LGPD	GDPR
TR01	O software utiliza os dados pessoais apenas para fins específicos, explícitos e legítimos para qual foi originalmente coletado e informado ao titular de dados?	X	X	X
TR02	O software realiza tratamento de dados previstos na lei de forma adequada e compatível com a finalidade para qual foi originalmente coletado?	X	X	
TR03	O software permite acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e a duração do tratamento, sempre que o titular de dados requisitar?	X	X	X
TR04	O software mantém registros dos dados pessoais precisos e atualizados, sem demora, para cumprimento das suas finalidades?	X		X
CO01	O software permite que o titular de dados dê o seu consentimento de forma livre e clara aos termos e condições, políticas de privacidade, para realizar o tratamento de seus dados?	X	X	X
CO02	O software exige o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?	X		
CO03	O software mantém registros para provar que o consentimento foi obtido em conformidade com o disposto nesta lei, atendendo as condições de consentimento livre, específico, informado e presumido?	X	X	X

Fonte: (MENDES; VIANA; RIVERO, 2021).

3.2 *UPDATE* DA REVISÃO SISTEMÁTICA DA LITERATURA

Como ponto inicial deste trabalho, partimos de uma revisão sistemática da literatura (RSL) sobre adequação à LGPD na computação realizada por Mendes et al. (MENDES; VIANA; RIVERO, 2021). Esta RSL teve como objetivo identificar atributos de qualidade, requisitos e a identificação de métodos para avaliar a aderência dos sistemas computacionais em relação a LGPD. A base de artigos identificados pela RSL funcionou com uma base inicial de artigos para esta pesquisa. Os artigos desta base foram analisados para identificar trabalhos que envolvessem dispositivos IoT e a LGPD.

Visto que a LGPD é relativamente recente, poucos artigos vêm sendo publicados neste tópico (RAPÔSO et al., 2019). Extrapolando esse fato, são ainda mais restritos os artigos que apresentam alguma relação entre a LGPD e IoT. Diante disso, realizou-se uma atualização da RSL de Mendes et al. (MENDES; VIANA; RIVERO, 2021). Para guiar esse *update* da RSL foram adotados os guias de Kitchenham e Charters (KITCHENHAM; CHARTERS, 2007) e Nepomuceno e Soares (NEPOMUCENO; SOARES, 2020). Desta forma, a primeira fase de acordo com os guias adotados é a identificação dos artigos usando engenhos de busca. As bases de dados utilizadas foram a ACM e IEEE, estudos semelhantes adotaram as mesmas bases (WHITMORE; AGARWAL; XU, 2015; DANTAS et al., 2018). Após a calibragem da *String* (incluindo sinônimos e palavras semelhantes), adotamos o seguinte resultado:

> ("IOT"*OR "Internet of Things"*) *AND* ("GDPR"*OR* "LGPD") *AND* ("security"*OR "equipment"OR "software"OR "hardware"*)

A quantidade de artigos retornados na IEEE com busca de 2018 a 2021 foi 55 e na ACM 34 artigos. Após a coleta dos artigos nas bases específicas, passamos para a fase da aplicação dos critérios de seleção dos artigos. Os critérios de inclusão do estudo estão representados no Quadro 3.

Quadro 3 – Critérios de inclusão.

Critério de Inclusão	**Descrição**
CI-1	Artigos completos disponíveis na bases
CI-2	Artigos que tratam de proteção de dados em dispositivos IoT
CI-3	Artigos que relacionam IoT e a LGPD ou GDPR

Fonte: O autor (2022).

Os critérios de exclusão do estudo estão representados no Quadro 4. Dentre os critérios apresentados, somente foi aplicado o critério CE-1.

Quadro 4 – Critérios de exclusão.

Critério de Exclusão	**Descrição**
CE-1	Artigos duplicado
CE-2	Artigos resumidos ou sem revisão por pares
CE-3	Artigos não escritos em português ou inglês

Fonte: O autor (2022).

Três artigos permaneceram após a fase de seleção de inclusão e exclusão de artigos. Com o pequeno número de trabalhos que relacionam as leis de proteção de dados à IoT, o Google Acadêmico foi utilizado para encontrar trabalhos em outras bases de dados. A mesma string foi usada e mais quatro trabalhos relevantes foram identificados. Em seguida, utilizou-se uma técnica conhecida como *backward snowballing*. Essa técnica visa encontrar artigos por meio das referências de um artigo que está sendo analisado (JUNEJA; KAUR, 2019). Após a aplicação desta técnica, dois artigos a mais foram encontrados. Desta forma, totalizando nove estudos primários complementares à RSL de Mendes et al. (MENDES; VIANA; RIVERO, 2021). Diante disso, os artigos complementares foram: (OLIVEIRA et al., 2019; TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018; MEDEIROS et al., 2017; BADII et al., 2020; PIRES et al., 2015; FERENCZ; DOMOKOS; KOVÁCS, 2021; BUI et al., 2019; TEDESCO et al., 2019).

3.3 VERSÃO EXTENSÍVEL DO CHECKLIST

Com o propósito de tornar o *checklist* extensível para se adequar às características de projetos IoT, em um esforço mútuo, nosso grupo colaborou no desenvolvimento da segunda versão do *checklist*. Além de proporcionar formas de estender o *checklist*, a nova versão contou com melhorias que contou com identificação e exclusão de itens duplicados, aperfeiçoamento dos itens através das melhorias textuais e mudança na estrutura do *checklist*.

A segunda versão do *checklist* possui 47 itens obrigatórios (exigidos pela LGPD) e nove itens não obrigatórios (itens recomendados). Os itens dessa nova versão foram classificados nas mesmas categorias que a anterior: Transparência de dados, Consentimento do Titular, Direito do Titular, Segurança de Dados e Responsabilidade do Controlador.

Um avaliador que queira usar essa nova versão do *checklist* pode ter acesso à planilha

(disponível no Apêndice D.) com todas as instruções para averiguação de adequação à LGPD. Cada item do *checklist* tem três opções: **sim**, **não**, ou **não se aplica**. A opção **sim** significa que o sistema avaliado está em conformidade com este tópico específico da LGPD. A opção **não** significa que o sistema avaliado possui uma inconformidade com a lei. Finalmente, a opção **não se aplica** significa que o sistema avaliado não é influenciado pelas propriedades apresentadas no item.

Figura 2 exemplifica o preenchimento do instrumento proposto. No exemplo, o item de código **T-03** foi respondido como não aderente à LGPD. O avaliador pode ainda ler as recomendações com relação à lei de acordo com a revisão bibliográfica realizada. Desta forma, ele terá uma referência do que deverá ser feito para que este item se torne aderente à LGPD.

Figura 2 – Segunda versão do *checklist*.

ITENS OBRIGATÓRIOS					
CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIO DO AVALIADOR	RECOMENDAÇÕES
	Sobre Transparência de Dados (T)				
T-01	As finalidades de tratamento de dados foram definidas na organização?	Sim			*Crie um documento definindo uma Política de Privacidade e os Termos de Consentimento, descrevendo quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.*
T-02	O tratamento de dados pessoais é realizado de acordo com uma base legal?	Sim			*Na documentação da Política de Privacidade e dos Termos de Consentimento, explique a base legal em que fundamenta o tratamento de dados pessoais. Exemplos de base legais: I - Mediante o fornecimento de consentimento pelo titular; II - Para o cumprimento de obrigação legal ou regulatória pelo controlador. Ver completo na lei, disponível: Capítulo 2, Seção 1, artigo 7.*
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	Não			*O sistema deve disponibilizar a Política de Privacidade e/ou Termos de Consentimento para o titular dos dados, sobre as finalidades de tratamento.*

Fonte: (MENDES, 2022).

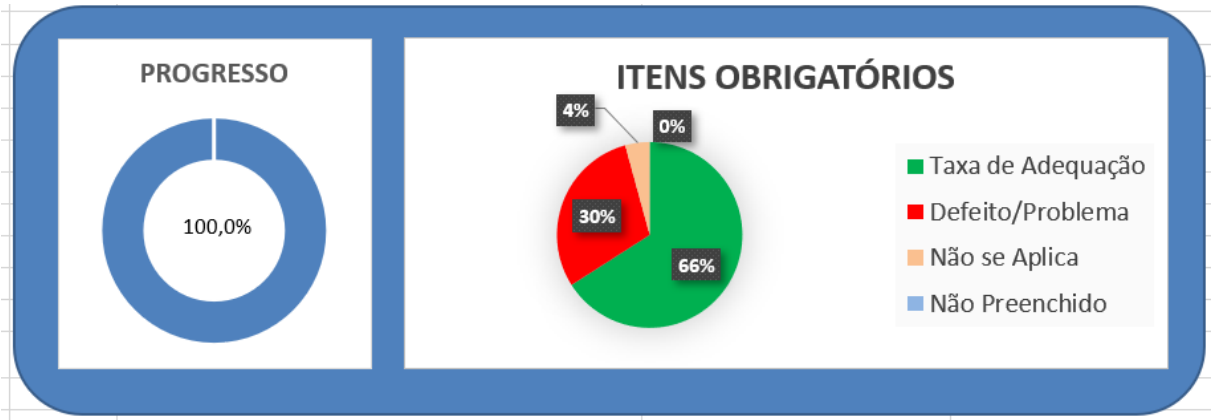
Para melhor exemplificar a Figura 2, será descrito o que cada coluna representa:

- **Código**: É um método para identificar o item, cada código tem as iniciais da categoria e o final a numeração. Como por exemplo, T-01 é a primeira pergunta da categoria Transparência.
- **Itens de avaliação**: São as perguntas do *checklist* para identificar a conformidade do sistema em relação a LGPD.
- **Respostas**: É onde o avaliador vai responder, sim para conformidade, não para inconformidade e não se aplica para se o item não estiver no contexto da empresa.
- **Grau de severidade**: É um método para o avaliador julgar o nível da inconformidade, entre Leve, Grave ou Catastrófico.

- **Comentários do avaliador**: É livre para os avaliadores realizarem anotações.
- **Recomendações**: São possíveis formas para resolver a inconformidade do sistema em relação a LGPD.

A nova versão do *checklist* é capaz de fornecer ainda um gráfico de progresso. Este gráfico é gerado em tempo de execução e exibe o progresso que o preenchimento está sendo realizado. O gráfico gerado apresenta todos os itens que foram assinados em **sim** e calcula a porcentagem do sistema em relação a aderência com a LGPD. O gráfico também apresenta os itens que não estão em conformidade com a LGPD (ou seja, os defeitos ou problemas). Uma observação importante é que os itens que foram classificados como **não se aplica** serão apresentados no gráfico, contudo ele será contabilizado para o cálculo do progresso de preenchimento. Figura 3 representa um exemplo do progresso do preenchimento e não o resultado oficial de aderência.

Figura 3 – Segunda versão do *checklist* - Gráfico de progresso.



Fonte: (MENDES, 2022).

3.4 EXTENSÃO DO *CHECKLIST* PARA AVALIAÇÃO DE PROJETOS IOT

Como dito anteriormente, o instrumento apresentado na Seção 3.1 foi idealizado para avaliar qualquer tipo de sistema, levando em consideração somente os fundamentos da LGPD. Em cenários mais específicos é necessária uma busca mais técnica para encontrar defeitos. Em particular, explorando a parte que a lei relata sobre boas práticas de segurança, a lei menciona sobre as responsabilidades de quem controla os dados. O controlador desses dados deve criar mecanismos de proteção. Este tipo de cenário é particularmente importante quando há dispositivos IoT envolvidos no projeto. Além disso, a literatura acadêmica cita diversos

trabalhos relatando sobre vulnerabilidades e um grande desafio sobre métodos de proteção para os dispositivos IoT que possam estar em aderência com a LGPD (OLIVEIRA et al., 2019; RIBEIRO; NAKAMURA, 2019; BERNARDI et al., 2020). Diante disso, foi desenvolvido uma extensão do *checklist* de Mendes (MENDES, 2022), tendo como público-alvo principal projetos que envolvam IoT. Desta forma, analistas poderão realizar uma avaliação completa do sistema, podendo encontrar defeitos específicos nos dispositivos IoT.

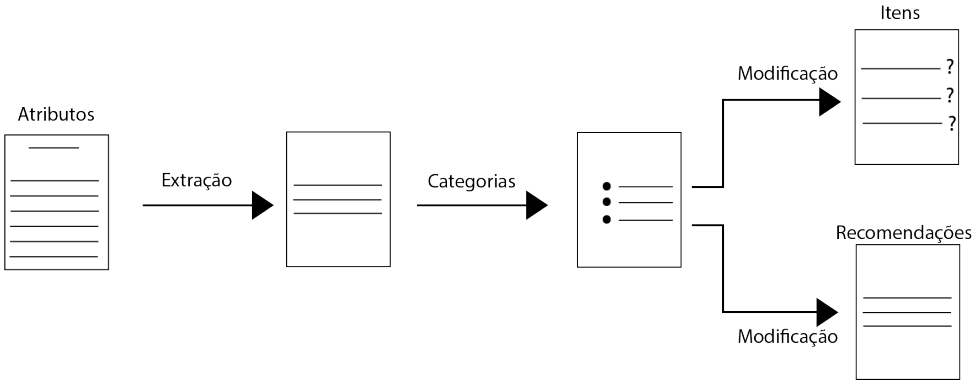
Para criação do desenvolvimento deste mecanismo de inspeção, teve como primeiro passo a realização da update de uma RSL que foi apresentada na Seção 3.2. Com base nos resultados desta etapa anterior, iniciamos a fase de análise dos artigos selecionados e a proposição do mecanismo de inspeção. Para analisar os dados, utilizamos técnicas baseadas nos procedimentos metodológicos da Teoria Fundamentada nos Dados (TFD), do inglês Grounded Theory (CASSIANI; CALIRI; PELÁ, 1996). A teoria fundamentada nos dados tem o objetivo de criar uma teoria a partir dos dados coletados e analisados sistematicamente, e o processo central é a codificação que diz respeito ao processo de analisar dados segundo Corbin e Strauss (CORBIN; STRAUSS, 2008).

Segundo a linha proposta por Corbin, durante a codificação são identificados conceitos (ou códigos) e categorias. Um conceito (ou código) dá nome a um fenômeno de interesse para o pesquisador. Categorias são agrupamentos de conceitos unidos em um grau de abstração mais alto. O produto final da pesquisa na teoria fundamentada é uma série de conceitos fundamentados e integrados em torno de uma categoria ou questão central para formar um arcabouço teórico que explique como e porque as pessoas reagem a determinados acontecimentos, desafios ou problemáticas.

O processo de codificação seguiu somente o processo de codificação aberta. Na codificação aberta, são realizadas a quebra, a análise, a comparação e a categorização dos dados. Segundo Merriam (MERRIAM, 2009), codificação aberta envolve etiquetar qualquer unidade de dados que possa ser relevante para o estudo. Para Flick (FLICK, 2009), a codificação aberta é o processo analítico pelo qual os conceitos são identificados e desenvolvidos em termos de suas propriedades e dimensões, em que se tem a finalidade de expressar dados e fenômenos na forma de conceitos e esses dados são primeiramente segmentadas e classificadas pela unidade de significados, em sequências curtas de palavras. No nosso contexto, tivemos que ler todos os artigos e destacamos trechos que relacionavam IoT e leis de proteção de dados. Neste estudo, lemos todos os artigos e destacamos cada trecho (código) relacionado à IoT e às leis de proteção de dados. Por isso, agrupamos todos os códigos, criando atributos (alguns autores

os chamam de categorias). Posteriormente, cada atributo gerou dois artefatos: (i) um item do questionário e (ii) uma recomendação. Figura 4 apresenta a visão geral do processo. As recomendações foram desenvolvidas para facilitar a compreensão do item. Além disso, eles ajudam os usuários a resolver possíveis problemas. Quadro 5 apresenta alguns itens derivados do nosso processo de criação.

Figura 4 – Processo de criação de itens e recomendações.



Fonte: O autor (2022).

Quadro 5 – Item e recomendação.

Cod	Itens	Recomendações
F01	O dispositivo possui certificação para comprovar os padrões de qualidade?	Ao utilizar certificações, é comprovado que o dispositivo possui níveis de qualidade e segurança que são determinadas pela regulamentação. É de grande importância possuir uma certificação, como por exemplo: Certificação Anatel.
F02	O dispositivo está protegido contra tentativas de redefinição de fábrica por pessoas não autorizadas?	Somente pessoas autorizadas podem ter acesso aos dispositivos e deve ter proibição de intrusos, não permitindo o uso do dispositivo. Caso o reset de fábrica não seja restrito, uma solução é blindar o equipamento, vedando seu acesso.
F03	O dispositivo criptografa os dados armazenados para impedir a identificação de dados pessoais?	Ao armazenar os dados pessoais utilizando criptografia, os dados ficarão mais protegidos. Se ocorrer uma violação, os dados não serão facilmente acessados.

Fonte: O autor (2022).

Cada item tem o intuito de detectar um problema. Desta maneira, cada item possui um método de resolução ou guia para que o avaliador possa resolver o problema. Por exemplo, considerando o Quadro 5, na linha do código **F02**, a descrição do item é *"O dispositivo é protegido contra tentativas de ser resetado para configuração de fábrica por pessoas não autorizadas?"*. Desta forma, para que o problema descrito pelo item seja solucionado (ou ao menos mitigado) o dispositivo só deve ser acessado por pessoas autorizadas. Outras soluções

podem ser adotadas, mas devem estar alinhadas com a recomendação. Considerando o mesmo exemplo apresentado no código **F02**, uma outra solução pode fazer com que o dispositivo esteja em um local em que pessoas não autorizadas não possam ter acesso a ele. Esta solução blinda o equipamento sem a necessidade de impor autorização.

Esta extensão do *checklist* contém 27 itens extra (disponível no Apêndice D), onde estão classificados em quatro categorias, duas foram alocadas em categorias existentes do *checklist* de (MENDES, 2022) (Seção 3.3). Como alguns itens não se encaixam nessas categorias originais, foi acrescentado duas categorias extra:

- **Segurança física:** Está relacionado a parte física do dispositivo, levando em consideração as funcionalidades, proteção contra o acesso físico e condições ambientes.
- **Acesso ao dispositivo**: Está relacionado ao controle de acesso ao dispositivo, permitindo apenas pessoas autorizadas.

Para diferenciar os itens específicos dos outros itens, foi modificada a cor dos itens, tornando os itens específicos para IoT com a cor roxa de acordo com a Figura 5. A estrutura da nossa extensão específica para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT seguiu a mesma estrutura da versão da Seção 3.3. Logo, nossa extensão do *checklist* possui os itens grau de severidade, comentários do avaliador e as recomendações, a metodologia utilizada para criação dos itens e das recomendações.

Figura 5 – Extensão específico para dispositivo IoT.

	Sobre Responsabilidade do Controlador (R)				
R-01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?				*Armazene e documente o histórico de atividades do encarregado DPO.*
R-02	A organização realiza capacitação para seus funcionários sobre a aderência à LGPD?				*Capacite os funcionários e colaboradores sobre as informações que a LGPD determina. Exemplo: Através de treinamentos, cursos e palestras, certificações e etc.*
R-03	São realizadas capacitações para os funcionários que utilizam os dispositivos?				*Realizar capacitações com os funcionários para garantir a qualidade e eficiência de todo o processo.*
	Acesso ao Dispositivo (A)				
A-01	A organização fornece credenciais diferentes para cada utilizador?				*Deve ser realizado o controle de acesso para cada utilizador, criando uma lista de pessoas autorizadas.*
A-02	São atribuídas senhas diferentes a cada dispositivo para fortalecer a segurança?				*Ao utilizar a mesma senha para cada dispositivo, a segurança fica enfraquecida, o ideal é ter senhas diferentes. Uma solução é utilizar um algoritmo para gerar as senhas*
A-03	Houve mudança da senha padrão do dispositivo, para evitar acesso não autorizado?				*É de suma importância a mudança imediata da senha padrão do dispositivo, a senha padrão já é disponibilizada no manual dos dispositivos que facilmente é encontrado no site do fabricante.*

Fonte: O autor (2022).

3.4.1 Itens do checklist

Para criação dos itens foram analisados todos os artigos de acordo com seus métodos de proteção de dados para os dispositivos IoT. As subseções a seguir detalham cada uma das categorias encontradas. Apresentando os quadros para cada categoria, também demonstra as referências nas quais cada item foi baseado. Itens com mais de uma referência tiveram um processo de escolha da referência através do melhor atributo. O melhor atributo para criação de cada item é apresentado na descrição de cada item.

3.4.1.1 Sobre Segurança de Dados

Essa Seção apresenta os itens da categoria Segurança dos Dados, os itens estão relacionados à proteção dos dados pessoais. Os Quadros 6 e 7 apresentam os itens dessa categoria. Foi dividido em dois quadros para melhor representar a categoria.

Para a realização do item S-08 foi baseado no artigo de Tikkinen-Piri et al. (TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018), onde representa que a empresa deve comprovar todo o processo de tratamento de dados e as empresas são aconselhadas a possuir certificações de proteção dos dados. Com isso, é de suma importância que os equipamentos utilizados possuam certificações, para comprovar os padrões de qualidade do equipamento.

Para o desenvolvimento do item S-09 foi baseado no artigo de Medeiros et al. (MEDEIROS et al., 2017), onde é apresentado os riscos de ataques de força bruta, além de demonstrar métodos de configurações para fortalecer a segurança, como o bloqueio do usuário ao dispositivo após algumas tentativas inválidas de login.

Para a realização do item S-10 foi baseado no artigo de Gomes (GOMES, 2019), o autor relata sobre a realização de uma bateria de testes para prevenir ataques contra os dispositivos IoT que os tornam indisponíveis e que os dispositivos precisam identificar quando estão recebendo uma tentativa de invasão para conseguir bloquear. Diante disso, realizar testes no cenário real da empresa é fundamental para a proteção dos dispositivos IoT.

O item S-11 foi baseado do artigo no artigo Badii et al. (BADII et al., 2020), neste trabalho é relatado sobre as etapas de uma comunicação segura entre os dispositivos IoT, relatando sobre técnicas de criptografia, soluções para proteção de todo o ciclo dos dados e diferentes técnicas para proteção de uma comunicação segura entre dispositivos IoT.

O item S-12 foi realizado baseado no artigo Badii et al. (BADII et al., 2020), onde o artigo faz

Quadro 6 – Itens sobre Segurança de Dados. Primeira parte.

Cod	Itens	Recomendações	Referência
S-08	O dispositivo possui certificação para comprovar os padrões de qualidade?	Ao utilizar certificações, é comprovado que o dispositivo possui níveis de qualidade e segurança que são determinadas pela regulamentação. É de grande importância possuir uma certificação, como por exemplo: Certificação Anatel.	(TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018; SHAO; OINAS-KUKKONEN, 2019)
S-09	O dispositivo é seguro contra ataques de "força bruta"e/ou outras tentativas abusivas de login?	Um ataque de força bruta é uma maneira de conseguir acesso privilegiado através de inúmeras tentativas. Uma solução é criar mecanismos para bloquear os utilizadores após várias tentativas inválidas de acesso.	(GOMES, 2019; MEDEIROS et al., 2017)
S-10	O dispositivo possui mecanismos contra ataques conhecidos atualmente, como buffer overflow, DDoS, entre outros?	Realizar uma bateria de testes de ataques mais conhecidos atualmente como forma de prevenção.	(GOMES, 2019; MEDEIROS et al., 2017)
S-11	Os dispositivos utilizam técnicas de proteção para realizar uma comunicação segura?	Ao compartilhar os dados entre os dispositivos, é necessário que técnicas de proteção sejam implementadas.	(GOMES, 2019)
S-12	As senhas ficam encriptadas na base de dados do dispositivo?	As senhas que ficam salvas na base de dados do dispositivo, se elas estiverem encriptografadas, se tornam mais seguras, se alguém tiver acesso ao dispositivo, não conseguirá visualizar a senha facilmente.	(BADII et al., 2020)
S-13	O dispositivo encaminha os dados devidamente para o seu destino?	Realizar verificações para identificar se os dados estão sendo encaminhados apenas para seu devido destino.	(MEDEIROS et al., 2017; BADII et al., 2020)
S-14	O dispositivo utiliza protocolos como SSL e TLS para criptografar as comunicações?	Os protocolos SSL (Secure Socket Layer) e TLS (Transport Layer Security) servem para encriptar as comunicações, proporcionando a segurança na troca de dados e das informações.	(MEDEIROS et al., 2017; BUI et al., 2019; GOMES, 2019)

Fonte: O autor (2022).

comparação entre o armazenamento dos dados dos dispositivos IoT com a GDPR, relacionando a importância em utilizar criptografia diante a lei, para evitar a visualização das informações, se caso ocorrer uma invasão, os dados vão estar criptografados.

Realizou-se o item S-13 através do embasamento do trabalho de Medeiros et al. (MEDEIROS et al., 2017), o trabalho explica sobre vazamento de dados através dos dispositivos IoT e explica a importância em analisar se o dispositivo não está enviando uma cópia de dados para um destino indevido.

O desenvolvimento do item S-14 teve como base o artigo Gomes (GOMES, 2019), este trabalho apresenta sobre os protocolos de segurança que devem ser usados pelos dispositivos, demonstrando que os protocolos SSL (Secure Socket Layer) e TLS (Transport Layer Security) permite uma comunicação segura com outros equipamentos e servidores.

O item S-15 foi baseado no artigo de Oliveira et al. (OLIVEIRA et al., 2019), o artigo realiza uma abordagem sobre os dispositivos IoT com pouco processamento, comparando com os

Quadro 7 – Itens Sobre Segurança de Dados. Segunda parte.

Cod	Itens	Recomendações	Referência
S-15	A organização cria mecanismos de segurança para os dispositivos com pouco processamento?	Em cenários que dispositivos não suportam protocolos como por exemplo, CoAP. Nesse caso será necessário a interação entre os equipamentos. Uma alternativa é a utilização de gateways, onde enviará as informações para um ponto na rede e realizará o tratamento e procedimentos que o dispositivo restrito não consegue.	(OLIVEIRA et al., 2019)
S-16	O dispositivo recebe atualizações de segurança?	As atualizações de segurança corrigem falhas e o quanto mais rápido essas falhas forem corrigidas, diminui os riscos contra invasões.	(BUI et al., 2019; MEDEIROS et al., 2017; ISO, 2013; GOMES, 2019)
S-17	O dispositivo encripta os dados armazenados para impedir a identificação de dados pessoais?	Ao armazenar os dados pessoais utilizando criptografia, os dados ficarão mais protegidos. Se ocorrer uma violação, os dados não serão facilmente acessados.	(GOMES, 2019)
S-18	Existe um profissional de segurança fiscalizando atividades suspeitas ou incomuns e pronto para agir imediatamente?	Ter um profissional fiscalizando todo o processo diminuirá bastante as chances de um incidente de dados, visto que ele estará sempre a disposição para agir imediatamente.	(ISO, 2013)
S-19	Os dispositivos são alocados em uma VLAN específica, separando-se de ambientes de usuário/visitantes?	Realizar o gerenciamento de toda a rede, separando o acesso a internet de usuários/visitantes com a rede de acesso dos dispositivos.	(GOMES, 2019)
S-20	Quando a senha do dispositivo é trocada, a organização recebe uma notificação?	É importante a notificação após mudanças de senhas, porque se alguém sem autorização conseguir realizar a mudança de senha, a organização poderá tomar medidas protetivas imediatamente.	(ISO, 2013)
S-21	A organização recebe notificações em caso de acessos não autorizados?	Criar mecanismos para notificações se ocorrer acessos indevidos, com o intuito de conseguir agir imediatamente em caso de invasões.	(ISO, 2013)

Fonte: O autor (2022).

fundamentos da LGPD. Também apresenta aplicabilidade dos conceitos para proteção dos dispositivos IoT com pouco processamento, descrevendo os desafios desses equipamentos e demonstrando formas para proteção ou para minimizar as vulnerabilidades.

O item S-16 foi realizado baseado no artigo de Bui et al. (BUI et al., 2019), onde é relatado sobre a importância das atualizações para o bom funcionamento do dispositivo IoT. As atualizações podem corrigir falhas anteriores, tornando o dispositivo mais protegido.

O item S-17 baseou-se no artigo de Gomes (GOMES, 2019), este artigo apresenta sobre a importância de armazenar os dados pessoais que sejam armazenados com criptografia, para uma maior proteção da informação.

Para o desenvolvimento do item S-18, foi baseado na norma NBR ISO/IEC 27002:2013 (ISO, 2013), onde é relatado sobre a importância das atividades de monitoramento por profissionais de segurança da informação, para uma maior proteção aos dados. Em caso de violação, os profissionais estarão disponíveis para resolver o possível problema imediatamente.

Para criar o item S-19, teve como base o artigo de Gomes (GOMES, 2019), o artigo relata sobre o gerenciamento da rede para proteger os dispositivos IoT, realizando a separação da rede para usuários e outra para os dispositivos. Se por acaso, pessoas externas, que não são funcionários, tiverem acesso a *internet* na mesma rede que os equipamentos, é um risco a segurança porque os dados estão trafegando na mesma rede e um indivíduo mal intencionado pode usar mecanismos para conseguir acesso não autorizado a outras partes da rede.

Os itens S-20 e S-21 foram baseados na ISO/IEC 27002:2013 (ISO, 2013), onde é apresentado sobre a importância das atividades de segurança através de notificações, para que a empresa através das notificações consigam monitorar todo o ambiente, como por exemplo, recebendo notificações de possíveis ocorrências de vulnerabilidades, alterações suspeitas e acessos não autorizados.

3.4.1.2 Sobre Responsabilidade do Controlador

Essa Seção apresenta o item da categoria Responsabilidade do Controlador, está relacionada a importância da capacitação dos funcionários para prevenir problemas de segurança. No Quadro 8 apresenta o item desta categoria.

Quadro 8 – Itens sobre o Acesso ao Dispositivo.

Cod	Itens	Recomendações	Referência
R-03	São realizadas capacitações para os funcionários que utilizam os dispositivos?	Realizar capacitações com os funcionários para garantir a qualidade e eficiência de todo o processo.	(FERENCZ; DOMOKOS; KOVÁCS, 2021)

Fonte: O autor (2022).

Para a criação do item R-03, foi baseado no artigo Ferncz et al. (FERENCZ; DOMOKOS; KOVÁCS, 2021) onde relatam sobre a importância dos funcionários receberem capacitações de segurança, podendo ser fundamental para prevenir erros que sejam prejudiciais à segurança.

3.4.1.3 Acesso ao Dispositivo

Esta seção apresenta os itens da categoria Acesso ao dispositivo, onde são itens relacionados ao controle de acesso aos dispositivos e gerenciamento para proteção contra acessos indevidos. No Quadro 9 é apresentado os itens desta categoria.

O item A-01 teve como base o artigo de Gomes (GOMES, 2019), onde apresenta a impor-

Quadro 9 – Itens sobre o Acesso ao Dispositivo.

Cod	Itens	Recomendações	Referência
A-01	É fornecido credenciais diferentes para cada utilizador?	Deve ser realizado o controle de acesso para cada utilizador, criando uma lista de pessoas autorizadas.	(GOMES, 2019)
A-02	São atribuídas senhas diferentes a cada dispositivo para fortalecer a segurança?	Ao utilizar a mesma senha para cada dispositivo, a segurança fica enfraquecida, o ideal é ter senhas diferentes. Uma solução é utilizar um algoritmo para gerar as senhas	(MEDEIROS et al., 2017)
A-03	Houve mudança da senha padrão do dispositivo, para evitar acesso não autorizado?	É de suma importância a mudança imediata da senha padrão do dispositivo, a senha padrão já é disponibilizada no manual dos dispositivos que facilmente é encontrado no site do fabricante.	(MEDEIROS et al., 2017; GOMES, 2019; ISO, 2013)
A-04	O dispositivo garante que a senha seja forte e segura?	Para o fornecimento de uma maior proteção a segurança, é fundamental senhas fortes, como por exemplo: Uso de letras maiúsculas, letras minúsculas, números e símbolos	(MEDEIROS et al., 2017; GOMES, 2019)
A-05	São registradas falhas ou possíveis suspeitas de vulnerabilidade?	Realizar registros de todas as falhas e suspeitas reais, possuir esta documentação pode ajudar na organização e prevenções.	(PIRES et al., 2015)

Fonte: O autor (2022).

tância de fornecer credenciais diferentes para cada usuário, demonstrando a importância em realizar um controle de acesso de autorizações para os utilizadores.

Para a criação dos itens A-02, A-03 e A-04 que são itens específicos para senhas dos dispositivos, foi baseado no artigo de Medeiros et al. (MEDEIROS et al., 2017), onde é relatado que deve ser modificada a senha padrão dos dispositivos IoT, visto que as senhas padrões são fornecidas nos manuais dos equipamentos, tornando-se facilmente acessíveis. Também apresenta a importância em obter senhas fortes, utilizando letras maiúsculas e minúsculas, números e caracteres especiais.

Para o desenvolvimento do item do A-05 teve como base o artigo de Pires et al. (PIRES et al., 2015), onde apresenta a importância do gerenciamento de sistemas IoT e os registros de falhas. Uma falha no sistema pode ser um caminho para um invasor conseguir acesso indevido. Registrar as falhas e vulnerabilidade não resolve o problema, mas é uma documentação importante para ajudar a resolver, para os funcionários da empresa ter acesso e poder consultar como ocorreu a falha ou vulnerabilidade e criar mecanismos para não ocorrer novamente.

3.4.1.4 Segurança física

Essa Seção apresenta os itens da categoria Segurança Física dos dispositivos. Garantir a segurança física dos dispositivos é de grande importância, pois armazenam dados pessoais e se um indivíduo mal intencionado conseguir inserir um *software* malicioso através do contato

físico com o equipamento ou até mesmo trocar por um dispositivo adulterado com intenções maliciosas, poderá conseguir acesso aos dados, ocorrendo assim um vazamento de dados. São diversas situações que podem causar um vazamento de dados pessoais. O Quadro 10 apresenta os itens desta categoria.

Quadro 10 – Itens sobre Segurança Física.

Cod	Itens	Recomendações	Referência
SF-01	O dispositivo possui apenas portas em funcionamento, não permitindo portas desnecessárias?	Todas as portas que não estão em uso, deverão ser desativadas. Exemplos de portas: RJ45 e USB.	(MEDEIROS et al., 2017)
SF-02	O dispositivo não possibilita o acesso facilmente de pessoas não autorizadas, evitando riscos à segurança física do mesmo?	Analisar o ambiente no qual o dispositivo se encontra, analisando possíveis riscos que o dispositivo poderá sofrer.	(ISO, 2013)
SF-03	O dispositivo está protegido contra tentativas de redefinição de fábrica por pessoas não autorizadas?	Apenas pessoas autorizadas poderão ter acesso aos dispositivos e deve ter proibição de intrusos, não permitindo utilização do dispositivo. Se o reset de fábrica não estiver restrito, uma solução é a blindagem do equipamento vedando o seu acesso.	(GOMES, 2019)
SF-04	O dispositivo é resistente para o ambiente que está alocado?	Realizar uma análise das condições ambientais, como temperatura e umidade, identificando se irá afetar negativamente o dispositivo que irá ser utilizado.	(TEDESCO et al., 2019)
SF-05	A manutenção do dispositivo é realizada conforme recomendação do fornecedor?	O ideal é que as manutenções dos dispositivos sejam realizadas nos intervalos recomendados pelo fornecedor e de acordo com suas recomendações.	(ISO, 2013)
SF-06	A manutenção e consertos dos dispositivos são realizados por uma equipe autorizada?	Para a confiabilidade deste procedimento, é de grande importância ser realizado por uma equipe autorizada.	(ISO, 2013)
SF-07	São registradas todas as manutenções preventivas?	A manutenção preventiva é a garantia do bom funcionamento do dispositivo e o registro se torna a comprovação e organização de quando realizou-se o procedimento.	(ISO, 2013)

Fonte: O autor (2022).

Para a criação do item SF-01, baseou-se no artigo de Medeiros et al. (MEDEIROS et al., 2017), onde é relatado que se existir funcionalidades do dispositivo IoT e portas físicas que não estão sendo utilizadas, deverão ser desativadas. É uma prevenção, para nenhum indivíduo conseguir estabelecer uma conexão através de portas como por exemplo, USB.

Para o desenvolvimento do item SF-02, foi baseado na ISO/IEC 27002:2013 (ISO, 2013), onde relatam que os dispositivos devem ser protegidos fisicamente, porque podem ser roubados se estiverem em um local não protegido. Isso poderá causar riscos à segurança de dados, visto que o dispositivo pode estar armazenando conteúdos importantes.

Para criar o item SF-03 teve como base o artigo de Gomes (GOMES, 2019), onde o autor relata que os equipamentos IoT não podem ficar exposto, devem ser colocados em lugares que as pessoas não autorizadas não tenha acesso ou protegê-lo através de caixas apropriadas com

cadeados.

Para criação do SF-04 foi baseado no artigo de Tedesco et al. (TEDESCO et al., 2019), o trabalho relata sobre a importância da manutenção dos dispositivos IoT, o autor também defende a manutenção antecipada dos equipamentos.

Para criação dos itens SF-05, Sf-06 e SF-07, foi baseado na ISO/IEC 27002:2013 (ISO, 2013), onde é relatado sobre a manutenção dos equipamentos, que deve ser realizada nos intervalos recomendados, com profissionais autorizados e que sejam registradas todas as manutenções preventivas. Documentar as manutenções é de grande importância, porque serve para o controle das futuras manutenções, como para qualquer comprovação que a empresa seguiu todos os procedimentos para o bom funcionamento dos equipamentos.

3.5 RESUMO DO CAPÍTULO

Este capítulo apresentou o processo para concepção do *checklist* de inspeção para aderência de sistemas à LGPD. Em seguida foi apresentado a extensão proposta considerando os trabalhos específicos para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT. Além disso, detalhamos cada um dos itens e as recomendações foram criadas para os problemas apresentados. É importante chamar atenção para a importante colaboração estabelecida com pesquisadores da UFMA (MENDES; VIANA; RIVERO, 2021; MENDES, 2022) que permitiu que este trabalho se concentrasse nas especificidades da IoT.

4 AVALIAÇÃO

Este capítulo tem o objetivo apresentar o processo de avaliação do mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT. A Seção 4.1 descreve os perfis dos participantes. A Seção 4.2 apresenta os resultados da avaliação onde os participantes, após terem sido introduzidos ao mecanismo proposto, responderam uma série de perguntas sobre a utilidade, facilidade e intenção de uso do mecanismo. A Seção 4.3 apresenta o resultado da avaliação seguinte, onde todos os participantes fizeram parte de um grupo focal sobre o mecanismo proposto. Por fim, a Seção 4.5apresenta o resumo do capítulo.

Essa avaliação ocorreu juntamente com a avaliação do mecanismo geral, apresentado na Seção 3.3, porém, este trabalho só apresentará os resultados referente a extensão do *checklist* específico para IoT, os dados da avaliação do mecanismo geral está no trabalho de Mendes (MENDES, 2022).

4.1 PERFIL DOS PARTICIPANTES

Os participantes desta pesquisa são funcionários de um instituto de inovação privado ligado à inovação industrial. A avaliação foi feita em um projeto que provê uma solução baseada em IoT para empresas industriais onde há o tratamento de dados pessoais e equipamentos de IoT. Para inicialização da avaliação desta pesquisa, primeiramente foi realizada uma reunião com a empresa, com o intuito de selecionar os profissionais adequados para utilizar o mecanismo de inspeção. Como pré-requisito obrigatório, o participante teve que ter um desses dois perfis: i) Profissional com conhecimento técnico (arquitetura utilizada, decisões de projeto, padrões implementados, infraestrutura de TI, entre outros) sobre a solução a ser avaliada; ou ii) Conhecimento técnico sobre os dispositivos IoT utilizados na empresa. Com isso, a empresa selecionou quatro participantes.

A seguir, é apresentado o perfil dos participantes, relatando seus cargos na empresa, experiência profissional e os níveis de conhecimento em relação a LGPD e IoT. Quatro funcionários da empresa se colocaram à disposição para avaliar o instrumento proposto. Contudo, durante a realização da avaliação um dos participantes não pôde participar e, portanto, seus dados foram suprimidos.

De acordo com a primeira pergunta do Quadro 11, dois dos três participantes possuem pós-

graduação. Contudo, o participante que não possui pós-graduação está cursando mestrado. Para avaliar o conhecimento dos participantes em IoT e LGPD fizemos as perguntas de número três, quatro e cinco do Quadro 11. Ainda sobre o quadro, para identificar os cargos que os participantes ocupam, fizemos as perguntas de número seis e sete.

Quadro 11 – Dados dos participantes.

Nº	Pergunta:	P1	P2	P3
1	Qual seu nível de escolaridade?	Pós-graduação	Mestrado	Pós-graduação
2	Você possui conhecimento sobre a LGPD?	Sim	Sim	Sim
3	Descreva qual o nível de conhecimento sobre a LGPD?	Intermediário	Baixo	Intermediário
4	Você possui conhecimento sobre IoT	Sim	Sim	Sim
5	Descreva qual o nível de conhecimento sobre IoT?	Intermediário	Médio	Avançado
6	Qual cargo atual na empresa?	Consultor de Empresas	Analista de Informática I	Desenvolverdor de Tecnologia e Inovação
7	Quanto tempo de experiência no cargo?	3 anos	2 anos e 7 meses	3 anos

Fonte: O autor (2022).

4.1.1 Aplicação do mecanismo de inspeção

Como pré-requisito, os participantes assinaram um termo de consentimento (disponível no Apêndice A), enviado através dos e-mails. Nesse termo, explicou que todas as informações e coletas de dados são utilizadas apenas para fins de pesquisa, sendo preservadas as identidades dos participantes. Posteriormente, os participantes baixaram os materiais do estudo através do *drive*, onde, havia as instruções gerais (disponível no Apêndice B) e treinamento por vídeo de utilização do mecanismo de inspeção. A equipe de pesquisadores ficou à disposição para qualquer dúvida dos participantes ou qualquer problema técnico que viesse a acontecer. Quadro 12 descreve o cronograma desta avaliação.

Quadro 12 – Cronograma.

1	Termo de consentimento e caracterização	15/02/2022
2	Preenchimento do mecanismo de inspeção	15/02/2022 - 18/02/2022
3	Questionário pós-insoeção	15/02/2022 - 18/02/2022
4	Grupo Focal	21/02/2022

Fonte: O autor (2022).

4.1.2 Piloto

Com o intuito de identificar algo que não foi previsto, realizou-se um estudo piloto, foi executado com dois desenvolvedores de *software*, com conhecimento em LGPD e IoT. Um possui quatro anos de experiência e o outro dois anos, os dois são formados em Ciência da Computação. Foi realizado testes dos instrumentos e artefatos criados, sendo eles: Guia de procedimento, termo de consentimento, questionário de caracterização, questionário de pós-inspeção, treinamento, mecanismo de inspeção e a lousa digital interativa. Através do piloto foram identificadas algumas sugestões de mudanças, como por exemplo, um dos participantes sugeriu um dicionário para palavras como: Controlador de dados, titular e demais termos utilizados pela LGPD. Outro participante encontrou defeitos em itens do mecanismo de inspeção. Todas as sugestões foram atendidas.

4.2 QUESTIONÁRIO DE PÓS-INSPEÇÃO

Com o objetivo de responder a segunda questão de pesquisa (QP2- O *checklist* proposto ajuda na identificação de problemas em relação à soluções computacionais específicas de IoT frente a LGPD?). Foi elaborado um questionário para os participantes responderem após preenchimento do mecanismo proposto de inspeção, o questionário, disponível no Apêndice C, teve questões referente a facilidade de uso, utilidade de uso e intenção de uso do mecanismo de inspeção proposto. As questões de pesquisa são respondidas na Seção 4.4.

Uma vez que os participantes foram recrutados, foi disponibilizado nosso instrumento de averiguação para que eles pudessem aplicar sobre os projetos que eles estavam atuando naquele momento. Em seguida, foi apresentado aos participantes um questionário de pós-inspeção que visa avaliar o ponto de vista deles sobre a aplicação do nosso instrumento no contexto dos participantes. Essa Seção tem como objetivo apresentar os resultados da análise das respostas dos participantes no que diz respeito à viabilidade do mecanismo de inspeção proposto em termos de utilidade, facilidade e intenção de uso. A facilidade de uso percebida está relacionada ao grau de compreensão em utilizar uma ferramenta tecnológica (VENKATESH; GOYAL, 2010). A utilidade percebida é o quanto uma pessoa acredita que a ferramenta tecnológica é capaz de ajudar no desempenho do seu trabalho (VENKATESH; MORRIS, 2000); E a intenção de uso, está relacionada às intenções do indivíduo perante um sistema (VENKATESH et al., 2003).

Os participantes responderam um questionário através de um formulário no Google Forms

Apendice C. A seguir será apresentado as questões, as respostas dos participantes e a análise de cada uma delas.

4.2.1 Respostas do questionário de pós-inspeção

A primeira parte do questionário é "Como base no uso deste *checklist*, selecione o seu grau de concordância com as afirmativas a seguir com relação a sua percepção de facilidade de uso do mesmo". Esta primeira parte do questionário tem o propósito identificar a facilidade de uso do *checklist* através das respostas dos participantes. Para cada item utilizamos uma escala Likert-4. As respostas estão presentes no Quadro 13. A primeira frase de concordância foi: "O checklist utilizado foi claro e fácil de entender". Dois dos três participantes concordaram totalmente, enquanto o terceiro concordou parcialmente. No segundo item, a frase de concordância foi: "De maneira geral, eu acho fácil encontrar defeitos / problemas no sistema com o *checklist* utilizado". Todos os três participantes concordaram totalmente. Por fim, a última frase de concórdia foi: "O *checklist* utilizado demandou pouco esforço mental". Onde cada um dos respondentes deu uma resposta diferente: concordo totalmente, concordo parcialmente e discordo parcialmente. Diante das respostas, podemos evidenciar que os participantes tiveram facilidade em encontrar defeitos no sistema. De maneira geral, os participantes relatam que acharam fácil e claro a utilização do *checklist* e houve uma discordância sobre achar que o *checklist* demanda pouco esforço mental. Esse participante relatou que o *checklist* abordava assuntos que não conhecia, fazendo com que ele pesquisasse sobre a temática, resultando em mais trabalho ao responder o *checklist*, pois precisava estudar mais sobre o assunto. Não é possível dizer que esse foi o motivo pelo qual ele não concordou que o *checklist* exigia pouco esforço mental, pois o participante não deixou claro se estava se referindo ao esforço mental. No entanto, acreditamos que esse tenha sido o motivo, dado seu relato de demora em responder os itens devido ao estudo detalhado que teve que fazer.

O segundo questionamento teve o intuito de identificar a utilidade do mecanismo de inspeção, onde os participantes responderam através do grau de concordância. A primeira frase de concordância foi: "O *checklist* utilizando me permite realizar a inspeção do sistema mais rapidamente". O Quadro 14 apresenta que todos os participantes concordaram totalmente. Diante das respostas obtidas, podemos considerar que os participantes acreditam que o *checklist* permite encontrar defeitos no sistema de forma rápida. A frase de concordância do item dois diz: "O *checklist* utilizado melhora a minha produtividade ao identificar defeitos /problemas

Quadro 13 – Facilidade de uso do *checklist*.

Itens de concordância	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
O *cklist* utilizado foi claro e fácil de entender.	2	1		
De maneira geral, eu acho fácil encontrar defeitos / problemas no sistema com o checklist utilizado.	3			
O *cklist* utilizado demandou pouco esforço mental.	1	1	1	

Fonte: O autor (2022).

no sistema. Onde dois concordam totalmente e um concorda parcialmente. Os dados revelam que na visão dos participantes o *checklist* melhora a produtividade em relação a identificar defeitos no sistema. Por fim, a última frase de concordância do item três diz: "Eu acho que o *checklist* utilizado é útil para encontrar defeitos / problemas no sistema". Os dados desse item, apresentam que por unanimidade, os participantes acreditam que o *checklist* possui utilidade para encontrar defeitos.

Quadro 14 – Utilidade de uso do Mecanismo de inspeção.

Itens de concordância	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente.
O *checklist* utilizado me permite realizar a inspeção do sistema mais rapidamente.	3			
O *checklist* utilizado melhora a minha produtividade ao identificar defeitos / problemas no sistema.	2	1		
Eu acho que o *checklist* utilizado é útil para encontrar defeitos / problemas no sistema.	3			

Fonte: O autor (2022).

O terceiro questionamento foi a respeito da intenção dos participantes em utilizarem o mecanismo de inspeção em outros sistemas e se recomendariam para outras empresas. Diante disso, o primeiro item de concordância foi: "Eu pretendo usar o *checklist* para encontrar defeitos / problemas no sistema futuramente". O Quadro 15, mostra que todos os três respondentes concordaram totalmente. O segundo item de concordância foi: "Assumindo que eu tenha acesso

ao *checklist*, pretendo usá-lo para encontrar defeitos / problemas em outros sistemas". Onde todos os participantes concordaram totalmente. Por fim, o terceiro item de concordância, que diz: "Eu recomendaria o *checklist* utilizado para outras empresas." Onde também todos os três respondentes concordaram totalmente. Diante dessas informações coletadas, o questionamento à intenção de uso foi muito satisfatório, visto que todos concordaram totalmente dos três itens de concordância, com isso, os dados levam ao entendimento que os participantes têm a intenção de usar o *checklist* futuramente.

Quadro 15 – Intenção de uso do *checklist*.

Itens de concordância	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
Eu pretendo usar o *checklist* para encontrar defeitos / problemas no sistema futuramente.	3			
Assumindo que eu tenha acesso ao *checklist*, pretendo usá-lo para encontrar defeitos / problemas em outros sistemas.	3			
Eu recomendaria o *checklist* utilizado para outras empresas.	3			

Fonte: O autor (2022).

4.2.2 Discriminação de defeitos

Após os participantes realizarem a inspeção do sistema, enviaram os arquivos com todos os possíveis defeitos encontrados por eles. Posteriormente, foi realizada a análise para identificar os defeitos que o sistema da empresa possui, os dados das inspeções foram analisadas através de uma planilha, onde as respostas de cada inspetor para cada item foi marcada com **Não** para defeito e **Sim** para conformidade. Dessa forma, facilitou a identificação das discrepâncias. Discrepância é um possível defeito identificado, que pode de fato ser um defeito ou um falso positivo (KALINOWSKI et al., 2007).

Ocorreu uma reunião com os participantes sobre as discrepâncias de defeitos. De acordo com Kalinowski (KALINOWSKI et al., 2007) a discriminação de defeitos serve para identificar se a discrepância é um defeito ou um falso positivo, deve reunir os inspetores e discutir todas as discrepâncias. Foi apresentada todas as discrepâncias aos participantes, onde debateram

entre eles, chegando a uma conclusão por unanimidade. Após discriminação de defeitos, foi classificado em quatro categorias: i) Defeito: Para os defeitos encontrados durante a inspeção por unanimidade; ii) Defeito após discriminação: Para os itens discrepantes que durante a reunião foi determinado como defeito; iii) Conformidade: Para os itens em conformidade encontrados durante a inspeção por unanimidade; iv) Conformidade após inspeção: Para os itens discrepantes que durante a reunião foi determinado como conformidade; e v) Não se aplica: Para itens que as empresas não abrangem.

A Figura 6 apresenta os itens após a discriminação de defeitos. O **IP1** da terceira coluna, significa inspetor um, as outras duas colunas ao lado, são os outros dois inspetores. E a ultima coluna **DF**, significa discriminação de defeitos, onde o vermelho com o **x** representa que por unanimidade os participantes relataram ser um defeito. O verde representa os itens em conformidade diante do relato dos participantes. Ocorreram 12 discrepâncias, nove dessas discrepâncias foram identificadas como defeito por unanimidade. As outras três foram identificadas como conformidade.

É possível identificar que o inspetor dois foi o inspetor que mais identificou defeitos. Das sete discrepâncias, ele identificou cinco defeitos. O participante dois é o participante que menos possui experiência em LGPD, mas foi o participante que mais identificou defeitos. Como visto na Seção 4.1, não foi preciso possuir conhecimento em LGPD para responder o *checklist*.

O resultado total do índice de adequação da empresa após reunião com os participantes sobre a discriminação dos defeitos é de 59,3% (16) de adequação dos itens específicos em IoT e 40,75% (11) de defeitos.

Após a análise de todas as discrepâncias, os participantes perceberam que a empresa possui uma grande porcentagem de defeitos encontrados e demonstraram bastante interesse, onde relataram que irão resolver todos os defeitos encontrados e aplicar na segunda versão do sistema.

Figura 6 – Discriminação de defeitos.

COD	ITEM DE AVALIAÇÃO	IP1	IP2	IP3	DF
	Sobre Segurança de Dados (S)				
S-10	O dispositivo possui mecanismos contra ataques conhecidos atualmente, como buffer overflow, DDoS, entre outros?	Não	Sim	Sim	X
S-14	O dispositivo utiliza protocolos como SSL e TLS para criptografar as comunicações?	Sim	Não se aplica	Sim	
S-15	A organização cria mecanismos de segurança para os dispositivos com pouco processamento?	Sim	Sim	Não	X
S-17	O dispositivo encripta os dados no armazenamento, para evitar a identificação dos dados pessoais?	Não	Sim	Sim	X
S-18	Existe um profissional de segurança fiscalizando atividades suspeitas ou incomuns e pronto para agir imediatamente?	Sim	Não	Não	
S-19	Os dispositivos são alocados em uma VLAN específica, separando-se de ambientes de	Não	Não	Sim	X
	Acesso ao Dispositivo (A)				
A-01	A organização fornece credenciais diferentes para cada utilizador?	Sim	Não	Sim	
A-02	São atribuídas senhas diferentes a cada dispositivo para fortalecer a segurança?	Sim	Não	Sim	X
A-03	Houve mudança da senha padrão do dispositivo, para evitar acesso não autorizado?	Não	Não	Sim	X
A-04	O dispositivo garante que a senha seja forte e segura?	Sim	Não	Sim	X
A-05	São registradas falhas ou possíveis suspeitas de vulnerabilidade?	Sim	Sim	Não	X
	Segurança Física (SF)				
SF-07	São registradas todas as manutenções preventivas?	Não se aplica	Não	Não	X

Fonte: O autor (2022).

4.3 GRUPO FOCAL

Esta Seção tem como objetivo obter uma maior interação com os participantes e comentários detalhados sobre qualidade, benefício e melhorias do mecanismo de inspeção, realizou-se o grupo focal. O grupo focal aconteceu através do serviço de comunicação Google Meet, foi escolhida essa ferramenta devido a sua facilidade e meios eficazes para gravação da reunião. Foi utilizado uma lousa digital *online* para tornar o grupo focal mais interativo. Para o desenvolvimento das perguntas do questionário, foi utilizado os métodos da autora Vieira (VIEIRA, 2009), onde exemplifica como construir perguntas para questionários de pesquisa.

4.3.1 Metodologia do grupo focal

Grupo focal é um método muito utilizado nas pesquisas, onde é feito uma reunião com um grupo de pessoas, tendo como o intuito ocasionar a interação entre os participantes, onde coletivamente é possível expressar suas opiniões de acordo com uma metodologia rápida e fácil (DEBUS, 1994). Foi escolhido esse método para conseguir extrair dos participantes informações detalhadas, o instituto de inovação privado disponibilizou os funcionários para a pesquisa, permitindo o acesso direto a todos os participantes.

4.3.1.1 Método de aplicação

Utilizou-se uma ferramenta colaborativa com uma lousa digital *online*, chamada Jamboard[1], que proporciona maior interação com os participantes. A dinâmica foi a seguinte: a cada pergunta, os participantes tiveram dois minutos para responder os *post-its* digitais, enquanto os participantes escreviam no *post-its*, os outros participantes não conseguiam visualizar, mas quando o participante publicava sua resposta, todos conseguiam visualizar. Em seguida ocorreu a discussão entre as perguntas, com o intuito de debater sobre o posicionamento de cada um.

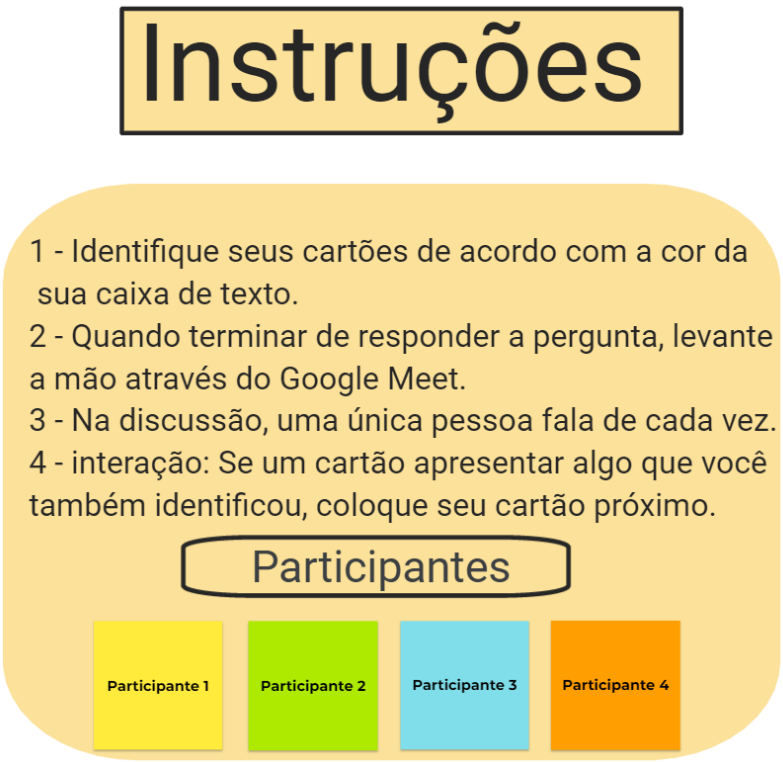
Cada participante teve seu nome escrito na lousa digital em um *post it* de cor diferente, pois a cada pergunta, o participante só podia responder no cartão indicado com sua cor. Os participantes ao terminarem de escrever nos *post-its*, demonstravam levantando a mão através do Google Meet, com isso, não era necessário esperar dois minutos se todos os participantes respondessem antes. Para uma discussão mais compreensível, determinou-se que cada participante tivesse a sua vez de falar. Também foi determinado que se um participante identificasse a mesma opinião de outro participante, era só colocar o seu *post-it* ao lado do *post-it* do outro participante, para representar a sua concordância. A Figura 7 mostra as instruções para o grupo focal.

Para execução do grupo focal, foram seguidos princípios associados a quatro pontos:

1. **Tempo** – O grupo focal deve ser objetivo, com intuito de não ultrapassar duas horas para não causar cansaço e desgaste mental, visto que essa técnica provoca discussões, podendo deixar os participantes fatigados (MAZZA; MELO; CHIESA, 2009). Diante disso,

[1] https://jamboard.google.com/

Figura 7 – Instruções



Fonte: O autor (2022).

foi limitada a quantidade de perguntas e a reunião foi bem objetiva, totalizando uma hora e meia de reunião.

2. **Ambiente** – O encontro ocorreu através de uma reunião *online*, devido que grande parte dos profissionais estão trabalhando *home office*, foi utilizado o serviço de comunicação Google Meet[2].

3. **Gravação** – A reunião foi gravada para documentar todo o processo do estudo e serviu como material para a transcrição do grupo focal.

4. **Equipe** – A equipe foi composta por dois pesquisadores, possuindo o papel de coordenador e observador do estudo. De acordo com Dall et al. (DALL; TRENCH et al., 1999) o coordenador e o observador precisam ter uma boa comunicação com os participantes, demonstrando total domínio dos objetivos do estudo e não podem permitir que a discussão saia do contexto do estudo. Com isso, os avaliadores empenharam-se para possuir essas qualidades através de reuniões com pesquisador experiente em grupo focal, leituras de artigos e aplicação do estudo piloto. Debus et al. (DEBUS, 1994) relata que

[2] https://meet.google.com/

o grupo focal deve possuir no mínimo um coordenador e um observador. Diante disso, a aplicação do grupo focal contou com um coordenador e um observador. Sendo dois pesquisadores, um da UFPE e o outro da UFMA.

4.3.2 Resultados do grupo focal

Esta seção faz uma análise qualitativa das respostas dos participantes a cada uma das perguntas do grupo focal.

Pergunta 1: Quais são os principais benefícios que o *checklist* traz para sua empresa?

Nesta pergunta um dos participantes respondeu que o *checklist* apresentou situações que eles não tinham pensado, também mostrou situações que não conhecia. Onde o participante relatou que se eles ficaram em dúvidas entre alguns assuntos abordados nos itens, eles não sabiam se o sistema atende ao item, e complementou dizendo que fez com que ele pesquisasse mais sobre o assunto. O participante um relatou:

> "Ver os pontos cegos, aqueles pontos que ou não sabe ou tem dúvida, tipo se não sabe ou tem dúvida é porque não ficou claro, se não ficou claro é porque realmente a gente não tem certeza se está em conformidade ou não."

O participante dois argumentou sobre a importância do *checklist* para inspeção do sistema, descrevendo:

> "(..) e isso é muito massa, porque a gente não só pode aplicar nesse projeto que a gente aplicou, mas também estender isso para outros projetos"

Diante das informações dos participantes é notório que o *checklist* apresentou situações desconhecidas pelo participante que o participante chamou de "pontos cegos", ajudando a identificar situações de segurança que acaba ficando negligenciado. Além disso, foi demonstrado o interesse em usar o *checklist* em outros projetos, onde ele fortalece a intenção de uso, que foi uma das perguntas do questionário na Seção4.2.

Pergunta 2: Quais mudanças você faria no *checklist* para melhorar a identificação de defeitos/problemas no sistema?

O participante três relatou que a parte dos comentários do inspetor, por não ser obrigatório, poderá ser retirado ou ser adicionado como obrigatório, o participante evidenciou:

> "Talvez o comentário do avaliador por não ser obrigatório, uma coisa muito aberta, pode ficar meio perdido, as pessoas podem dizer não se aplica e não comentar nada. (..) Eu não comentei porque eu não fui obrigado a isso. Acho que foi mais isso, se vocês quisessem, poderiam até trancar, ou obrigar a pessoa."

Esse participante foi o único que sugeriu mudanças, os outros dois participantes apenas falaram:

> Participante dois: "Eu não, referente a isso, eu não tenho nenhuma mudança."

> Participante um: "Eu não, eu estou bem tranquilo, eu gostei."

De acordo com os relatos dos participantes, só houve uma sugestão de mudança, mas foi relacionado a uma parte opcional do *checklist*, relacionado ao comentário, o participante sugeriu retirar os comentários ou torná-los obrigatório. Os outros participantes não sugeriram mudanças, um deles relata que gostou do *checklist* e não tem mudanças, isso demonstra a aceitação do *checklist* pelo participante para identificação de defeitos.

Pergunta 3: Vocês acharam as recomendações úteis no entendimento da pergunta em si, e que é possível ajudar a resolver possíveis defeitos?

Essa pergunta não estava no planejamento, mas ao decorrer das discussões, foi realizada como acréscimo, com o intuito de identificar se as recomendações tiveram utilidade para os participantes. Com isso, o participante um respondeu que:

> "No meu entendimento ajudou, e até inclusive me forçou a pesquisar informações que achava que fazia e não fazia, e coisas que eu fazia que não sabia que fazia. Então no meu caso ajudou bastante"

O participante três acrescentou que:

> "As recomendações para mim foram uma surpresa boa, que eu consegui entender o contexto daquilo em relação a pergunta, ficou muito mais claro, parece que as recomendações respondem até onde exatamente o que se trata a pergunta, fiquei olhando pra um e pro outro (pergunta e recomendação). Pra mim foi positivo."

O participante dois apenas concordou com os demais.

Diante os relatos dos participantes, podemos identificar que as recomendações foram importantes para o entendimento de alguns itens, isso faz uma reflexão, que talvez as perguntas

possam ser mais claras para o participante compreender sem a necessidade de olhar as recomendações para entender o contexto das questões, ou se o participante não conhecia algum termo utilizado na pergunta e por isso as recomendações foram úteis para identificar o contexto da pergunta, visto que um dos participantes diz que as recomendações o induziu a pesquisar mais sobre o assunto.

Pergunta 4: Para vocês as instruções e o vídeo de treinamento para preenchimento do *checklist* foram úteis?

Essa foi a segunda pergunta adicional, teve como o objetivo entender se os participantes precisavam do vídeo para realizar a inspeção. Os participantes relataram que não achou necessário, ressaltando que apenas o *checklist* no Excel consegue guiar os inspetores. O participante três disse:

> "No meu ponto de vista, o próprio Excel já me orienta muito bem aonde que eu devo colocar as informações."

O participante um complementou:

> "Eu achei as orientações do Excel bem didático"

Por fim, o participante dois concordou com os anteriores. Diante os relatos, os participantes acreditam que não é necessário assistir o vídeo para realizar a inspeção, mas poderá ser um adicional para facilitar a utilização de outros inspetores.

Pergunta 5: Você considera o checklist completo para identificação de problemas de segurança nos dispositivos IoT? Se não, que aspectos você acha que devem ser incluídos para que todos os possíveis defeitos sejam identificados?

Essa pergunta foi realizada com o intuito de identificar problemas de segurança nos dispositivos IoT que essa versão do *checklist* não abrangeu, para que o *checklist* possa ter futuras versões, abrangendo partes não identificadas neste estudo. O participante um sugeriu:

> "É focar na questão das redes *cloud*, redes de nevoeiro que é um conceito mais ou menos novo, que surgiu em 1997 por aí, e nas redes LAN convencionais. (..) Então seria legal pesquisar os meios que são mais utilizados e focar neles, depois aí fica padrão, como vocês vão pegar já os métodos mais utilizados os que estão em baixo emergentes eu não daria muito critério agora, não daria muita credibilidade, porque esses meios tendem a se fundir ou desaparecer com o decorrer do tempo.

> Aí seria só focar nos métodos mais utilizados, nos tipos de nuvem mais utilizados para IoT, aí ajudava bastante vocês, seria um direcionamento mais preciso, não ficaria tão abrangente."

Os demais participantes não tiveram sugestões. O participante três destacou:

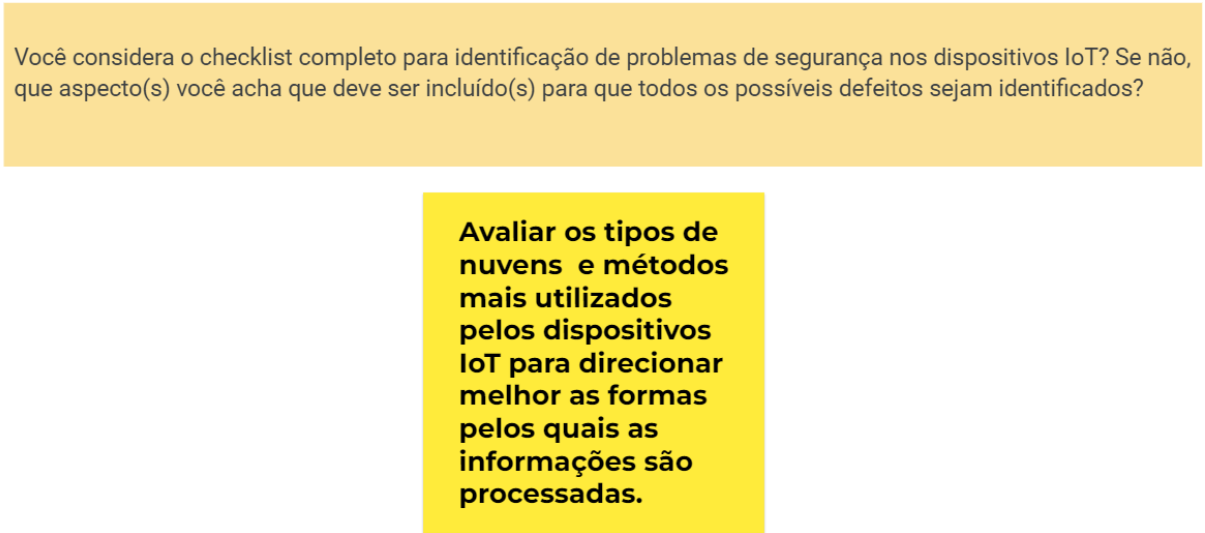
> "Eu achei bem interessante a forma como conseguiu se aprofundar mais tecnicamente em relação a LGPD".

> "Eu vi que a forma que vocês colocaram ficou mais em relação a infra geral como um todo, e eu acho bacana, eu concordo com que já está no *checklist*."

Através dos relatos dos participantes, um deles sugeriu que o *checklist* abrangesse aos sistemas de rede em nuvem, servindo como um direcionamento para a expansão do *checklist*, isso pode impactar o *checklist* para criações de novas versões relacionadas a diversas áreas dos sistemas IoT.

Alguns participantes optaram por não responder no *post it digital*, preferiram apenas se expressar oralmente, porém, em algumas perguntas os participantes registraram um resumo do seu posicionamento. Como pode ser visto na Figura 8

Figura 8 – Questão do grupo focal.



Fonte: O autor (2022).

Pergunta 6: Quais aspectos foram fáceis e difíceis ao utilizar o *checklist* na inspeção?

No questionário apresentado na Seção4.2, foram realizadas perguntas sobre a facilidade de uso, onde teve resultados satisfatórios, mas para investigar mais detalhadamente, essa

questão tem o intuito de identificar o que foi fácil de usar, adicionando também o que eles acharam difícil. Os participantes não apresentaram nenhum aspecto difícil, apenas destacaram a facilidade de usá-lo. Um dos participantes comentou que a dificuldade foi só em entender perguntas sobre assuntos que o participante não conhecia e isso fez ele pesquisar sobre o assunto e poder responder de maneira correta, o participante também disse que teve um grande aprendizado. A resposta do participante um foi:

> "Pra mim foi bem tranquilo, a dificuldade que teve foi natural, em relação somente com aquelas perguntinhas assim de coisas que eu realmente desconhecia (..) fui provocado a pesquisar, isso aí é massa, é bom, a ideia é essa mesmo, tanto pesquisar no sentido de conhecer quanto dizer olha realmente a gente não faz isso, e aí a gente que discutir com o time agora para entrar essa recomendação aí no jogo, então achei muito massa."

O participante três complementou com o texto:

> "Em relação ao checklist eu achei bem prático, bem direto ao ponto"

4.4 SUMÁRIO DOS RESULTADOS DE CADA QUESTÕES DE PESQUISA

Para responder a questão de pesquisa (questão 1: Como propor um *checklist* de inspeção de soluções computacionais específicas de IoT frente a LGPD?). Existem várias formas de propor um mecanismo de inspeção, mas para responder a essa pergunta, apresentamos o processo da proposta desenvolvida neste trabalho. Foi necessário todo um planejamento de pesquisa, onde a criação do *checklist* teve como base inicial uma revisão sistemática, sendo possível encontrar soluções computacionais específicas de IoT frente a LGPD. Em seguida foi desenvolvido o *checklist*, que é detalhado no Capítulo 3. No qual apresenta todo o processo de desenvolvimento. Por fim, a importância de realizar a avaliação com o público alvo do *checklist*, que foi avaliado com um instituto privado de inovação. Diante disso, todo processo de pesquisa, desenvolvimento e avaliação do mecanismo é um caminho de como propor um *checklist* de inspeção. Esse método de criação pode ser melhorado. Temos que levar em consideração que este não é um mecanismo perfeito. Como na Seção 5.1 são abordadas algumas limitações e ameaças à validade, onde deve ser levado em consideração ao seguir o mesmo procedimento de criação deste mecanismo de inspeção.

A segunda pergunta de pesquisa (questão 2 - O checklist proposto ajuda na identificação de problemas em relação à soluções computacionais específicas de IoT frente a LGPD?) é respondida através na Subseção 4.2.2, onde apresenta o resultado total do índice de adequação da empresa, demonstrando uma porcentagem de 40,7%(11) de problemas identificados no sistema. Além disso, na Seção 4.2, apresenta os resultados de um questionário de utilidade, de acordo com os dados, é identificado que os participantes acreditam que o *checklist* ajuda na identificação a encontrar defeito/problemas nos sistemas.

4.5 RESUMO DO CAPÍTULO

Este capítulo apresentou o processo de avaliação do mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT. Apresentou o perfil dos participantes, relatando formação e experiências profissionais. Descreveu os resultados do questionário para identificar a viabilidade do mecanismo de inspeção proposto em termos de utilidade, facilidade e intenção de uso. Apresentou os resultados da análise das discrepâncias das respostas dos participantes, conseguindo identificar os defeitos reais. Por fim, foi apresentado os resultados de um grupo focal com os participantes, debatendo as discrepâncias das respostas.

5 CONCLUSÕES

A proposta preliminar deste trabalho foi explorar os problemas da indústria ligados à verificação de conformidade de sistemas/dispositivos IoT à normas de proteção de dados. Foi realizado uma pesquisa exploratória na literatura e através de relatos de profissionais de desenvolvimento de *software* em uma empresa de Pernambuco, identificamos que um grande desafio que se mostrava para a indústria de *software* brasileira era a conformidade com a LGPD. Trabalhos semelhantes que também obtiveram a mesma percepção (RAPÔSO et al., 2019; MENDES; VIANA; RIVERO, 2021). Aprofundando a pesquisa, definimos unir as duas frentes de pesquisa, LGPD e IoT.

Com o objetivo de operacionalizar um mecanismo de averiguação da conformidade de projetos IoT com a LGPD, propomos um *checklist*. Esse *checklist* foi proposto com base nas características específicas do dispositivos de IoT. O *checklist* proposto neste trabalho pode ser considerado uma extensão de um outro *checklist*, mas este outro foca na averiguação da conformidade com a LGPD de forma geral em projetos de *software*. Em conjunto, os *checklists* auxiliam os analistas e consultores na averiguação antes, durante e depois da realização de projetos de *software* onde dados são consumidos por dispositivos IoT.

A avaliação do *checklist* proposto foi feita através da percepção de profissionais que trabalham em projetos IoT de um instituto privado de inovação. Nesta avaliação, de acordo com a percepção dos avaliados, o *checklist* proposto foi capaz de auxiliar os profissionais na averiguação de adequação à LGPD em projetos que envolvem IoT.

Podemos ressaltar alguns resultados. No questionário de pós inspeção (Seção 4.2), demonstraram a intenção em utilizar o mecanismo proposto para avaliar outros sistemas, reforçaram a intenção durante o grupo focal (Seção 4.3), onde constantemente relataram essa pretensão. Além disso, um dos coordenadores da empresa de inovação tecnológica que acompanhou todo o processo da pesquisa (inclusive participou como ouvinte do grupo focal) concordou com todos os defeitos encontrados. Além disso, este mesmo coordenador declarou que utilizará o instrumento para avaliar a segunda versão do sistema que foi tomado como exemplo.

5.1 LIMITAÇÕES E AMEAÇAS A VALIDADE

Este trabalho apresenta limitações e ameaças a validade que precisam ser consideradas. São apresentadas a seguir:

A avaliação ocorreu em apenas uma empresa. Por isso, devemos ressaltar que os resultados obtidos não podem ser generalizados, visto que ocorreram em apenas uma empresa. Portanto, é necessário realizar replicações para identificar se esses resultados se aplicam a outras empresas.

A pesquisa foi avaliada com profissionais sem muita experiência, principalmente em LGPD. Diante disso, não pudemos avaliar a completude do *checklist* com base na experiência dos participantes em relação a LGPD.

Os itens do *checklist* que não foram identificados como discrepantes. Quando todos os avaliadores por unanimidade identificaram que o item era defeituoso ou aderente no questionário de pós-inspeção, foi imediatamente classificado como defeituoso ou aderente. Como os participantes não possuem muita experiência, esses itens deveriam ter sido apresentados na discussão da subseção 4.2.2, para ocorrer uma discussão sobre a discriminação de defeitos dos itens e identificar se de fato todos continuavam com a mesma opinião que relataram no questionário de pós-inspeção.

5.2 TRABALHOS FUTUROS

Como trabalho futuro pretendemos automatizar o mecanismo para auxiliar a averiguação de adequação à LGPD considerando as características específicas com IoT. Uma ferramenta web colaborativa poderá facilitar a utilização do instrumento por inspetores, além de possibilitar o compartilhamento das avaliações.

Outro trabalho futuro é a replicação do estudo em outras empresas. Desta forma, poderemos identificar se os resultados encontrados podem ser observados em outras empresas. Além disso, está replicação possibilitará melhorias em versões futuras do instrumento.

Outro trabalho futuro é identificar outras demandas de extensões do *checklist* genérico para avaliação de conformidade e evoluir seguindo a mesma metodologia desta dissertação, ampliando o *checklist* para outras áreas.

Outro trabalho futuro é realizar a avaliação com participantes com muita experiência em LGPD para conseguir avaliar a completude do instrumento.

REFERÊNCIAS

AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M.; AYYASH, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, IEEE, v. 17, n. 4, p. 2347–2376, 2015.

ALNEYADI, S.; SITHIRASENAN, E.; MUTHUKKUMARASAMY, V. A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, v. 62, p. 137–152, 2016. ISSN 1084-8045. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804516000102>.

ALVES, C. B. Segurança da informação vs engenharia social: Como se proteger para não ser mais uma vítima. *Brasília: UDF*, 2010.

ANGST, C. M.; BLOCK, E. S.; D'ARCY, J.; KELLEY, K. When do it security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. *Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches (January 24, 2016). Angst, CM, Block, ES, D'Arcy, J., and Kelley, K*, p. 893–916, 2017.

ASHTON, K. et al. That 'internet of things' thing. *RFID journal*, v. 22, n. 7, p. 97–114, 2009.

ATAMLI, A. W.; MARTIN, A. Threat-based security analysis for the internet of things. In: *2014 International Workshop on Secure Internet of Things*. [S.l.: s.n.], 2014. p. 35–43.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer networks*, Elsevier, v. 54, n. 15, p. 2787–2805, 2010.

BADII, C.; BELLINI, P.; DIFINO, A.; NESI, P. Smart city iot platform respecting gdpr privacy and security aspects. *IEEE Access*, v. 8, p. 23601–23623, 2020.

BARANAUSKAS, M. C. C.; SOUZA, C. S. de; PEREIRA, R. Grandihc-br: prospecção de grandes desafios de pesquisa em interação humano-computador no brasil. In: *Companion Proceedings of the 11th Brazilian Symposium on Human Factors in Computing Systems*. [S.l.: s.n.], 2012. p. 63–64.

BARATI, M.; RANA, O.; PETRI, I.; THEODORAKOPOULOS, G. Gdpr compliance verification in internet of things. *IEEE Access*, IEEE, v. 8, p. 119697–119709, 2020.

BARRIONUEVO, J. M.; BERRONE, P.; RICART, J. E. Smart cities, sustainable progress. *Iese Insight*, v. 14, n. 14, p. 50–57, 2012.

BERNARDI, E.; MIYAKE, M. Y.; SANTOS, A. S. dos; MERICHELLI, M. P.; PEREIRA, M. J.; POLKORNY, M. Brazilian scenarios for smart cities deployment from public policies perspectives. In: *2020 IEEE International Smart Cities Conference (ISC2)*. [S.l.: s.n.], 2020. p. 1–8.

BOCHIE, K.; GONZALEZ, E. R.; GISERMAN, L. F.; CAMPISTA, M. E. M.; COSTA, L. H. M. Detecção de ataques a redes iot usando técnicas de aprendizado de máquina e aprendizado profundo. In: SBC. *Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2020. p. 257–270.

BORMANN, C.; ERSUE, M.; KERANEN, A. Terminology for constrained-node networks. *Internet Engineering Task Force (IETF): Fremont, CA, USA*, p. 2070–1721, 2014.

BRASILINE. *Dados De 70 Milhões De Brasileiros Com CNH Foram Vazados Pelo Detran*. 2019. Urlhttps://bityli.com/WDcRY.

BUI, N. H.; PHAM, C.; NGUYEN, K. K.; CHERIET, M. Energy efficient scheduling for networked iot device software update. In: *2019 15th International Conference on Network and Service Management (CNSM)*. [S.l.: s.n.], 2019. p. 1–5.

CAMELO, M. N. *G-Priv: Um Guia para Especificação de Requisitos de Privacidade em Conformidade com a LGPD*. 139 p. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Pernambuco, 2022.

CASSIANI, S. H. D. B.; CALIRI, M. H. L.; PELÁ, N. T. R. A teoria fundamentada nos dados como abordagem da pesquisa interpretativa. *Revista latino-americana de enfermagem*, SciELO Brasil, v. 4, p. 75–88, 1996.

CHAGAS, G. A.; BIAZOTTO, L. H. Gestão de tecnologia da informação na visão da lgpd. *Prospectus (ISSN: 2674-8576)*, v. 3, n. 1, p. 3–32, 2021.

CHANDRAMOHAN, M.; TAN, H. B. K. Detection of mobile malware in the wild. *Computer*, IEEE Computer Society, v. 45, n. 09, p. 65–71, 2012.

CHEN, L.-A.; ZHUO, J.-Z.; CAI, Y.-Z.; WANG, Y.-T.; TSAI, M.-H. Finding periodicity of subflows in sdn-based iot. In: *2020 International Computer Symposium (ICS)*. [S.l.: s.n.], 2020. p. 304–309.

CORBIN, J.; STRAUSS, A. Strategies for qualitative data analysis. *Basics of Qualitative Research. Techniques and procedures for developing grounded theory*, v. 3, n. 10.4135, p. 9781452230153, 2008.

DALL, C. M.; TRENCH, M. H. et al. Grupos focais como estratégia metodológica em pesquisas na enfermagem. *Revista Gaúcha de Enfermagem*, v. 20, n. 1, p. 5, 1999.

DANTAS, Á. M. C.; VIANA, H.; ABIJAUDE, J.; SOBREIRA, P. Internet das coisas e aprendizagem colaborativa: Revisao sistemática da literatura. In: *Brazilian Symposium on Computers in Education (Simpósio Brasileiro de Informática na Educação-SBIE)*. [S.l.: s.n.], 2018. v. 29, n. 1, p. 278.

DEBUS, M. Manual para excelencia en la investigación mediante grupos focales. In: *Manual para excelencia en la investigación mediante grupos focales*. [S.l.: s.n.], 1994. p. 97–97.

DHILLON, P. K.; KALRA, S. A lightweight biometrics based remote user authentication scheme for iot services. *Journal of Information Security and Applications*, v. 34, p. 255–270, 2017. ISSN 2214-2126. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214212616301442>.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, v. 12, n. 2, p. 91–108, 2011.

FERENCZ, K.; DOMOKOS, J.; KOVÁCS, L. Review of industry 4.0 security challenges. In: *2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. [S.l.: s.n.], 2021. p. 245–248.

FLICK, U. *Qualidade na pesquisa qualitativa: coleção pesquisa qualitativa*. [S.l.]: Bookman editora, 2009.

FOLLONE, R. A.; FILHO, A. S. A conexão da lgpd e cdc: A proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental. In: *Anais do Congresso Brasileiro de Processo Coletivo e Cidadania*. [S.l.: s.n.], 2020. p. 937–959.

FURFARO, A.; ARGENTO, L.; PARISE, A.; PICCOLO, A. Using virtual environments for the assessment of cybersecurity issues in iot scenarios. *Simulation Modelling Practice and Theory*, v. 73, p. 43–54, 2017. ISSN 1569-190X. Smart Cities and Internet of Things. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1569190X16302374>.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-BARRETTO, M. R. *Lei Geral de Proteção de Dados (LGPD): guia de implantação*. [S.l.]: Editora Blucher, 2020.

GARG, H.; DAVE, M. Securing iot devices and securelyconnecting the dots using rest api and middleware. In: *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. [S.l.: s.n.], 2019. p. 1–6.

GERSHENFELD, N.; KRIKORIAN, R.; COHEN, D. The internet of things. *Scientific American*, JSTOR, v. 291, n. 4, p. 76–81, 2004.

GOBEO, A.; FOWLER, C.; BUCHANAN, W. J. 1 the gdpr fundamentals. In: _____. *GDPR and Cyber Security for Business Information Systems*. [S.l.: s.n.], 2020. p. 1–36.

GOMES, J. T. C. *Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde*. Tese (Doutorado), 2019.

GUO, Z.; KARIMIAN, N.; TEHRANIPOOR, M. M.; FORTE, D. Hardware security meets biometrics for the age of iot. In: IEEE. *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*. [S.l.], 2016. p. 1318–1321.

HUANG, X.; LU, Y.; LI, D.; MA, M. A novel mechanism for fast detection of transformed data leakage. *IEEE Access*, v. 6, p. 35926–35936, 2018.

ISO, A. *ASSOCIAçãO BRASILEIRA DE NORMAS TéCNICAS. NBR/ISO/IEC 27002:2013 tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação*. Brasília, DF: Senado: [s.n.], 2013.

JUNEJA, P.; KAUR, P. Software engineering for big data application development: Systematic literature survey using snowballing. In: *2019 International Conference on Computing, Power and Communication Technologies (GUCON)*. [S.l.: s.n.], 2019. p. 492–496.

KALINOWSKI, M.; SPíNOLA, R.; NETO, A. C. D.; BOTT, A.; TRAVASSOS, G. Inspeções de requisitos de software em desenvolvimento incremental: Uma experiência prática. In: *Anais do VI Simpósio Brasileiro de Qualidade de Software*. Porto Alegre, RS, Brasil: SBC, 2007. p. 389–396. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbqs/article/view/15591>.

KHANDELWAL. *10 real world applications of the internet of things (IoT)*. 2019. Urlencurtador.com.br/iORUW.

KHANDELWAL. *Hackers Stole Customers' Credit Cards from 103 Checkers and Rally's Restaurants.* 2019. Urlhttp://bit.do/e25P6.

KHASHIROVA, T. Y.; MAMUCHIEV, I. I.; MAMUCHIEVA, M. I.; OZHIGANOVA, M. I.; KOSTYUKOV, A. D.; SHUMEIKO, I. Assessment of information security in integrated systems. In: *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT QM IS)*. [S.l.: s.n.], 2021. p. 201–205.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Citeseer, 2007.

KOURTIT, K.; NIJKAMP, P.; ARRIBAS, D. Smart cities in perspective–a comparative european study by means of self-organizing maps. *Innovation: The European journal of social science research*, Taylor & Francis, v. 25, n. 2, p. 229–246, 2012.

LEITE, L. R. C. Internet das coisas (iot): vulnerabilidades de segurança e desafios. Faculdade de Tecnologia de Americana, 2019.

LOHAN, E. S.; KOIVISTO, M.; GALININA, O.; ANDREEV, S.; TOLLI, A.; DESTINO, G.; COSTA, M.; LEPPANEN, K.; KOUCHERYAVY, Y.; VALKAMA, M. Benefits of positioning-aided communication technology in high-frequency industrial iot. *IEEE Communications Magazine*, v. 56, n. 12, p. 142–148, 2018.

MACHADO, R.; KREUTZ, D.; PAZ, G.; RODRIGUES, G. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. In: *Anais da XVII Escola Regional de Redes de Computadores*. Porto Alegre, RS, Brasil: SBC, 2019. p. 154–159. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/9230>.

MANSFIELD-DEVINE, S. Android malware and mitigations. *Network Security*, Elsevier, v. 2012, n. 11, p. 12–20, 2012.

MAZZA, V. de A.; MELO, N. S. F. de O.; CHIESA, A. M. O grupo focal como técnica de coleta de dados na pesquisa qualitativa: relato de experiência. *Cogitare Enfermagem*, v. 14, n. 1, 2009.

MEDEIROS, L. S.; STRAUSS, E.; NICOLAU, A. dos S.; MELLO, F. L. de; JÚNIOR, M. V. B.; FAZZIONI, P. F. P. da C. Mba em governança, projetos e serviços de ti (mgps). 2017.

MENDES, J. *Desenvolvimento de um Checklist para Avaliação da Adequação de Sistemas Computacionais à Lei Geral de Proteção de Dados Brasileira*. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal do Maranhão, 2022.

MENDES, J.; VIANA, D.; RIVERO, L. 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: *Brazilian Symposium on Software Engineering*. [S.l.: s.n.], 2021. p. 263–268.

MENEGHELLO, F.; CALORE, M.; ZUCCHETTO, D.; POLESE, M.; ZANELLA, A. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, v. 6, n. 5, p. 8182–8201, 2019.

MERRIAM, S. B. Qualitative research: A guide to design and implementation. 2009.

NEPOMUCENO, V.; SOARES, S. Avoiding plagiarism in systematic literature reviews: An update concern. In: *Proceedings of the 14th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. New York, NY, USA: Association for Computing Machinery, 2020. (ESEM '20). ISBN 9781450375801. Disponível em: <https://doi.org/10.1145/3382494.3422170>.

NESHENKO, N.; BOU-HARB, E.; CRICHIGNO, J.; KADDOUM, G.; GHANI, N. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys Tutorials*, v. 21, n. 3, p. 2702–2733, 2019.

OLIVEIRA, N. de; GOMES, M.; LOPES, R.; NOBRE, J. Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019.

PARENT, D. *Data Breachers - The Worst So Far*. 2019. Urlhttps://www.identityforce.com/blog/2019-data-breaches.

PATEL, A. A.; SONI, S. J. A novel proposal for defending against vampire attack in wsn. In: *2015 Fifth International Conference on Communication Systems and Network Technologies*. [S.l.: s.n.], 2015. p. 624–627.

PEREIRA, A. G. Sistema de irrigação automatizado utilizando o conceito de iot para tomada de decisão. 2020.

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

PIRES, P. F.; DELICATO, F.; BATISTA, T.; BARROS, T.; CAVALCANTE, E.; PITANGA, M. Plataformas para a internet das coisas. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 2015.

POHLMANN, S. *Sobre cintos de segurança, LGPD, pequenas empresas e interpretação*. 2020. Urlhttps://www.serpro.gov.br/lgpd/noticias/2020/cinto-seguranca-lgpd-pequenas-empresas-interpretaca o.

POONIA, A. S.; SINGH, S. Malware detection by token counting. In: *2014 International Conference on Contemporary Computing and Informatics (IC3I)*. [S.l.: s.n.], 2014. p. 1285–1288.

PRESSER, M.; GLUHAK, A. The internet of things. *Connecting the Real World with the Digital World, EURESCOM mess@ ge–The Magazine for Telecom Insiders*, v. 2, p. 28, 2009.

RAPÔSO, C. F. L.; LIMA, H. M. de; JUNIOR, W. F. de O.; SILVA, P. A. F.; BARROS, E. E. de S. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. *RACE-Revista de Administração do Cesmac*, v. 4, p. 58–67, 2019.

RIBEIRO, S. L.; NAKAMURA, E. T. Privacy protection with pseudonymization and anonymization in a health iot system: Results from ocariot. In: *2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*. [S.l.: s.n.], 2019. p. 904–908.

RILEY, D. *Massachusetts general hospital data breach latest failure to protect patient data*. 2019.

SACHIDANANDA, V.; SIBONI, S.; SHABTAI, A.; TOH, J.; BHAIRAV, S.; ELOVICI, Y. Let the cat out of the bag: A holistic approach towards security analysis of the internet of things. In: *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*. [S.l.: s.n.], 2017. p. 3–10.

SARACINO, A.; SGANDURRA, D.; DINI, G.; MARTINELLI, F. Madam: Effective and efficient behavior-based android malware detection and prevention. *IEEE Transactions on Dependable and Secure Computing*, v. 15, n. 1, p. 83–97, 2018.

SHAO, X.; OINAS-KUKKONEN, H. How does gdpr (general data protection regulation) affect persuasive system design: design requirements and cost implications. In: SPRINGER. *International Conference on Persuasive Technology*. [S.l.], 2019. p. 168–173.

SHARMEEN, S.; HUDA, S.; ABAWAJY, J. H.; ISMAIL, W. N.; HASSAN, M. M. Malware threats and detection for industrial mobile-iot networks. *IEEE Access*, v. 6, p. 15941–15957, 2018.

SOUZA, J. S. de; ABE, J. M.; LIMA, L. A. de; SOUZA, N. A. de. The general law principles for protection the personal data and their importance. *arXiv preprint arXiv:2009.14313*, 2020.

TEDESCO, I. C.; SANTOS, B. N. D.; BRUNHEROTO, P. H.; CRUZ, N. D. D. L. D.; DESCHAMPS, F. Implementação de dispositivos iot para manutenção preditiva: Um estudo de caso. 2019.

TEKEOGLU, A.; TOSUN, A. A testbed for security and privacy analysis of iot devices. In: *2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. [S.l.: s.n.], 2016. p. 343–348.

TIKKINEN-PIRI, C.; ROHUNEN, A.; MARKKULA, J. Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, Elsevier, v. 34, n. 1, p. 134–153, 2018.

TOMA, I.; SIMPERL, E.; HENCH, G. A joint roadmap for semantic technologies and the internet of things. In: *Proceedings of the Third STI Roadmapping Workshop, Crete, Greece*. [S.l.: s.n.], 2009. v. 1, p. 140–53.

URQUHART, L.; LODGE, T.; CRABTREE, A. Demonstrably doing accountability in the internet of things. *International Journal of Law and Information Technology*, Oxford University Press, v. 27, n. 1, p. 1–27, 2019.

VARDHINI, P. H.; RAVINDER, M.; REDDY, P.; SUPRAJA, M. Iot based wireless data printing using raspberry pi. *Journal of Advanced Research in Dynamical and Control Systems*, v. 11, n. 4, p. 2141–2145, 2019.

VENKATESH, V.; GOYAL, S. Expectation disconfirmation and technology adoption: polynomial modeling and response surface analysis. *MIS quarterly*, JSTOR, p. 281–303, 2010.

VENKATESH, V.; MORRIS, M. G. Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior. *MIS quarterly*, JSTOR, p. 115–139, 2000.

VENKATESH, V.; MORRIS, M. G.; DAVIS, G. B.; DAVIS, F. D. User acceptance of information technology: Toward a unified view. *MIS quarterly*, JSTOR, p. 425–478, 2003.

VIEIRA, S. Como elaborar questionários. In: *Como elaborar questionários*. [S.l.: s.n.], 2009. p. 159–159.

VIGNAU, B.; KHOURY, R.; HALLé, S. 10 years of iot malware: A feature-based taxonomy. In: *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. [S.l.: s.n.], 2019. p. 458–465.

WACHTER, S. Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr. *Computer law & security review*, Elsevier, v. 34, n. 3, p. 436–449, 2018.

WAZID, M.; DAS, A. K.; RODRIGUES, J. J. P. C.; SHETTY, S.; PARK, Y. Iomt malware detection approaches: Analysis and research challenges. *IEEE Access*, v. 7, p. 182459–182476, 2019.

WHITMORE, A.; AGARWAL, A.; XU, L. D. The internet of things—a survey of topics and trends. *Information systems frontiers*, Springer, v. 17, n. 2, p. 261–274, 2015.

WU, B.; LU, T.; ZHENG, K.; ZHANG, D.; LIN, X. Smartphone malware detection model based on artificial immune system. *China Communications*, IEEE, v. 11, n. 13, p. 86–92, 2014.

WURM, J.; HOANG, K.; ARIAS, O.; SADEGHI, A.-R.; JIN, Y. Security analysis on consumer and industrial iot devices. In: IEEE. *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*. [S.l.], 2016. p. 519–524.

YANG, K.; FORTE, D.; TEHRANIPOOR, M. M. Protecting endpoint devices in iot supply chain. In: *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. [S.l.: s.n.], 2015. p. 351–356.

ZHOU, W.; YU, B. A cloud-assisted malware detection and suppression framework for wireless multimedia system in iot based on dynamic differential game. *China Communications*, v. 15, n. 2, p. 209–223, 2018.

ZYGIARIS, S. Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of the knowledge economy*, Springer, v. 4, n. 2, p. 217–231, 2013.

APÊNDICE A – TERMO DE CONSENTIMENTO E CARACTERIZAÇÃO

Termo de Consentimento e Caracterização

Prezado(a) Participante,

O DEINF - Departamento de Informática (Universidade Federal do Maranhão) e o CIN - Centro de informática (Universidade Federal de Pernambuco) eventualmente realizam estudos experimentais para caracterizar/avaliar uma determinada tecnologia de software. Você foi previamente selecionado pelo seu perfil/conhecimento/experiência e está sendo convidado a participar desta pesquisa. Esta pesquisa será feita com base em dados coletados a partir de um trabalho prático. Embora o trabalho prático faça parte da disciplina, você tem o direito de não permitir a utilização dos dados do seu trabalho na pesquisa.

1) Procedimentos
O estudo será executado de forma individual, seguindo sempre o planejamento do estudo feito pelo pesquisador(a) responsável. Ao final do estudo será solicitado ao participante que responda um questionário de avaliação sobre a tecnologia de software que está sendo caracterizada/avaliada e uma entrevista Focus Group.

2) Tratamento de possíveis riscos e desconfortos
Serão tomadas todas as providências durante a coleta de dados de forma a garantir a sua privacidade e seu anonimato.

3) Benefícios e Custos
Espera-se que, como resultado deste estudo, você possa aumentar seus conhecimentos, de maneira a contribuir para o aumento da qualidade das atividades com as quais você trabalhe ou possa vir a trabalhar. Este estudo também contribuirá com resultados importantes para a pesquisa de um modo geral para o DEINF. Você não terá nenhum gasto ou ônus com a sua participação no estudo e também não receberá qualquer espécie de reembolso ou gratificação devido à autorização dos seus dados na pesquisa.

4) Confidencialidade da Pesquisa
Toda informação coletada neste estudo é confidencial e seu nome não será identificado de modo algum, a não ser em caso de autorização explícita para este fim. Quando os dados forem coletados, seu nome será removido dos mesmos e não será utilizado em nenhum momento durante a análise ou apresentação dos resultados.

5) Participação
Sua participação neste estudo é muito importante e voluntária, pois requer a sua aprovação para utilização dos dados coletados neste estudo. Você tem o direito de não querer participar ou de sair deste estudo a qualquer momento, sem penalidades. Em caso de você decidir se retirar do estudo, favor notificar o pesquisador(a) responsável.

6) Declaração de Consentimento
Declaro que li e estou de acordo com as informações contidas neste documento e que toda linguagem técnica utilizada na descrição deste estudo de pesquisa foi explicada satisfatoriamente, recebendo respostas para todas as minhas dúvidas. Compreendo que sou livre para não autorizar a utilização dos meus dados neste estudo em qualquer momento, sem qualquer penalidade. Declaro ter mais de 18 anos e concordo de espontânea vontade em participar deste estudo.

*Obrigatório

1. E-mail *

2. Nome Completo do participante *

3. Idade *

4. Genêro *

5. Qual seu nível atual de escolaridade? *

Marcar apenas uma oval.

- Ensino Médio Completo
- Graduação Incompleto
- Graduação Completo
- Pós-Graduação
- Mestrado Incompleto
- Mestrado Completo
- Doutorado Incompleto
- Doutorado Completo

6. Qual o nome do seu curso ou formação acadêmica *

7. Qual cargo atual na empresa *

8. Quanto tempo de experiência no cargo: *

9. Você possui conhecimento sobre inspeção de software? *

Marcar apenas uma oval.

- Sim
- Não

10. Você possui conhecimento sobre a LGPD? *

Marcar apenas uma oval.

- Sim
- Não

11. Descreva qual o nível de conhecimento sobre a LGPD?

12. Você possui conhecimento sobre IoT? *

Marcar apenas uma oval.

- Sim
- Não

13. Descreva Qual o nível de conhecimento sobre IoT?

APÊNDICE B – INSTRUÇÕES DO ESTUDO

Instruções para o Estudo do Checklist LGPD

Este documento contém instruções de como avaliar a viabilidade do uso do checklist de inspeção LGPD.

DEXTERS Lab
Development and User Experience of Technologies and Research in Software Lab

Objetivo do Estudo

- Este estudo propõe avaliar a viabilidade do uso do checklist de inspeção sobre a Lei Geral de Proteção de Dados LGPD, em termos de utilidade, facilidade e intenção de uso.

Guia de Procedimentos

DXT Lab
DEXTERS Lab

Cronograma

ETAPAS	DATA
1-Disponibilização do Material	15/02/2022
2- Termo de Consentimento e Caracterização	15/02/2022
3- Preenchimento do Checklist LGPD	15/02/2022 - 18/02/2022
4- Questionário Pós-Inspeção	15/02/2022 - 18/02/2022
5- Focus Group	21/02/2022

DXT Lab
DEXTERS Lab

Etapa 1-Disponibilização do Material

Após realizado o download do material:

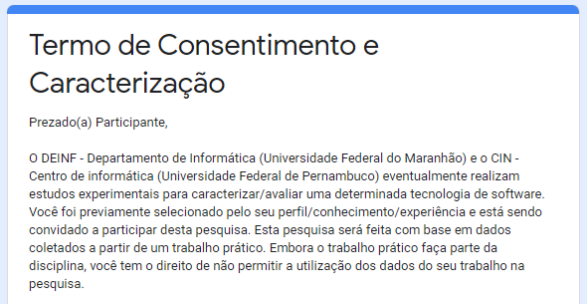
- Descompacte o arquivo baixado em uma pasta.
- O material terá os seguintes arquivos:
- **1-Instruções.pdf** : Passo a passo das etapas do estudo.
- **2-Treinamento.mp4** : Instruções de como preencher o checklist.
- **3-Checklist.xlsx : A**rquivo do checklist de inspeção para LGPD.

DXT Lab
DEXTERS Lab

Etapa 2 - Termo de Consentimento e Caracterização

Você deve responder sobre o termo de consentimento e sobre o seu perfil de participante no link abaixo:

- https://docs.google.com/forms/d/e/1FAIpQLSdjwztMceEqAq6H5xfPPRhaEkXcAbbCKOceMu0VIPEoM3cy-A/viewform


Termo de Consentimento e Caracterização

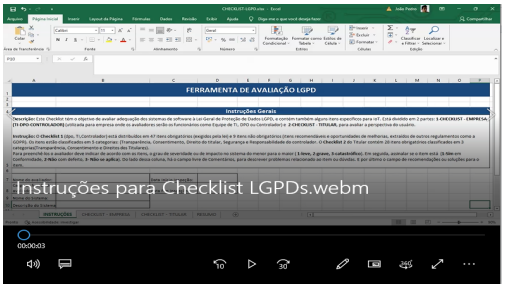
Prezado(a) Participante,

O DEINF - Departamento de Informática (Universidade Federal do Maranhão) e o CIN - Centro de informática (Universidade Federal de Pernambuco) eventualmente realizam estudos experimentais para caracterizar/avaliar uma determinada tecnologia de software. Você foi previamente selecionado pelo seu perfil/conhecimento/experiência e está sendo convidado a participar desta pesquisa. Esta pesquisa será feita com base em dados coletados a partir de um trabalho prático. Embora o trabalho prático faça parte da disciplina, você tem o direito de não permitir a utilização dos dados do seu trabalho na pesquisa.

Preenchimento do Checklist

Etapa 3-Instruções para preenchimento do Checklist

- É disponibilizado um vídeo de treinamento para melhor preenchimento do checklist.
- Duração: 5 minutos.
- Arquivo: Treinamento.mp4



DEXTERS Lab
Development and User Experience of Technologies and Research in Software Lab

Etapa 3-Instruções do Checklist

- O checklist está dividido em 2 partes: 47 Itens Obrigatórios (exigidos pela Lei LGPD) e 36 Itens Não Obrigatórios (itens recomendáveis, oportunidades de melhorias).
- Para dar início ao preenchimento, abra o arquivo Checklist.xlsx em uma ferramenta própria para arquivos de planilha (desejável Excel).

Etapa 3-Instruções do Checklist

Como responder:

Opções de Resposta do Checklist:
- 1 Sim- Em conformidade
- 2 Não- Com defeito
- 3 Não se aplica- item fora do contexto da empresa.

ITENS OBRIGATÓRIOS					
CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIO DO AVALIADOR	RECOMENDAÇÕES
	Sobre Transparência de Dados				
T-01	As finalidades de tratamento de dados foram definidas na organização?	Sim			*Crie um documento definindo uma Política de Privacidade, e descreva quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.*
T-02	O tratamento de dados pessoais é realizado de acordo com a base legal?	Não	Grave		*Na documentação da Política de Privacidade, explique a base legal em que fundamenta o tratamento de dados pessoais.* *Exemplos de base legais:* *I - Mediante o fornecimento de consentimento pelo titular;* *II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;* *Ver completo na lei, disponível: Capítulo 2, Seção 1, artigo 7.*
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	Não se aplica			*O sistema deve disponibilizar a política de privacidade ou termo de consentimento para o titular dos dados, sobre as finalidades.*

Etapa 3-Instruções do Checklist

Grau de Severidade

Caso encontre defeito, preencher o grau de severidade do item:
1 Leve
2 Grave
3 Catastrófico

ITENS OBRIGATÓRIOS					
CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIO DO AVALIADOR	RECOMENDAÇÕES
	Sobre Transparência de Dados				
T-01	As finalidades de tratamento de dados foram definidas na organização?	Sim			*Crie um documento definindo uma Política de Privacidade, e descreva quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.*
T-02	O tratamento de dados pessoais é realizado de acordo com a base legal?	Não	Grave		*Na documentação da Política de Privacidade, explique a base legal em que fundamenta o tratamento de dados pessoais.* *Exemplos de base legais:* *I - Mediante o fornecimento de consentimento pelo titular;* *II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;* *Ver completo na lei, disponível: Capítulo 2, Seção 1, artigo 7.*
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	Não se aplica			*O sistema deve disponibilizar a política de privacidade ou termo de consentimento para o titular dos dados, sobre as finalidades.*

Etapa 3-Instruções do Checklist

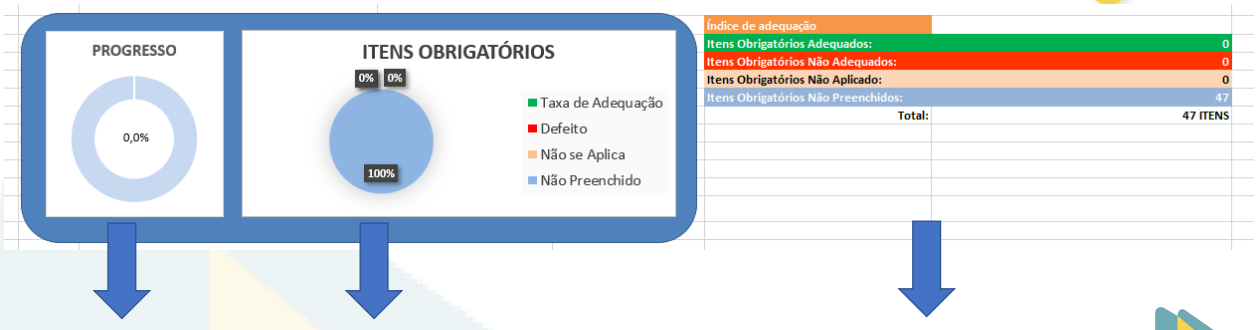
Comentários do Avaliador:

Opcional:
Espaço para comentar sobre as dúvidas, Dificuldades, Entendimento do item etc.

ITENS OBRIGATÓRIOS					
CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIO DO AVALIADOR	RECOMENDAÇÕES
	Sobre Transparência de Dados				
T-01	As finalidades de tratamento de dados foram definidas na organização?	Sim			*Crie um documento definindo uma Política de Privacidade, e descreva quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.*
T-02	O tratamento de dados pessoais é realizado de acordo com a base legal?	Não	Grave		*Na documentação da Política de Privacidade, explique a base legal em que fundamenta o tratamento de dados pessoais.* *Exemplos de base legais:* *I - Mediante o fornecimento de consentimento pelo titular;* *II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;* *Ver completo na lei, disponível: Capítulo 2, Seção 1, artigo 7.*
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	Não se aplica			*O sistema deve disponibilizar a política de privacidade ou termo de consentimento para o titular dos dados, sobre as finalidades.*

Etapa 3-Instruções do Checklist

- GRAFICO: PROGRESSO + INDICE DE ADEQUAÇÃO



Progresso dos Itens que foram preenchidos todo o checklist.

Progresso dos Itens em conformidade, defeito e não aplicáveis..

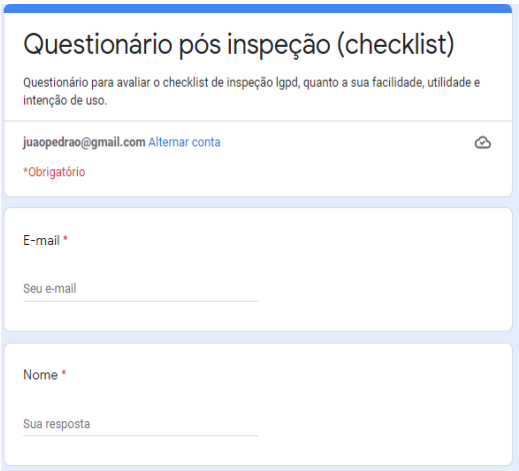
Índice de adequação correspondente.

Etapa 4- Formulário Pós – Inspeção

Após o preenchimento do checklist, responda o Questionário de Pós-Inspeção no link abaixo:

- https://docs.google.com/forms/d/e/1FAIpQLScIidDXSqtKiCKf89jHz--lzRwt-SHvxsGfLuykI1eH0uoHNA/viewform

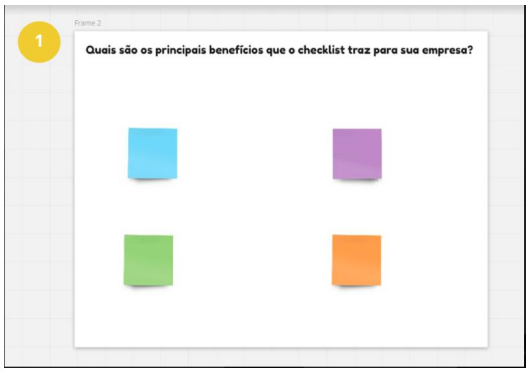
- No final do formulário, anexe o arquivo do checklist preenchido (as informações sigilosas da empresa e dos participantes serão protegidas).



DEXTERS Lab
Development and User Experience of Technologies and Research in Software Lab

Etapa 5- Focus Group

- Reunião Google Meet + ferramenta colaborativa (lousa digital).
- Discussão sobre o checklist LGPD.



DXT Lab
DEXTERS Lab

APÊNDICE C – QUESTIONÁRIO DE PÓS INSPEÇÃO

Questionário pós inspeção (checklist)

Questionário para avaliar o checklist de inspeção lgpd, quanto a sua facilidade, utilidade e intenção de uso.

Os arquivos enviados por upload serão compartilhados fora da organização a que pertencem.
*Obrigatório

1. Nome *

2. Como base no uso deste checklist, selecione o seu grau de concordância com as afirmativas a seguir com relação a sua percepção de FACILIDADE DE USO do mesmo. *

Marcar apenas uma oval por linha.

	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
O checklist utilizado foi claro e fácil de entender.				
De maneira geral, eu acho fácil encontrar defeitos / problemas no sistema com o checklist utilizado.				
O checklist utilizado demandou pouco esforço mental.				

3. Com base na UTILIDADE DO USO. *

Marcar apenas uma oval por linha.

	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
O checklist utilizando me permite realizar a inspeção do sistema mais rapidamente.				
O checklist utilizado melhora a minha produtividade ao identificar defeitos / problemas no sistema.				
Eu acho que o checklist utilizado é útil para encontrar defeitos / problemas no sistema.				

4. Com base na INTENÇÃO DE USO. *

Marcar apenas uma oval por linha.

	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
Eu pretendo usar o checklist para encontrar defeitos / problemas no sistema futuramente.				
Assumindo que eu tenha acesso ao checklist, pretendo usá-lo para encontrar defeitos / problemas em outros sistemas.				
Eu recomendaria o checklist utilizado para outras empresas.				

5. Faça upload do arquivo do checklist.xls respondido após a inspeção.

   Arquivos enviados:

APÊNDICE D – CHECKLIST

1 - CHECKLIST EMPRESA

Índice de adequação	
Itens Obrigatórios Adequados:	0
Itens Obrigatórios Não Adequados:	0
Itens Obrigatórios Não Aplicado:	0
Itens Obrigatórios Não Preenchidos:	0
Total:	47 ITENS

Legenda Para preenchimento:	
Resposta	Sim / Não / Não se aplica
Grau de Severidade	Leve / Grave / Catastrófico
Comentário do avaliador	Aberto (Dúvida,sugestões,crítica)

ITENS OBRIGATÓRIOS

CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIO DO AVALIADOR	RECOMENDAÇÕES
	Sobre Transparência de Dados (T)				
T-01	As finalidades de tratamento de dados foram definidas na organização?				*Crie um documento definindo uma Política de Privacidade e os Termos de Consentimento, descrevendo quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.*
T-02	O tratamento de dados pessoais é realizado de acordo com uma base legal?				*Na documentação da Política de Privacidade e dos Termos de Consentimento, explique a base legal em que fundamenta o tratamento de dados pessoais.* *Exemplos de base legais: I - Mediante o fornecimento de consentimento pelo titular; II - Para o cumprimento de obrigação legal ou regulatória pelo controlador. Ver completo na lei, disponível: Capítulo 2, Seção 1, artigo 7.*
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?				*O sistema deve disponibilizar a Política de Privacidade e/ou Termos de Consentimento para o titular dos dados, sobre as finalidades de tratamento.*
T-04	O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?				*Revisar o consentimento e implementar as alterações que não estão de acordo com o que foi informado ao titular.*
T-05	O sistema informa para o titular a forma e duração do tratamento dos seus dados pessoais de maneira gratuita e acessível?				*Descreva no documento da Política de Privacidade e no Termo de Consentimento, sobre a forma que se realizará o tratamento de dados e qual a sua duração, disponibilizando essas informações sempre para o titular.*
T-06	O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?				*Crie um canal de comunicação entre o titular e a empresa para facilitar que o titular possa requisitar a integralidade dos seus dados pessoais, sempre de forma gratuita e sem lentidão da operação. Exemplo: Disponibilizar e-mail, telefone, ou criar uma página exclusiva para a comunicação.*

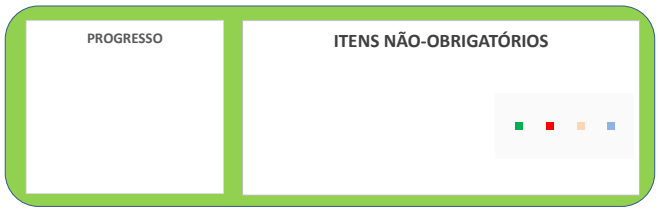
T-07	O sistema armazena com exatidão e clareza os dados pessoais coletados dos titulares?				*Durante a coleta, garanta que os dados pessoais estão sendo informados corretamente. EX: Usar uma validação de campos nos formulários (CPF, Cep).*
T-08	O sistema mantém atualizados os dados pessoais, conforme necessário e para o cumprimento da finalidade de seu tratamento?				*Crie um processo para mapear e revisar os dados pessoais no banco de dados, e se descobrir que os dados pessoais estão incorretos, é necessário corrigir ou apagar o mais rápido possível. E sempre que necessário, pedir ao titular que atualize seus dados para cumprimento da finalidade de tratamento.*
T-09	O sistema disponibiliza para o titular as informações sobre a realização do tratamento de dados e a identidade do controlador?				*Disponibilizar para o titular na Política de Privacidade e no Termo de Consentimento, informações claras e precisas sobre: a) Finalidades de Processamento; b) A identidade e contato do controlador; c) Os dados envolvidos; d) A base legal; e) Detalhes de transferências de dados fora do brasil; f) Período de retenção de dados; g) Os direitos do titular.*
T-10	A organização realiza o tratamento de dados quando baseado no seu legítimo interesse, de forma adequada com a lei?				*A empresa realizará uma análise do legítimo interesse para verificar se a hipótese de tratamento pode se enquadrar na base legal. Essa análise deve demonstrar que: a) Há um interesse legítimo válido; b) O processamento de dados é estritamente necessário na busca do interesse legítimo; e c) O processamento não é prejudicial ou anulado pelos direitos do indivíduo.*
T-11	O sistema mantém registros das operações de tratamento de dados, especialmente quando baseado em seu legítimo interesse?				*Armazenar no banco de dados informações sobre as operações de tratamento dos dados, para possíveis comprovações legais.*
T-12	O sistema informa para o titular e autoridades competentes sobre informações de tratamento de dados, principalmente quando baseado em seu legítimo interesse?				*Elaborar relatórios das operações de tratamento de dados, principalmente quando baseado no seu legítimo interesse, e disponibilizar quando requisitado para o titular e para as autoridades competentes, como a ANPD.*
T-13	O sistema realiza o tratamento de dados pessoais ou dados sensíveis, de forma que não possam ser conectados a um titular de dados, quando for requisitado?				*Analisar quais dados pessoais deverão ser anonimizados, ou em outros casos, realizar uma pseudonimização. Exemplo: Uma versão semelhante aos dados originais, mas sem revelar a verdadeira informação do titular.*
T-14	O sistema informa ao titular de dados sobre a existência de tratamento dos seus dados, antes da coleta?				*Disponibilizar ao titular, sempre em destaque e com avisos, sobre os dados pessoais que serão coletados e solicitar o consentimento do titular.*
	Sobre Consentimento do Titular (C)				
C-01	O sistema permite que o titular forneça o seu consentimento de forma autônoma e clara, para realizar o tratamento de seus dados?				*No Termo de Consentimento, recomenda-se usar uma linguagem clara e objetiva, sem propaganda enganosa, evitando caixas pré-marcadas, e também possuir uma opção para que o titular possa negar ou retirar o seu consentimento sem ter nenhum prejuízo.*
C-02	O sistema solicita o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?				*É obrigatório ser transparente para o titular sobre a finalidade de tratamento dos seus dados. Principalmente quando for compartilhar os dados com outros controladores, o titular deverá ser informado no consentimento de forma clara.*

C-03	O sistema armazena o consentimento dado pelo titular para comprovações legais?				*Armazenar no banco de dados os registros de consentimento do titular para comprovação.*
C-04	O sistema permite ao titular de dados meios para recusar ou retirar o consentimento sem prejuízo ao titular?				*O titular deve ter acesso ao seu termo de consentimento ou contrato com a opção de negar a realização do tratamento de dados.*
C-05	O sistema realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico pelos pais ou responsável legal, de uma forma acessível e fácil de entender?				*Deve certificar que apenas o responsável legítimo poderá dar o consentimento, e somente ele poderá atualizá-lo. Um exemplo é realizar autenticação do titular.*
C-06	O sistema informa o titular sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?				*Sempre que for alterar a finalidade de tratamento, deverá informar o titular da mudança e solicitar o novo consentimento para realizar o tratamento de dados, com a opção de negar o tratamento caso o titular discorde da alteração.*
C-07	O sistema fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo termos abusivos?				*O Termo de Consentimento deve ser bem escrito, com linguagem de fácil compreensão, respeitando os direitos do titular.*
C-08	O sistema informa o titular de dados sobre todos os seus direitos no consentimento?				*Informar no Termo de Consentimento e na Política de Privacidade, os direitos que os titulares de dados possuem.*
	Sobre os Direitos do Titular (D)				
D-01	O sistema armazena os dados pessoais em formato que facilite o titular de dados acessá-los?				*Para facilitar o acesso aos titulares, os dados pessoais devem ser armazenados em formato comumente usados por computador, em arquivos estruturados, para que os aplicativos de software possam facilmente identificar, reconhecer e extrair os dados pessoais. alguns exemplos: CSV, XML e JSON.*
D-02	O sistema fornece ao titular de dados, meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?				*Disponibilizar o contato de DPO ou responsável pelo tratamento de dados, na política de privacidade ou uma página exclusiva para reclamações.*
D-03	O sistema fornece a cópia eletrônica integral dos dados pessoais para o titular?				*Transmitir diretamente os dados solicitados ao titular; ou fornecer acesso a uma ferramenta que permite que o próprio titular extraia os dados solicitados.*
D-04	O sistema permite que o titular atualize seus dados pessoais?				*De acordo com a finalidade de tratamento, é necessário solicitar a atualização dos dados pessoais do titular. É recomendado criar um mecanismo para que o próprio titular possa atualizar seus dados pessoais.*
D-05	O sistema utiliza apenas dados relevantes e adequados à finalidade?				*É necessário realizar a minimização dos dados pessoais, utilizando apenas dados relevantes para o tratamento. É recomendado realizar a anonimização de dados desnecessários, realizar bloqueio ou eliminação dos dados pessoais irrelevantes.*
D-06	O sistema permite a portabilidade de dados a outro controlador mediante requisição do titular?				*Os dados pessoais devem ser armazenados em formato acessível e legível por máquina, para poder exportar os dados do titular quando ele requisitar.*

D-07	O sistema permite excluir os dados pessoais do titular, mediante a sua requisição?				*Criar um mecanismo para que o titular possa solicitar a remoção dos seus dados pessoais.*
D-08	O sistema remove os dados pessoais do titular após o término de seu tratamento?				*É necessário excluir os dados pessoais do titular após o cumprimento da finalidade, no prazo estabelecido.*
D-09	O sistema fornece informações sobre entidades públicas e privadas, caso tenha realizado compartilhamento de dados pessoais?				*Armazenar as informações das entidades e das operações de tratamento realizadas, como o compartilhamento de dados, para comprovações legais e disponibilizar quando requisitado.*
D-10	O sistema informa o titular sobre a possibilidade de não fornecer consentimento e sobre as consequências caso seja negada?				*Deve fornecer no Termo de Consentimento a possibilidade de recusar o tratamento, e as consequências caso não queira consentir.*
D-11	O sistema informa o titular quando o tratamento de dados for uma condição para fornecimento de produto, serviço ou para o exercício de direito?				*Deve ficar claro no momento do consentimento do titular os objetivos e pré-requisitos do tratamento de dados.*
D-12	O sistema permite aos titulares, o direito de se opor a um tratamento de dados de forma fácil?				*É necessário fornecer um mecanismo para que o titular consiga retirar seu consentimento. Caso o consentimento seja retirado, os dados do titular não poderão ser mais processados.*
D-13	O sistema informa ao titular, as razões do não exercício imediato dos direitos do titular?				*Quando não for possível realizar imediatamente uma operação requisitada, é necessário enviar uma resposta ao titular em que poderá em alguns casos: I - comunicar que a empresa não é agente de tratamento dos dados e indicar, sempre que possível, o agente responsável; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da operação.*
D-14	O sistema informa ao titular quando uma decisão foi tomada com base no tratamento automatizado, incluídas as decisões destinadas à criação do seu perfil pessoal?				*Disponibilizar para o titular as informações das decisões automatizadas que serão realizadas. Caso seja requisitado, fornecer o registro dessas informações.*
D-15	O sistema fornece a opção do titular contestar ou solicitar revisão da decisão automatizada?				*Caso seja requisitado, deverá revisar a decisão automatizada contestada, podendo interromper o tratamento de dados e realizar um novo consentimento para essa finalidade.*
	Sobre Segurança de Dados (S)				
S-01	O sistema realiza o tratamento de dados de uma forma segura, incluindo proteção contra acesso não autorizado?				*Garantir a segurança no tratamento dos dados pessoais, possibilitando apenas indivíduos autorizados possam ler, modificar ou excluir dados do sistema. Exemplo recomendado seria criar uma lista de controle de acesso.*
S-02	O sistema respeita as normas de transferência de dados pessoais para países internacionais, com grau de proteção de dados pessoais adequado às normas da LGPD?				*Verifique se o país destino da transferência tenha um nível de proteção igual ou superior aos previstos na LGPD, e/ou que a empresa destinatária comprove possuir as mesmas garantias de proteção por meio de normas ou certificados. Verifique também se a Autoridade Nacional do Brasil ANPD autoriza tais operações.*

S-03	O sistema informa para o titular sobre as informações das transferências dos dados pessoais realizadas para países internacionais?				*Informar no documento da Política de Privacidade e no Termo de Consentimento, informações sobre a realização de transferências de dados para países internacionais.*
S-04	O sistema utiliza mecanismos para prevenir a ocorrência de danos, destruição ou perda de dados?				*É necessário criar mecanismo para prevenir a perda e danos aos dados pessoais do titular. Como boas práticas, deve-se implementar um backup de dados, armazenamento em nuvem, e qualquer outras ações que protegerão as informações originais em caso de danos, destruição ou perda de dados.*
S-05	O sistema utiliza medidas de proteção adequadas para dados pessoais sensíveis?				*É necessário implementar uma camada adicional à segurança e armazenamento, especialmente aos dados pessoais sensíveis. Como exemplos, em alguns casos, usar encriptação dos dados, o controle de acesso, entre outras técnicas recomendadas.*
	Sobre Responsabilidade do Controlador (R)				
R-01	A organização indica um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais?				*A organização deverá indicar um encarregado pelo tratamento de dados pessoais (DPO), podendo ser pessoa física ou pessoa jurídica, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional (ANPD). A ANPD poderá estabelecer normas complementares sobre as atividades do DPO, inclusive a dispensa de sua indicação, conforme a natureza da organização.*
R-02	A organização divulga publicamente de forma clara e objetiva a identidade e as informações de contato do encarregado DPO?				*A informação deve estar de forma clara, na Política de Privacidade e no Termo de Consentimento, para que os titulares e a autoridade nacional possam ter acesso facilitado.*
R-03	A organização comunica à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos titulares, nos prazos estabelecidos pelas autoridades?				*Na ocorrência de incidente de segurança, é necessário comunicar ao titular e autoridade nacional ANPD. O prazo recomendado para comunicação pela ANPD é de 2 dias úteis contados da ciência do incidente (mesmo que ainda não esteja confirmado e sob apuração) uma comunicação preliminar deverá ser enviada, sob pena de haver violação à LGPD. O conteúdo da comunicação deve abrange minimamente, o que está previsto no §1º do art. 48, da LGPD, e/ou no formulário disponível em (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca)*
R-04	A organização realiza avaliação de impacto à proteção de dados pessoais, quando o tratamento resulta em um alto risco para os direitos e liberdades dos titulares dos dados?				*A organização deve realizar uma avaliação de impacto de proteção de dados, quando existir um elevado risco no tratamento de dados. Certificar que a avaliação é sempre revisada, especialmente se o grau de risco de tratamento de dados for alto.*

R-05	A organização realiza relatório de impactos à proteção de dados pessoais e disponibiliza a autoridade nacional, quando solicitado?				*É necessário realizar um relatório de impactos à proteção de dados e disponibilizar-lo quando requisitado. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.*



Índice de adequação	
Itens Obrigatórios Adequados:	0
Itens Obrigatórios Não Adequados:	0
Itens Obrigatórios Não Aplicado:	0
Itens Obrigatórios Não Preenchidos:	0
Total:	36 ITENS

Legenda

Divisão dos itens não obrigatórios:

Itens gerais
Itens específicos para IoT

Itens Não Obrigatórios - (Itens Recomendáveis, Oportunidades de Melhorias)

CÓDIGO	ITEM DE AVALIAÇÃO	RESPOSTA	GRAU DE SEVERIDADE	COMENTÁRIOS	RECOMENDAÇÕES
	Sobre Segurança de Dados (S)				
S-01	O sistema utiliza boas práticas de proteção de privacidade, como privacy by design?				*Como boa prática para o desenvolvimento e adequação do sistema, implementar a metodologia privacy by design.*
S-02	O sistema realiza o mapeamento dos dados pessoais e mantém em segurança?				*Organizar os locais onde os dados são coletados e armazenados.*
S-03	O sistema fornece a confidencialidade, usando medidas técnicas apropriadas?				*Realizar a proteção contra acesso não autorizado, no uso de dados pessoais armazenados ou em transição, como exemplos realizar a autenticação e controle de acesso.*
S-04	O sistema fornece a integridade dos dados pessoais, impedindo modificações?				*Verificar a integridade dos dados durante a coleta e no tratamento dos dados pessoais.*
S-05	O sistema mantém registros de auditorias de conformidades e disponibiliza informação ao titular de dados, caso requisitado?				*Uma solução seria documentar os dados das auditorias realizadas para fornecer ao titular.*

S-06	A organização possui um plano de correção a incidentes de privacidade e segurança?				*A organização deve documentar um plano para correção de falhas ou incidentes de segurança.*
S-07	O sistema possui certificação ou selos, para comprovar a observância e o cumprimento das normas de proteção de dados pessoais?				*É recomendável que os sistemas tenha uma certificação, que comprovem que seguem um código de conduta ou política de segurança confiável para aderência da lei de proteção de dados. Alguns exemplos: ISO 27001, ISO 27701.*
S-08	O dispositivo possui certificação para comprovar os padrões de qualidade?				*Ao utilizar certificações, é comprovado que o dispositivo possui níveis de qualidade e segurança que são determinadas pela regulamentação.* *É de grande importância possuir uma certificação, como por exemplo: Certificação Anatel.*
S-09	O dispositivo é seguro contra ataques de 'força bruta' e/ou outras tentativas abusivas de login?				*Um ataque de força bruta é uma maneira de conseguir acesso privilegiado através de inúmeras tentativas.* *Uma solução é criar mecanismo para bloquear os utilizadores após várias tentativas inválidas de acesso*
S-10	O dispositivo possui mecanismos contra ataques conhecidos atualmente, como buffer overflow, DDoS, entre outros?				*Realizar uma bateria de testes de ataques mais conhecidos atualmente como forma de prevenção.*
S-11	Os dispositivos utilizam técnicas de proteção para realizar uma comunicação segura?				*Ao compartilhar os dados entre os dispositivos, é necessário que técnicas de proteção sejam implementadas.*
S-12	As senhas ficam encriptadas na base de dados do dispositivo?				*As senhas que ficam salvas na base de dados do dispositivo, se elas estiverem encriptografadas, se tornam mais seguras, se alguém tiver acesso ao dispositivo, não conseguirá visualizar a senha facilmente.*
S-13	O dispositivo encaminha os dados devidamente para para o seu destino?				*Realizar verificações para identificar se os dados estão sendo encaminhados apenas para seu devido destino.*
S-14	O dispositivo utiliza protocolos como SSL e TLS para criptografar as comunicações?				*Os protocolos (Secure Socket Layer) e TLS (Transport Layer Security) servem para encriptar as comunicações, proporcionando a segurança na troca de dados e das informações.*
S-15	A organização cria mecanismos de segurança para os dispositivos com pouco processamento?				*Em cenários que dispositivos não suportam protocolos como por exemplo, CoAP. Nesse caso será necessário a interação entre os equipamentos. Uma alternativa é a utilização de gateways, onde enviará as informações para um ponto na rede e realizará o tratamento e procedimentos que o dispositivo restrito não consegue.*
S-16	O dispositivo recebe atualizações de segurança?				*As atualizações de segurança corrigem falhas e o quanto mais rápido essas falhas forem corrigidas, diminui os riscos contra invasões.*

S-17	O dispositivo encripta os dados no armazenamento, para evitar a identificação dos dados pessoais?				*Ao armazenar os dados pessoais utilizando criptografia, os dados ficarão mais protegidos. Se ocorrer uma violação, os dados não serão facilmente acessados.*
S-18	Existe um profissional de segurança fiscalizando atividades suspeitas ou incomuns e pronto para agir imediatamente?				*Ter um profissional fiscalizando todo o processo diminuirá bastante as chances de um incidente de dados, visto que ele estará sempre a disposição para agir imediatamente.*
S-19	Os dispositivos são alocados em uma VLAN específica, separando-se de ambientes de usuário/visitantes?				*Realizar o gerenciamento de toda a rede, separando o acesso a internet de usuários/visitantes com a rede de acesso dos dispositivos.*
S-20	Quando a senha do dispositivo é trocada, a organização recebe uma notificação?				*É importante a notificação após mudanças de senhas, porque se alguém sem autorização conseguir realizar a mudança de senha, a organização poderá tomar medidas protetivas imediatamente.*
S-21	A organização recebe notificações em caso de acessos não autorizados ?				*Criar mecanismos para notificações se ocorrer acessos indevidos, com o intuito de conseguir agir imediatamente em caso de invasões.*
	Sobre Responsabilidade do Controlador (R)				
R-01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?				*Armazene e documente o histórico de atividades do encarregado DPO.*
R-02	A organização realiza capacitação para seus funcionários sobre a aderência à LGPD?				*Capacite os funcionários e colaboradores sobre as informações que a LGPD determina. Exemplo: Através de treinamentos, cursos e palestras, certificações e etc.*
R-03	São realizadas capacitações para os funcionários que utilizam os dispositivos?				*Realizar capacitações com os funcionários para garantir a qualidade e eficiência de todo o processo.*
	Acesso ao Dispositivo (A)				
A-01	A organização fornece credenciais diferentes para cada utilizador?				*Deve ser realizado o controle de acesso para cada utilizador, criando uma lista de pessoas autorizadas.*
A-02	São atribuídas senhas diferentes a cada dispositivo para fortalecer a segurança?				*Ao utilizar a mesma senha para cada dispositivo, a segurança fica enfraquecida, o ideal é ter senhas diferentes. Uma solução é utilizar um algoritmo para gerar as senhas*
A-03	Houve mudança da senha padrão do dispositivo, para evitar acesso não autorizado?				*É de suma importância a mudança imediata da senha padrão do dispositivo, a senha padrão já é disponibilizada no manual dos dispositivos que facilmente é encontrado no site do fabricante.*
A-04	O dispositivo garante que a senha seja forte e segura?				*Para o fornecimento de uma maior proteção a segurança, é fundamental senhas fortes, como por exemplo: Uso de letras maiúsculas, letras minúsculas, números e símbolos*
A-05	São registradas falhas ou possíveis suspeitas de vulnerabilidade?				*Realizar registros de todas as falhas e suspeitas reais, possuir esta documentação pode ajudar na organização e prevenções.*

	Segurança Física (SF)				
SF-01	O dispositivo possui apenas portas em funcionamento, não perminintdo portas desnecessarias?				*Todas as portas que não estão em uso, deverão ser desativadas. Exemplos de portas: rj45 e usb.*
SF-02	O dispositivo não possibilita o acesso facilmente de pessoas não autorizadas, evitando riscos à segurança física do mesmo?				*Analisar o ambiente no qual o dispositivo se encontra, analisando possíveis riscos que o dispositivo poderá sofrer.*
SF-03	O dispositivo é protegido contra tentativas de ser resetado para configuração de fábrica por pessoas não autorizadas?				*Apenas pessoas autorizadas poderão ter acesso aos dispositivos e deve ter proibição de intrusos, não permitindo utilização do dispositivo. Se o reset de fábrica não estiver restrito, uma solução é a blindagem do equipamento vedando o seu acesso.*
SF-04	O dispositivo é resistente para o ambiente que está alocado?				*Realizar uma análise das condições ambientais, como temperatura e umidade, identificando se irá afetar negativamente o dispositivo que irá ser utilizado.*
SF-05	A manutenção do dispositivo é realizada conforme recomendação do fornecedor?				*O ideal é que as manutenções dos dispositivos sejam realizadas nos intervalos recomendados pelo fornecedor e de acordo com suas recomendações.*
SF-06	A manutenção e consertos dos dispositivos são realizados por uma equipe autorizada?				*Para a confiabilidade desse procedimento, é de grande importância ser realizado por uma equipe autorizada.*
SF-07	São registradas todas as manutenções preventivas?				*A manutenção preventiva é a garantia do bom funcionamento do dispositivo e o registro se torna a comprovação e organização de quando realizou-se o procedimento.*

APÊNDICE E – CHECKLIST DE INSPEÇÃO - LGPD

CHECKLIST DE INSPEÇÃO – LGPD

Legenda

Categoria	a. TR – Transparência b. CO – Consentimento c. DI – Direitos do titular d. SE – Segurança de dados e. RE – Responsabilidade do controlador
Classificação dos itens	a. Sistema de Software b. Empresa ou Controlador de dados
Lei	Análise 13.709/2018
LGPD	Análise Literatura
GDPR	Análise Literatura
Versão	02

CHECKLIST DE INSPEÇÃO – LGPD				
CATEGORIA	**ITENS**	**LEI**	**LGPD**	**GPDR**
	RELACIONADO AO SISTEMA DE SOFTWARE			
TR01	O software utiliza os dados pessoais apenas para fins específicos, explícitos e legítimos para qual foi originalmente coletado e informado ao titular de dados?	X	X	X
TR02	O software realiza tratamento de dados previstos na lei de forma adequada e compatível com a finalidade para qual foi originalmente coletado?	X	X	
TR03	O software permite acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e a duração do tratamento, sempre que o titular de dados requisitar?	X	X	X
TR04	O software mantém registros dos dados pessoais precisos e atualizados, sem demora, para cumprimento das suas finalidades?	X		X
TR05	O software informa o titular de dados da política de privacidade, das finalidades de processamento, fornecendo notificação adequada com informação clara e precisa sobre seu âmbito?	X	X	X
TR06	O software é transparente sobre o tratamento de dados baseado em seu legítimo interesse, disponibiliza informação sobre o que faz e porque faz?	X		X
TR07	O software mantém registro das operações de tratamento de dados pessoais que realizam especialmente quando baseado em seu legítimo interesse?	X	X	
TR08	O software realiza o processamento de dados pessoais ou dados sensíveis de forma que não possam ser conectados a um titular de dados aplicando anonimização e pseudonimização de acordo com as finalidades?	X		X
TR09	O software informa o titular de dados da existência de tratamento dos seus dados?	X		
TR10	O software fornece ao titular de dados, nos termos e compromisso ou mediante solicitação, informações sobre a identidade e contato do controlador, os dados envolvidos, a base legal, detalhes de transferências de dados fora do brasil, período de retenção de dados e os direitos do titular?		X	X

CO01	O software permite que o titular de dados dê o seu consentimento de forma livre e clara aos termos e condições, políticas de privacidade, para realizar o tratamento de seus dados?	X	X	X
CO02	O software exige o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?	X		
CO03	O software mantém registros para provar que o consentimento foi obtido em conformidade com o disposto nesta lei, atendendo as condições de consentimento livre, específico, informado e presumido?	X	X	X
CO04	O software permite o titular de dados meios para recusar ou retirar o consentimento sem prejuízo a qualquer momento?	X		X
CO05	O software realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico, de fácil compreensão e em destaque dado pelos pais ou responsável legal, e certifica que é o responsável legítimo que dar o consentimento e que somente ele pode atualizá-lo?	X	X	X
CO06	O software informa ou notifica previamente o titular de dados sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	X		X
CO07	O software fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo linguagem e termos abusivos?		X	X
CO08	O software atende os requisitos de consentimento para cada uso de dados pessoais, de dados sensíveis e suas finalidades?		X	
DI01	O software fornece ao titular o acesso aos seus dados pessoais que estão sendo utilizados de forma gratuita, sempre que requisitar?	X		X
DI02	O software armazena os dados pessoais em formato que facilite o titular de dados acessá-los?	X	X	
DI03	O software fornece ao titular de dados, meios para registrar reclamações em relação a proteção e no processamento de seus dados pessoais?	X		X
DI04	O software fornece a cópia eletrônica integral dos dados pessoais para utilização subsequente em outras operações de tratamento previsto na lei, em caso de consentimento ou contrato?	X		X
DI05	O software permite a inserção de dados pessoais corrigidos ou retificados para armazenamento, caso requisitado?	X		X
DI06	O software utiliza apenas dados úteis, relevantes e adequados a finalidades, garantindo que não há nenhum dado extra, fora do escopo, realizando anonimização, bloqueio ou eliminação de dados desnecessários?	X	X	X
DI07	O software permite a portabilidade de dados a outro fornecedor de serviço ou produto mediante requisição expressa do titular?	X	X	X
DI08	O software permite excluir os dados pessoais do titular nos prazos estabelecidos, mediante seu consentimento?	X	X	X
DI09	O software fornece mecanismo para revisar periodicamente os dados pessoais que mantém e remover após o término de seu tratamento, quando cumprimento legal, transferência a terceiro, respeitando a lei, por órgão de pesquisa ou uso exclusivo do controlador, desde que anonimizados?	X	X	X
DI10	O software possui meios para fornecer informações por meio de sua política de privacidade e/ou requisição dos titulares dos	X	X	X

	dados sobre entidades públicas e privadas com as quais realizou o uso compartilhado de dados?			
DI11	O software informa o titular de dados sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?	X		
DI12	O software informa o titular de dados com destaque sobre quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou para o exercício de direito?	X		X
DI13	O software permite aos titulares de dados o direito de se opor a um processamento de dados de forma fácil e segura, onde o tratamento é interrompido e os dados associados não podem mais ser processados, modificados ou excluídos?	X		X
DI14	O software notifica os titulares de dados ou representante legal em caso de impossibilidade de adoção imediata dos direitos dos titulares?	X		
DI15	O software informa o titular de dados quando uma decisão foi tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a criação do seu perfil pessoal, possuindo o direito de contestar ou solicitar revisão da decisão?	X	X	X
SE01	O software processa os dados de uma forma segura, incluindo proteção contra acesso não autorizado ou ilegal, contra perda acidental, destruição ou dano, usando medidas técnicas ou administrativas apropriadas?	X		X
SE02	O software possui mecanismo para transferir dados pessoais para países internacionais com grau de proteção de dados pessoais adequado ao previsto nesta lei, para a cooperação jurídica internacional ou quando o titular tiver fornecido o seu consentimento e em destaque para a transferência?	X	X	X
SE03	O software utiliza mecanismo para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?	X	X	X
SE04	O software é implementado com práticas de proteção de privacidade desde o design (privacy by design)?		X	X
SE05	O software utiliza mecanismo para garantir o anonimato e aplica medidas organizacionais e técnicas de segurança aos dados pessoais?		X	
SE06	O software permite mapear os dados pessoais utilizados, bem como registrar onde e como eles estão armazenados e utilizados? Além disso, permite mapear os dados pessoais sensíveis e aplicar as medidas de proteção adequadas?		X	X
SE07	O software fornece certificação, selos e mantém registros recomendados pelas autoridades para comprovar a observância e o cumprimento das normas de proteção de dados pessoais?	X	X	X
SE08	O software fornece a disponibilidade de dados em formato comumente usados, legível por máquina, interoperável e informa ao titular de dados por quanto tempo os dados pessoais serão armazenados e disponíveis?			X
SE09	O software fornece a confidencialidade que nenhuma pessoa tenha permissão para acessar os dados pessoais sem autorização?			X
SE10	O software fornece a integridade dos dados pessoais a serem processados para permanecer intactos e completos?			X
SE11	O software permite ao titular de dados o controle sobre seus próprios dados pessoais e são informadas sobre todos os seus direitos?		X	X

SE12	O software mantém registros de auditorias de conformidades realizadas periodicamente e disponibiliza informação ao titular de dados?	X	X	X
	RELACIONADO A EMPRESA OU CONTROLADOR DE DADOS			
RE01	Sua empresa ou controlador de dados indicou um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais e divulga publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador, a identidade e as informações de contato do encarregado?	X	X	X
RE02	Sua empresa ou controlador de dados de dados comunica à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos prazos, conforme definido pela autoridade nacional?	X	X	X
RE03	Sua empresa ou controlador de dados fornece sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada?	X		X
RE04	Sua empresa ou controlador de dados realiza avaliação de impacto à proteção de dados pessoais, quando o processamento resulta em um alto risco para os direitos e liberdades dos titulares dos dados e se esse processo é registrado e documentado para envio e publicação de relatórios de impacto à proteção de dados pessoais quando solicitado pela autoridade nacional a agentes do Poder Público?	X		X
RE05	Sua empresa ou controlador de dados planeja e realiza o mapeamento dos riscos de segurança de informações e proteção de dados e fornece um plano de mitigação?	X	X	X
RE06	Sua empresa ou controlador de dados fornece relatórios para autoridades competentes com informações sobre todas as atividades realizadas pelo oficial de proteção de dados (DPO)?			X
RE07	Sua empresa ou controlador de dados fornece ao titular de dados, informações e dados pessoais por meio eletrônico ou sob forma impressa?	X		
	Total de Atributos	41	29	42