S.M.M.I.O.T: SUSTENTAVEL MODELO DE MATURIDADE DA INTERNET DAS COISAS BASEADA NA ISO 27400

Eber da Silva de Santana

Privacidade e Segurança Da Informação / PPEE - Programa de Pós-Graduação Profissional em Engenharia Elétrica – Universidade de Brasília (UNB)
Salvador – BA – Brasil

Departamento de Engenharia Elétrica

eberss@gmail.com

Resumo. *A rápida adoção de dispositivos IoT, impulsionada pela sua conveniência e capacidade de conectividade, tem ocorrido a um ritmo que frequentemente ultrapassa o desenvolvimento e a implementação de medidas de segurança robustas. Esta disparidade cria uma lacuna substancial, tornando um grande número de dispositivos suscetíveis a exploração no que tange à segurança da informação. A diversidade de hardware, software, bem como sistemas operacionais e firmware utilizados em dispositivos IoT complica ainda mais os esforços da segurança da informação, uma vez que uma abordagem única raramente é suficiente. As vulnerabilidades de segurança em dispositivos IoT referem-se às fraquezas que os tornam suscetíveis a acesso não autorizado, comprometimento por atacantes e violações de dados. Devido ao surgimento massivo de dispositivos para a IoT, houve preocupação com a segurança de tais dispositivos, sendo assim a ISO 27400 se preocupa em atribuir segurança e controles e fornece diretrizes para mitigar os riscos, para a segurança e privacidade de soluções de Internet das Coisas (IoT). A Internet das Coisas (IoT) é uma das principais preocupações de qualquer sistema de tecnologia da informação e comunicação (TIC), e os sistemas IoT apresentam desafios particulares na segurança da informação. A rápida expansão da IoT gera grandes volumes de dados e uma interconectividade crescente entre objetos, trazendo consigo desafios significativos em termos de segurança e proteção de dados. A criação de soluções IoT, especialmente em setores críticos, exige uma abordagem rigorosa para mitigar os riscos cibernéticos associados. A necessidade de soluções de segurança específicas para IoT tem levado à criação de normas como a ISO/IEC 27400, que oferece diretrizes para a implementação de*

medidas de segurança adequadas, desde o design e desenvolvimento até a operação e desativação dos dispositivos. Apesar dos avanços em normas de segurança e melhores práticas, ainda existem lacunas significativas na implementação dessas soluções. A complexidade dos dispositivos IoT e a falta de uma padronização global para todas as entidades não são possíveis devido à implementação de soluções de segurança específicas. Para elucidar a questão-problema e atingir os objetivos propostos, foi desenvolvida uma pesquisa de cunho exploratório de método misto (qualitativo e quantitativo), através de pesquisa bibliográfica e documental. Como resultado, foram verificados os impactos por uso dos controles da ISO 27400 para mitigar as vulnerabilidades em dispositivos IoT perante seus ecossistemas, que são infraestruturas e serviços baseados numa rede de organizações e partes interessadas.

1. Introdução

Com o avanço da tecnologia, a popularização de dispositivos interconectados e a grande demanda por informação, surgiu o termo IoT, ou Internet das Coisas, que se refere a uma rede de objetos físicos conectados utilizando sensores para reunir e transmitir dados. Essas redes vêm sendo cada vez mais aprimoradas de forma que os equipamentos e seus recursos ofereçam maior conforto e agilidade nas tarefas a serem realizadas, sendo incorporadas ao cotidiano da população, principalmente no âmbito residencial e/ou comercial.

Muitos desses dispositivos IoT são de baixo custo, com interfaces e usabilidade limitadas, e são desprovidos de características de segurança comuns. Tais dispositivos seguem diversos tipos de padrões de sistemas de acordo com seus fabricantes, o que consequentemente os torna vulneráveis, devido à falta de atualização dos firmwares destes dispositivos em tempo hábil, que muitas vezes são concebidos para funcionar durante um longo período de tempo sem atualizações. Porém, as ameaças podem encontrar brechas nos dispositivos conectados e comprometer a segurança, colocando em risco não somente os dados pessoais do usuário, mas também sua infraestrutura tecnológica.

Assim, a pesquisa se justifica pela necessidade de identificar as vulnerabilidades em dispositivos IoT e/ou seu ecossistema, avaliando o impacto dos controles de implantação para mitigar essas vulnerabilidades, propondo assim avaliar o nível de maturidade da segurança da informação do ecossistema da IoT com o uso da norma ISO/IEC 27400, visto que um dos motivos que levam à implantação dos controles previstos em normas de Segurança da Informação é a

necessidade de restringir e mitigar o acesso não-autorizado dos dados e/ou informações para tentar conter a vazão dos mesmos, visto que há uma inspiração do teste de conformidade da ISO/IEC 27002 para implementar os controles da ISO/IEC 27400.

Ao novo método de avaliação foi dada a nomenclatura de Sustentável Modelo De Maturidade Da Internet Das Coisas (S.M.M.I.O.T), este nome se justifica por enfatizar as principais premissas da conjuntura do S.M.M.I.O.T, bem como sua classificação que mede a performance de cada dispositivos nos indicadores definidores de cada domínio com isso se espera que seja periódico e constante de maneira a medir a evolução ou involução dos indicadores.

O desenvolvimento deste artigo foi impulsionado pela necessidade de desenvolver um modelo de maturidade para dispositivos da Internet das Coisas (IoT), baseados num padrão que visa garantir a sua padronização, o qual foram escolhidos para se tomar como base os indicadores apresentados na ISO 27400, o modelo dos níveis de maturidade apresentado no CMMI e inspiração dos processos de melhoria contínua apresentados pelo COBIT.

Justifica-se a criação deste modelo devido a não existência de um modelo ao qual venha se avaliar o nível de vulnerabilidade em dispositivos IoT.

O presente artigo se propõe a fazer um estudo sobre como a norma ISO/IEC 27400 pode ser aplicada para mitigar as vulnerabilidades de segurança cibernética em um ecossistema de IoT. Através de uma análise das diretrizes oferecidas pela norma, trataremos de como essas práticas podem ser implementadas em diferentes setores, abordando não apenas a segurança dos dispositivos em si, mas também a gestão de riscos e a proteção de dados. Este artigo pretende fornecer uma compreensão mais aprofundada dos desafios de segurança cibernética na IoT e oferecer soluções práticas para enfrentar essas ameaças, utilizando a ISO/IEC 27400 como um referencial fundamental para a construção de ambientes mais seguros e resilientes.

A necessidade de destacar o modelo S.S.M.M.I.O.T, é de ser um instrumento de apoio na mitigação destinadas a melhorar o desempenho de segurança no intuito de diminuir as vulnerabilidades destes dispositivos. A necessidade de melhoria e mitigação das vulnerabilidades recorrentes dos dispositivos da Internet das Coisas (IoT) é cada vez mais evidente, tanto em sua residência quanto em ambientes organizacionais e em outros locais, causando assim a violação da infraestrutura tecnológica, ocasionando a falta de acessibilidade e a violação da privacidade dos dados, bem como a indisponibilidade destes dispositivos. O aumento populacional contribuiu para o surgimento cada vez maior desses dispositivos ao redor do mundo, sendo inevitável sua utilização, o

que gera uma total dependência tecnológica. Com isso, surge mais uma forma de acesso às das informações e disponibilidade dos dados.

Observa-se que a percepção de detectar e mitigar as vulnerabilidades em dispositivos IoT é ampla devido a existência de diversos modelos ao qual fica dificultoso detectar e mitigar por fabricantes, porém não é fácil saber se um dispositivo X, Y ou Z está vulnerável e quais os métodos que são adotados para atualizar e mitigar essas vulnerabilidades. Dessa forma, entendendo a importância do desenvolvimento e preocupação de diminuir essas vulnerabilidades, tem-se a seguinte questão problema norteadora desse artigo: De que forma é possível avaliar o nível de maturidade das vulnerabilidades dos dispositivos e sistema de segurança da informação de um ecossistema IoT?

Este artigo objetiva avaliar o nível de maturidade e os impactos das vulnerabilidades no ecossistema dos dispositivos da IoT bem como descrever os processos necessários para realização da mitigação das vulnerabilidades do ecossistema da IoT, realizar uma revisão teórica sobre IoT e normas de procedimentos e processos, identificar as vulnerabilidades dos dispositivos IoT, desenvolver um modelo de processo para mensuração dos níveis de amadurecimento das dos dispositivos do ecossistema de IoT, aplicar os controles das normas ISO/IEC 27400 definindo as conformidades de segurança e privacidade e mensurar o modelo proposto através da aplicação em organizações e seus dispositivos IoT.

2. Principais Conceitos Da IoT

A Internet das Coisas (IoT) refere-se à rede de dispositivos conectados que interagem entre si e com outros sistemas por meio da internet, permitindo a coleta, troca e análise de dados em tempo real. Esses dispositivos variam de sensores simples a sistemas complexos em áreas como saúde, automação residencial, cidades inteligentes, indústrias automotivas e indústrias no contexto geral, oferecendo uma gama de benefícios como automação, monitoramento remoto e melhoria da eficiência operacional. A rápida expansão da IoT gera grandes volumes de dados e uma interconectividade crescente entre objetos, trazendo consigo desafios significativos em termos de segurança e proteção de dados (GUBBI ET AL., 2013; ATZORI ET AL., 2010).

A segurança da informação é uma das principais preocupações de qualquer sistema de tecnologia da informação e comunicação (TIC), e os sistemas de Internet das Coisas (IoT) não são exceção. Os sistemas IoT apresentam desafios particulares para a segurança da informação na medida em que são altamente distribuídos e envolvem um grande número de entidades diversas. Nesse caso,

a ISO/IEC 27400 fornece orientações sobre riscos, princípios e controles relacionados à Internet das Coisas (IoT) para a segurança e a privacidade. Embora não seja mais novidade, vale a pena salientar que, por meio dela, sensores, capacidade de processamento, software e outras tecnologias se conectam e trocam dados com outros dispositivos e sistemas. Graças aos milhares de dispositivos e sistemas conectados, eles podem facilitar as atividades e tarefas diárias e melhorar a eficiência dos processos de trabalho, o que poupa tempo, gerando assim dinamismo no seu dia a dia. É para este fim que a norma ISO/IEC 27400 foi desenvolvida pela organização com o comitê técnico de informações sobre segurança e privacidade para IoT.

A crescente implementação de soluções IoT, especialmente em setores críticos como saúde e infraestrutura, exige uma abordagem rigorosa para mitigar os riscos cibernéticos associados. Os dispositivos conectados são alvos potenciais de ataques devido à sua vulnerabilidade a falhas de segurança, que podem comprometer não apenas os dispositivos em si, mas também sistemas maiores, como redes industriais e sistemas de controle de tráfego. Nesse contexto, a aplicação de normas de segurança cibernética, como a ISO/IEC 27400, que fornece diretrizes específicas para a proteção de dispositivos IoT, é essencial para garantir que as implementações sejam seguras e resilientes (ISO, 2022).

Diversos estudos têm explorado os desafios de segurança cibernética na IoT, abordando desde a vulnerabilidade de dispositivos individuais até as ameaças em sistemas complexos. Segundo a ISO/IEC 2022, a maioria dos dispositivos IoT é projetada com foco na funcionalidade e no custo, muitas vezes negligenciando a segurança. Isso resulta em dispositivos com protocolos de comunicação inseguros, armazenamento de dados mal protegido e mecanismos de autenticação frágeis, o que aumenta a exposição a ataques cibernéticos (ISO, 2022).

Estudos apontam que os ataques mais comuns incluem a interceptação de dados, a manipulação de dispositivos e ataques de negação de serviço (DDoS), que podem comprometer a integridade e a confiabilidade dos sistemas IoT (HE ET AL., 2016). Além disso, a abordagem tradicional de segurança cibernética, que foca em firewalls e criptografia em redes centralizadas, não é totalmente aplicável à IoT devido à sua natureza descentralizada e à diversidade de dispositivos conectados. A necessidade de soluções de segurança específicas para IoT tem levado à criação de normas como a ISO/IEC 27400, que oferece diretrizes para a implementação de medidas de segurança adequadas (ISO, 2022). A norma abrange aspectos como criptografia, autenticação, controle de acesso e monitoramento contínuo, visando criar um ambiente mais seguro para a utilização desses dispositivos em larga escala (ZHAO ET AL., 2018).

No entanto, apesar dos avanços em normas de segurança e melhores práticas, ainda existem lacunas significativas na implementação dessas soluções. A complexidade dos dispositivos IoT e a falta de uma padronização global para todas as tecnologias envolvidas dificultam a aplicação universal de medidas de segurança. Como resultado, a vulnerabilidade a novos tipos de ataques e a falta de educação sobre segurança em ambientes de IoT continuam sendo desafios relevantes que precisam ser superados (SICARI ET AL., 2015).

Um ecossistema de Internet das Coisas (IoT) refere-se à rede interconectada de dispositivos, sensores, softwares e plataformas que permitem a comunicação e a troca de dados entre eles via internet. Esse ecossistema desempenha um papel crucial em várias áreas, como cidades inteligentes, saúde, agricultura e automação industrial, permitindo uma melhor eficiência e monitoramento, como demonstrado na Figura 01.

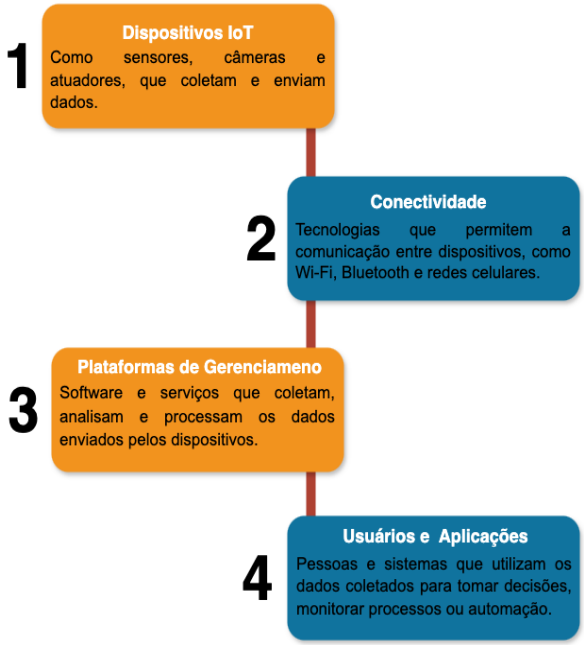

Figura 01 - Ecossistema da Internet das Coisas (IoT).

3. Iso 27400 Aplicadas a IoT

A segurança da informação é uma das principais preocupações de qualquer organização e as soluções da Internet das Coisas (IoT) não são exceção. Os sistemas IoT apresentam desafios específicos para a segurança dos ativos envolvidos, na medida em que são altamente distribuídos e envolvem um grande número de entidades diversas. Isto implica que existe uma superfície de ataque muito grande e um desafio significativo para o sistema de gestão da segurança da informação (SGSI) aplicar e manter controles de segurança adequados em toda a solução.

A proteção da privacidade ou das informações de identificação pessoal (IPI) é uma preocupação importante para alguns tipos de sistemas IoT. Quando um sistema IoT adquire ou utiliza informações de identificação pessoal, normalmente existem leis e regulamentos que se aplicam à aquisição, armazenamento e processamento dessas informações. Mesmo quando os regulamentos não são uma preocupação, o tratamento de informações que identificam pessoalmente as pessoas por um sistema IoT continua a ser um problema de reputação e de confiança para as organizações envolvidas; por exemplo, se as informações que identificam as pessoas forem roubadas ou utilizadas indevidamente, causarão algum tipo de dano a essas pessoas identificadas pelas informações.

Os controles de segurança e privacidade da ISO/IEC 27400 são desenvolvidos para as partes interessadas em um ambiente de sistema IoT, de modo a serem utilizados por cada uma delas ao longo do ciclo de vida do sistema IoT.

Para implementar a segurança e a privacidade em um sistema IoT, é importante conhecer as partes interessadas do sistema. Dependendo do seu papel, estas definem o nível de segurança e privacidade necessário para o sistema, ao qual tentam contribuir de maneira a mitigar os riscos, com a aplicação de seus controles para tentar alcançar as mitigações dos dispositivos da IoT.

A norma ISO/IEC 27400 define três tipos de funções: Fornecedor de serviços IoT, Criador de serviços IoT e Utilizadores IoT, como mostra na Figura 02.

Figura 02 - Partes interessadas dos sistemas IoT

3.1 - As Partes interessadas dos sistemas IoT são:

Fornecedor de serviços de IoT: No qual este gera e opera os serviços de um sistema IoT que são oferecidos e utilizados pela IoT. Os serviços comuns prestados pelos fornecedores de serviços de IoT incluem serviços de conectividade, serviços de coleta e gestão de dados, bem como serviços de gestão de ativos relacionados com a IoT, como os dispositivos IoT. O serviço IoT tem de corresponder às necessidades do utilizador IoT e depende de um caso de utilização específico ou de um ecossistema IoT relevante. Os prestadores de

serviços IoT têm de compreender os requisitos funcionais e não funcionais dos utilizadores de IoT para os serviços prestados e satisfazer os utilizadores IoT com os serviços, nomeadamente em termos de segurança e privacidade. Para tal, os prestadores de serviços IoT também precisam de compreender plenamente todos os vetores de ameaça relevantes, a fim de poderem efetuar uma avaliação dos riscos e selecionar opções eficazes de tratamento dos riscos, para controles específicos que têm de ser considerados por um prestador de serviços IoT (ISO, 2022).

Criador de serviços IoT: Os programadores de serviços IoT são responsáveis pela conceção, implementação e integração dos serviços IoT. Os programadores de serviços IoT podem ser ainda mais especializados, por exemplo, assumindo o papel de arquitetos de soluções ou plataformas IoT, de projetistas e/ou implementadores de aplicações IoT, ou de projetistas e implementadores de dispositivos IoT. Em cada função, os criadores de serviços IoT devem seguir as melhores práticas de conceção e desenvolvimento, aderindo assim aos princípios de segurança e privacidade desde a conceção ou utilizando ciclos de vida de desenvolvimento de software seguros. Uma das subfunções dos programadores de serviços IoT é a de programador de dispositivos IoT; este desenvolve e produz equipamento de hardware específico para ser utilizado em sistemas IoT, nomeadamente dispositivos IoT. Os dispositivos IoT podem ser operados e utilizados diretamente por um utilizador IoT ou por um fornecedor de serviços IoT, e o mesmo dispositivo pode ser tecnicamente utilizado em vários casos de utilização IoT diferentes. É importante que um programador de dispositivos IoT tenha em conta os requisitos de segurança e privacidade dos potenciais cenários de utilização do dispositivo na fase de conceção, a fim de poder oferecer dispositivos com o conjunto certo de funcionalidades e características para satisfazer as necessidades dos seus clientes. Os criadores de serviços IoT têm de compreender e considerar as expectativas e os requisitos de segurança e privacidade dos prestadores de serviços IoT, bem como dos utilizadores IoT, de modo a que sejam selecionados os controles necessários para garantir o tratamento adequado dos riscos do sistema IoT. Para mais informações sobre os controles que têm de ser considerados pelos criadores de serviços IoT (ISO, 2022).

Utilizadores de IoT: Um utilizador IoT é o utilizador final de um serviço IoT e pode ser classificado em utilizador humano e utilizador digital. O utilizador humano é um indivíduo que utiliza o serviço IoT, enquanto o utilizador digital é um utilizador não humano do serviço IoT, que pode ser um serviço automatizado que atua em nome de um utilizador humano. No caso do utilizador humano, este pode ser representado por um indivíduo, por exemplo, no caso de sistemas IoT ao nível do consumidor, ou por uma organização, por

exemplo, no caso de sistemas IoT industriais. Em qualquer caso, o utilizador da IoT define diretamente ou, pelo menos, influencia os requisitos funcionais e não funcionais de um sistema ou serviço IoT. É do interesse fundamental do utilizador da IoT que um sistema ou serviço IoT possa ser utilizado sem introduzir riscos inaceitáveis no domínio da segurança e da privacidade (ISO, 2022).

O nível de segurança e privacidade que um sistema ou serviço IoT deve proporcionar é principalmente determinado pelas expectativas ou considerações de risco feitas pelos utilizadores da IoT. No entanto, os utilizadores da IoT muitas vezes podem não ter conhecimento das implicações das tecnologias para a segurança. Para qualquer caso de utilização, é crucial um conhecimento profundo dos utilizadores da IoT e das suas necessidades e requisitos. Para poder tratar adequadamente os riscos relacionados com a IoT, existem também controles que um utilizador da IoT deve considerar e implementar (ISO, 2022). As dependências entre os fornecedores de serviços IoT, os criadores de serviços IoT e os utilizadores IoT no contexto da segurança e da privacidade num sistema IoT podem ser descritas como um ecossistema, uma analogia com o conceito de ecologia.

3.2 - Características dos sistemas IoT

As aplicações dos sistemas IoT são diversas, o que torna impraticável a definição de um conjunto de características de aplicação geral para cada sistema IoT. Como forma prática de descrever as características dos sistemas IoT, elas podem ser identificadas como 'características comuns' e 'características específicas para áreas de aplicação', conforme descreve o quadro abaixo (ISO, 2022).

Quadro 01 - Características dos sistemas IoT

Características dos sistemas IoT
Os sistemas IoT partilham as características incomum.
Os sistemas IoT incluem dispositivos IoT, que são equipamentos específicos de hardware e software utilizados em conjunto ou ligados a objetos ou materiais físicos.
Os dispositivos IoT estão ligados a redes e têm a capacidade de transmitir e receber dados. Podem ser utilizadas em redes com e sem fios.
Os dispositivos IoT têm normalmente capacidades de detecção, por

exemplo, para detectar estados ou movimentos do ambiente.
Os dispositivos IoT podem ter capacidades de atuação, ao receber dados de controles para iniciar ações físicas.
Os sistemas IoT incluem aplicações IoT para processar dados de dispositivos IoT, para gerar e enviar dados de controe e para permitir a integração com outros sistemas.
Os sistemas IoT incluem componentes operacionais que permitem a configuração e o funcionamento de dispositivos e aplicações IoT.
Os sistemas IoT apoiam utilizadores humanos ou digitais.

3.3 - IoT – Internet das Coisas

A definição de Internet das Coisas, em inglês IoT (Internet of Things), é um conceito que representa objetos que contêm sensores programados para reportar determinados parâmetros que originam ações específicas. Exemplos do nosso dia a dia incluem supermercados sem qualquer tipo de controle no que diz respeito ao pagamento ou frigoríficos que reconhecem os alimentos em falta e organizam listas de compras. A troca de dados e/ou informações é operada pela internet, sem intervenção humana, o que significa que esses dispositivos podem se gerenciar sozinhos. No entanto, a IoT apresenta algumas questões no âmbito da segurança da informação que necessitam ser revistas e melhoradas devido às suas vulnerabilidades. (MENEGHELLO, HOSSAIN, M. M.; FOTOUHI, M.; HASAN, R. 2015) Esses dispositivos estão sempre ligados, e a questão da segurança adquire uma acessibilidade acrescida, sabendo que existem certas facilidades de acesso não previstas e maliciosas. A Internet das Coisas (IoT) refere-se a uma vasta rede de dispositivos que estão conectados à internet, permitindo que coletem, troquem e atuem sobre dados. Essa conectividade abre um leque enorme de possibilidades para automação, monitoramento, otimização e criação de novos serviços em diversos setores (MOSENIA, A.; JHA, N. K. 2017).

No entanto, essa crescente conectividade traz consigo desafios significativos no campo da segurança da informação. A negligência por parte de alguns fabricantes em relação à segurança da informação de seus softwares embarcados é uma preocupação muito válida e com consequências potencialmente sérias. A IoT tende a criar novas dinâmicas de mercado e novos modelos de transações digitais, mais baseados em ações proativas do que reativas, já que dispensa a atenção humana e o desencadear de ações por

humanos. As empresas que estiverem mais atentas a essas alterações, através de departamentos tecnológicos corretamente estruturados, terão um conjunto de vantagens concorrenciais e de participação de uma forma mais eficiente na maneira de fazer negócios (MAHMOUD, R. et al. 2015)

3.4 - A IoT e o envolvimento da Segurança da Informação

A segurança da informação em IoT abrange um conjunto de práticas e tecnologias projetadas para proteger a confidencialidade, integridade e disponibilidade dos dados gerados, processados e transmitidos por dispositivos IoT, bem como a própria segurança desses dispositivos e das redes às quais estão conectados. O envolvimento é intrínseco e essencial por diversos motivos, como o grande volume e a sensibilidade dos dados que os dispositivos da IoT coletam, uma quantidade massiva de dados, muitas vezes incluindo informações pessoais e sensíveis, como dados de saúde, localização, hábitos de consumo e até mesmo imagens e áudios. A falta de segurança pode levar a vazamentos de dados com graves implicações para a privacidade dos usuários. A superfície de ataque expandida que cada dispositivo IoT conectado à rede representa um novo ponto de entrada potencial para cibercriminosos. Quanto maior o número de dispositivos, maior a superfície de ataque, tornando a rede mais vulnerável a invasões. Ressaltando ainda os recursos limitados dos dispositivos da IoT, muitos dispositivos IoT possuem recursos computacionais limitados em termos de poder de processamento, como memória e bateria; isso dificulta a implementação de soluções de segurança robustas, como criptografia complexa e softwares de segurança tradicionais. O ciclo de vida longo e a falta de atualizações de softwares nos quais alguns dispositivos IoT são projetados nem sempre recebem atualizações de segurança regulares. Essa falta de atualizações deixa vulnerabilidades conhecidas sem correção, expondo os dispositivos a ataques, impactando assim no mundo físico os mais diversos tipos de sistemas de informação, sendo os mais tradicionais. Vulnerabilidades em dispositivos IoT podem ter um impacto direto no mundo físico; ataques a carros, as chamadas VANET, ou Vehicular Ad-hoc Network, são redes de comunicação sem fio ad-hoc, onde os veículos se comunicam entre si (V2V - Vehicle-to-Vehicle) e são redes móveis onde são estabelecidas comunicações intra-carros (SRIVASTAVA, A. et al. 2020).

Com todo esse contexto, traz-se a grande proliferação dos dispositivos IoT desprotegidos, tendo a facilidade de produção maciça desses dispositivos no contexto global. A pressão por preços competitivos muitas vezes leva fabricantes a cortar custos em segurança, resultando em dispositivos com vulnerabilidades de fábrica. Esses dispositivos desprotegidos podem ser

facilmente explorados para realizar ataques em larga escala, como botnets, uma rede de computadores, dispositivos móveis, IoT e outros dispositivos conectados à internet infectados com malware e controlados por um cibercriminoso, e ataques DDoS (Distributed Denial of Service), um tipo de ataque cibernético que sobrecarrega um servidor, serviço ou rede com tráfego malicioso, com o objetivo de torná-los indisponíveis a usuários legítimos (POURRAHMANI, H. et al. 2023).

Segundo Pourrahmani, H. et al. 2023, é fundamental que haja uma mudança de postura tanto por parte dos fabricantes quanto dos usuários e reguladores, e algumas medidas importantes poderiam ser aplicadas, como a regulamentação. Governos e órgãos reguladores precisam estabelecer padrões mínimos de segurança para dispositivos IoT, exigindo que os fabricantes implementem medidas de proteção adequadas e forneçam atualizações de segurança regulares. Por isso, neste artigo foi desenvolvido um modelo para mensuração de vulnerabilidade através da ISO/IEC 27400. A Internet das Coisas oferece um potencial transformador, mas a segurança da informação é um pilar fundamental para garantir que essa transformação ocorra de forma segura e confiável. A negligência de alguns fabricantes em relação à segurança é um problema sério que precisa ser enfrentado com urgência através de uma abordagem multifacetada envolvendo regulamentação, responsabilidade da indústria e conscientização dos usuários. O modelo S.S.M.M.I.O.T: Modelo de Maturidade da Internet das Coisas vem para minimizar esse negligenciamento.

3.5 - Segurança da Informação e suas vulnerabilidades em dispositivos IoT

Dispositivos de Internet das Coisas (IoT) são predominantes na vida diária e em várias indústrias e negócios. Eles podem variar desde o uso de eletrodomésticos inteligentes até sofisticados sistemas de controle industrial, os quais fornecem funcionalidade de conveniência, eficiência e aquisição de dados. Porém, a conectividade e as restrições de recursos da maioria dos dispositivos IoT são, de fato, desafios de segurança. Com a proliferação do ecossistema IoT, a preocupação com os riscos, que está crescendo gradualmente, é um tópico de preocupação. O conhecimento dessas vulnerabilidades é crucial para ajudar fabricantes e usuários a elaborar uma segurança eficiente (KATZ, 2024).

A rápida adoção de dispositivos IoT, apoiada pela conveniência e conectividade que proporcionam, ocorreu a uma velocidade que frequentemente ultrapassou o desenvolvimento e a implantação de segurança de alto nível. Essa diferença introduz uma lacuna significativa, onde muitos dispositivos são vulneráveis a serem comprometidos (SAAE, 2024). A heterogeneidade de dispositivos, incluindo hardware, chipsets, sistemas operacionais e firmware em IoT, agrava o trabalho de segurança da informação (SAAE, 2024). Problemas de segurança

dos dispositivos IoT, as vulnerabilidades nos dispositivos IoT são falhas que podem expô-los a mau funcionamento, acesso não autorizado, contaminação por adversários e intrusões que frequentemente resultam em vazamentos de privacidade e informação. Em relação a esses problemas, as vulnerabilidades dos dispositivos IoT serão explicadas da seguinte forma:
Senhas Fracas:

De acordo com Rossi (2024), uma das principais e mais exploradas vulnerabilidades entre dispositivos IoT é o uso de senhas padrão de fábrica predefinidas. A maioria dos fabricantes até envia seus produtos com senhas comuns, publicamente disponíveis ou fáceis de adivinhar, expondo-os ao tipo de ataque de "fruto ao alcance das mãos". Combinações amplamente usadas, como "admin" e "123456", foram utilizadas através de credenciais roubadas (SENTINELONE, 2025). Com essa prática descuidada, invasores não autorizados podem facilmente sequestrar os dispositivos. Além disso, alguns dispositivos IoT têm senhas codificadas em seu firmware e estão na posição de permitir que o usuário as modifique (ROSSI, 2024). Essa brecha persistente continua a ser uma exposição de segurança muito grande; invasores que sabem o tipo de dispositivo em uso podem frequentemente simplesmente procurar as credenciais padrão e fazer login nos dispositivos. O uso de senhas fracas foi um grande contribuinte para a construção de grandes botnets, como a Mirai, que foi notória por usar credenciais padrão para comprometer muitos dispositivos IoT (Internet das Coisas) e utilizá-los para realizar ataques de negação de serviço distribuída (DDoS) massivos. O uso repetido de senhas padrão e fracas - apesar da abundância de conhecimento sobre os riscos - revela alguma falha nos processos dos fabricantes e nos hábitos dos usuários. As empresas tendem a tornar as configurações mais fáceis como padrão e a segurança é dada baixa prioridade, ou o usuário final não sabe ou simplesmente esquece de definir uma senha adequada em seu dispositivo (ROSSI, 2024). Isso deixa uma enorme janela de vetor de ataque e é explorado consideravelmente, não sendo apenas um problema em si o único dispositivo que foi comprometido; um simples dispositivo com capacidade DDoS pode levar a um impacto massivo.

3.5.1 - Ausência de Autenticação de Dois Fatores (2FA) e Autenticação Multifator (MFA):

A autenticação de dois fatores e multifator vai além da simples interface usuário-senha, fazendo com que os usuários forneçam duas (ou, de fato, mais) das seguintes: algo que eles sabem (um nome de usuário ou senha) (SENTINELONE, 2025). Conforme relatado por Sentinelone (2025), a implantação de MFA ainda é uma exceção na maioria dos dispositivos e ecossistemas IoT,

apesar de sua contribuição comprovada para a segurança de contas. Essa falta constitui uma grande vulnerabilidade, pois permite que invasores ganhem acesso a contas com credenciais roubadas ou forçadas brutalmente. A adoção de 2FA e MFA, mesmo que apenas enviando códigos únicos para um dispositivo alternativo, seria um grande passo para prevenir o acesso não autorizado. A dificuldade está na capacidade de processamento e na potência da interface de alguns dispositivos IoT, devido à qual os mecanismos tradicionais de 2FA (autenticação de dois fatores) e MFA (autenticação multifator) podem se tornar difíceis de implementar (SENTINELONE, 2025).

3.5.2 - Autenticação e Autorização:

De acordo com Rossi (2024), as vulnerabilidades nos protocolos e métodos utilizados para verificar a identidade de dispositivos e usuários representam outra preocupação crítica de segurança. Mecanismos de autenticação podem permitir que atacantes se façam passar por usuários, obtendo acesso não autorizado a funcionalidades e dados do dispositivo; além disso, uma autorização indevida pode levar usuários não autorizados a acessar funções sensíveis bem como a modificá-las, gerando impactos críticos. As vulnerabilidades na autenticação e autorização vão além das senhas; as falhas nos protocolos e na forma como os dispositivos e usuários são verificados podem ser exploradas mesmo com senhas fortes. APIs inseguras nas interfaces de nuvem ou móveis ligadas a dispositivos IoT proporcionam outra via para os atacantes contornarem a segurança ao nível do dispositivo. A filtragem adequada de entrada e saída é crucial para evitar ataques de injeção e outras formas de manipulação (LAZURCA, 2024).

3.5.3 - Software e Firmware e a falta de atualização adequada:

De acordo com Rossi (2024), é importante atualizar software e firmware para corrigir problemas de segurança para a segurança dos dispositivos IoT, mas muitos dispositivos IoT enfrentam desafios de atualização. As restrições de infraestrutura, poder computacional e conectividade de rede, assim como o número de dispositivos interconectados e implantados, podem tornar difícil e demorado atualizá-los. Isso permite que os atacantes introduzam malware ou firmware malicioso nos dispositivos, comprometendo sua funcionalidade e segurança. A ausência de recursos anti-rollback também é considerada uma ameaça, pois o dispositivo não pode reverter o desastre de segurança para sua última atualização conhecida como boa (Lazurca, 2024). Já para Sentinelone (2025), entende-se que, com inúmeros fabricantes e diferentes níveis de compromisso com o suporte a longo prazo, contribui significativamente para o

problema do firmware desatualizado. A heterogeneidade na forma como as atualizações são tratadas piora a situação, uma vez que os atacantes buscam ativamente comprometer dispositivos com vulnerabilidades conhecidas e não corrigidas; portanto, atualizações rápidas e confiáveis são necessárias para remediar os riscos.

3.5.5 - Componentes de Hardware e Software Desatualizados:

Muitos dispositivos IoT utilizam componentes de software e hardware desatualizados ou inseguros, que podem conter vulnerabilidades conhecidas; estes componentes, que vão desde bibliotecas de software a módulos de hardware, podem não receber mais atualizações de segurança ou patches dos seus fabricantes, expondo os dispositivos a uma variedade de ameaças (ROSSI, 2024). A utilização de componentes de código aberto, embora ofereça flexibilidade e rentabilidade, também introduz o risco de herdar vulnerabilidades que podem não ser prontamente abordadas (LAZURCA, 2024). Os fabricantes devem implementar processos rigorosos de verificação de componentes e manter um inventário atualizado de todos os componentes de software e hardware utilizados nos seus dispositivos (DAVIS, 2024).

3.5.6 - Desenvolvimento e práticas inseguras no desenvolvimento de Software inseguros:

Conforme comenta Portnox (2025), codificação deficiente, testes de segurança deficientes e revisão de segurança deficiente podem resultar em vulnerabilidades no software do dispositivo. Neste contexto, o foco dos fabricantes geralmente reside em trazer produtos ao mercado o mais rápido possível e minimizar os custos, em vez de necessariamente se concentrarem nas práticas de codificação seguras, levando a software que implementa erros de codificação vulneráveis (ROSSI, 2024). A utilização de dependências não verificadas e credenciais predefinidas simples, devido a uma codificação deficiente, também contribui para a vulnerabilidade. A segurança deve ser integrada no ciclo de vida de desenvolvimento de software (SDLC) desde a fase inicial de concepção até o final. A falta de práticas de codificação seguras e inadequadas irá gerar diversos erros que podem introduzir inúmeras vulnerabilidades que os atacantes podem explorar; as auditorias de segurança regulares, revisões de código e testes de penetração são essenciais para identificar e corrigir estas falhas antes da implementação (PORTNOX, 2025).

3.5.7 - Vulnerabilidades de Serviços e Protocolos de Rede:

A presença de serviços de rede indesejados ou vulneráveis em dispositivos IoT, particularmente aqueles com abertura para a internet, é uma ameaça séria à segurança (SENTINELONE, 2025). Serviços padrão como Telnet e FTP são comumente deixados abertos com senhas fáceis de adivinhar, que podem ser usadas para conseguir acesso não autorizado ao sistema. Além disso, muitos dispositivos IoT transmitem tráfego por protocolos que são propensos a fragilidades de segurança. Alguns deles, como MQTT (Message Queuing Telemetry Transport), podem ter mecanismos de segurança fracos, e informações sensíveis em tais aplicações podem ser vazadas durante a comunicação. Além disso, o CoAP (Constrained Application Protocol) é outro exemplo em que ele usa extensivamente o UDP, tornando-se suscetível a ataques do tipo Man-in-the-Middle (MiTM) e replay. O HTTP (HyperText Transfer Protocol) também é vulnerável e aqui estão alguns exemplos: Cross-Site Scripting (XSS) e injeção de SQL. Protocolos proprietários utilizados em redes privadas (Zigbee, Z-Wave, etc.) também podem estar em risco devido a senhas fracas ou mal utilizadas. Serviços de rede desnecessários aumentam a superfície de ataque e oferecem portas de entrada distintas para agentes maliciosos (KATZ, 2024).

3.5.8 - Armazenamento e Transferência de Dados Inseguros:

Para Rossi (2024) e Sentinelone (2025), a transmissão de dados sensíveis em texto não criptografado é uma vulnerabilidade comum em dispositivos IoT; sem criptografia, os dados transmitidos entre dispositivos e servidores na nuvem podem ser facilmente interceptados e lidos por atacantes através de técnicas como o "sniffing" (captura de tráfego de rede) ou ataques MiTM. A utilização de protocolos de segurança desatualizados, como versões antigas do TLS (Transport Layer Security, um protocolo de segurança que visa proteger a confidencialidade e integridade das comunicações na Internet), também expõe os dados a riscos. Além disso, muitos dispositivos não criptografam os dados no estado off-line, quer armazenados no próprio dispositivo, quer na nuvem, tornando-os vulneráveis a violações de dados (ROSSI, 2024). A falta de mecanismos de controle de acesso para os dados armazenados agrava ainda mais este problema (LAZURCA, 2024). A falha em criptografar os dados sensíveis, tanto durante a transmissão quanto no armazenados, expõe à intercepção e roubo. Isso é particularmente preocupante dada a vasta quantidade de informações pessoais e potencialmente sensíveis recolhidas por muitos dispositivos IoT. A implementação de protocolos de criptografia seguros

e atualizados e de mecanismos robustos de controle de acesso são essenciais para proteger a confidencialidade e a integridade dos dados (ROSSI, 2024).

3.5.9 - Segmentação de Rede Inadequada:

A segmentação de rede, conforme apontado por Saae (2024), permite que os atacantes tenham acesso dentro de uma rede depois de comprometerem um único dispositivo IoT. Se os dispositivos IoT não estiverem isolados da infraestrutura de rede, um dispositivo comprometido pode servir de porta de entrada para que os atacantes acessem dados confidenciais ou tenham controle e acesso aos sistemas críticos. Por exemplo, um termóstato inteligente comprometido na mesma rede que os sistemas de controle industriais poderia potencialmente fornecer acesso a esses sistemas e, com uma brecha de vulnerabilidade, ter acesso à sua infraestrutura. A implementação de uma segmentação de rede robusta, isolando os dispositivos IoT em VLANs ou sub-redes separadas com políticas de controle de acesso rigorosas, é crucial para limitar o impacto de uma potencial violação de dados. Muitos dispositivos IoT são implementados nas mesmas redes que os sistemas de Tecnologia da Informação (T.I), criando um risco significativo. Se um atacante obtiver acesso a um dispositivo IoT com vulnerabilidade, poderá utilizá-lo como um trampolim para se infiltrar em outras partes mais críticas da rede. A implementação de uma segmentação de rede mais robusta, isolando os dispositivos IoT nas suas próprias VLANs ou sub-redes com políticas de controle e acesso rigorosos, é crucial para limitar o impacto de uma potencial violação (OLAES, 2025).

3.5.10 - Risco de Privacidade e Segurança de Dados:

Uma variedade de dispositivos IoT coleta e envia informações pessoais, que muitas vezes são deixadas desprotegidas, com privacidade, imparcialidade e provavelmente não levando à sua divulgação e violações pessoais, resultando em perdas financeiras, roubo de identidade e outros abusos (ROSSI, 2024). Em alguns casos, os dispositivos podem recolher dados sem o consentimento do usuário, armazená-los sem controles de segurança adequados ou compartilhá-los com terceiros sem as permissões apropriadas (LAZURCA, 2024). A crescente quantidade de informações pessoais que entram e saem destes dispositivos, como as de assistentes de voz como a Alexa, aumenta ainda mais os riscos de privacidade. Muitos dispositivos IoT recolhem grandes quantidades de dados pessoais, desde estatísticas básicas de utilização a informações sensíveis, como dados de saúde ou localização. A falta de transparência sobre quais dados são recolhidos, como são utilizados e com quem são compartilhados levanta preocupações significativas sobre a privacidade. Medidas de segurança são

insuficientes para proteger estes dados, que podem levar a consequências graves para os usuários (THOMAS, 2021).

3.5.11 - Tratamento de Informações Pessoais de Forma Insegura:

As informações pessoais armazenadas em dispositivos IoT ou na nuvem podem ser utilizadas de forma insegura, imprópria ou sem permissão. A falta de controles de segurança adequados para o armazenamento de dados, juntamente com o compartilhamento de dados com terceiros sem as permissões apropriadas, pode expor informações sensíveis a acesso não autorizado. Mesmo que os dados sejam compartilhados com algum nível de consentimento, práticas de tratamento inseguras ainda podem levar a violações. Isso inclui armazenar dados em formatos não criptografados, não implementar controles de acesso adequados e compartilhar dados com terceiros sem acordos de segurança apropriados. O cumprimento de regulamentos de privacidade, como a Lei Geral de Proteção de Dados (LGPD), o Regulamento Geral de Proteção de Dados (RGPD) e o California Consumer Privacy Act (CCPA), é crucial para as organizações que lidam com dados pessoais, ambos são leis de privacidade de dados (LAZURCA, 2024).

3.5.12 - Exposição Causada pela Configuração Incorreta de Dispositivos IoT:

Vários dispositivos IoT são implementados sem um suporte de segurança adequado, incluindo gestão e parametrização de ativos, gestão de atualizações, monitoramento de sistemas e capacidades de resposta. Esta falta de gestão eficaz pode comprometer toda a rede, permitindo que os atacantes manipulem e/ou controlem remotamente os dispositivos IoT (ROSSI, 2024). Um exemplo clássico são os certificados SSL expirados em dispositivos devido à falta de atualizações que podem levar a comunicações não seguras através do protocolo HTTP (WATTLECORP, 2024). O monitoramento e a gestão eficiente destes dispositivos são cruciais para manter a segurança das implementações IoT ao longo do seu ciclo de vida. A falta de processos adequados de inventário e monitoramento pode deixar os dispositivos vulneráveis e proporcionar oportunidades para os atacantes. As plataformas de gestão centralizada são essenciais para obter visibilidade e controle sobre o número crescente de dispositivos conectados (ROSSI, 2024).

3.5.13 - Vulnerabilidades das Configurações Predefinidas:

Muitos dispositivos IoT são enviados com configurações predefinidas que acabam sendo inseguras, como portas de rede abertas, acesso remoto ativado e configurações de segurança mínimas. Estas configurações tornam os dispositivos alvos fáceis para os atacantes, que podem explorar essas configurações predefinidas para obter acesso não autorizado, interromper a funcionalidade do dispositivo ou transformar esses dispositivos em botnets (ROSSI, 2024). Para Wattlecorp (2024), as senhas codificadas e os serviços expostos que operam com permissões de root representam riscos adicionais. Os fabricantes muitas vezes priorizam a facilidade de utilização em detrimento da segurança ao enviarem dispositivos com configurações predefinidas permissivas. Os usuários podem não estar cientes dessas configurações ou de como alterá-las, deixando os dispositivos expostos. A implementação dos princípios da segurança da informação através da configuração segura inicial são passos essenciais para mitigar vulnerabilidades (ROSSI, 2024).

3.5.14 - Vulnerabilidades de Segurança e Meios Físicos:

A segurança física dos dispositivos IoT é muitas vezes negligenciada, tornando-os suscetíveis a alteração, roubo e ataques diretos. Os dispositivos implementados em locais não seguros ou públicos correm um risco particular, uma vez que os atacantes podem acessar fisicamente a eles para utilizar medidas como extrair dados ou inserir parametrizações maliciosas. Embora os ciberataques sejam uma grande preocupação, a segurança física dos dispositivos IoT não deve ser ignorada, especialmente para dispositivos implementados em locais públicos ou remotos. A alteração do hardware pode fornecer aos atacantes acesso direto aos componentes internos do dispositivo, potencialmente ignorando as medidas de segurança baseadas em software. A implementação de medidas de segurança física é importante devido a ser mais um mecanismo de detecção de segurança (ROSSI, 2024).

Em seguida um quadro simplificado com as consequências de vulnerabilidade mais comuns em dispositivos IoT.

Quadro 02: Consequências de vulnerabilidade Comuns em dispositivos IoT.

Categoria de Vulnerabilidade	Vulnerabilidade Específica	Exemplo	Potenciais Consequências
Autenticação e	Senha	"admin"/"password"	Acesso não

Controle de Acesso	Predefinida e Fracas	como credenciais predefinidas	autorizado ao dispositivo, recrutamento para botnets
Software e Firmware	Mecanismo de Atualizações Inseguras	Atualização de firmware via HTTP sem verificação de assinatura	Instalação de firmware malicioso, comprometimento do dispositivo
Rede e Comunicação	Transferência de Dados Não Criptografados	Dados de sensores transmitidos via MQTT não criptografada	Interceção de dados sensíveis, ataques Man-in-the-Middle
Dados e Privacidade	Proteção de Privacidade Insuficiente	Recolha de dados de localização sem consentimento explícito	Violação de privacidade, roubo de identidade
Gestão e Configuração	Configurações Predefinidas e Inseguras	Porta Telnet aberta por defeito	Acesso remoto não autorizado ao dispositivo
Segurança Física	Falta de Controle Físico	Dispositivo de controle de acesso em local público sem proteção	Adulteração física do dispositivo, desativação ou comprometimento

A seguir, alguns incidentes cibernéticos envolvendo dispositivos de IoT são descritos:

Mirai Botnet: Em outubro de 2016, o botnet Mirai explorou senhas predefinidas fracas em dispositivos IoT, como câmeras de segurança e DVRs, para lançar um ataque DDoS massivo contra o fornecedor de serviços DNS Dyn. Este ataque interrompeu o acesso a inúmeros sites populares, incluindo Twitter, Reddit e Netflix, demonstrando o potencial dos dispositivos IoT comprometidos para serem usados como armas em ciberataques em larga escala. O botnet Mirai, em particular, serve como um forte lembrete do potencial de dispositivos IoT comprometidos a serem transformados em armas de ataque massivos (FRANKLIN, 2024).

Verkada Hack: Em março de 2021, atacantes conseguiram obter acesso a feeds de vídeo direto de mais de 150.000 câmeras de segurança da Verkada,

explorando credenciais de administradores que foram encontradas em bases online. Este incidente destacou os riscos associados a senhas fracas e à utilização de superusuários (root), com privilégios excessivos, uma vez que mais de 100 funcionários tinham privilégios de superusuário (HUSAR, 2022).

Ataques a Dispositivos Médicos: Em 2017, a FDA alertou para vulnerabilidades críticas encontradas em pacemakers implantáveis da St. Jude Medical. Estas vulnerabilidades poderiam permitir que um atacante acessasse os dispositivos e esgotasse as baterias ou administrasse choques incorretos, representando uma ameaça direta à vida dos pacientes (HENKE, 2023).

Ataques a Casas Inteligentes: Vários incidentes demonstraram as vulnerabilidades dos dispositivos de casas inteligentes. Em 2019, um casal em Milwaukee teve sua casa inteligente invadida por hackers que tocaram música perturbadora através do sistema de vídeo, falaram com eles através de uma câmera na cozinha e alteraram a temperatura ambiente para 90 graus Fahrenheit, explorando o termóstato da casa (SRINIVAS, 2020). As câmeras de segurança também foram comprometidas, permitindo que atacantes acessassem feeds de vídeo e se comunicassem remotamente com os proprietários (FRANKLIN, 2024).

Ataques a dispositivos IoT Industrial: O worm Stuxnet, descoberto em 2010, visou uma instalação de enriquecimento de urânio no Irã, explorando vulnerabilidades no software Siemens Step7 para manipular centrifugadores, causando danos físicos significativos. Em 2016, um ataque na Finlândia desligou o aquecimento em dois edifícios residenciais, explorando vulnerabilidades em sistemas de controle de aquecimento conectados à Internet (HUSAR, 2022).

Jeep Hack: Em 2015, investigadores demonstraram a capacidade de controlar remotamente um Jeep SUV através da rede celular, explorando uma vulnerabilidade na atualização do firmware. Eles conseguiram controlar a velocidade do veículo e até mesmo desviá-lo da estrada, destacando os riscos de segurança em veículos conectados (FRANKLIN, 2024).

Termômetro de Aquário de Casino: Em 2018, um cassino foi hackeado através de um termômetro inteligente em um aquário. Os atacantes utilizaram o termômetro conectado à Internet como ponto de entrada para a rede do cassino, acabando por acessar a base de dados de grandes apostadores (PATEL, 2021).

Roku Breach: Em 2024, a empresa de streaming Roku sofreu duas violações de dados resultantes de credential stuffing (coleta de credenciais de contas roubadas), onde os atacantes tentaram combinações de nome de usuário e senha que tinham vazado em violações de dados anteriores encontradas na

internet. Estas violações resultaram no comprometimento de centenas de milhares de contas de usuários (ASIMILY, 2024).

Smart Bulb Hack: Investigadores da Universidade do Texas em San Antonio demonstraram que lâmpadas inteligentes com infravermelhos podem ser hackeadas enviando comandos através de luz infravermelha invisível, que pode então ser utilizada para explorar outros dispositivos IoT conectados em uma rede doméstica (SRINIVAS, 2020).

Escovas de Dentes Hackeadas: Em fevereiro de 2024, foi noticiado que hackers tinham infectado 3 milhões de escovas de dentes conectadas à Internet com malware. Embora este incidente fosse teórico, serviu como um aviso para os consumidores sobre a crescente superfície de ataque dos dispositivos IoT (ASIMILY, 2024).

Estes exemplos do mundo real mostram os riscos significativos associados às vulnerabilidades de IoT. As consequências podem variar desde violações de privacidade e perdas financeiras até danos físicos, interrupção de infraestruturas críticas e ciberataques em larga escala. A crescente frequência e sofisticação destes ataques destacam a necessidade urgente de medidas de segurança melhoradas. A seguir, um quadro simplificado com mais ataques ocorridos em dispositivos IoT e suas vulnerabilidades exploradas."

Quadro 03: Ataques ocorridos em Dispositivos IoT e suas Vulnerabilidades Exploradas

Nome do Ataque	Ano	Tipo de Dispositivo IoT Alvo	Principal Vulnerabilidade Explorada	Consequências
Mirai Botnet	2016	Câmaras de Segurança, DVRs	Senhas Predefinidas Fracas	Ataque DDoS massivo, interrupção de grandes sites
Verkada Hack	2021	Câmaras de Segurança Inteligentes	Credenciais de Administrador Roubadas	Acesso a feeds de vídeo em direto de milhares de câmeras
Pacemakers St. Jude	2017	Pacemakers Implantáveis	Vulnerabilidades de Firmware	Potencial esgotamento da bateria, administração de choques incorretos
Ataque a	2019	Termóstatos,	Credenciais	Controle não

Casa Inteligente		Câmaras de Segurança	Fracas, Falhas de Software	autorizado de dispositivos domésticos, invasão de privacidade
Stuxnet	2010	Controladores Lógicos Programáveis (PLCs)	Vulnerabilidades de Software	Danos físicos a centrifugadores de enriquecimento de urânio
Jeep Hack	2015	SUV Conectado	Vulnerabilidade de Atualização de Firmware	Controle remoto da velocidade e direção do veículo
Ataque ao Aquecimento na Finlândia	2016	Sistemas de Controle de Aquecimento	Vulnerabilidades de Software	Interrupção da distribuição de aquecimento em edifícios residenciais
Roku Breach	2024	Dispositivos de Streaming Roku	Credential Stuffing	Comprometimento de centenas de milhares de contas de utilizadores

Foram retratadas as descrições de várias categorias de vulnerabilidades comuns encontradas em dispositivos IoT, incluindo aquelas relacionadas com autenticação e controle de acesso, software e firmware, rede e comunicação, segurança de dados e privacidade, gestão e configuração de dispositivos, segurança física e a cadeia de abastecimento. Estas vulnerabilidades não existem isoladamente, o que significa que podem ser exploradas em combinação, levando a consequências de segurança ainda mais graves (OLAES, 2025). Para enfrentar eficazmente estes desafios de segurança em evolução, é necessária uma abordagem multifacetada e proativa. Por isso, foi desenvolvido o S.S.M.M.I.O.T: Modelo De Maturidade Da Internet Das Coisas, no qual a intenção é mitigar as vulnerabilidades dos dispositivos IoT, sabendo que não existe segurança 100%, mas a intenção é alertar sobre o nível de vulnerabilidade que existe no ecossistema de dispositivos IoT. Como boa prática, os utilizadores e/ou usuários devem adotar práticas de segurança diligentes, como alterar as senhas predefinidas, manter o software atualizado e segmentar as suas redes. Os profissionais de segurança precisam implementar sistemas de monitoramento contínuo e utilizar informações sobre ameaças para detectar e responder a potenciais incidentes de segurança.

4. Metodologia

O percurso metodológico é especificado para descrever os procedimentos que foram desenvolvidos com a finalidade de responder às questões desta pesquisa, bem como atingir os objetivos delineados. Assim, é apresentada a classificação da pesquisa quanto à sua natureza, objetivos, procedimentos e abordagem a ser estudada. Este estudo buscou investigar e analisar as vulnerabilidades em dispositivos IoT, bem como as soluções propostas na literatura científica. O processo metodológico foi delineado em etapas que visam garantir uma abordagem abrangente na seleção e análise dos artigos relevantes. Foram utilizadas três etapas:

O percurso metodológico é especificado para avaliar o nível de maturidade de um ecossistema IoT, utilizando o arcabouço S.M.M.I.O.T, baseado nos indicadores e controles da ISO 27400, no processo de mensuração dos níveis de maturidade do CMMI e no processo de avaliação e melhoria contínua do COBIT.

Quanto à natureza, esta pesquisa pode ser classificada como pesquisa aplicada, pois objetiva gerar conhecimento prático direcionado à solução de problemas específicos (GIL, 2008). Se classifica como exploratória quanto aos seus objetivos, pois se encontra em fase preliminar e tem como finalidade desenvolver mais informações sobre o assunto a ser estudado, onde é examinado um conjunto de fenômenos (WAZLAWICK, 2017). Quanto à abordagem, a pesquisa é de natureza quantitativa, pois utiliza e propõe fórmulas e estatísticas para a análise dos dados obtidos na validação do arcabouço S.M.M.I.O.T (GIL, 2008).

Quanto aos seus procedimentos para embasar a coleta dos dados e a análise dos resultados, foi realizada uma pesquisa bibliográfica, além de um estudo de caso. Bibliográfica por ser elaborada a partir de material já publicado, tais como livros, artigos científicos, teses e outras publicações usualmente disponibilizadas por editoras e indexadas. Documental, por utilizar materiais que ainda não receberam tratamento analítico, tais como arquivos de sites governamentais (FONSECA, 2002).

Pesquisa inicial: Identificação dos primeiros artigos com a utilização do Google Acadêmico.

Snowballing: Identificação e coleta de novos estudos que abordam a segurança de dispositivos IoT, a partir dos estudos iniciais.

Elaboração de catálogo: Utilização de critérios para avaliação de falhas de segurança em dispositivos IoT.

A realização da escolha dos trabalhos correlatos foi feita através da recuperação de trabalhos científicos obtidos com a execução dos termos nas bases de dados previamente selecionadas (Google, Google Scholar, Scielo e IEEE Explore) e a inserção dos trabalhos selecionados na ferramenta Publish or Perish, que é utilizada como gerenciador de referências para a manipulação das publicações recuperadas pelas máquinas de busca, facilitando a organização do trabalho, permitindo a categorização das referências e o mapeamento dos documentos, possibilitando a aplicação dos critérios de inclusão e exclusão. Inicialmente, conduziu-se uma pesquisa no Google Acadêmico, empregando uma variedade de strings de busca em inglês e português relacionadas às vulnerabilidades em dispositivos IoT. As strings incluíram termos como 'iot vulnerabilities systematic review', 'vulnerabilities in iot', 'security in iot' e 'what makes iot so insecure?'. A busca foi realizada utilizando diferentes combinações de termos, com o objetivo de abranger ao máximo o conteúdo relevante disponível na literatura. Foi obtida uma média de aproximadamente 1.330.000 resultados, ou seja, um milhão trezentos e trinta mil resultados, numa linha do tempo de 2000 a 2025 durante as buscas, percorrendo duas a três páginas por resultado. A percepção obtida durante a pesquisa revelou que, embora muitos artigos abordassem a segurança em IoT, a maioria estava mais voltada para os protocolos existentes nas redes do que para as vulnerabilidades e ataques em si. Essa observação ressalta a necessidade de um maior enfoque em estudos que abordem diretamente as vulnerabilidades e os ataques enfrentados por dispositivos IoT, a fim de fortalecer a segurança nesse campo em rápida evolução.

Após essa pesquisa inicial, foram selecionados 38 artigos com base em critérios de relevância e qualidade:

Relação do artigo com o tema de estudo;

Trabalhos escritos apenas em inglês e português;

Foi usado um critério de tempo para a busca dos artigos, por ser um tema novo, contudo de alta relevância para a comunidade científica e a sociedade contemporânea.

5. Desenvolvimento do Modelo

O artigo propõe um modelo de maturidade para avaliar vulnerabilidades no ecossistema da Internet das Coisas (IoT), baseado em padrões como ISO 27400, CMMI e COBIT. O CMMI descreve cinco níveis de maturidade organizacional: Inicial, Gerenciado, Definido, Gerenciado Quantitativamente e Otimizado. Cada

nível estabelece objetivos e práticas para melhoria contínua, o COBIT um framework de governança de TI, é dividido em quatro domínios: Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar, e Monitorar e Avaliar, ele é utilizado para avaliar e melhorar processos de TI, garantindo que atenda aos requisitos do negócio, ambos os modelos são compatíveis e podem ser aplicados no contexto da IoT para medir e gerenciar riscos à segurança da informação, promovendo uma melhoria contínua dos processos. A aplicação do CMMI e COBIT permite que as organizações atinjam um nível de maturidade desejado, contribuindo para a eficácia e competitividade no mercado. O CMMI foi estruturado para descrever níveis de maturidade organizacional, organizados em áreas de processos (Áreas de Processos - PA). Cada PA abrange atividades específicas que, quando realizadas em conjunto, são direcionadas para alcançar metas significativas relacionadas à melhoria contínua (TRUDEL et al., 2006). Para a aplicação do CMMI, a avaliação de um PA utiliza o método Standard CMMI Appraisal Method for Process Improvement (SCAMPI). Este método visa determinar o nível de conformidade de um processo com as práticas definidas pelo modelo CMMI. A avaliação das práticas de cada PA utiliza uma classificação semelhante ao modelo ISO/IEC 15504, conhecido como SPICE, que foca na melhoria de processos de software. Esta norma estabelece um conjunto de diretrizes para a avaliação de processos e é uma referência na área de tecnologia da informação. Os parâmetros de classificação incluem: N (Não atendido), P (Parcialmente atendido), L (Largamente atendido) e F (Totalmente atendido). Para que uma prática-chave seja considerada em um nível de maturidade, é necessário que uma avaliação mínima seja L ou F, com F exigida nas práticas-chave anteriores. Níveis de Maturidade o CMMI define cinco níveis de maturidade que uma organização pode atingir: 1 – Inicial, 2 – Gerenciado, 3 – Definido, 4 - Gerenciado Quantitativamente e 5 Otimizado, esses níveis refletem a evolução e o desempenho organizacional ao longo do tempo. Pesquisas demonstram que as organizações obtêm melhores resultados quando se concentram na melhoria de seus processos, o que exige um controle cada vez mais sofisticado à medida que a maturidade avança (SOUSA, 2006). Já o COBIT propõe uma abordagem que não visa apenas controlar processos, mas também identificar quais deles impactam ou introduzem riscos para os negócios, essa identificação é crucial para priorizar o gerenciamento dessas áreas. O framework estabelece objetivos de controle e indicadores de desempenho, permitindo que as organizações meçam sua eficácia e melhorem continuamente, cada processo dentro do COBIT gera objetivos de controle que são requisitos fundamentais para a governança corporativa em TI.

As análises e modelos de maturidade associados a esses processos garantem às organizações uma forma estruturada de avaliar e aprimorar seu desempenho,

Integrando assim com outros modelos sendo o COBIT compatível com outros padrões de mercado, pois adota uma abordagem genérica que abrange diversos processos de TI. Ele não especifica como cada processo deve ser implementado, o que facilita sua integração com outros frameworks existentes. Além disso, ao definir que os processos tecnológicos devem agregar valor às partes interessadas, o COBIT estabelece um conjunto de objetivos interconectados que podem ser geridos de forma eficaz. Organizações de diferentes tamanhos podem aplicar o COBIT de maneiras que atendam às suas necessidades específicas. Enquanto as empresas menores podem optar por menos processos, as organizações maiores podem precisar de uma estrutura mais complexa, uma vez que todos os objetivos de governança sejam cobertos.

Então Inspirado nos modelos do CMMI e COBIT e a norma ISO/IEC 27400 que foi desenvolvido o arcabouço aqui proposto o S.M.M.I.O.T, tem como objetivo sugerir uma padronização para mensuração do nível de segurança e mitigar as vulnerabilidades de um ecossistema de IoT sejam eles em ambientes organizacionais e/ou dentre outros ambientes. A intenção é que seja um modelo universal, podendo assim ser aplicado a qualquer ambiente. O S.M.M.I.O.T toma por base os indicadores da ISO 27400, os níveis de maturidade do CMMI e os processos do COBIT.

O S.M.M.I.O.T é composto de 5 etapas, conforme pode ser visualizado na Figura 03. Dessa forma, deve-se realizar a seleção dos domínios, passando pela seleção dos controles e através das perguntas dos controles ao qual é o conjunto do teste de maturidade depois gera o índice de conformidades por domínios em conjunto que ao final gera o indicie de conformidade geral ao qual é atribuída o nível final da situação de maturidade inspirado no CMMI e processos das informações inspirado no COBIT. Cada etapa será descrita a seguir.

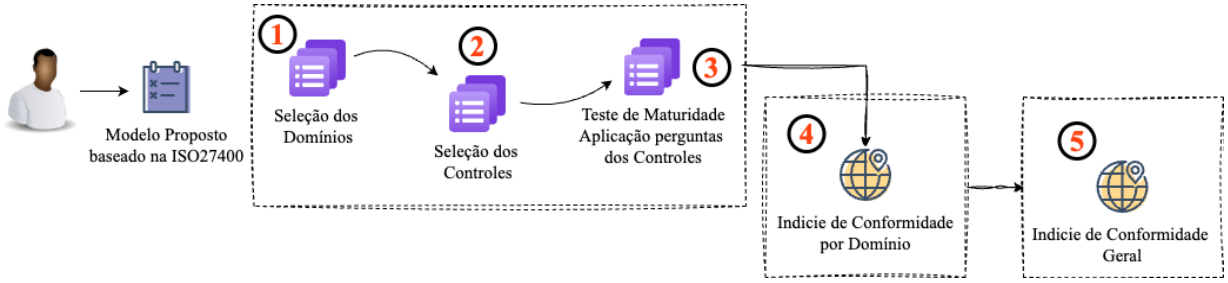

Figura 03 - Arcabouço S.M.M.I.O.T- Modelo De Maturidade IoT

SELEÇÃO DOS DOMÍNIOS

Conforme descrito na Metodologia, a primeira etapa de aplicação do S.M.M.I.O.T é a aplicação da Seleção dos Domínios, após a seleção do

dispositivo IoT a ser analisado. Outro ponto a ser considerado é que o teste pode ser aplicado em sua completude ou apenas em alguns Domínios selecionados previamente como destaca a ISO (2017) salientando que as organizações que utilizam a norma como referência deverão informar pelo menos 50% dos controles desta norma (ISO, 2017). Aqui, o primeiro passo realizado foi a escolha de todos os Domínios, estabelecida pela norma ISO 27400.

ETAPAS 1, 2 e 3

Conforme indicado, a fim de validar o Teste de Conformidade inspirado na ISO/IEC 27400 e utilizando os domínios e controles da mesma, serão selecionados todos os 04 Domínios e os 47 Controles, que consistem no passo 1. Ele é composto pelos domínios, sendo eles: Operação e Gestão, Utilizador, Aplicação de Serviço e Detecção e Controle, tomando como base a ISO 27400, serão utilizados os 47 controles, que são compostos por 47 perguntas, são essas perguntas que irão corresponder a cada controle a ser avaliado. No Anexo A, é possível identificar cada uma dessas perguntas de acordo com cada domínio específico.

ETAPA 4 - Cálculo dos Índices de Conformidades por Domínio

O domínio e os controles a serem calculados fazem parte do ecossistema da IoT da ISO/IEC 27400 e devem ser encontrados a partir de dispositivos conectados à internet e que tenham como entendimento serem pertencentes à IoT. (ISO, 2022). Depois de preencher as 47 questões do teste, nota-se a amplitude dos quesitos abordados pela norma e obviamente, a complexidade em planejar, implementar e gerir todos os controles de segurança a fim de proteger a confidencialidade, integridade e disponibilidade das informações.

Seria ingênuo prometer com este teste o mesmo resultado de uma análise de riscos, mas, através dos índices obtidos com a pontuação final, será possível determinar em que nível de maturidade os dispositivos do ecossistema da IoT estão. Esta situação está presente na maioria dos ambientes e acontece comumente pela ausência de um diagnóstico abrangente e capaz de integrar o levantamento de ameaças, impactos, vulnerabilidades físicas, tecnológicas e humanas, associando-as às reais necessidades. Sem uma análise de riscos desse tipo, as ações tornam-se desorientadas, mal priorizadas, redundantes muitas vezes, e assim não alcançam o retorno esperado e medido pelo nível de segurança.

Após definido os dispositivos, serão analisados os domínios e controles esse é o momento de realizar no passo 3 e identificar a escala de avaliação de parâmetros dos controles. À avaliação do teste de maturidade consiste em um questionário composto por 47 questões, que está apresentada no Anexo A ou vide Norma ISO/IEC 27400 desta pesquisa. Cada questão, que corresponde a um indicador possui três opções de resposta que foram inspiradas e adaptadas do modelo de avaliação do CMMI e a ISO/IEC 27002. As três opções consistem no parâmetro de avaliação, a escala de avaliação de parâmetros vai de 0 a 2, onde 0 corresponde aos parâmetros NA = Não atendido, 1 corresponde a PA = Parcialmente atendido e 2 corresponde a TA = Totalmente atendido. Para chegar a um desses parâmetros (NA, PA ou TA) é necessário ter passado pelos passos anteriores, pois é o valor calculado do indicador que irá determinar o valor da escala, conforme Quadro 04 que foi inspirado nos graus de maturidade do CMMI.

Quadro 04 - Escala da avaliação de parâmetro

Escala de Avaliação de Parâmetros		
NA – Não atendido	0	0 – 15%
PA – Parcialmente atendido	1	15,1% - 85%
TA – Totalmente atendido	2	85,1% - 100%

Após análise dos domínios e controles, os componentes que definirão o índice de maturidade dos dispositivos do ecossistema IoT chegam a um ponto de formulação de dados que implica em uma agregação dos índices calculados para cada domínio e controle, consistindo na Etapa 3. Os índices são instrumentos extremamente importantes para melhorar a comunicação, pois buscam a simplificação da informação sobre fenômenos complexos, de maneira que seu entendimento fique claro para todo tipo de público e, assim, possam nortear a tomada de decisão. Muitas vezes, a composição do índice pode dar pesos diferentes para seus componentes, o que pode ser questionado como subjetividade, uma vez que, dependendo dos pesos atribuídos para cada domínio e controle, o resultado do índice pode variar e muito. O grande diferencial do teste proposto é a sua padronização internacional, vide ISO, e a abordagem orientada aos usuários. Além disso, mais do que um simples teste de avaliação, a proposta não é a de apenas criar mais um teste de conformidade, mas sim a de servir como um instrumento de aprendizagem das

melhores práticas e, desta forma, servir de apoio na formulação de novas políticas de segurança da informação e mitigação das vulnerabilidades. Em função de todos os domínios e controles, optou-se por utilizar-se da lógica estatística e/ou média aritmética dos domínios e controles da ISO/IEC 27400, o que implica em dar o mesmo peso e importância para cada um de seus domínios e controles. Assim, a fórmula de cálculo, para cada controle, pode ser assim representada:

Índice de Conformidade Geral (ICG)

O Índice de Conformidade Geral (ICG) é o índice que vai indicar o nível de maturidade que o ecossistema de IoT se encontra no aspecto global, pois para seu cálculo envolve todos os controles. É a média ponderada multiplicando o ICD (Índice de Conformidade do Domínio) pelo PD (Peso do Domínio) dividido pela soma do PD, sendo k = 1, 2, 3 ... p onde p é o total de Domínios. Variando de 0 a 100%, sua fórmula é definida pela equação (1).

$$ICG = \frac{\sum_{k=1}^{p} ICD_k \times PD_k}{\sum_{k=1}^{p} PD_k}$$

(1)

Onde:

ICG = ÍNDICE DE CONFORMIDADE GERAL

Sendo que PD (Peso dos Domínios) é a soma do ICD (Peso dos Subdomínios) representado pela equação (2).

$$PD = \sum_{j=1}^{m} ICD_m$$

(2)

Onde:

PD = PESO DO DOMÍNIO

Índice de Conformidade do Domínio (ICD)

O Índice de Conformidade do Domínio (ICD) é o índice que vai indicar o nível de maturidade encontra no domínio, para seu cálculo são selecionados os controles do domínio específico. É uma média ponderada o qual é calculado multiplicando o IMD (Índice de Maturidade do Domínio) pelo PD (Peso do Domínio) dividido pela soma do PD tendo j = 1, 2, 3 ... m, sendo o m o total de Domínios, variando de 0 a 100% e sua fórmula é definida pela equação (3).

$$ICD = \frac{\sum_{j=1}^{m} IMD_j \times PD_j}{\sum_{j=1}^{m} PD_j}$$

(3)

Onde:

ICD = ÍNDICE DE CONFORMIDADE DO DOMÍNIO;

IMD = ÍNDICE DE MATURIDADE DO DOMÍNIO;

PD = PESO DO DOMÍNIO.

A Escala da Avaliação é a soma do produto entre a EAP e RI, onde EAP é a Escala da Avaliação de Parâmetros (0 = NA (Não Atendido), 1 = PA (Parcialmente Atendido) e 2 = TA (Totalmente Atendido)) e RI é o Resultado de Indicadores, divido pelo TCI (Total de Controles da ISO) multiplicado pelo EAP[TA] (Escala Totalmente Atendido da Avaliação de Parâmetros) tendo i = 1, 2, 3 ... n, sendo n o total de indicadores de cada subdomínio. Definido pela equação (4).

$$ICD = \frac{\sum_{i=1}^{n} EAP_i \times RI_i}{TCI \times EAP[TA]}$$

(4)

Onde:

EAP = ESCALA DA AVALIAÇÃO DE PARÂMETROS (NA, PA, TA);

RI = RESULTADO DOS CONTROLES;

TTI = TOTAL DE CONTROLES ISO.

ETAPA 5 – NÍVEL DE MATURIDADE GERAL

A Etapa 5 consiste, em direcionar os processos, fazendo com que o resultado final atenda às necessidades e expectativas das áreas, através do planejamento e monitoramento dos resultados obtidos na etapa 1,2 e 3. É nessa etapa que é possível, por meio dos níveis de maturidade inspirados no CMMI, avaliar em que nível o ecossistema de IoT da organização está, ao qual se encontra, dentro de uma escala que varia de 1 até 5, sendo: 1 - Inicial, 2 - Gerenciado, 3 - Definido, 4 - Quantitativamente Gerenciado e 5 - Em Otimização. No nível 1, a

cidade não dispõe ou não realiza atividades ou ações nesta dimensão utilizando recursos tecnológicos ou TIC'S, e sendo 5 se encontra em Otimização (SANTANA; NUNES; SANTOS, 2018), conforme Quadro 05. No Quadro 05 é possível verificar a descrição dos 5 níveis de maturidade inspirados no CMMI, COBIT e ISO27400. Nele é mostrado a representação por estágios, onde se propõe a melhoria de capacidade dos dispositivos IoT através da evolução dos níveis de maturidade. Cada nível de maturidade abrange um conjunto de áreas que devem ser contemplados para que o nível pretendido seja atingido. Por exemplo, para se obter o nível 3 de maturidade, todas os Indicadores dos domínios relacionadas ao nível 1, nível 2 e nível 3 devem ser contempladas.

Quadro 05 - Nível do grau de maturidade inspirado no CMMI, COBIT e ISO/IEC 27400

NÍVEL DE MATURIDADE	DETALHAMENTO	MELHORES PRÁTICAS
1 - Inicial (Não Atingido) (0 á 15%)	O objetivo deste nível deve ser estabelecer uma consciência mínima e iniciar a implementação dos controles mais fundamentais. A descrição deve refletir um ponto de partida onde a organização reconhece as suas deficiências e começa a endereçar os riscos mais básicos. A organização reconhece a importância da segurança IoT, mas as práticas são inconsistentes. Existe uma ausência significativa de controles formais, resultando e alta vulnerabilidade. Iniciam-se esforços para identificar os principais riscos e implementar controles básicos. Iniciar a identificação	Reforço na Conscientização: Adicione a necessidade de treinamentos básicos sobre segurança da informação para todos os colaboradores, destacando a importância da segurança em IoT. Identificação de Ativos: Inicie um inventário dos dispositivos IoT e suas vulnerabilidades, mesmo que a segurança não seja uma prioridade.

	dos principais ativos IoT e das ameaças mais óbvias. Não é uma avaliação de risco formal, mas um levantamento preliminar. Começar a documentar as funcionalidades básicas dos dispositivos IoT e, se possível, notificar o responsável pela área de segurança mesmo que informalmente. Identificar e alterar senhas padrão em dispositivos críticos. Implementar uma política básica de senhas fortes. Identificar se os dispositivos podem ser atualizados e, se sim, aplicar atualizações de segurança críticas manualmente, mesmo que não haja um mecanismo seguro automatizado. Criar um inventário simples dos dispositivos IoT conectados.	
	O foco deve ser em estabelecer processos gerenciados para controles fundamentais, incluindo a capacitação e a implementação de mecanismos de atualização seguros. A organização começa a gerir ativamente a segurança de alguns dos seus sistemas IoT. Existem processos básicos definidos para controles essenciais, embora a sua aplicação possa ser inconsistente.	**Implementação de Políticas de Segurança: Estabeleça políticas de segurança claras para o uso e gerenciamento de dispositivos IoT, alinhadas com as diretrizes da ISO/IEC 27400.** **Capacitação Contínua: Invista em treinamentos e capacitação para as equipes que operam e**

2- Gerenciado (Parcialmente Atingido) (>15% á 50%)	Reconhece-se a necessidade de competências específicas e iniciam-se esforços para capacitação. Mecanismos de atualização de software/firmware começam a ser implementados ou melhorados, com foco na segurança. Implementar um processo simplificado, mas formal, de avaliação de riscos para os principais sistemas IoT. Documentar os riscos identificados e os planos de tratamento básicos. Desenvolver e comunicar políticas básicas de segurança IoT, incluindo uma política de suporte de segurança que defina responsabilidades e o ciclo de vida das atualizações. Estabelecer um canal para receber notificações de vulnerabilidades (interno ou externo) e um processo básico para avaliar e endereçar para áreas responsáveis. Implementar ou assegurar que os dispositivos IoT críticos possuam um mecanismo para atualizações de software/firmware que verifique a autenticidade e integridade das atualizações. Definir e aplicar configurações de segurança padrão para novos dispositivos IoT. Controlar quem pode alterar	**mantêm os dispositivos IoT, com foco em práticas seguras e atualizações sobre ameaças.**

	configurações críticas. Identificar dados sensíveis em dispositivos IoT e aplicar controles básicos de proteção (ex: criptografia dos dados). Garantir que todas as interfaces (físicas, lógicas) tenham mecanismos de autenticação. Desativar interfaces não utilizadas. Implementar programas de formação para as equipas relevantes sobre segurança IoT e as políticas definidas.	
3- Definidos (Em grande parte alcançado)	O foco é garantir que os processos e controles de segurança IoT definidos sejam mantidos, atualizados e consistentemente aplicados em toda a organização. A organização possui um conjunto definido e documentado de políticas, procedimentos e controles de segurança IoT, alinhados com as melhores práticas. Estes processos são compreendidos e seguidos consistentemente. Existe um esforço ativo para manter os controles atualizados e gerir as vulnerabilidades de forma proativa. A gestão de riscos é um processo estabelecido e revisto periodicamente. O processo de gestão de risco é aplicado a todos os sistemas IoT, revisto regularmente e atualizado com base em novas ameaças	**Adoção de Controles de Segurança: Incorpore controles de segurança específicos da norma ISO/IEC 27400, como autenticação forte, criptografia de dados e gestão de identidade.** **Avaliação de Risco: Realize avaliações de risco regulares para identificar e mitigar vulnerabilidades nos dispositivos IoT, garantindo que as medidas de segurança estejam atualizadas.**

(>50 á 85%)	e vulnerabilidades. As políticas de segurança IoT são revistas e atualizadas periodicamente para refletir mudanças no ambiente de ameaças e nos requisitos do negócio. Implementar ferramentas e processos para identificação proativa de vulnerabilidades. O processo de tratamento é bem definido e os prazos de correção são monitorizados. Incorporar requisitos de segurança e privacidade nas fases de desenho e aquisição de novas soluções IoT. Aplicar controles de criptografias fortes para dados sensíveis. Implementar controles de acesso baseados em funções (RBAC) Controle de Acesso Baseado em Funções método de segurança que permite que os administradores de sistemas de TI concedam permissões aos usuários com base nas suas funções no sistema, em vez de conceder permissões individualmente a cada usuário. Processos definidos e testados para a exclusão segura de dados do administrador quando necessário ou no fim de vida do dispositivo. Utilizar protocolos de comunicação seguros e criptografia como padrão para todas as comunicações IoT.	

	Implementar o registo de eventos "logs" de segurança relevantes e monitorizar alertas para detectar atividades suspeitas. Definir processos para a gestão da segurança ao longo de todo o ciclo de vida dos dispositivos e serviços IoT, incluindo a interrupção definitiva das operações deste dispositivo.	
4- Quantitativamente Gerenciado (Totalmente alcançado) (> 85 á 100%)	O foco é na medição do desempenho da segurança, na utilização de dados quantitativos para a tomada de decisões e na implementação de controles avançados. A organização gere quantitativamente os seus processos de segurança IoT. São recolhidas métricas de desempenho para os controles de segurança, e estas métricas são usadas para identificar áreas de melhoria e para gerir os riscos de forma proativa. A segurança e a privacidade são integradas em todos os aspetos dos serviços IoT, com uma forte ênfase na resiliência e na proteção de dados avançada. Definir e recolher métricas para medir a eficácia dos controles de segurança IoT (ex: tempo para corrigir vulnerabilidades, número de incidentes, conforme	**Monitoramento e Resposta a Incidentes: Estabeleça um sistema de monitoramento contínuo dos dispositivos IoT e um plano de resposta a incidentes, baseado em práticas recomendadas da ISO.** **Relatórios e Métricas: Utilize métricas para avaliar a eficácia das medidas de segurança implementadas, garantindo que os dados coletados sejam utilizados para melhorias contínuas.**

	políticas). Utilizar dados e modelos quantitativos para avaliar a probabilidade e o impacto dos riscos de segurança IoT. Implementar controles como proteção contra engenharia reversa, segurança de hardware, proteção de propriedade intelectual, resistência a ataques. Implementar autenticação multifator (MFA), gestão de identidades federadas e princípios de privilégio mínimo de forma rigorosa. Planos de resiliência e recuperação de desastres testados regularmente para garantir a continuidade dos serviços IoT críticos. Implementar e monitorizar controles de privacidade, como minimização de dados, gestão de consentimento e avaliações de impacto sobre a privacidade regulares. Avaliar e monitorizar continuamente os riscos de segurança provenientes de fornecedores e componentes de terceiros. Realizar testes de penetração e avaliações de segurança de forma regular e abrangente.	
5- Em Otimização (Otimizado) (100%)	O foco é na melhoria contínua, inovação e liderança em segurança e privacidade IoT, a organização demonstra uma cultura de melhoria contínua	**Gestão de Segurança Integrada: Promova uma abordagem de segurança integrada que inclua gestão de riscos, conformidade e governança, com a**

	e inovação em segurança e privacidade IoT. Os processos são constantemente revistos e otimizados com base em análises de tendências, novas ameaças e tecnologias emergentes. A organização é pioneira na adoção de soluções de segurança avançadas e contribui ativamente para as melhores práticas da indústria. A gestão de riscos é totalmente integrada e dinâmica, sob uma governação de segurança robusta liderada por um Security Officer (ou função similar). Implementação de um ciclo PDCA (Plan-Do-Check-Act) robusto para todos os aspetos da segurança IoT. Dedicar recursos para investigar e testar novas tecnologias e abordagens de segurança e privacidade IoT. Utilizar inteligência de ameaças e análise preditiva para antecipar futuros riscos de segurança. Automatizar processos de segurança sempre que possível (ex: resposta a incidentes, gestão de vulnerabilidades, monitorização de conformidade). Participar em fóruns da indústria, partilhar lições aprendidas e contribuir para o desenvolvimento de normas e melhores práticas. Foco na capacidade de	**supervisão de um Security Officer qualificado.** **Inovação e Melhoria Contínua: Estabeleça um processo de inovação contínua em segurança, incorporando novas tecnologias e práticas recomendadas, e revisando regularmente as políticas de segurança em resposta a novas ameaças.**

	antecipar, resistir, recuperar e adaptar-se a ciberataques e disrupções. O Security Officer (ou CISO) tem um papel estratégico na definição da direção da segurança IoT, alinhada com os objetivos de negócio.	

6. Discursão dos Resultados

Conforme descrito na Metodologia, a primeira etapa de aplicação do S.M.M.I.O.T é a análise da norma, escolha dos domínios, sejam eles em sua completude ou deverão informar pelo menos 50% dos controles e aplicação do questionário dos mesmos. Por fim, o Teste de Maturidade, bem como a seleção do dispositivo IoT a ser analisado, outro ponto a ser considerado é que, antes do teste, foi feita uma avaliação de estudo de caso de um sistema de CFTV em uma empresa XPTO para podermos validar e dimensionar os indicadores do modelo proposto. Sendo assim, foi possível aplicar, em sua completude, os Domínios selecionados previamente, aos quais todos os Domínios e controles foram utilizados baseados pela norma ISO 27400.

Para avaliação e aplicação do S.M.M.I.O.T, deveremos analisar e identificar cenários de risco aos quais são utilizados os serviços dos dispositivos IoT, que devem ser identificados e analisados caso a caso. De forma a criar o estudo de caso, estes podem ser em ambientes como lojas, escolas e empresas, onde os criadores de serviços IoT e os prestadores de serviços IoT podem utilizar esta amostra como referência para desenvolver os seus próprios cenários de risco, que incluirão elementos detalhados sobre fontes, eventos e consequências do risco. Devem ser fornecidos diferentes cenários de risco para diferentes perspectivas, a fim de mostrar claramente as cadeias de causas e consequências. Ao final, para avaliar o nível de maturidade de segurança dos seus sistemas, utilizará a planilha do S.M.M.I.O.T (Modelo de Maturidade da Internet das Coisas), que classificará seu nível de segurança, sendo ele geral ou por domínio.

Para o estudo de caso, vamos utilizar a empresa XPTO em um cenário de risco de câmeras de monitoramento, dispositivo IoT.

Os quadros 06, 07 e 08 abordarão o cenário de risco de um sistema de CFTV e/ou dispositivo IoT. Nesta amostra, o modelo de sistema IoT é um sistema de câmeras de monitoramento que:

É implantado em uma instalação, de uma loja (mercado), onde o sistema de monitoramento de câmeras, tem câmeras ligadas em rede e servidores que conservam as imagens das câmeras, armazenando seus dados em disco e na nuvem.

Quadro 06 - Cenário de risco de câmeras de vigilância de um sistema IoT

Câmeras de Monitoramento de Sistema CFTV– Fontes de Risco
1) Fontes de risco relacionadas com as configurações e ambientes do sistema:
As câmeras estão ligadas aos servidores através da rede.
As câmeras estão localizadas em locais fisicamente desprotegidos.
As câmeras estão situadas em locais onde os fenómenos naturais e as condições ambientais podem afetar o seu funcionamento.
2) Fontes de risco relacionadas com as infraestruturas críticas:
O funcionamento do sistema depende do fornecimento de energia eléctrica.
O funcionamento do sistema depende dos serviços de rede.
3) Fontes de risco relacionadas com a qualidade e a funcionalidade do sistema e dos componentes:
As câmeras, outros componentes do sistema ou as configurações do sistema têm vulnerabilidades.
As câmaras aceitam palavras-passe fracas.
As actualizações de software não são aplicadas a câmaras ou outros componentes.
A configuração da rede permite o acesso às câmaras e a outros componentes por pessoas não autorizadas pessoas.
4) Fontes de risco relacionadas com os fornecedores e a cadeia de abastecimento das TIC:
Os criadores da câmera e do sistema não possuem os conhecimentos e as competências necessárias para o desenvolvimento seguro de sistemas e aplicações.
Os criadores da câmera e do sistema não aplicam metodologias de desenvolvimento estabelecidas.
O sistema e os seus componentes são produzidos em cadeias de fornecimento de TIC.
Os utilizadores não estão bem informados dos requisitos para a utilização segura do

sistema.
5) Fontes de risco relacionadas com as pessoas envolvidas na utilização e fornecimento do sistema:
Os utilizadores não possuem os conhecimentos e as competências necessárias para utilizar e manter o sistema de forma segura.
Pode haver erros humanos nos processos de utilização do sistema.
6) Fontes de risco relacionadas com pessoas com intenções maliciosas:
Há pessoas que têm a intenção maliciosa de atacar ou abusar de sistemas através de redes.

Quadro 07 - Cenário de risco de câmeras de vigilância de um sistema IoT

Câmeras de Monitoramento de serviço IoT – Eventos
1) Acontecimentos de origem externa:
Falha no fornecimento de energia eléctrica durante o funcionamento.
Falha nos serviços de rede em funcionamento.
O sistema é atacado.
O sistema é invadido.
2) Eventos relacionados com as câmaras e o sistema:
As câmeras estão danificadas devido às más condições climatéricas.
As câmeras são destruídas ou roubadas.
As câmeras e o sistema estão infectados com malware.
O sistema para o seu funcionamento.
As câmaras estão inoperacionais.
As imagens das câmeras são divulgadas a pessoas não autorizadas.
As imagens das câmeras estão expostas no sítio Web.
As imagens das câmeras não estão disponíveis nas telas de monitoramento.
3) Acontecimentos que afetam as partes externas:
As câmeras enviam pacotes que analisam ou atacam equipamentos de terceiros.
O equipamento de terceiros está infetado com malware.
As câmeras são utilizadas para ataques DDoS a infraestruturas críticas de uma nação

ou de outras organizações.

Quadro 08 - Cenário de risco de câmeras de vigilância de um sistema IoT

Câmeras de Monitoramento de serviço IoT – Consequências
1) Consequências relacionadas com a organização:
O processo comercial que utiliza as imagens das câmeras não é operado.
A segurança física da instalação está enfraquecida.
A monitoramento como função de segurança numa fábrica está inoperacional.
A organização sofre perdas monetárias.
A organização sofre danos na sua reputação.
2) Consequências relacionadas com as partes externas
A privacidade das pessoas captadas nas imagens das câmeras é violada
O funcionamento das infraestruturas críticas de um país é afetado.

O cenário de risco da empresa XPTO pode estar relacionado com a confidencialidade das informações, o segundo cenário pode estar relacionado com a integridade, disponibilidade das informações e dos equipamentos, por consequência para a continuidade das atividades da organização. O terceiro cenário de risco pode envolver ataques a equipamentos de terceiros, como eventos e efeitos adversos sobre os mesmos, como consequências.

Para tornar conciso o cenário de risco da empresa XPTO, foram descritos nos quadros 05, 06 e 07 elementos que potencializam os riscos. A partir deste cenário, será aplicado o Teste de Maturidade da ISO 27400, ao qual avaliaremos as suas conformidades por domínio e chegaremos ao índice de conformidade geral, ao qual avaliaremos em que situação este dispositivo IoT (sistema CFTV) está. Após estabelecida a estrutura conceitual do modelo, procedeu-se à seleção dos domínios e seus controles para avaliar e classificar cada uma das dimensões do modelo proposto. Nesta fase, além da obediência ao critério de coerência com o conceito adotado, alguns aspectos metodológicos foram observados e algumas escolhas metodológicas feitas. O modelo de classificação proposto, S.M.M.I.O.T, observa com rigor o conceito adotado do ecossistema de IoT, de maneira que todos os componentes escolhidos, além de constarem explicitamente no conceito, formam sua base e destacam os valores importantes para a análise do S.M.M.I.O.T. (ISO, 2022).

Na Figura 04, é possível observar os quatro domínios e seus respectivos controles, totalizando 47. Cada domínio possui seus indicadores/controles, os quais têm seus pesos, que são utilizados para o cálculo dos índices. O protótipo foi concebido para contemplar os quatro domínios de classificação de um dispositivo IoT. Conforme explicitado, foi realizado um estudo dos indicadores a serem utilizados em cada um dos domínios. A escolha de indicadores adequados é fundamental para a confiabilidade e transparência de qualquer modelo de avaliação, mas é uma tarefa extremamente difícil e facilmente questionável.

ICG	DOMINIOS	ICD	CONTROLES	PERGUNTAS	NA	PA	TA	PD
					0	1	2	
72%	1. Operação e Gestão	82%	01: Política de segurança da IoT	1 - Existe uma política de segurança da IoT, aprovada pela direção, publicada, comunicada ao pessoal relevante e às partes externas relevantes e revista a intervalos planejados pela direção?			X	50
			02: Organização da segurança da IoT	2 - As funções de responsabilidades pela segurança da IoT devem ser definidas e atribuídas.			X	
			03: Gestão de ativos	3 - Devem ser identificadas as informações, os dispositivos e sistemas IoT e as suas funções e operações a proteger.			X	
			04: Equipamentos e ativos localizados fora das áreas físicas protegidas	4 - Devem ser aplicadas medidas de segurança específicas aos equipamentos e bens da Internet das coisas que estão localizados ou funcionam fora das zonas físicas protegidas.			X	
			05: Eliminação ou reutilização segura do equipamento	5 - Todos os equipamentos que contenham suportes de armazenamento devem ser verificados para garantir que quaisquer dados sensíveis e software licenciado foram removidos ou substituídos de forma segura antes de serem eliminados ou reutilizados.			X	
			06: Aprender com os incidentes de segurança	6 - Os conhecimentos adquiridos com a análise e a resolução de incidentes de segurança da IoT devem ser utilizados para reduzir a probabilidade ou o impacto de futuros incidentes.			X	
			07: Ambiente e procedimentos de desenvolvimento seguros	7 - O ambiente e os procedimentos de desenvolvimento seguro devem ser aplicados ao desenvolvimento de sistemas IoT.			X	
			08: Segurança dos sistemas IoT em prol da segurança	8 - Os princípios de segurança que apoiam a segurança devem ser aplicados ao desenvolvimento de sistemas IoT			X	
			09: Segurança na ligação de dispositivos IoT variados	9 - Um sistema IoT deve ser concebido e implementado para garantir e manter a segurança na ligação de vários dispositivos IoT.			X	
			10: Verificação da conceção dos dispositivos e sistemas IoT	10 - A conceção e a implementação de dispositivos e sistemas IoT devem ser verificadas.			X	
			11: Monitorização e registo	11 - Os estados, eventos e tráfego de rede dos dispositivos e sistemas IoT devem ser monitorizados e registados.			X	
			12: Proteção dos registos	12 - Os registos dos dispositivos e sistemas IoT devem ser protegidos contra fugas, destruição e alterações não intencionais.			X	
			13: Utilização de redes adequadas para os sistemas IoT	13 - As tecnologias de rede e de comunicação aplicadas à IoT e aos sistemas devem satisfazer as necessidades de função, capacidade e segurança de comunicação, bem como de função e desempenho dos dispositivos IoT.			X	
			14: Definições e configurações seguras no fornecimento de dispositivos e serviços IoT.	14 - Os dispositivos e serviços IoT devem ser fornecidos com definições e configurações seguras			X	
			15: Autenticação de utilizadores e dispositivos.	15 - Deve ser implementada e aplicada a função de autenticação dos utilizadores e dos dispositivos IoT para acederem aos sistemas e serviços IoT.			X	
			16: Fornecimento de actualizações de software e firmware.	16 - Deve ser concebido, implementado e operado um mecanismo para atualizar o software e o firmware dos dispositivos e sistemas IoT.			X	
			17: Compartilhar informações sobre vulnerabilidades.	17 - As vulnerabilidades dos dispositivos, sistemas e serviços IoT devem ser monitorizadas e informadas aos utilizadores da IoT e às partes interessadas, juntamente com os riscos associados.			X	
			18: Medidas de segurança adaptadas ao ciclo de vida dos sistemas e serviços IoT.	18 - As medidas de segurança do sistema e do serviço IoT devem ser adaptadas e mantidas durante as fases do ciclo de vida, incluindo o seu desenvolvimento, funcionamento, manutenção e destruição.			X	
			19: Orientações para os utilizadores da Internet das Coisas sobre a utilização adequada dos dispositivos e serviços da Internet das Cois	19 - Os utilizadores da IoT devem receber orientações sobre a utilização adequada dos dispositivos IoT, com os riscos e os efeitos indesejáveis do sistema e do serviço IoT que podem resultar de uma utilização inadequada dos dispositivos IoT.			X	
			20: Determinação das funções de segurança das partes interessadas	20 - As funções do criador do serviço IoT, do fornecedor do serviço IoT e de outras partes interessadas na segurança do sistema e do serviço IoT devem ser determinadas e acordadas entre as partes interessadas.			X	
			21: Gestão de dispositivos vulneráveis	21 - Os dispositivos IoT vulneráveis devem ser detectados, registados e devem ser fornecidos alertas aos utilizadores e administradores de IoT destes dispositivos.			X	
			22: Gestão das relações com os fornecedores no domínio da segurança da IoT	22 - As especificações e as obrigações de apoio dos fornecedores em matéria de segurança da informação do dispositivo IoT e do serviço IoT devem ser geridas pela organização adquirente com base nos contratos com os fornecedores.			X	
			23: Prevenção de eventos invasivos da privacidade	23 - Os dispositivos e serviços IoT devem incorporar capacidades de reforço da privacidade.			X	
			24: Privacidade da IoT por defeito	24 - As partes interessadas num sistema IoT devem garantir que, sem qualquer interação ou intervenção do utilizador IoT, as definições de privacidade mais rigorosas se apliquem por defeito.			X	
			25: Fornecimento de aviso de privacidade 1	25 - O utilizador da IoT deve receber um aviso de privacidade que indique os dados pessoais recolhidos pelo dispositivo IoT e pelo serviço IoT e a finalidade da sua utilização.			X	
			26: Fornecimento de aviso de privacidade 2	26 - O consentimento do utilizador da IoT para o aviso de privacidade deve ser obtido antes de recolher os dados pessoais ou de alterar a finalidade da utilização.			X	
			27: Verificação da funcionalidade IoT	27 - Deve ser fornecida uma verificação independente do dispositivo IoT, dos componentes de dados e dos componentes do serviço IoT para dar visibilidade e garantia a todas as partes interessadas de que o dispositivo ou serviço IoT está a funcionar de acordo com os objetivos declarados.			x	
			28: Consideração dos utilizadores da IoT	28 - Os requisitos e preocupações dos utilizadores finais em matéria de privacidade devem ser tidos em conta na conceção do dispositivo IoT e serviço.			x	
			29: Gestão dos controlos de privacidade da IoT	29 - A eficácia dos controlos de privacidade no dispositivo e serviço IoT deve ser revista e devem ser identificados continuamente novos riscos de privacidade, tendo em conta a evolução das necessidades de privacidade dos utilizadores finais e os requisitos regulamentares.				
			30: Identidade única do dispositivo 01	30 - Os criadores de sistemas IoT (especialmente os criadores de dispositivos) devem utilizar um método que identifique exclusivamente cada dispositivo IoT para melhorar a privacidade na identificação de dispositivos IoT suspeitos de serem relevantes para um incidente cibernético.		x		
			31: Identidade única do dispositivo 02	31 - Os prestadores de serviços IoT devem utilizar, se necessário, um método que permita um mapeamento único entre um determinado dispositivo IoT e um utilizador IoT para melhorar a privacidade na identificação do mapeamento entre o dispositivo IoT e o(s) utilizador(es) IoT.			x	
			32: Autenticação à prova de falhas	32 - Uma vez que o dispositivo (coisa) muitas vezes não está com o utilizador, e as consequências de um utilizador errado que se ligue ao dispositivo podem causar sérios danos em termos de segurança, perdas financeiras, riscos para a saúde, etc. No caso do serviço de autenticação tradicional, o resultado				
			33: Minimização da recolha indireta de dados	33 - A recolha de dados de fontes indiretas deve ser minimizada ou não deve ser recolhida de todo.				
			34: Comunicação das preferências de privacidade	34 - As preferências do utilizador em relação aos controlos de privacidade só devem ser adicionadas, modificadas ou eliminadas quando o utilizador autorizado estiver autenticado no sistema.				
			35: Verificação da decisão automatizada	35 - A decisão automatizada fornecida pelos serviços IoT deve ser verificada.		x		
			36: Responsabilização das partes interessadas	36 - Deve ser estabelecida a responsabilidade dos vários intervenientes.		x		
			37: Desvinculação das informações pessoais	37 - O sistema IoT deve garantir que as informações pessoais do utilizador proprietário de um dispositivo não possam ser identificadas.				
					0	3	29	
	2. Utilizador	64%	1: Contatos e serviço de apoio	1 - Os utilizadores de IoT só devem escolher dispositivos e serviços IoT que forneçam informações de contacto para apoio serviço.			x	25
			2: Definições iniciais do dispositivo e serviço IoT	2 - As definições iniciais do dispositivo IoT e do serviço devem ser aplicadas corretamente.				
			3: Desativação de dispositivos não utilizados	3 - Os dispositivos IoT devem ser desativados e as credenciais revogadas quando deixarem de ser utilizados.			x	
			4: Eliminação ou reutilização segura do dispositivo IoT	4 - Os dados e o software licenciado armazenados no dispositivo IoT devem ser removidos ou substituídos de forma segura antes de serem eliminados ou reutilizados.		x		
			5: Consentimento do utilizador	5 - O consentimento para a utilização de dados pessoais para o dispositivo e serviço IoT só deve ser dado depois de se ter considerado a necessidade e o seu provável impacto em caso de violação de dados. O consentimento deve ser retirado se o resultado da IoT já não for necessário ou se houver algum				
			6: Utilização propositada para ligação a outros dispositivos e serviços	6 - A ligação de um dispositivo e serviço IoT a outros dispositivos ou serviços só deve ser permitida se houver uma necessidade válida.			x	
			7: Certificação e validação da proteção das informações pessoais	7 - Certificação ou validação das características de proteção da privacidade no que respeita ao dispositivo e serviço IoT deve ser procurado.			x	
					0	1	4	
	3. Aplicação de Serviço	50%	1: Princípios de engenharia de sistemas IoT seguros	1 - Os princípios para a engenharia de sistemas IoT seguros que abordam a conceção e a implementação de funções de segurança, a defesa em profundidade e o endurecimento de sistemas e software devem ser aplicados ao desenvolvimento de sistemas IoT.		x		5
					0	1	0	
	4. Detecção e Controle	50%	1: Divulgação segura de informações sobre a segurança dos dispositivos IoT	1 - As informações sobre o dispositivo IoT relevantes para a segurança dos serviços IoT devem ser documentadas e divulgadas apenas às partes que as solicitem.				10
			2: Partilha de informações sobre as medidas de proteção dos dispositivos IoT	2 - As medidas de proteção relacionadas com o risco para a privacidade nos dispositivos IoT devem ser geridas de forma adequada e apenas divulgadas às partes que delas necessitem.			x	
					0	0	1	

Figura 04 - Partes interessadas dos sistemas IoT

A partir desses dados foi realizado o cálculo dos Indicadores dos Domínios, com base no teste disponibilizado pelos controles da ISO 27400, gerando após as análises dos cálculos estatísticos no Excel ao qual remete a Figura 05. Com tudo a garantir a confiabilidade e a validade dos dados.

Total de Indicadores	47
Índice de Conformidade Geral (ICG)	72%
Índice De Conformidade Por Domínio	ICD
1. Operação e Gestão	86,4%
2. Utilizador	64,3%
3. Aplicação de Serviço	50,0%
4. Detecção e Controle	50,0%

Figura 05 - Base de avaliação

O primeiro indicador calculado foi referente ao índice de conformidade geral (ICG), que, por sua vez, para se chegar aos 72%, foram utilizados os 47 Indicadores. Esse índice de 72% está em um nível definido (em grande parte alcançado) (>50 a 85%), O foco é garantir que os processos e controles de segurança IoT definidos sejam mantidos, atualizados e consistentemente aplicados em toda a organização. A organização possui um conjunto definido e documentado de políticas, procedimentos e controles de segurança IoT, alinhados com as melhores práticas. Estes processos são compreendidos e seguidos consistentemente. Existe um esforço ativo para manter os controles atualizados e gerir as vulnerabilidades de forma proativa. A gestão de riscos é um processo estabelecido e revisto periodicamente. O processo de gestão de risco é aplicado a todos os sistemas IoT, revisto regularmente e atualizado com base em novas ameaças e vulnerabilidades. As políticas de segurança IoT são revistas e atualizadas periodicamente para refletir mudanças no ambiente de ameaças e nos requisitos do negócio. Implementar ferramentas e processos para identificação proativa de vulnerabilidades. O processo de tratamento é bem definido e os prazos de correção são monitorizados. Incorporar requisitos de segurança e privacidade nas fases de desenho e aquisição de novas soluções IoT. Aplicar controles de criptografias fortes para dados sensíveis. Implementar controles de acesso baseados em funções (RBAC) Controle de Acesso Baseado em Funções método de segurança que permite que os administradores de sistemas de TI concedam permissões aos usuários com base nas suas funções no sistema, em vez de conceder permissões individualmente a cada usuário. Processos definidos e testados para a exclusão segura de dados do administrador quando necessário ou no fim de vida do dispositivo. Utilizar protocolos de comunicação seguros e criptografia como padrão para todas as comunicações IoT. Implementar o registo de eventos "logs" de segurança relevantes e monitorizar alertas para detectar atividades suspeitas. Definir processos para a gestão da segurança ao longo de todo o ciclo de vida dos dispositivos e serviços IoT, incluindo a interrupção definitiva das operações deste dispositivo.

O próximo índice é o de conformidade por domínio (ICD), que está dividido em 4 domínios. O primeiro é o de OPERAÇÃO E GESTÃO ao qual foi avaliado a 86,4% se encontrando no nível de maturidade QUANTITATIVAMENTE GERENCIADO ao qual o foco é na medição do desempenho da segurança, na utilização de dados quantitativos para a tomada de decisões e na implementação de controles avançados. A organização gere quantitativamente os seus processos de segurança IoT. São recolhidas métricas de desempenho para os controles de segurança, e estas métricas são usadas para identificar

áreas de melhoria e para gerir os riscos de forma proativa. A segurança e a privacidade são integradas em todos os aspetos dos serviços IoT, com uma forte ênfase na resiliência e na proteção de dados avançada. Definir e recolher métricas para medir a eficácia dos controles de segurança IoT (ex: tempo para corrigir vulnerabilidades, número de incidentes, conforme políticas). Utilizar dados e modelos quantitativos para avaliar a probabilidade e o impacto dos riscos de segurança IoT. Implementar controles como proteção contra engenharia reversa, segurança de hardware, proteção de propriedade intelectual, resistência a ataques. Implementar autenticação multifator (MFA), gestão de identidades federadas e princípios de privilégio mínimo de forma rigorosa. Planos de resiliência e recuperação de desastres testados regularmente para garantir a continuidade dos serviços IoT críticos. Implementar e monitorizar controles de privacidade, como minimização de dados, gestão de consentimento e avaliações de impacto sobre a privacidade regulares. Avaliar e monitorizar continuamente os riscos de segurança provenientes de fornecedores e componentes de terceiros. Realizar testes de penetração e avaliações de segurança de forma regular e abrangente.

O domínio UTILIZADOR está com 64,3% do nível de maturidade ao qual denominasse que ele se enquadro na maturidade DEFINIDOS. Neste nível, a empresa XPTO tem o foco é garantir que os processos e controles de segurança IoT definidos sejam mantidos, atualizados e consistentemente aplicados em toda a organização. A organização possui um conjunto definido e documentado de políticas, procedimentos e controles de segurança IoT, alinhados com as melhores práticas. Estes processos são compreendidos e seguidos consistentemente. Existe um esforço ativo para manter os controles atualizados e gerir as vulnerabilidades de forma proativa. A gestão de riscos é um processo estabelecido e revisto periodicamente. O processo de gestão de risco é aplicado a todos os sistemas IoT, revisto regularmente e atualizado com base em novas ameaças e vulnerabilidades. As políticas de segurança IoT são revistas e atualizadas periodicamente para refletir mudanças no ambiente de ameaças e nos requisitos do negócio. Implementar ferramentas e processos para identificação proativa de vulnerabilidades. O processo de tratamento é bem definido e os prazos de correção são monitorizados. Incorporar requisitos de segurança e privacidade nas fases de desenho e aquisição de novas soluções IoT. Aplicar controles de criptografias fortes para dados sensíveis. Implementar controles de acesso baseados em funções (RBAC) Controle de Acesso Baseado em Funções método de segurança que permite que os administradores de sistemas de TI concedam permissões aos usuários com base nas suas funções no sistema, em vez de conceder permissões individualmente a cada usuário.

Processos definidos e testados para a exclusão segura de dados do administrador quando necessário ou no fim de vida do dispositivo. Utilizar protocolos de comunicação seguros e criptografia como padrão para todas as comunicações IoT. Implementar o registo de eventos "logs" de segurança relevantes e monitorizar alertas para detectar atividades suspeitas. Definir processos para a gestão da segurança ao longo de todo o ciclo de vida dos dispositivos e serviços IoT, incluindo a interrupção definitiva das operações deste dispositivo.

O domínio de APLICAÇÕES DOS SERVIÇOS e de DETECÇÃO ambos estão com 50% adequados assim no nível de maturidade GERENCIADO ao qual o foco deve ser em estabelecer processos gerenciados para controles fundamentais, incluindo a capacitação e a implementação de mecanismos de atualização seguros. A organização começa a gerir ativamente a segurança de alguns dos seus sistemas IoT. Existem processos básicos definidos para controles essenciais, embora a sua aplicação possa ser inconsistente. Reconhece-se a necessidade de competências específicas e iniciam-se esforços para capacitação. Mecanismos de atualização de software/firmware começam a ser implementados ou melhorados, com foco na segurança. Implementar um processo simplificado, mas formal, de avaliação de riscos para os principais sistemas IoT. Documentar os riscos identificados e os planos de tratamento básicos. Desenvolver e comunicar políticas básicas de segurança IoT, incluindo uma política de suporte de segurança que defina responsabilidades e o ciclo de vida das atualizações. Estabelecer um canal para receber notificações de vulnerabilidades (interno ou externo) e um processo básico para avaliar e endereçar para áreas responsáveis. Implementar ou assegurar que os dispositivos IoT críticos possuam um mecanismo para atualizações de software/firmware que verifique a autenticidade e integridade das atualizações. Definir e aplicar configurações de segurança padrão para novos dispositivos IoT. Controlar quem pode alterar configurações críticas. Identificar dados sensíveis em dispositivos IoT e aplicar controles básicos de proteção (ex: criptografia dos dados). Garantir que todas as interfaces (físicas, lógicas) tenham mecanismos de autenticação. Desativar interfaces não utilizadas. Implementar programas de formação para as equipas relevantes sobre segurança IoT e as políticas definidas.

A interpretação do valor obtido nesse indicador do ICG como mostra na Figura 06 é a seguinte: quanto maior for o número de ICG, melhor e mais forte será o nível de segurança e a preocupação com a atualização dos dispositivos IoT. A privacidade é uma questão importante para produtos e serviços baseados em IoT. Embora os dados obtidos de sensores IoT e os dados gerados a partir de

serviços IoT estejam sendo utilizados para criar novos modelos de negócios e serviços em vários campos, por outro lado, a proteção da privacidade do usuário também está se tornando uma preocupação social.

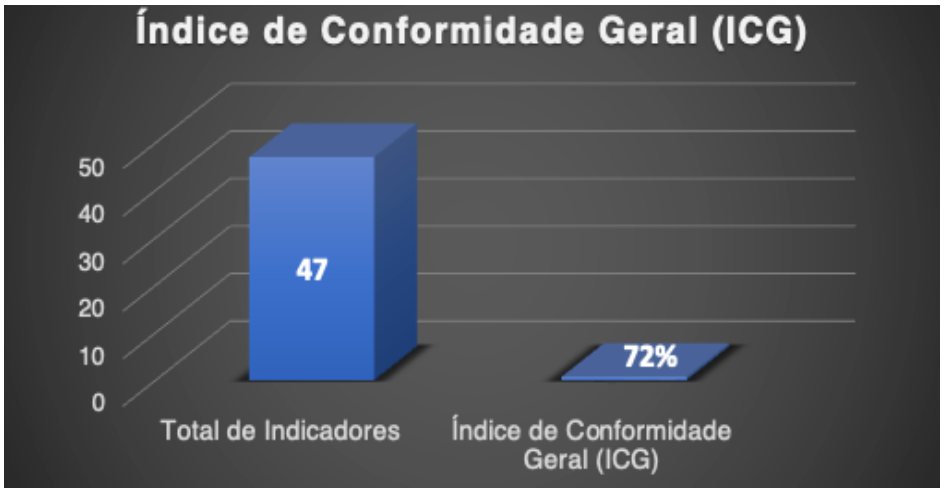

Figura 06 - Base de avaliação

7. Conclusão e Trabalhos Futuros

Este artigo buscou analisar de que forma é possível avaliar o nível de maturidade e os impactos das vulnerabilidades no ecossistema da IoT, bem como desenvolver um arcabouço para mensurar o nível de maturidade desse ecossistema de IoT. Para o desenvolvimento do artigo, foram identificados cinco objetivos específicos e, para alcançá-los, foi desenvolvida a pesquisa.

Observou-se que a maioria dos indicadores utilizados no ecossistema IoT não seguem um padrão e não são comparáveis ao longo do tempo e entre si. Neste sentido, não foram encontrados na literatura padrões que fornecem um conjunto de indicadores como uma recomendação do que medir e como deve ser medido, (ISO, 2022).

Buscou-se, neste artigo, desenvolver um modelo para mensuração dos níveis de maturidade para dispositivos IoT, ao qual possamos ter noção do nível de vulnerabilidade dos ecossistemas de IoT para as organizações. Assim, foi desenvolvido o S.M.M.I.O.T, um arcabouço que utiliza como inspiração os indicadores da ISO 27400, os níveis de maturidade propostos pelo CMMI e os processos de avaliação contínua do COBIT.

O S.M.M.I.O.T é composto de 5 etapas, dessa forma, deve-se realizar a seleção dos domínios, passando pela seleção dos controles e através das perguntas dos controles ao qual é o conjunto do teste de maturidade depois gera o índice de

conformidades por domínios em conjunto que ao final gera o indicie de conformidade geral ao qual é atribuída o nível final da situação de maturidade inspirado no CMMI e processos das informações inspirado no COBIT. Cada etapa será descrita a seguir. Conforme descrito, a primeira etapa de aplicação do S.M.M.I.O.T é a aplicação da Seleção dos Domínios, após a seleção do dispositivo IoT a ser analisado. Outro ponto a ser considerado é que o teste pode ser aplicado em sua completude ou apenas em alguns Domínios selecionados previamente como destaca a ISO (2017) salientando que as organizações que utilizam a norma como referência deverão informar pelo menos 50% dos controles desta norma (ISO, 2017). Aqui, o primeiro passo realizado foi a escolha de todos os Domínios, estabelecida pela norma ISO 27400.

Para a avaliação do modelo proposto e, assim, sua devida avaliação, o S.M.M.I.O.T foi aplicado na empresa XPTO, onde foram aplicadas todas as etapas do arcabouço. Os dados utilizados foram obtidos através de um estudo de caso na própria empresa XPTO. Ressalta-se que o S.M.M.I.O.T pode ser aplicado em seus 4 domínios e seus 47 controles, ao qual é recomendada a aplicação de sua totalidade.

Com a aplicação do S.M.M.I.O.T, foi possível verificar que a empresa XPTO está em um nível considerado como Quantitativamente Gerenciado, ao qual é a fase em que o foco é na medição do desempenho da segurança, implementação de controles avançados da organização. Neste nível o ecossistema da IoT está num estágio de recursos totalmente integrados e disponíveis na forma de serviços tanto para cidadãos como para aplicações. Nesta fase o uso de computação visa estar disponível em todo e qualquer lugar disponibilizado pela computação em nuvem, buscando atualizações necessárias para mitigar as vulnerabilidades dos dispositivos IoT.

Através deste artigo, é possível indicar que a avaliação da aplicabilidade do arcabouço S.M.M.I.O.T nas organizações e seus dispositivos contribui para: a) sumarização comparativa entre diferentes modelos e normas existentes, bem como ferramentas no contexto de segurança da informação. Por ser um modelo que tem a capacidade de analisar somente os 4 domínios em conjunto, o S.M.M.I.O.T é um modelo engessado e tem a capacidade de atender às necessidades identificadas de cada organização e/ou de outros ambientes que desejam saber se há em demasia vulnerabilidades em seus dispositivos IoT. Assim, com o S.M.M.I.O.T, é possível ter uma padronização de método de avaliação e mensuração. Dessa forma, com a avaliação do modelo de mensuração proposto, foi possível verificar que o modelo serve como uma ferramenta eficiente para aqueles que buscam transformar suas organizações,

dentre outras, em ambientes menos propensos a ataques hackers, bem como mitigando, de certa forma, as vulnerabilidades dos dispositivos IoT.

O S.M.M.I.O.T permite identificar em qual domínio a organização e seu sistema de ecossistema IoT precisam se desenvolver, possibilitando a aplicação de outras normas e ferramentas para auxiliar o S.M.M.I.O.T com maior efetividade. Entende-se que a contribuição supracitada é relevante para o estudo, pois os resultados apresentados neste artigo indicam informações peculiares de um ambiente específico que podem ser utilizadas como referências para os mais diversos contextos.

Para atenuar esta pesquisa, foram utilizados como referência trabalhos que investigaram as mais diversas vulnerabilidades e estudos de casos reais, mostrando os mais diversos tipos de vulnerabilidades e exploração nos mais variados dispositivos IoT.

O S.M.M.I.O.T deve ser aplicado para o maior número possível de ambientes e contextos de diversos portes e características diferentes para que possa ter uma maior robustez em sua validação.

Trabalhos futuros poderão ser produzidos para a inserção de novos módulos ao arcabouço S.M.M.I.O.T, como adequação de novas normas ISO/IEC e ferramentas de análises no que se trata de segurança da informação e suas vulnerabilidades em dispositivos IoT, os resultados da aplicação do modelo proposto neste artigo, tendo como estudo de caso a empresa XPTO, fazendo assim análise dos sistemas de CFTV e seus servidores para validação.

Para ser caracterizado como uma ferramenta de aprendizagem e de avaliação, o S.M.M.I.O.T pode ser aplicado para obter dados de novas pesquisas e relatórios de outros ambientes e contextos. Esta pesquisa permitiu avaliar o grau de maturidade das vulnerabilidades dentro de um âmbito organizacional e passível de outros contextos afins de mitigá-los, tanto quanto sua evolução ou involução em sua trajetória para ampliar o nível de segurança desses dispositivos, sempre em busca da melhoria contínua.

Incorporar os princípios da ISO/IEC 27400 em sua análise de maturidade não apenas fortalecerá a segurança da IoT, mas também garantirá que as práticas estejam alinhadas com padrões internacionais reconhecidos. A ênfase na capacitação, avaliação de riscos e inovação contínua ajudará a criar um ecossistema de IoT mais seguro e resiliente e desenvolvimento de uma aplicação web e um app para gerenciamento dos teste de maturidade do S.M.M.I.O.T.

8. Referêrncias

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Knuth 1984], [Boulic and Renault 1991]; or dates in parentheses, e.g. Knuth (1984), Smith and Jones (1999).

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

References

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002, Tecnologia da informação - Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2022.

ASIMILY. The Top Internet of Things (IoT) Cybersecurity Breaches in 2024. 2024. Disponível em: https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2024/. Acesso em: 04 maio 2025.

ATZORI, L., ET AL. (2010). "The Internet of Things: A survey." Computer Networks, 54(15), 2787-2805. Disponível em DOI: https://doi.org/10.1016/j.comnet.2010.05.010 Acesso em: 04 nov. 2024.

BALDECCHI, Rodrigo; DE CALIDAD, Gerente Corporativo. Implementación efectiva de un SGSI ISO 27001. Disponível em: https://www.academia.edu/26325423/Implementaci%C3%B3n_efectiva_de_un_SGSI_ISO_27001 Acesso em: 06 nov. 2024.

BALBO, Anderson Pinheiro; VENDRAMEL, Wilson; TOLEDO, Maria Beatriz Felgar de. Medição de Software no CMMI e MPS.BR. 2014. Devmedia. Disponível em: https://www.devmedia.com.br/medicao-de-software-no-cmmi-e-mps-br/30522. Acesso em: 01 out. 2024.

DAVIS, Chris. IoT Adoption: Security Risks and Mitigation Strategies for Businesses. 2024. Disponível em: https://www.ion247.com/insights/iot-adoption-security-risks-and-mitigation-strategies-for-businesses/. Acesso em: 03 maio 2025.

FRANKLIN, Tamara. IoT security is a top concern — and for good reason. 2024. Disponível em: https://www.liquidweb.com/blog/iot-security-is-a-top-concern-for-2024-and-for-good-reason/. Acesso em: 03 maio 2025.

FONSECA, J. J. S. Metodologia da pesquisa científica. Fortaleza: Universidade Estadual do Ceará, 2002. Apostila.

GUIMARÃES, José Geraldo de Araújo. Cidades inteligentes: proposta de um modelo brasileiro multi ranking de classificação. 2018. 278 f. Tese (Doutorado em Administração)- Universidade de São Paulo - USP, São Paulo, 2018. Disponível em: http://www.teses.usp.br/teses/disponiveis/12/12139/tde-05072018 120958/publico/CorrigidoJoseGeraldo.pdf. Acesso em: 21 jan. 2025.

GUBBI, J., ET AL. (2013). "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems, 29(7), 1645-1660. Disponível em DOI: http://dx.doi.org/10.1016/j.future.2013.01.010 Acesso em: 05 nov. 2024

GIL, A. C. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008

HE, H., ET AL. (2016). "Security and privacy in the internet of things: A survey." IEEE Access, 4, 6693-6700. Disponível em DOI: 10.1109/ICECCPCE46549.2019.203774 Acesso em: 02 nov. 2024.

HENKE, Christian. What Is IoT Security? Risks, Examples, and Solutions. 2023. Disponível em: https://www.emnify.com/blog/iot-security. Acesso em: 04 maio 2025.

HOSSAIN, M. M.; FOTOUHI, M.; HASAN, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: 2015 IEEE World Congress on Services. [S.l.: s.n.], 2015. p. 21–28. Disponível em DOI: https://doi.org/10.1109/SERVICES.2015.12. Acesso em: 16 nov. 2024.

HUSAR, Alex. IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities. 2022. Disponível em: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities. Acesso em: 04 maio 2025.

_____. ISO 37122. Sustainable development in communities — Indicators for Smart Cities. 2017. International Organization for Standardization. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:37122:dis:ed-1:v1:en. Acesso em: 27 maio. 2025.

ISACA. IT Governance Institute, COBIT 5. Disponível em: http://www.isaca.org Acesso em: 27 out. 2024.

ISO (THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION). ISO/IEC 27400:2022(E): INTERNATIONAL STANDARD ISO/IEC 2740 - Cybersecurity — IoT security and privacy — Guidelines Cybersécurité — Sécurité et protection de la vie privée pour l'IoT — Lignes directrices. 1 ed. Switzerland, 2022. 50 p.

KATZ, Eyal. Top 5 Most Commonly Used IoT Protocols and Their Security Issues. 2024. Disponível em: https://spectralops.io/blog/top-5-most-commonly-used-iot-protocols-and-their-security-issues/. Acesso em: 03 maio 2025.

LAZURCA, Florin. Top 10 Vulnerabilities that Make IoT Devices Insecure. 2024. Disponível em: https://www.cyberark.com/resources/blog/top-10-vulnerabilities-that-make-iot-devices-insecure. Acesso em: 03 maio 2025.

MAHMOUD, R. et al. Internet of things (iot) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). [S.l.: s.n.], 2015. p. 336–341. Disponível em DOI: 10.1109/ICITST.2015.7412116. Acesso em: 20 nov. 2024.

MOSENIA, A.; JHA, N. K. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, v. 5, n. 4, p. 586–602, 2017. Disponível em DOI: 10.1109/TETC.2016.2606384. Acesso em: 20 nov. 2024.

OLAES, Terry. Top IT, OT, and IoT Security Challenges and Best Practices. 2025. Disponível em: https://www.balbix.com/insights/addressing-iot-security-challenges/. Acesso em: 03 maio 2025.

POURRAHMANI, Hossein et al. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. Internet of Things, v. 23,

p. 100888, 2023. Available at: Disponível em https://www.sciencedirect.com/science/article/pii/S2542660523002111. Acesso em: 02 dez. 2024.

PATEL, Neil. The Smartest Smart Home Attacks of All Time and the Not-So Smart Devices that Made Them Possible. 2021. Disponível em: https://www.dlink.com/fr/fr/resource-centre/blog/the-smartest-smart-home-attacks-of-all-time. Acesso em: 04 maio 2025.

PORTNOX. Examining IoT Security Issues. 2025. Disponível em: https://www.portnox.com/cybersecurity-101/iot-security-issues/. Acesso em: 03 maio 2025.

ROSSI, Bruno. What Are IoT Vulnerabilities? 2024. Disponível em: https://sternumiot.com/iot-blog/top-10-iot-vulnerabilities-and-how-to-mitigate-them/. Acesso em: 02 maio 2025.SENTINELONE. Top 10 IoT Security Risks and How to Mitigate Them. 2025. Disponível em: https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/. Acesso em: 02 maio 2025.

SAAE. Top 10 Best Practices for Enhancing IoT Security in Manufacturing. 2024. Disponível em: https://www.sustainablemanufacturingexpo.com/en/articles/best-practices-iot-security.html. Acesso em: 01 maio 2025.

SANTANA, Eber da Silva de; NUNES, Éldman de Oliveira; SANTOS, Leandro Brito. The use of ISO 37122 as standard for assessing the maturity level of a smart city. International Journal Of Advanced Engineering Research And Science, v. 5, n. 12, p.309-315, 2018. AI Publications. http://dx.doi.org/10.22161/ijaers.5.12.42.

SANTANA, Eber da Silva de; NUNES, Éldman de Oliveira; PASSOS, Diego Costa; SANTOS, Leandro Brito. SMM: A Maturity Model of Smart Cities Based on Sustainability Indicators of the ISO 37122. International Journal of Advanced Engineering Research and Science, v. 6, n. 2, p.013-020, 2019. AI Publications. http://dx.doi:10.22161/ijaers.6.2.2.

SEI - SOFTWARE ENGINEERING INSTITUTE. CMMI® para Desenvolvimento – Versão 1.2". Carnegie Mellon University, 2006. Disponível em: http://www.spinsp.org.br/CMMI/CMMIDEV.pdf . Acesso em: 12 jan. 2025.

SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: The road ahead. Computer networks, v. 76, p. 146-164, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971. Acesso em: 12 jan. 2025.

SOUSA, William Teixeira Silva de. Estudo da implantação do modelo de qualidade cmmi nas organizações. 2006. 112 f. Monografia (Especialização em Engenharia da Computação, Engenharia Eletrônica e de Computação)- Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: http://monografias.poli.ufrj.br/monografias/monopoli10002986.pdf. Acesso em: 10 jan. 2025.

SRIVASTAVA, A. et al. Future iot-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems, v. 33, n. 12, p. e4443, 2020. E4443 IJCS-19-0930.R3. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4443. Disponível em DOI https://doi.org/10.1002/dac.4443. Acesso em: 04 dez. 2024.

SRINIVAS, Rudra. 10 IoT Security Incidents That Make You Feel Less Secure. 2020. Disponível em: https://cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/. Acesso em: 04 maio 2025.

THOMAS, Jimara. ANALYSIS OF VULNERABILITIES IN IOT DEVICES AND THE SOLUTIONS. 2021. 60 f. Monografia (Especialização) - Curso de Computer Science, B.S Computer Science, Texas Southern University, Texas, 2021. Disponível em: https://digitalscholarship.tsu.edu/cgi/viewcontent.cgi?article=1021&context=frj. Acesso em: 03 maio 2025.

TRUDEL, Sylvie et al. PEM: The small company-dedicated software process quality evaluation method combining CMMISM and ISO/IEC 14598. Software Quality Journal, [s.l.], v. 14, n. 1, p.7-23, mar. 2006. Springer Nature. http://dx.doi.org/10.1007/s11219-006-5997-8.04 nov. 2024.

WATTLECORP. OWASP IoT Top 10 Vulnerabilities. 2024. Disponível em: https://www.wattlecorp.com/owasp-iot-top-10/. Acesso em: 03 maio 2025.

WAZLAWICK, R. Metodologia de Pesquisa para Ciência da Computação. [S.l.]: Elsevier Brasil, 2017. v. 2.

WEBER, R. H., ET AL. (2010). "The internet of things: Legal perspectives." Springer Science & Business Media. Disponível em DOI: 10.1007/978-3-642-11710-7 Acesso em: SICARI, S., ET AL. (2015). "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks, 76, 146-164. Disponível em: https://doi.org/10.1016/j.comnet.2014.11.008. Acesso em: 01 nov. 2024.

ZHAO, K., ET AL. (2018). "A survey of IoT security: Threats, challenges and solutions." Computer Networks, 151, 124-142. Disponível em DOI: 10.1109/ROEDUNET.2018.8514146. Acesso em: 02 nov. 2024.

APÊNDICE A

Controle – 01: Política de segurança da IoT
Descrição: Deve ser definida uma política de segurança da IoT, aprovada pela direção, publicada, comunicada ao pessoal relevante e às partes externas relevantes e revista a intervalos planeados ou se ocorrerem alterações significativas.
Objetivo: Fornecer direção de gestão e apoio à segurança da Internet das coisas no âmbito do criador de serviços Internet das coisas ou do prestador de serviços Internet das coisas, em conformidade com os requisitos comerciais e as expectativas das partes interessadas.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 02: Organização da segurança da IoT
Descrição: As funções e responsabilidades pela segurança da IoT devem ser definidas e atribuídas.
Objetivo: Estabelecer e manter um quadro de gestão para iniciar e controlar a implementação e o funcionamento da segurança da IoT no âmbito do fornecedor de serviços IoT ou do criador de serviços IoT.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 03: Gestão de ativos
Descrição: Devem ser identificadas as informações, os dispositivos e sistemas IoT e as suas funções e operações a proteger.
Objetivo: Identificar os ativos dos dispositivos e sistemas IoT para conceber medidas de proteção adequadas.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 04: Equipamentos e ativos localizados fora das áreas físicas protegidas

Descrição: Devem ser aplicadas medidas de segurança específicas aos equipamentos e bens da Internet das coisas que estão localizados ou funcionam fora das zonas físicas protegidas.
Objetivo: Para evitar perdas, danos, roubo ou comprometimento de dispositivos IoT e a interrupção do funcionamento da IoT serviços.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 05: Eliminação ou reutilização segura do equipamento
Descrição: Todos os equipamentos que contenham suportes de armazenamento devem ser verificados para garantir que quaisquer dados sensíveis e software licenciado foram removidos ou substituídos de forma segura antes de serem eliminados ou reutilizados.
Objetivo: Impedir a fuga de informações e a utilização maliciosa do dispositivo IoT e de outros equipamentos do sistema IoT aquando da sua eliminação ou reutilização.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 06: Aprender com os incidentes de segurança
Descrição: Os conhecimentos adquiridos com a análise e a resolução de incidentes de segurança da IoT devem ser utilizados para reduzir a probabilidade ou o impacto de futuros incidentes.
Objetivo: Reduzir os efeitos negativos dos incidentes na prestação e utilização de serviços IoT.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 07: Princípios de engenharia de sistemas IoT seguros
Descrição: Os princípios para a engenharia de sistemas IoT seguros que abordam a conceção e a implementação de funções de segurança, a defesa em profundidade e o endurecimento de sistemas e software devem ser aplicados ao desenvolvimento de sistemas IoT.

Objetivo: Garantir que a segurança seja concebida e implementada no desenvolvimento de sistemas IoT.
Público-alvo: Programador de serviços IoT
Domínio IoT: Aplicação e Serviço

Controle – 08: Ambiente e procedimentos de desenvolvimento seguros
Descrição: O ambiente e os procedimentos de desenvolvimento seguro devem ser aplicados ao desenvolvimento de sistemas IoT.
Objetivo: Evitar a introdução de insegurança nos sistemas IoT durante o desenvolvimento.
Público-alvo: Programador de serviços IoT
Domínio IoT: Operações e gestão

Controle – 09: Segurança dos sistemas IoT em prol da segurança
Descrição: Os princípios de segurança que apoiam a segurança devem ser aplicados ao desenvolvimento de sistemas IoT
Objetivo: Apoiar a segurança nos sistemas IoT
Público-alvo: Programador de serviços IoT
Domínio IoT: Operações e gestão

Controle – 10: Segurança na ligação de dispositivos IoT variados
Descrição: Um sistema IoT deve ser concebido e implementado para garantir e manter a segurança na ligação de vários dispositivos IoT.
Objetivo: Para manter a segurança do sistema IoT ao ligar dispositivos IoT variados, incluindo os que não são necessariamente verificados pelo criador do serviço IoT ou pelo fornecedor do serviço IoT.
Público-alvo: Programador de serviços IoT
Domínio IoT: Operações e gestão

Controle – 11: Verificação da conceção dos dispositivos e sistemas IoT
Descrição: A conceção e a implementação de dispositivos e sistemas IoT devem

ser verificadas.
Objetivo: Garantir a segurança e a proteção do dispositivo IoT e do sistema IoT
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 12: Monitorização e registo
Descrição: Os estados, eventos e tráfego de rede dos dispositivos e sistemas IoT devem ser monitorizados e registados.
Objetivo: Detectar e rastrear anomalias e incidentes de dispositivos e sistemas IoT.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 13: Proteção dos registos
Descrição: Os registos dos dispositivos e sistemas IoT devem ser protegidos contra fugas, destruição e alterações não intencionais.
Objetivo: Para garantir a capacidade e a confiabilidade dos dados.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 14: Utilização de redes adequadas para os sistemas IoT
Descrição: As tecnologias de rede e de comunicação aplicadas à IoT e aos sistemas devem satisfazer as necessidades de função, capacidade e segurança de comunicação, bem como de função e desempenho dos dispositivos IoT.
Objetivo: Utilizar a rede que satisfaz as necessidades de segurança, desempenho e outras do sistema IoT.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 15: Definições e configurações seguras no fornecimento de dispositivos e serviços IoT.

Descrição: Os dispositivos e serviços IoT devem ser fornecidos com definições e configurações seguras
Objetivo: Garantir a segurança dos dispositivos e serviços IoT na entrega
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 16: Autenticação de utilizadores e dispositivos.
Descrição: Deve ser implementada e aplicada a função de autenticação dos utilizadores e dos dispositivos IoT para acederem aos sistemas e serviços IoT.
Objetivo: Para proteger as informações, os dispositivos IoT, os sistemas e os serviços contra o acesso não autorizado e outras violações de segurança.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 17: Fornecimento de actualizações de software e firmware.
Descrição: Deve ser concebido, implementado e operado um mecanismo para atualizar o software e o firmware dos dispositivos e sistemas IoT.
Objetivo: Para garantir a segurança da atualização do software e do firmware do dispositivo IoT e do sistema IoT.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 18: Compartilhar informações sobre vulnerabilidades.
Descrição: As vulnerabilidades dos dispositivos, sistemas e serviços IoT devem ser monitorizadas e informadas aos utilizadores da IoT e às partes interessadas, juntamente com os riscos associados.
Objetivo: Garantir que as partes interessadas relevantes sejam informadas das vulnerabilidades dos dispositivos, sistemas e serviços da IoT e estejam conscientes dos riscos daí decorrentes.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 19: Medidas de segurança adaptadas ao ciclo de vida dos sistemas e serviços IoT.
Descrição: As medidas de segurança do sistema e do serviço IoT devem ser adaptadas e mantidas durante as fases do ciclo de vida, incluindo o seu desenvolvimento, funcionamento, manutenção e destruição.
Objetivo: Manter a segurança do sistema e do serviço IoT durante todo o seu ciclo de vida.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 20: Orientações para os utilizadores da Internet das Coisas sobre a utilização adequada dos dispositivos e serviços da Internet das Coisas
Descrição: Os utilizadores da IoT devem receber orientações sobre a utilização adequada dos dispositivos IoT, com os riscos e os efeitos indesejáveis do sistema e do serviço IoT que podem resultar de uma utilização inadequada dos dispositivos IoT.
Objetivo: Sensibilizar os utilizadores da IoT para os riscos de segurança na utilização de dispositivos IoT e garantir a aplicação de medidas de segurança.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 21: Determinação das funções de segurança das partes interessadas
Descrição: As funções do criador do serviço IoT, do fornecedor do serviço IoT e de outras partes interessadas na segurança do sistema e do serviço IoT devem ser determinadas e acordadas entre as partes interessadas.
Objetivo: Garantir a segurança do sistema e serviço IoT que envolve entidades que participam no fornecimento e utilização do sistema e serviço IoT.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 22: Gestão de dispositivos vulneráveis
Descrição: Os dispositivos IoT vulneráveis devem ser detectados, registados e devem ser fornecidos alertas aos utilizadores e administradores de IoT destes

dispositivos.
Objetivo: Para manter a segurança dos dispositivos IoT.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 23: Gestão das relações com os fornecedores no domínio da segurança da IoT
Descrição: As especificações e as obrigações de apoio dos fornecedores em matéria de segurança da informação do dispositivo IoT e do serviço IoT devem ser geridas pela organização adquirente com base nos contratos com os fornecedores.
Objetivo: Para garantir o fornecimento contínuo de dispositivos e serviços IoT seguros.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 24: Divulgação segura de informações sobre a segurança dos dispositivos IoT
Descrição: As informações sobre o dispositivo IoT relevantes para a segurança dos serviços IoT devem ser documentadas e divulgadas apenas às partes que as solicitem.
Objetivo: Para garantir a segurança dos serviços IoT que utilizam o dispositivo IoT.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Detecção e controle.

Controle – 25: Contatos e serviço de apoio
Descrição: Os utilizadores de IoT só devem escolher dispositivos e serviços IoT que forneçam informações de contacto para apoio serviço.
Objetivo: Garantir a segurança na utilização de dispositivos e serviços IoT.
Público-alvo: Utilizador da IoT
Domínio IoT: Utilizador

Controle – 26: Definições iniciais do dispositivo e serviço IoT
Descrição: As definições iniciais do dispositivo IoT e do serviço devem ser aplicadas corretamente.
Objetivo: Para garantir definições iniciais seguras dos dispositivos e serviços IoT.
Público-alvo: Utilizador da IoT
Domínio IoT: Utilizador

Controle – 27: Desativação de dispositivos não utilizados
Descrição: Os dispositivos IoT devem ser desativados e as credenciais revogadas quando deixarem de ser utilizados.
Objetivo: Para reduzir os riscos de segurança causados pelo dispositivo IoT que já não é utilizado.
Público-alvo: Utilizador da IoT
Domínio IoT: Utilizador

Controle – 28: Eliminação ou reutilização segura do dispositivo IoT
Descrição: Os dados e o software licenciado armazenados no dispositivo IoT devem ser removidos ou substituídos de forma segura antes de serem eliminados ou reutilizados.
Objetivo: Garantir a proteção das informações aquando da eliminação ou reutilização de dispositivos IoT.
Público-alvo: Utilizador da IoT
Domínio IoT: Utilizador

Controle – 29: Prevenção de eventos invasivos da privacidade
Descrição: Os dispositivos e serviços IoT devem incorporar capacidades de reforço da privacidade.
Objetivo: Prevenir eventos invasivos da privacidade no fornecimento e utilização de dispositivos e serviços IoT.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT

Domínio IoT: Operações e gestão

Controle – 30: Privacidade da IoT por defeito
Descrição: As partes interessadas num sistema IoT devem garantir que, sem qualquer interação ou intervenção do utilizador IoT, as definições de privacidade mais rigorosas se apliquem por defeito.
Objetivo: Para proteger as informações pessoais sem necessidade de interação ou intervenção do utilizador
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 31: Fornecimento de aviso de privacidade 01
Descrição: O utilizador da IoT deve receber um aviso de privacidade que indique os dados pessoais recolhidos pelo dispositivo IoT e pelo serviço IoT e a finalidade da sua utilização.
Objetivo: Para garantir a utilização dos dados pessoais.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 32: Fornecimento de aviso de privacidade 02
Descrição: O consentimento do utilizador da IoT para o aviso de privacidade deve ser obtido antes de recolher os dados pessoais ou de alterar a finalidade da utilização.
Objetivo: Para garantir a recolha e utilização consentida de dados pessoais.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 33: Verificação da funcionalidade IoT
Descrição: Deve ser fornecida uma verificação independente do dispositivo IoT, dos componentes de dados e dos componentes do serviço IoT para dar visibilidade e garantia a todas as partes interessadas de que o dispositivo ou serviço IoT está a funcionar de acordo com os objetivos declarados.

Objetivo: Para garantir funcionalidades WYSIWYG (What You Sees Is What You Get - O que você vê é o que você obtém) para dispositivos e serviços IoT.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 34: Consideração dos utilizadores da IoT
Descrição: Os requisitos e preocupações dos utilizadores finais em matéria de privacidade devem ser tidos em conta na conceção do dispositivo IoT e serviço.
Objetivo: Assegurar que os requisitos e as preocupações dos utilizadores da Internet das Coisas (IoT) em matéria de privacidade sejam tidos em conta no dispositivo e no serviço IoT e reforçar a confiança dos utilizadores da IoT.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 35: Gestão dos controles de privacidade da IoT
Descrição: A eficácia dos controles de privacidade no dispositivo e serviço IoT deve ser revista e devem ser identificados continuamente novos riscos de privacidade, tendo em conta a evolução das necessidades de privacidade dos utilizadores finais e os requisitos regulamentares.
Objetivo: Justificar a eficácia dos controles da privacidade nos dispositivos e serviços IoT.
Público-alvo: Fornecedor de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 36: Identidade única do dispositivo 01
Descrição: Os criadores de sistemas IoT (especialmente os criadores de dispositivos) devem utilizar um método que identifique exclusivamente cada dispositivo IoT para melhorar a privacidade na identificação de dispositivos IoT suspeitos de serem relevantes para um incidente cibernético.
Objetivo: Permitir a identificação do dispositivo IoT suspeito de ser relevante para um incidente cibernético.
Público-alvo: Programador de serviços IoT.

Domínio IoT: Operações e gestão

Controle – 37: Identidade única do dispositivo 02
Descrição: Os prestadores de serviços IoT devem utilizar, se necessário, um método que permita um mapeamento único entre um determinado dispositivo IoT e um utilizador IoT para melhorar a privacidade na identificação do mapeamento entre o dispositivo IoT e o(s) utilizador(es) IoT.
Objetivo: Identificar de forma única um mapeamento entre o dispositivo IoT e o(s) utilizador(es) IoT
Público-alvo: Fornecedor de serviços IoT.
Domínio IoT: Operações e gestão

Controle – 38: Autenticação à prova de falhas
Descrição: O sistema deve garantir que a autenticação implementada não possa ser contornada, adulterada ou falsificada por qualquer método razoável.
Objetivo: Uma vez que o dispositivo (coisa) muitas vezes não está com o utilizador, e as consequências de um utilizador errado que se ligue ao dispositivo podem causar sérios danos em termos de segurança, perdas financeiras, riscos para a saúde, etc. No caso do serviço de autenticação tradicional, o resultado do acesso é evidente para o utilizador, uma vez que este pode testemunhar as consequências da sua ação.
Público-alvo: Programador de serviços IoT ou fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 39: Minimização da recolha indireta de dados
Descrição: A recolha de dados de fontes indiretas deve ser minimizada ou não deve ser recolhida de todo.
Objetivo: Para impedir a recolha de dados sem a participação e o consentimento dos utilizadores da IoT.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 40: Comunicação das preferências de privacidade
Descrição: As preferências do utilizador em relação aos controles de privacidade só devem ser adicionadas, modificadas ou eliminadas quando o utilizador autorizado estiver autenticado no sistema.
Objetivo: Ao contrário dos cenários convencionais, em que as preferências de privacidade são conhecidas pela organização que recolhe as IPI, no caso da IdC o mesmo não é possível, uma vez que existem vários dispositivos e serviços que necessitam de aceder aos dados.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 41: Verificação da decisão automatizada
Descrição: A decisão automatizada fornecida pelos serviços IoT deve ser verificada.
Objetivo: Para evitar danos irreversíveis causados por decisões automáticas erróneas tomadas por um dispositivo ou sistema IoT.
Público-alvo: Fornecedor de serviços IoT
Domínio IoT: Operações e gestão

Controle – 42: Responsabilização das partes interessadas
Descrição: Deve ser estabelecida a responsabilidade dos vários intervenientes.
Objetivo: Definir responsabilidades entre as partes interessadas do sistema IoT. Em caso de violação de dados ou de pedidos dos titulares dos dados, que entidade responderá, quem atenderá aos pedidos de divulgação de dados.
Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT
Domínio IoT: Operações e gestão

Controle – 43: Desvinculação das informações pessoais
Descrição: O sistema IoT deve garantir que as informações pessoais do utilizador proprietário de um dispositivo não possam ser identificadas.
Objetivo: Impedir a recolha de informações pessoais através da monitorização de um dispositivo IoT.

Público-alvo: Fornecedor de serviços IoT ou programador de serviços IoT
Domínio IoT: Operações e gestão

Controle – 44: Partilha de informações sobre as medidas de proteção dos dispositivos IoT
Descrição: As medidas de proteção relacionadas com o risco para a privacidade nos dispositivos IoT devem ser geridas de forma adequada e apenas divulgadas às partes que delas necessitem.
Objetivo: Para garantir a proteção das informações pessoais dos serviços IoT que utilizam o dispositivo IoT
Público-alvo: Programador de dispositivos IoT.
Domínio IoT: Detecção e controle.

Controle – 45: Consentimento do utilizador
Descrição: O consentimento para a utilização de dados pessoais para o dispositivo e serviço IoT só deve ser dado depois de se ter considerado a necessidade e o seu provável impacto em caso de violação de dados. O consentimento deve ser retirado se o resultado da IoT já não for necessário ou se houver algum problema com o dispositivo ou serviço IoT
Objetivo: Impedir a utilização de informações pessoais pelo dispositivo e serviço IoT sem o consentimento do utilizador
Público-alvo: Utilizador de IoT
Domínio IoT: Utilizador

Controle – 46: Utilização propositada para ligação a outros dispositivos e serviços
Descrição: A ligação de um dispositivo e serviço IoT a outros dispositivos ou serviços só deve ser permitida se houver uma necessidade válida.
Objetivo: Assegurar uma utilização correta dos dispositivos e serviços IoT
Público-alvo: Utilizador de IoT
Domínio IoT: Utilizador

Controle – 47: Certificação e validação da proteção das informações pessoais
Descrição: Certificação ou validação das características de proteção da privacidade no que respeita ao dispositivo e serviço IoT deve ser procurado.
Objetivo: Para garantir que as funcionalidades de proteção da privacidade do dispositivo e do serviço IoT são fiáveis.
Público-alvo: Utilizador de IoT
Domínio IoT: Utilizador