PONTIFICIA UNIVERSIDADE CATOLICA DE GOIAS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

STRIDE-IOT: CATÁLOGO DE PADRÕES DE REQUISITOS DE SEGURANÇA PARA SISTEMAS IOT

HIGOR CAVALCANTE DOS ANJOS

GOIÂNIA
2025

HIGOR CAVALCANTE DOS ANJOS

STRIDE-IOT: CATÁLOGO DE PADRÕES DE REQUISITOS DE SEGURANÇA PARA SISTEMAS IOT

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador(a): Prof. Dr. Ernesto Fonseca Veiga

Banca examinadora:

Prof.ª Dra. Solange da Silva

Prof.ª Ma. Mariana Crisóstomo Martins

GOIÂNIA

2025

HIGOR CAVALCANTE DOS ANJOS

STRIDE-IOT: CATÁLOGO DE PADRÕES DE REQUISITOS DE SEGURANÇA PARA SISTEMAS IOT

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em _____/_____/_____.

_____
Orientador (a): Prof. Dr. Ernesto Fonseca Veiga

_____
Prof.ª Dra. Solange da Silva

_____
Prof.ª Ma. Mariana Crisóstomo Martins

GOIÂNIA
2025

RESUMO

A Internet das Coisas (IoT) tem se expandido rapidamente em ambientes domésticos, industriais e urbanos, aumentando as preocupações relacionadas à segurança, privacidade e confiabilidade operacional. Devido à heterogeneidade, às limitações de hardware e à natureza distribuída dos dispositivos IoT, estabelecer requisitos de segurança consistentes e reutilizáveis ainda representa um desafio. Embora existam estudos que descrevem vulnerabilidades e boas práticas, poucos transformam esse conhecimento em padrões estruturados de requisitos capazes de apoiar a engenharia de requisitos.

Este trabalho propõe o STRIDE-IoT, um catálogo de padrões de requisitos de segurança para sistemas IoT, organizado segundo o modelo de ameaças STRIDE e estruturado com base na metodologia de Requirement Patterns de Withall. O catálogo foi construído a partir de um mapeamento sistemático da literatura e da análise e conversão de vulnerabilidades IoT — especialmente as documentadas por Pessoa (2025) — em padrões de requisitos funcionais e não funcionais (FRPs e NFRPs).

O catálogo resultante oferece uma estrutura multinível composta por *Requirement Pattern Groups* (RPGs), *Functional Requirement Patterns* (FRPs), *Non-Functional Requirement Patterns* (NFRPs) e infraestruturas de suporte, permitindo rastreabilidade entre ameaças, requisitos e tecnologias IoT.

O STRIDE-IoT contribui com uma abordagem sistemática, reutilizável e navegável para a engenharia de sistemas IoT, fortalecendo a especificação de requisitos e a integração entre modelagem de ameaças e práticas de segurança.

Palavras-chave: Internet das Coisas. Segurança em IoT. Engenharia de Requisitos. Padrões de Requisitos de Segurança. Modelo STRIDE.

ABSTRACT

The Internet of Things (IoT) has rapidly expanded across domestic, industrial, and urban environments, raising concerns regarding security, privacy, and operational reliability. Due to the heterogeneity, hardware limitations, and distributed nature of IoT devices, establishing consistent and reusable security requirements remains a significant challenge. Although the literature documents vulnerabilities and best practices, few efforts translate this knowledge into structured requirement patterns that effectively support requirements engineering.

This work proposes STRIDE-IoT, a catalog of security requirement patterns for IoT systems, organized according to the STRIDE threat model and structured using Withall's Requirement Patterns methodology. The catalog was developed based on a systematic mapping of the literature and on the analysis and conversion of IoT vulnerabilities—especially those documented by Pessoa (2025)—into functional and non-functional requirement patterns (FRPs and NFRPs).

The resulting catalog offers a multilayered structure composed of Requirement Pattern Groups (RPGs), Functional Requirement Patterns (FRPs), Non-Functional Requirement Patterns (NFRPs), and supporting infrastructures, enabling traceability between threats, requirements, and IoT technologies.

The STRIDE-IoT provides a systematic, reusable, and navigable approach to IoT systems engineering, strengthening requirements specification and the integration between threat modeling and security practices.

Keywords: Internet of Things. IoT Security. Requirements Engineering. Security Requirement Patterns. STRIDE Threat Model.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

IoT – Internet das Coisas

ER – Engenharia de Requisitos

STRIDE-IoT – Catálogo De Padrões De Requisitos De Segurança IoT

RPG – *Requirement Pattern Groups*

RP – *Requirement Patterns*

FRP – *Functional Requirement Patterns*

NFRP – *Non-Funcional Requirement Patterns*

CIA – *Confidentiality, Integrity and Availability*

STRIDE – *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege*

UML – *Unified Modeling Language*

1 INTRODUÇÃO

Este capítulo apresenta o contexto e a motivação do estudo, define o problema e os objetivos da pesquisa, descreve a metodologia empregada e organiza a estrutura do trabalho, introduzindo os principais desafios de segurança em IoT e a necessidade de um catálogo de requisitos sistematizado.

1.1 Contexto e Motivação

A Internet das Coisas (IoT) está se consolidando como uma tecnologia essencial em domínios domésticos, industriais, urbanos e organizacionais, trazendo consigo novos desafios para a segurança da informação (Sebestyen; Popescu; Zmaranda, 2025). Em contraste com sistemas tradicionais, o ecossistema IoT é composto por dispositivos heterogêneos, restritos em processamento, distribuídos geograficamente e frequentemente expostos a ambientes suscetíveis a ataques (Abdulhamid et al., 2023). Nesse cenário, requisitos de segurança tornam-se não apenas desejáveis, mas indispensáveis para assegurar privacidade, confiabilidade e operação contínua (Abdulhamid et al., 2023).

A Engenharia de Requisitos é uma disciplina fundamental para tratar essas questões, pois estabelece as bases que orientaram o desenvolvimento seguro das soluções IoT (Kudo, 2021). Entretanto, diversos estudos mostram que a definição adequada de requisitos de segurança nesse contexto é complexa e pouco sistematizada (Aguilar-Calderón et al., 2022). Por isso, catálogos de requisitos — quando bem estruturados — podem atuar como instrumentos importantes para orientar engenheiros e especialistas durante a elicitação de requisitos (Barcelos, 2016).

A literatura aponta limitações nos catálogos existentes: muitos catálogos de padrões de segurança não são abrangentes, carecem de atualização e raramente apresentam o processo utilizado em sua construção, o que inviabiliza sua evolução ou verificação de completude (Cordeiro; Vasconcelos; Correia, 2022).

De forma semelhante, (Papoutsakis et al., 2021) apontam que grande parte dos catálogos de segurança não possui critérios consistentes de classificação ou organização interna, o que dificulta a navegabilidade e compromete sua usabilidade para a Engenharia de Requisitos. Quanto à sua estrutura, (Shostack, 2014) observa

que bibliotecas e coleções de ameaças frequentemente apresentam inconsistências, alternando entre entradas com pouca informação e outras excessivamente específicas. Essa falta de uniformidade pode comprometer a coerência interna e dificultar que os usuários encontrem ou consultem, de forma sistemática, aspectos específicos dessas coleções.

1.2 Problema e Questão de Pesquisa

Estudos sobre Engenharia de Requisitos (ER) para sistemas IoT, mostram que essa área apresenta desafios particulares, como a identificação de necessidades das partes interessadas (Da Silva, 2021) e a compreensão precisa das características e comportamentos dos sistemas (Motta; De Oliveira; Travassos, 2020). Esses desafios reforçam a necessidade de ferramentas que apoiem a definição e organização de requisitos voltados à segurança.

Quando organizações precisam desenvolver seus próprios conjuntos de requisitos de segurança para projetos IoT, isso pode aumentar esforço, custo e variabilidade entre iniciativas (Cordeiro; Vasconcelos; Correia, 2022). Catálogos estruturados tornam-se recursos valiosos porque promovem consistência na definição de requisitos e soluções, ao padronizar descrições e reduzir ambiguidades, além de facilitar a comunicação entre diferentes perfis técnicos por meio de uma linguagem comum que apoia a elicitação e reduz lacunas de conhecimento. Eles também aceleram o desenvolvimento ao oferecer pontos de partida reutilizáveis e navegáveis, garantindo produtividade e evitando a reinvenção de soluções já consolidadas. Ao mesmo tempo, contribuem para a qualidade e completude das especificações, disseminando boas práticas, apoiando decisões de mitigação e assegurando rastreabilidade e conformidade com normas e processos de verificação (Barcelos, 2016; Cordeiro; Vasconcelos; Correia, 2022).

Apesar da existência de estudos sobre vulnerabilidades, boas práticas e frameworks, grande parte desse conhecimento ainda não está organizada diretamente na forma de requisitos práticos e reutilizáveis. A segurança e privacidade permanecem temas complexos, compostos por diversas facetas técnicas e organizacionais. Padrões de requisitos, enquanto soluções reutilizáveis

documentadas, oferecem um meio eficaz de capturar conhecimento especializado e torná-lo aplicável no processo de desenvolvimento.

Assim, a principal questão de pesquisa desta proposta de estudo é:

“Como desenvolver um catálogo de padrões de requisitos de segurança para sistemas IoT que relacione ameaças, requisitos e tecnologias?”

Para responder esta questão de pesquisa, a proposta deste trabalho consiste no desenvolvimento de um catálogo. Para isso este trabalho propõe uma abordagem sistemática para organizar o conhecimento de segurança em IoT, reduzindo a distância entre a análise, a especificação e a definição de requisitos de segurança. A análise, quando conduzida desde as fases iniciais do projeto, permite identificar riscos e cenários de mau funcionamento; já a especificação transforma essas descobertas em requisitos claros, completos e verificáveis, garantindo que as medidas de proteção sejam efetivamente incorporadas ao sistema.

1.3 Objetivo

O objetivo geral deste trabalho é desenvolver um catálogo de padrões de requisitos de segurança para IoT, baseado no modelo de ameaças STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege*), criado pela *Microsoft*.

Como objetivos específicos, destacam-se:

- Estruturar o catálogo de segurança em IoT utilizando a hierarquia de padrões de requisitos proposta por Withall (2007), garantindo consistência e padronização interna.
- Mapear vulnerabilidades de segurança relevantes ao contexto IoT e convertê-las em requisitos padronizados.
- Organizar os requisitos resultantes de forma navegável segundo o modelo de ameaças STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege*).

- Integrar aspectos tecnológicos e infraestruturais à definição dos requisitos, assegurando rastreabilidade entre ameaça, requisito e tecnologia.

1.4 Metodologia

Este trabalho iniciou-se com a elaboração de um protocolo de mapeamento, um método sistemático e reprodutível que visa fornecer uma visão geral do campo de pesquisa. O protocolo de pesquisa envolve a definição de questões, estratégias de busca e critérios de inclusão e exclusão. As referências foram organizadas na ferramenta Zotero, permitindo filtrar publicações relevantes a partir de bases como IEEE Xplore, Scopus e Google Scholar, que são bases de dados comumente adotadas em estudos de Engenharia de *Software*.

Com base nas leituras analisadas, observou-se que muitos catálogos existentes apresentam desafios relacionados à navegação e à organização de seu conteúdo. Isso pode dificultar o uso eficiente dos catálogos e comprometer a clareza necessária para apoiar engenheiros de requisitos ou especialistas em segurança, o que torna os catálogos existentes difíceis de navegar ou com descrições de baixa qualidade (Cordeiro; Vasconcelos; Correia, 2022). O uso do STRIDE se assemelha mais a uma técnica de elicitação, com a expectativa de que o usuário ou sua equipe compreendam a estrutura e saibam como usá-la (Shostack, 2014). Dessa observação surgiu a decisão de utilizar o modelo STRIDE como guia de organização do catálogo — para estruturar os requisitos de acordo com os tipos de ameaça.

Para a formulação dos padrões, foram analisados trabalhos como o Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT (Pessoa, 2025). Este catálogo reúne um conjunto de informações para apoiar a identificação e possíveis formas de mitigação de vulnerabilidades mapeadas em sistemas IoT, provenientes de estudos de literatura (*ad-hoc* e estruturados). A partir dessas referências, foi utilizado um processo de conversão de vulnerabilidades em requisitos de segurança, seguindo o modelo de padrões de requisitos proposto por (Withall, 2007).

1.5 Organização do Texto

Este trabalho está estruturado nos seguintes capítulos:

Capítulo 1 – Introdução

Apresentamos o contexto, a motivação, o problema de pesquisa, os objetivos e a metodologia adotada. Também são discutidos os desafios da Engenharia de Requisitos em IoT e a justificativa para o desenvolvimento de um catálogo de requisitos de segurança.

Capítulo 2 – Fundamentação Teóricos

Traz uma base conceitual necessária para compreender o trabalho. São abordados a arquitetura da Internet das Coisas e suas vulnerabilidades, os princípios da tríade CIA, o modelo STRIDE de ameaças e a estrutura de padrões de requisitos segundo (Withall, 2007).

Capítulo 3 – Metodologia De Desenvolvimento Do Catálogo Stride-Iot

São apresentadas as etapas utilizadas para criar o catálogo, incluindo o mapeamento sistemático da literatura, o uso do Catálogo de Vulnerabilidades IoT (Pessoa, 2025) em padrões de requisitos e o modelo adotado para estruturar RPGs, FRPs e NFRPs.

Capítulo 4 – Catálogo De Requisitos De Segurança Para Iot Baseado No Modelo Stride

Apresenta o catálogo final desenvolvido. São detalhadas sua arquitetura geral, o modelo visual das relações entre os padrões, os elementos estruturantes (RPGs, FRPs e NFRPs) e a organização por domínios STRIDE. Cada conjunto de padrões de cada domínio, explicações e exemplos.

Capítulo 5 – Conclusão

Traz a conclusão do trabalho, bem como as considerações finais, limitações e sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta os fundamentos necessários para o desenvolvimento do catálogo STRIDE-IoT, abordando inicialmente a Internet das Coisas e suas vulnerabilidades estruturais, seguido pelos princípios da segurança da informação por meio da tríade CIA. Em seguida, descreve o modelo STRIDE como referência para classificação sistemática de ameaças e discute conceitos essenciais da engenharia de requisitos e do uso de padrões, que permitem organizar, reutilizar e tornar rastreáveis os requisitos de segurança. Assim, este conjunto de conceitos estabelece a base teórica que sustenta as decisões metodológicas e a estruturação do catálogo proposto.

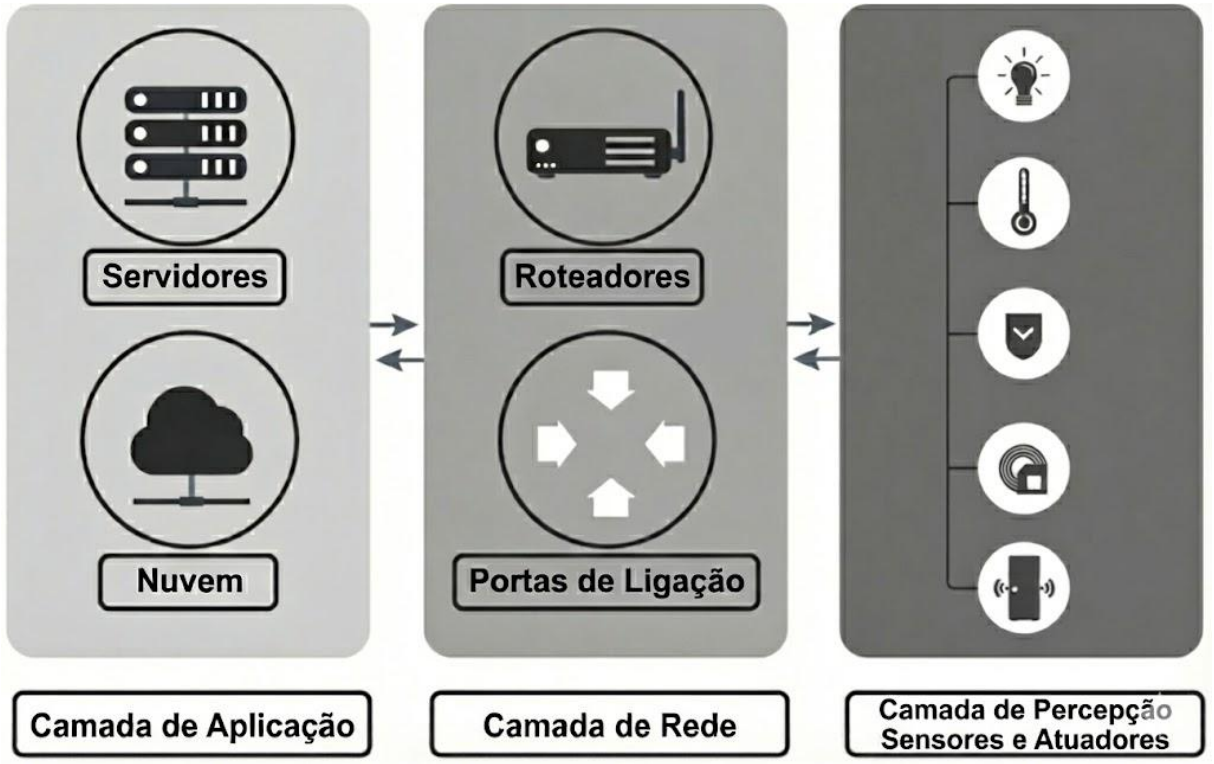
2.1 Internet das Coisas e suas Vulnerabilidades

A Internet das Coisas (IoT) conecta dispositivos físicos, sensores e sistemas digitais em uma mesma rede inteligente. Apesar de seu potencial em áreas como automação, saúde, indústria e cidades inteligentes, o ecossistema IoT apresenta limitações significativas — tanto em *hardware* quanto em *software* — que afetam diretamente a segurança (Aguilar-Calderón et al., 2022).

Essas limitações incluem baixo poder de processamento, memória restrita, protocolos heterogêneos e ausência de padrões universais de autenticação e atualização. Como consequência, os dispositivos IoT são especialmente vulneráveis a ataques que exploram falhas em *firmware*, comunicação ou gerenciamento de credenciais (Cetintav; Tahir Sandikkaya, 2025).

O paradigma IoT pode ser representado em três camadas como mostrado na figura abaixo:

Figura 1 - Estrutura das três camadas tradicionais de IIoT: percepção, rede e aplicação.



Fonte: Alotaibi, 2023

A **camada de dispositivo** é composta por vários objetos, como sensores, câmeras, robôs e sensores. Essa camada é responsável por coletar informações ou efetuar alguma ação no meio. Essas informações podem ser grandezas como movimento, substâncias químicas em um ambiente, vibrações, calor, aceleração ou umidade. Esses dados são passados para a camada de rede e em seguida para a camada de aplicação (Alotaibi, 2023).

A **camada de rede** transfere as mensagens de comunicação pela rede. Essas mensagens são enviadas pela interface do dispositivo IoT usando um protocolo de comunicação, passando por diferentes *links* de comunicação. Os pacotes transmitidos por dispositivos IoT geralmente são recebidos por nós na borda, como roteadores ou *gateways*, que processam e encaminham essas informações para o mundo externo(Alotaibi, 2023).

A última camada da arquitetura tradicional de IoT é a camada de aplicação. É nela que as informações são processadas e, normalmente, é também a parte final com a qual os clientes interagem. Esses sistemas são especialmente suscetíveis a

ataques de *ransomware* em alguns tipos de implantação IoT. Eles se tornam vulneráveis a diversos problemas de segurança porque, em geral, não suportam contramedidas adequadas, como criptografia, atualizações e aplicação de correções de segurança (Alotaibi, 2023).

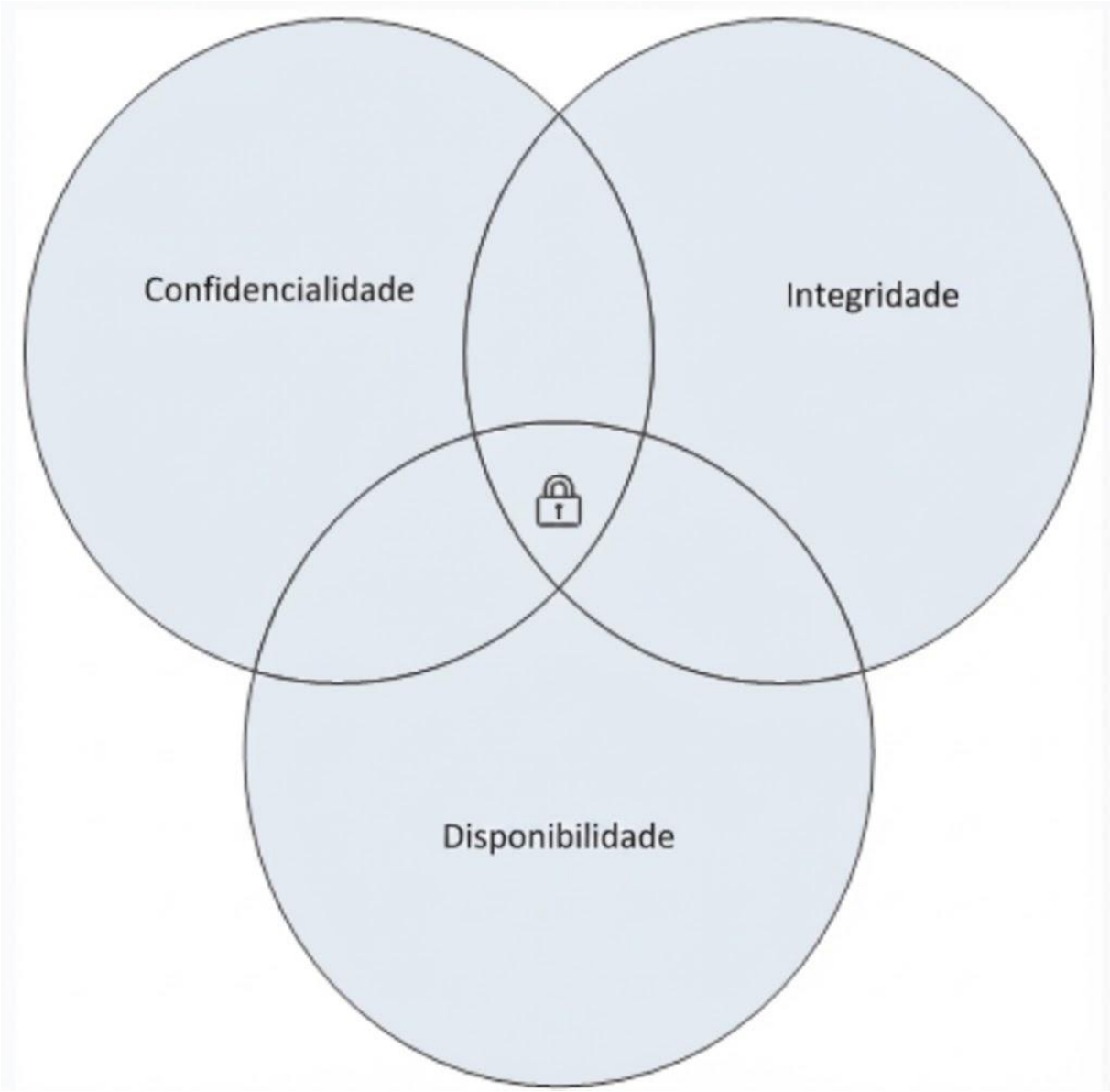
2.2 Segurança da Informação e a Tríade CIA

A tríade **CIA** — Confidencialidade (Confidentiality), Integridade (Integrity) e Disponibilidade (Availability) — é o alicerce da segurança da informação. Cada elemento define uma dimensão fundamental da proteção de sistemas (Death, 2017):

- Confidencialidade: garante que as informações sejam acessadas apenas por entidades autorizadas.
- Integridade: assegura que os dados não sejam modificados indevidamente, preservando sua precisão e consistência.
- Disponibilidade: garante que os sistemas e serviços permaneçam acessíveis sempre que necessário.

Embora conceitualmente independentes, os três pilares são interdependentes conforme mostrado na Figura 2. O fortalecimento de uma dessas dimensões pode fortalecer as demais.

Figura 2 - Representação da Tríade CIA, Confidencialidade, Integridade e Disponibilidade



Fonte: Death, 2017

Portanto a tríade CIA serve como um modelo fundamental para orientar toda a segurança da informação em qualquer sistema, incluindo os sistemas IoT (Death, 2017).

2.3 Modelo STRIDE de Ameaças

O modelo STRIDE, desenvolvido pela *Microsoft*, é um *framework* de classificação de ameaças utilizado para apoiar a análise de segurança de sistemas (Shostack, 2014). As ameaças STRIDE representam propriedades indesejáveis para

um sistema como autenticação, autorização, integridade, não repúdio, confidencialidade e disponibilidade. O Quadro 1, Categorias de Ameaças segundo o modelo STRIDE, apresenta as ameaças STRIDE, a propriedade correspondente que se deseja manter, uma definição, as vítimas mais típicas e exemplos (Shostack, 2014):

Quadro 1 - Categorias de Ameaças segundo o Modelo STRIDE

AMEAÇA	**PROPRIEDADE VIOLADA**	**DEFINIÇÃO DE AMEAÇA**	**VÍTIMAS TÍPICAS**	**EXEMPLOS**
Falsificação (Spoofing)	Autenticação (Authentication)	Fingir ser algo ou alguém diferente de si mesmo.	Processos, entidades externas, pessoas	Fingir ser um policial ou um médico.
Adulteração (Tampering)	Integridade (Integrity)	Modificar algo em um disco, em uma rede ou na memória.	Armazenamento de dados, fluxos de dados, processos	Alterar uma planilha, o binário de um programa importante ou o conteúdo de um banco de dados em disco; modificar, adicionar ou remover pacotes em uma rede, seja local ou remota pela Internet, com ou sem fio; alterar os dados que um

				programa está usando ou o próprio programa em execução.
Repúdio (Repudiation)	Não Repúdio (Non-Repudiation)	Alegar que você não fez algo ou que não foi responsável. A refutação pode ser honesta ou falsa, e a questão fundamental para os projetistas de sistemas é: que provas você tem?	Processo	Processo ou sistema: “Eu não apertei o botão vermelho” ou “Eu não encomendei aquela Ferrari”. ela transcende a natureza técnica das outras ameaças à camada de negócios.
Divulgação de Informação (Information Disclosure)	Confidencialidade (Confidentiality)	Fornecer informações a alguém não autorizado a vê-las.	Processos, armazenamento de dados, fluxos de dados	Permitir o acesso a arquivos, e-mails ou bancos de dados, mas a divulgação de informações também pode envolver nomes de

				arquivos ("Terminação para John Doe.docx"), pacotes em uma rede ou o conteúdo da memória do programa.
Negação de Serviço (Denial of Service)	Disponibilidade (Availability)	Absorver os recursos necessários para prestar o serviço.	Processos, armazenamento de dados, fluxos de dados	Um programa que pode ser enganado para usar toda a sua memória, um arquivo que preenche o disco ou tantas conexões de rede que o tráfego real não consegue passar.
Elevação de Privilégio (Elevation of Privilege)	Autorização (Authorization)	Permitir que alguém faça algo que não está autorizado a fazer.	Processo	Permitir que um usuário comum execute código como administrador; permitir que uma pessoa remota sem

				privilégios execute código.

Fonte: Shostack, 2014

O método permite mapear vulnerabilidades de forma sistemática e relacioná-las diretamente às propriedades que elas violam, funcionando como uma ponte entre a ameaça identificada e os controles necessários para mitigá-la.

2.4 Engenharia de Requisitos

A engenharia de requisitos é o processo responsável por identificar, documentar e gerenciar as necessidades que um sistema deve atender (Da Silva, 2021). Quando aplicada à segurança, ela enfrenta desafios, pois os requisitos de segurança são muitas vezes intangíveis, difíceis de testar e de difícil comunicação entre áreas técnicas e de negócio (Da Silva, 2021).

Uma estratégia para enfrentar esse problema pode ser a definição de padrões de requisitos, que descrevem boas práticas aplicáveis em diferentes contextos e aplicações. Cada padrão encapsula um problema recorrente e sua solução genérica, facilitando a reutilização de conhecimento e a padronização de práticas de especificação (Kudo, 2021). Os padrões de requisitos podem ser agrupados em catálogos para facilitar sua reutilização e um dos principais referenciais conceituais para essa abordagem é o modelo de *Requirement Patterns* proposto por Stephen Withall (Withall, 2007). Além disso, os padrões atuam como um ponto de partida para a especificação dos requisitos, em vez de o engenheiro começar do zero para resolver problemas conhecidos (Barcelos, 2016). Em ambientes complexos, como os de segurança, os padrões capturam o conhecimento de especialistas, tornando-o acessível a desenvolvedores e facilitando o desenvolvimento seguro (Papoutsakis et al., 2021).

2.5 Padrões de Requisitos

As definições e estruturas conceituais apresentadas nesta seção seguem o modelo proposto por (Withall, 2007), que organiza padrões de requisitos em níveis de abstração — domínios, grupos e padrões concretos, fornecendo uma base sistemática para especificar padrões de requisitos de forma clara, reutilizável e consistente.

Em sistemas de *software*, é comum a recorrência de requisitos com características semelhantes, especialmente em domínios que apresentam operações e estruturas repetitivas. Em sistemas de negócios, essa repetição se torna ainda mais evidente, uma vez que grande parte das necessidades levantadas pertence a um número reduzido de categorias funcionais.

Para promover consistência, padronização e qualidade na especificação desses elementos, utiliza-se o conceito de padrão de requisito. Um padrão de requisito constitui uma abordagem sistematizada para especificar um determinado tipo de requisito, oferecendo diretrizes claras sobre como descrevê-lo.

Ao elaborar um requisito, o padrão orienta quais aspectos documentar, quais atributos considerar e as informações complementares que podem ser necessárias. Após a finalização do requisito, o padrão cumpre seu papel imediato, mas permanece útil para outros atores do processo de desenvolvimento. Projetistas, desenvolvedores e testadores podem recorrer ao padrão para obter orientações adicionais sobre implementação ou sobre critérios de verificação e validação.

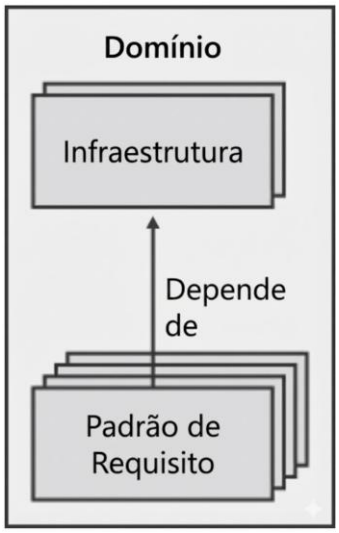
Os padrões podem variar em nível de detalhamento e em valor prático. Alguns tipos de requisitos podem ser definidos com grande exatidão, e suas instâncias variam muito pouco. Outros possuem elementos úteis em comum, mas variam tanto entre si que não é possível prescrever exatamente o que devem conter, essas variações são naturais. Para justificar a existência de um padrão ele precisa apenas ser útil — ele não precisa abranger tudo que um padrão poderia, em teoria, abranger. Por outro lado, o fato de encontrarmos repetidamente um determinado tipo de requisito não significa que criar um padrão para ele será automaticamente valioso. Pode ser difícil capturar o que esses requisitos têm em comum, e também será difícil fornecer orientações sobre como especificar suas instâncias.

2.5.1 Domínio e infraestrutura

Em engenharia de requisitos, um domínio é uma categoria temática que organiza padrões de requisitos com características, objetivos ou contextos semelhantes. Em vez de tratar cada padrão de forma isolada, o domínio agrupa padrões que lidam com um mesmo tipo de problema ou área funcional, como desempenho, segurança, manipulação de dados ou regras de negócio.

Todos os padrões de requisitos pertencem a um determinado domínio. Muitos dos requisitos que utilizam padrões dependem de algum tipo de infraestrutura de suporte. Por exemplo, requisitos relacionados a relatórios pressupõem a existência de uma infraestrutura capaz de gerar esses relatórios. Assim, além do requisito em si, é necessário definir requisitos específicos também para essa infraestrutura. A relação geral entre domínio, infraestrutura e padrões de requisitos é ilustrada na Figura 3, que ilustra como os padrões dependem das infraestruturas do domínio ao qual pertencem.

Figura 3 - Relações entre domínios, padrões de requisitos e infraestruturas



Fonte: Withall (2007)

Para evitar que cada padrão de requisito tenha de descrever individualmente a infraestrutura de que necessita, essa responsabilidade é atribuída ao domínio ao qual o padrão pertence. Isso ocorre porque uma mesma infraestrutura geralmente é compartilhada por diversos padrões dentro do mesmo domínio. Dessa forma, cada tipo de infraestrutura é descrito apenas uma vez, no domínio correspondente, eliminando redundâncias e garantindo consistência.

Um padrão de requisito pode utilizar infraestruturas pertencentes a outros domínios. No entanto, recomenda-se evitar dependências mútuas — se um elemento em um domínio depende de outro domínio, então nada neste segundo domínio deve depender do primeiro — sempre que possível. Da mesma forma, uma infraestrutura pode depender de outra, desde que essas relações sejam bem definidas e não criem ciclos de dependência.

2.5.2 Grupos de padrões de requisitos

Quando diferentes padrões de requisitos apresentam características semelhantes, podemos organizá-los em um grupo de padrões de requisitos (*Requirement Pattern Groups – RPG*). Esses grupos funcionam como um espaço para documentar os aspectos que são comuns entre os padrões, evitando repetições desnecessárias nas descrições individuais. É importante destacar que um RPG não é um padrão de requisito em si — logo, não é possível derivar requisitos diretamente a partir dele.

A diferença entre um domínio e um RPG é que os padrões dentro de um domínio compartilham um tema comum, enquanto os padrões dentro de um grupo possuem características detalhadas em comum. Os padrões de um grupo não precisam pertencer ao mesmo domínio.

Functional Requirement Patterns

Os *Functional Requirement Patterns* (FRPs) são padrões voltados para requisitos funcionais. Eles descrevem comportamentos específicos que o sistema deve fornecer como ações, respostas, operações, interações e funções observáveis. Um FRP é derivado de um RPG, especializando seus princípios em uma estrutura concreta que pode ser diretamente utilizada para a formulação de requisitos funcionais.

Non-Functional Requirement Patterns

Os *Non-Functional Requirement Patterns* (NFRPs) são padrões voltados para requisitos não funcionais, tais como desempenho, confiabilidade, segurança, restrições físicas, interoperabilidade, entre outros. Enquanto os FRPs tratam de “o que o sistema faz”, os NFRPs tratam de “como o sistema deve ser” ou “sob quais

condições ele deve operar”. Eles registram propriedades de qualidade e restrições que influenciam tanto o projeto quanto a implementação.

Dessa forma, RPGs, FRPs e NFRPs compõem uma hierarquia sugerida para organizar padrões de requisitos em camadas de abstração. E ainda podem ter subgrupos dentro de cada um conforme as características dos padrões agrupados.

2.5.3 Relações Entre Padrões de Requisitos

Ao utilizar um padrão de requisito, geralmente ele fornece todas as informações necessárias para criar um requisito daquele tipo. No entanto, um padrão pode fazer referência a outros padrões por diversos motivos. Existem dois tipos fundamentais de relacionamento entre padrões de requisitos:

***Refers to*:**

Um padrão de requisito pode mencionar outro padrão em algum ponto de sua definição. Isso pode ocorrer por várias razões:

- Um requisito define algo que contém (ou possui) outro elemento definido por um requisito diferente.
- Um requisito que é a instância de um padrão utiliza informações definidas por requisitos que seguem outro padrão.
- Um requisito pode sugerir a criação de outro requisito adicional, cuja forma de escrita é orientada por outro padrão disponível.
- Um padrão “desviador” pode levar você a optar por escrever um requisito baseado em um padrão diferente.
- Um padrão pode se referir a outro que contenha informações discursivas relevantes sobre um determinado tópico.

***Extends*:**

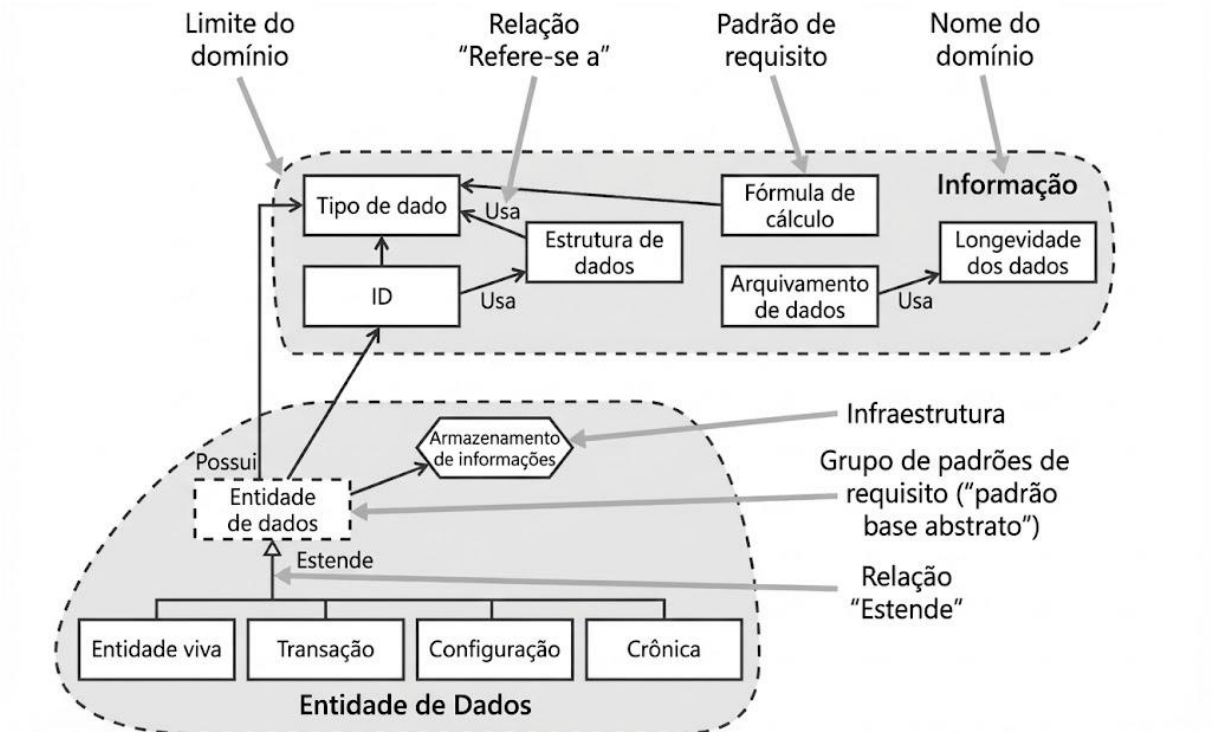
Um padrão de requisito pode ser construído com base em outro padrão, funcionando como sua especialização. Em termos de orientação a objetos, trata-se de uma relação de herança. Em vez de estender outro padrão, um padrão de requisito também pode se basear em um grupo de padrões de requisitos, que funciona como uma classe base abstrata.

Um padrão de requisito não pode estender mais de um padrão ou grupo — assim herança múltipla não é permitida nesse modelo.

2.5.4 Representação em Diagramas

É possível representar conjuntos de padrões e infraestruturas, assim como os relacionamentos entre eles, por meio de diagramas. A Figura 4 apresenta um exemplo com dois domínios, incluindo anotações sobre a notação utilizada.

Figura 4 - Diagrama com anotações de um padrão de requisito



Fonte: Withall, 2007

A relação de *extends* é considerada a mais importante. Para simplificar a visualização, todos os demais relacionamentos são exibidos apenas como *Refers to*, podendo ser rotulados para indicar papéis específicos.

Quando vários domínios são apresentados em um mesmo diagrama, pode se tornar inviável representar todas as relações. Nesses casos, recomenda-se:

- Mostrar todas as relações dentro de cada domínio,
- Mostrar todas as relações *extends* entre domínios,

- Omitir, quando necessário, as relações *refers to* entre domínios, para manter o diagrama legível.

O diagrama opera de modo análogo a um diagrama de classes em UML, representando os padrões como entidades estruturais e explicitando as relações entre eles.

2.5.5 Benefícios de se utilizar padrões de requisitos

As orientações fornecidas por um padrão de requisitos costumam ir além de apenas dizer o “impelente isso... ”. Ele fornece uma compreensão mais profunda do problema em questão e isso permite o engenheiro de requisitos fazer pe perguntas mais relevantes — e também até levantar a formulação de um requisito (ou vários) bastante diferente do que se tinha imaginado inicialmente.

Alguns padrões de requisitos exigem — ou ao menos sugerem — a definição de requisitos adicionais, sendo eles tanto requisitos subsequentes, que estendem o requisito original, quanto aos requisitos de caráter abrangentes ou sistêmicos, necessários para sustentar o próprio padrão. Pode ser útil manter o controle de quais padrões foram utilizados para que seja possível revisá-los posteriormente garantindo uma rastreabilidade. O reuso aproveita conhecimentos adquiridos em projetos anteriores, o que aumenta as chances de sucesso de novos projetos. Isso oferece uma alternativa viável para aumentar a produtividade no desenvolvimento de software.

2.5.6 Classificações de Padrões de Requisitos

Quando trabalhamos com padrões de requisitos, essa classificação se torna mais eficiente — em vez de rotular cada requisito manualmente, classificamos o padrão, e essa classificação se propaga automaticamente para todos os requisitos criados a partir dele. Isso reduz retrabalho, evita inconsistências e facilita entender o tipo de requisito que está sendo especificado. Podemos definir grupos dentro da classificação seguindo regras de negócios, documentos e outros.

Além disso, as classificações ajudam na organização e análise dos requisitos. Elas permitem, por exemplo, identificar rapidamente quais padrões geram funcionalidades do sistema e quais tratam de aspectos transversais, como segurança

ou desempenho. Também possibilitam gerar estatísticas e análises de complexidade do sistema, já que cada padrão leva consigo uma “identidade” que pode ser consultada ou filtrada em ferramentas de apoio.

2.5.7 Estrutura De Um Padrão De Requisitos

Um padrão de requisito precisa indicar quando deve ser utilizado e como escrever requisitos baseados nele, conforme o exemplo do Quadro 2. Ele também pode oferecer orientações sobre como implementar e testar requisitos desses tipos. Para transmitir essas informações, cada padrão de requisito contém as seguintes seções:

Quadro 2 - Estrutura de um padrão de requisitos

Nome do padrão
Precisa ter um nome único para que possa ser referenciado sem ambiguidade. Deve conter claramente a natureza do padrão — e tão conciso quanto possível; preferencialmente composto por uma única palavra, e nunca por mais do que três.
Detalhes básicos
Inclui a manifestação do padrão, o domínio ao qual pertence, padrões relacionados (se houver), frequência prevista de uso, classificações do padrão e o autor do padrão.
Aplicabilidade
Em quais situações o padrão pode ser aplicado? E em quais casos ele não deve ser utilizado?
Discussão
Como escrever um requisito desse tipo? Quais pontos precisam ser considerados ao defini-lo?
Modelos
Um ponto de partida para escrever um requisito desse tipo — podendo haver mais de um modelo, caso existam variações alternativas.
Exemplos
Um ou mais requisitos representativos escritos utilizando esse padrão.
Requisitos Extra

Que tipo de requisitos com frequência derivam de um requisito desse tipo? E que requisitos sistêmicos abrangentes podem ser necessários para sustentar todos os requisitos desse padrão?
Considerações para desenvolvimento
Dicas para os desenvolvedores e engenheiros de software como implementar requisitos desse tipo.
Considerações para testes
O que deve ser levado em conta ao decidir como testar um requisito desse tipo?

Fonte: Withall, 2007

2.6 Trabalhos Relacionados

Nesta seção, são apresentados trabalhos relacionados no que se refere à segurança de sistemas de internet das coisas, engenharia de requisitos e utilização de catálogos e padrões como forma de organizar o conhecimento técnico obtido e reaproveitá-lo.

Papoutsakis et al. (2021) apresentam uma coleção hierárquica de padrões de segurança e privacidade voltada a sistemas IoT e IIoT, organizada segundo propriedades de segurança, como confidencialidade e privacidade. O trabalho enfatiza o conceito de *security and privacy by design*, porém permanece concentrado nos níveis de arquitetura e design, sem explicitar a derivação de requisitos de segurança reutilizáveis nem sua ligação com modelos formais de ameaça.

Cordeiro, Vasconcelos e Correia (2022) propõem um catálogo consolidado de padrões de segurança, reunindo e avaliando um grande conjunto de padrões existentes com base em métricas de qualidade. O catálogo melhora a organização e a padronização das descrições, classificando os padrões por propriedades de segurança e fases do desenvolvimento. Apesar de sua relevância, a proposta não é direcionada especificamente ao contexto IoT e não utiliza a engenharia de requisitos como eixo central de organização.

No que se refere à identificação de fragilidades em ambientes IoT, Pessoa (2025) apresenta um Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT, resultante de estudos *ad hoc* e mapeamentos sistemáticos da literatura. O catálogo organiza vulnerabilidades segundo as camadas de aplicação, rede e dispositivo, oferecendo uma visão abrangente da superfície de ataque em IoT.

No contexto da engenharia de requisitos, trabalhos como os de Kudo (2021) e Barcelos (2016) exploram o uso de padrões e apoio ferramental para padronizar a especificação de requisitos. Essas abordagens contribuem para a reutilização e a melhoria da qualidade dos requisitos.

Em síntese, os trabalhos relacionados demonstram avanços importantes na catalogação de vulnerabilidades, padrões de segurança e requisitos. No entanto, observa-se a ausência de uma abordagem que integre, de forma estruturada, modelos de ameaça, vulnerabilidades conhecidas e padrões de requisitos de segurança em um único artefato voltado a sistemas IoT. O presente trabalho se diferencia ao propor o Catálogo STRIDE-IoT, que organiza requisitos de segurança a partir do modelo STRIDE e estabelece uma ligação direta entre ameaças, requisitos e tecnologias, contribuindo para reduzir a lacuna entre análise de risco e especificação de requisitos.

2.7 Considerações Finais

Os conceitos apresentados neste capítulo fornecem a base necessária para o desenvolvimento do catálogo proposto. As definições e relações entre os padrões de requisitos (*Refers to, Extends*) — estruturados em diferentes níveis, como **RPGs, FRPs e NFRPs** — são essenciais para promover clareza, consistência e qualidade na especificação, permitindo que conhecimento consolidado seja reaproveitado em novos projetos.

E também os grupos de padrões como elementos de abstração contribui para organizar características comuns, evitando redundâncias e tornando o processo de documentação mais coeso.

Essas bases conceituais servirão de apoio para os capítulos seguintes, nos quais serão apresentadas a metodologia e as etapas de desenvolvimento do catálogo.

3 METODOLOGIA DE DESENVOLVIMENTO DO CATÁLOGO STRIDE-IOT

Este capítulo apresenta a metodologia empregada na construção do Catálogo STRIDE-IoT, baseada em um mapeamento sistemático da literatura, na análise estruturada de vulnerabilidades IoT e em um processo formal de conversão dessas vulnerabilidades em padrões de requisitos.

3.1 Procedimentos Metodológicos

O desenvolvimento do Catálogo STRIDE-IoT seguiu uma abordagem metodológica exploratória e aplicada, estruturada para garantir rigor na identificação, análise e transformação de vulnerabilidades em padrões de requisitos de segurança aplicáveis a sistemas de Internet das Coisas. A metodologia foi organizada em etapas complementares que conectam técnicas formais de revisão sistemática da literatura, análise de vulnerabilidades e modelagem baseada em padrões, permitindo a construção de um artefato consistente, rastreável e alinhado a práticas de engenharia de requisitos.

A primeira etapa consistiu na realização de um Mapeamento Sistemático da Literatura, conduzido por meio da plataforma Parsif.al, seguindo um protocolo de pesquisa previamente definido. Esse mapeamento teve como objetivo identificar abordagens, desafios e práticas relacionadas a requisitos de segurança em IoT, bem como lacunas existentes em catálogos, métodos e *frameworks*. Os resultados forneceram a fundamentação teórica que orientou tanto a construção do catálogo quanto a definição dos critérios de extração e transformação.

Em seguida, adotou-se como insumo central o Catálogo de Vulnerabilidades IoT de (Pessoa, 2025), que organiza vulnerabilidades conhecidas segundo as três camadas tradicionais de arquiteturas IoT (aplicação, dispositivo e rede). Esse catálogo serviu como base para derivar requisitos de segurança vinculados a ameaças reais, garantindo que o catálogo proposto refletisse essas vulnerabilidades.

A etapa seguinte consistiu na definição de um processo sistemático de conversão de vulnerabilidades em requisitos, fundamentado em princípios de engenharia de requisitos e inspirado no modelo proposto por (Withall, 2007). Esse processo estabeleceu critérios para identificar e classificar cada vulnerabilidade

conforme sua natureza, determinando seu padrão de requisito correspondente (FRP ou NFRP), e formular descrições gerais, aplicáveis a diversos contextos IoT.

Por fim, os requisitos derivados foram organizados conforme os domínios de ameaça do modelo STRIDE, compondo uma hierarquia formada por *Requirement Pattern Groups*, *Functional Requirement Patterns* e infraestruturas de suporte.

3.2 Mapeamento Sistemático da Literatura

O Mapeamento Sistemático da Literatura, constituiu a etapa inicial e fundamental para a consolidação da base teórica do catálogo STRIDE-IoT. O estudo foi conduzido na plataforma Parsif.al, sob o título “Catálogo de padrões de requisitos de segurança para sistemas de Internet das Coisas (IoT)”, e teve como objetivo geral:

“Apresentar um mapeamento sistemático da literatura sobre catálogos de padrões de requisitos voltados à segurança em Internet das Coisas (IoT), identificando e classificando métodos, práticas e desafios associados à definição, análise e validação de requisitos de segurança nesses ambientes interconectados.”

Foi definido um protocolo estruturado contendo questões de pesquisa, critérios de inclusão e exclusão, *strings* de busca, bases de dados relevantes e procedimentos de análise. As buscas foram realizadas nas bases IEEE Xplore, Scopus e Google Scholar, e as referências foram organizadas no Zotero, facilitando o gerenciamento e a filtragem das publicações.

O processo permitiu identificar lacunas recorrentes nos catálogos existentes — principalmente quanto à navegabilidade, clareza semântica e ausência de mecanismos que conectem vulnerabilidades a requisitos e tecnologias específicas.

3.2.1 Protocolo de Revisão

Objetivo Específico:

Analisar o estado da arte dos catálogos de requisitos de segurança para IoT, mapeando metodologias, classificações, desafios e lacunas de pesquisa.

PICOC

Quadro 3 - Estrutura PICOC utilizada para definição das questões de pesquisa

Elemento	Descrição
Population	Sistemas de Internet das Coisas (IoT), sistemas ciberfísicos (CPS).
Intervention	Catálogos de requisitos, métodos de classificação e aplicação.
Comparison	Não é aplicável.
Outcome	Identificação de desafios, avaliação de aplicabilidade e lacunas.
Context	Ambientes IoT, automação industrial, ambientes inteligentes e engenharia de software.

Fonte: Elaborado pelo autor

Questões de Pesquisa:

1. Quais métodos de classificação de requisitos esses catálogos utilizam?
2. Quais são os principais desafios relatados na definição, análise e uso de catálogos de requisitos em ambientes IoT/CPS?
3. Como foi avaliada a aplicabilidade prática desses catálogos (estudos de caso, protótipos, validações empíricas)?
4. Quais lacunas e oportunidades de pesquisa são apontadas pelos autores para o aprimoramento desses catálogos?

***String* de Busca**:

A primeira *string* V1 mostrou-se ampla demais, resultando em grande quantidade de estudos não pertinentes ao escopo da pesquisa. Para melhorar a precisão da busca, optou-se por restringi-la por meio da *string* V2, que inclui termos adicionais relacionados a catálogos, padrões e reuso, proporcionando uma seleção mais adequada e alinhada ao propósito do mapeamento.

- V1: ("security requirements" OR "security catalogue" OR "security catalog") AND ("Internet of Things" OR IoT)

- V2: security AND (requirement OR requirements) AND (catalog OR catalogue OR pattern OR library) AND ("Internet of Things" OR IoT) AND reuse

Bases de Dados:

- IEEE Xplore
- Google Scholar
- Scopus

3.3 Catálogo De Vulnerabilidades Como Base De Derivação

A elaboração do Catálogo STRIDE-IoT utilizou como insumo central o Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT, proposto por (Pessoa, 2025). Esse catálogo reúne um conjunto estruturado de vulnerabilidades identificadas a partir de pesquisas ad hoc e mapeamentos sistemáticos, cobrindo as três camadas arquitetônicas típicas de sistemas IoT — dispositivo, rede e aplicação. Essa organização inicial mostrou-se especialmente adequada ao objetivo deste trabalho, pois fornece uma visão abrangente da superfície de ataque, alinhada às particularidades e restrições dos ambientes IoT.

A escolha deste catálogo como fonte principal de referência fundamenta-se em três fatores. Primeiro, ele consolida vulnerabilidades associadas a cenários reais de IoT, oferecendo descrições claras, contextualizadas e tecnicamente precisas. Segundo, as vulnerabilidades apresentadas incluem recomendações de mitigação, o que facilita sua conversão em requisitos de segurança — objetivo central deste estudo. Terceiro, o catálogo de (Pessoa, 2025) é compatível com uma abordagem de modelagem orientada a padrões, pois separa vulnerabilidades por categoria e fornece os elementos mínimos necessários para identificar atores, ações, objetos e mecanismos de proteção.

O processo de derivação dos padrões de requisitos funcionais (FRPs) tomou essas vulnerabilidades como ponto de partida, seguindo o princípio de que uma vulnerabilidade bem descrita contém implicitamente os requisitos necessários para sua mitigação. Assim, cada vulnerabilidade foi analisada para extrair seus componentes essenciais: ameaças associadas, mecanismos de ataque, condições de

exploração, impacto potencial e recomendações de proteção. Esses elementos foram utilizados como base para criar requisitos de segurança generalizados e aplicáveis a diferentes cenários IoT.

No catálogo de (Pessoa, 2025), as vulnerabilidades estão organizadas de acordo com as três camadas IoT, o que favoreceu a organização com o STRIDE-IoT. A partir dessa estrutura, cada vulnerabilidade foi mapeada para o domínio de ameaça correspondente (*Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service* ou *Elevation of Privilege*). Esse mapeamento representou uma etapa crucial, pois viabilizou a harmonização entre a taxonomia de riscos (STRIDE) e a arquitetura das camadas IoT, permitindo que os padrões resultantes fossem simultaneamente classificáveis por ameaça e por camada.

Além disso, a presença de recomendações de mitigação diretamente associadas às vulnerabilidades — como criptografia, autenticação, controle de acesso ou monitoramento de tráfego — ofereceu um insumo estruturado para transformar evidências empíricas em requisitos reutilizáveis. Cada conjunto de mitigações foi analisado e reinterpretado como uma “intenção de requisito”, posteriormente consolidada no formato padrão descrito por (Withall, 2007), que orienta a criação de padrões de requisitos.

3.4 Processo De Conversão De Vulnerabilidades Em Requisitos

O processo de conversão das vulnerabilidades identificadas no Catálogo de Vulnerabilidades de Segurança em Sistemas de *Software* IoT, em padrões de requisitos seguiu uma adaptação do método proposto por (Carneiro, 2024). Esse processo permitiu transformar vulnerabilidades em requisitos de segurança, generalizáveis e aplicáveis a cenários IoT.

As etapas seguidas foram as seguintes:

Etapa 1 - Identificação dos Atores

Consiste em determinar quais entidades participam da vulnerabilidade ou do mecanismo de mitigação — por exemplo, usuário legítimo, dispositivo IoT, atacante, administrador ou serviço de *backend*.

Etapa 2 - Identificação dos Verbos de Ação

Corresponde à extração dos verbos presentes nas recomendações de mitigação, tais como proteger, validar, registrar, monitorar, restringir ou autenticar. Esses verbos representam a intenção de segurança que deverá ser posteriormente expressa como requisito.

Etapa 3 - Determinação dos Objetos da Ação

Envolve identificar os elementos sobre os quais cada ação recai: dados sensíveis, credenciais, canais de voz, conexões de rede, logs de auditoria, entre outros. Essa etapa define o alvo do comportamento de segurança.

Etapa 4 - Classificação do Requisito

Cada ação é analisada para determinar se refere a um requisito funcional (FRP) — isto é, um comportamento observável do sistema — ou de um requisito não funcional (NFRP), caracterizado por propriedades, restrições ou qualidades desejadas. Essa distinção permite sua posterior organização nos domínios STRIDE e no IoT *Fundamental Domain*.

Etapa 5 - Reescrita e Generalização

Por fim, os elementos identificados são reestruturados em linguagem normativa, adotando a formulação típica de requisitos: “O sistema deve <verbo> <objeto> …”

3.4.1 Exemplo de Conversão de Vulnerabilidade em Padrão de Requisito

Para ilustrar a aplicação prática desse processo, apresenta-se a seguir a conversão completa da vulnerabilidade **“Canal de Voz”**, extraída do Catálogo de Vulnerabilidades de Segurança em Sistemas de *Software* IoT, convertido no padrão de requisito funcional FRP-SEC-004: Canal de Voz Seguro, incluído no domínio *Spoofing* do catálogo STRIDE-IoT no Quadro 4.

Vulnerabilidade Original (Pessoa, 2025)

Quadro 4 - Vulnerabilidade Canal de Voz (Pessoa, 2025)

Canal de Voz
DESCRIÇÃO
Associados à segurança e à privacidade quando os dispositivos IoT incorporam capacidades de voz, como assistentes pessoais ativados por voz, sistemas de controle de casa inteligente ou dispositivos de comunicação por voz. Em casas inteligentes, essas informações podem agora ser facilmente captadas ao explorar dispositivos IoT mal protegidos com sistemas de microfone integrados, como serviços de assistente pessoal (por exemplo, Google Home, Amazon Echo), brinquedos infantis e outros eletrodomésticos controlados por voz. Esses sistemas são vulneráveis a ataques como voz intrusa e mascaramento de voz
MITIGAÇÃO
Criptografia de Ponta a Ponta: Utilizar criptografia de ponta a ponta para proteger as comunicações de voz entre os dispositivos IoT e os servidores de processamento de voz, garantindo a confidencialidade e a integridade dos dados de voz. **Autenticação de Voz**: Implementar mecanismos robustos de autenticação de voz para verificar a identidade dos usuários e detectar tentativas de spoofing de voz ou falsificação de comandos de voz. **Monitoramento de Tráfego**: Monitorar o tráfego de voz na rede para detectar atividades suspeitas, como tentativas de interceptação de comunicações de voz ou manipulação de comandos de voz. **Atualizações de Segurança**: Manter os dispositivos IoT e os aplicativos associados atualizados com as últimas correções de segurança e patches de software para mitigar vulnerabilidades conhecidas que possam ser exploradas nos canais de voz. **Controle de Acesso**: Implementar políticas de controle de acesso para restringir o acesso aos dispositivos IoT e aos sistemas de comunicação de voz, garantindo que apenas usuários autorizados possam interagir com esses dispositivos.

Fonte: Pessoa, 2025

3.4.2 Processo de Conversão Aplicado

Etapa 1 — Identificação dos Atores

- Usuário legítimo
- Dispositivo IoT com microfone
- Serviço de processamento de voz
- Atacante (gravação falsificada, reprodução de áudio etc.)

Etapa 2 — Identificação das Ações

Os verbos de mitigação são transformados em intenções de requisito:

- proteger
- autenticar
- monitorar
- atualizar
- restringir

Etapa 3 — Identificação dos Objetos

- canal de voz
- comandos de voz
- tráfego de áudio
- credenciais
- políticas de atualização

Etapa 4 — Reescrita e Generalização

“O sistema deve proteger canais de voz em dispositivos IoT contra interceptação, falsificação e uso não autorizado, assegurando a autenticidade dos comandos e a confidencialidade das comunicações.”

Essa formulação dá origem ao padrão de requisito funcional do catálogo, apresentado no Quadro 5.

Quadro 5 - Padrão FRP-SEC-004: Canal de Voz Seguro

FRP-SEC-004: Canal de Voz Seguro
DESCRIÇÃO
O sistema deve proteger canais de voz em dispositivos IoT contra interceptação, falsificação e uso não autorizado, garantindo a autenticidade dos comandos de voz e a confidencialidade das comunicações de áudio.
RACIONAL
Dispositivos IoT com microfones integrados, como assistentes virtuais, brinquedos inteligentes e eletrodomésticos com comando de voz, são suscetíveis a ataques como voz intrusa ou mascaramento de voz. Essas vulnerabilidades podem expor informações privadas e permitir a execução de comandos falsos, comprometendo a privacidade e a segurança do ambiente IoT.
EXEMPLOS DE REQUISITOS
● O sistema deve utilizar **criptografia de ponta a ponta** nas comunicações de voz. ● O sistema deve implementar **autenticação robusta de voz** para validar a identidade dos usuários. ● O sistema deve monitorar **tráfego de voz em rede** para identificar atividades suspeitas. ● O sistema deve aplicar **atualizações de segurança** regularmente para corrigir vulnerabilidades conhecidas. ● O sistema deve implementar **controle de acesso** para restringir interações de voz apenas a usuários autorizados.
EXEMPLOS DE APLICAÇÃO
● Smart speakers (Google Home, Amazon Echo) que validam comandos de voz antes da execução. ● Brinquedos conectados que usam autenticação de voz para impedir interação com estranhos.

CONSIDERAÇÕES DE IMPLEMENTAÇÃO E TESTE
Implementação: criptografia TLS para tráfego de voz, integração com *Voice Biometric* para verificar a identidade de uma pessoa cadastrada, políticas de controle de acesso baseadas em identidade. **Teste:** simulação de spoofing de voz, testes com gravações reproduzidas para falsificar comandos de voz, inspeção de tráfego para identificar interceptações.

Fonte: Elaborado pelo autor

A vulnerabilidade **Canal de Voz** foi alocada no domínio *Spoofing* porque seu mecanismo de exploração central consiste na falsificação da identidade do emissor do comando de voz. O atacante tenta simular a voz do usuário legítimo — seja via gravação, síntese ou mascaramento — com o objetivo de enganar o dispositivo IoT e induzi-lo a executar ações não autorizadas. Esse comportamento corresponde diretamente à definição STRIDE de *Spoofing*, que envolve assumir a identidade de outra entidade para obter acesso ou executar ações ilícitas.

3.5 Materiais

O desenvolvimento do Catálogo STRIDE-IoT utilizou um conjunto de materiais que apoiaram as etapas de análise, modelagem e documentação do projeto. As atividades foram realizadas em um notebook Samsung Galaxy Book3 Ultra, equipado com Intel Core i7 e 32 GB de RAM, fornecendo capacidade computacional adequada para o processamento das fontes, edição de código e geração da documentação. A implementação de scripts auxiliares e automações foi conduzida em Python, utilizando o Visual Studio Code (VS Code) como editor de código principal, devido ao seu suporte integrado a extensões, Git e ferramentas de documentação.

Para o gerenciamento bibliográfico, empregou-se o Zotero, enquanto o Parsif.al foi utilizado na execução do Mapeamento Sistemático da Literatura. O projeto foi versionado por meio do Git e armazenado no GitHub, permitindo rastreabilidade das alterações e controle colaborativo. A modelagem visual dos padrões e de suas relações foi realizada no Draw.io. A documentação final do catálogo foi produzida em

Markdown e estruturada com MkDocs, sendo posteriormente hospedada no Read the Docs, que publica automaticamente o conteúdo e disponibiliza uma plataforma navegável para consulta pública.

4 CATÁLOGO DE REQUISITOS DE SEGURANÇA PARA IOT BASEADO NO MODELO STRIDE

Este capítulo apresenta a estrutura do Catálogo STRIDE-IoT, descrevendo seus tipos de padrões, o modelo visual adotado, a forma de organização por domínios STRIDE e sua implementação em plataforma navegável, finalizando com um exemplo prático de aplicação em um cenário IoT.

4.1 Visão Geral

O **Catálogo STRIDE-IoT**, estruturado para apoiar a aplicação prática dos padrões de requisitos de segurança em sistemas de Internet das Coisas. Construído sobre os conceitos estabelecidos nos capítulos anteriores, o catálogo organiza requisitos funcionais e não funcionais conforme os domínios de ameaça definidos pelo modelo STRIDE e os distribui em uma arquitetura composta por RPGs, FRPs, NFRPs e infraestruturas técnicas de suporte.

A proposta busca fornecer um artefato capaz de sistematizar, rastrear e reutilizar requisitos de segurança, permitindo que equipes de engenharia derivem soluções coerentes com as características e limitações dos ambientes IoT. O catálogo tem os níveis de abstrações definidos por (Withall, 2007), sendo:

- **RPGs**: Definem o escopo conceitual de cada domínio STRIDE
- **FRPs**: Padrões de requisitos funcionais — descrevem comportamentos concretos do sistema
- **Infraestruturas de suporte**: Interface do domínio com os serviços e tecnologias necessárias para implementar os FRPs;
- **NFRPs**: Padrões de requisitos NÃO funcionais — descrevem restrições, limitações e propriedades transversais. Atuam de forma transversal, impondo restrições arquitetônicas, infraestruturais e físicas que moldam a implementação dos requisitos em sistemas IoT.

4.2 Templates dos Padrões STRIDE-IoT

O catálogo STRIDE-IoT foi estruturado a partir de um modelo de documentação padronizado, projetado para garantir consistência, clareza e reutilização entre diferentes tipos de padrões.

Essa abordagem assegura que cada elemento — do conceito mais abstrato ao requisito aplicado — siga uma mesma lógica descritiva, facilitando sua compreensão e aplicação, facilitando a atualização de novos padrões no futuro.

Os templates adotados representam o formato dos padrões do catálogo e foram inspirados na proposta de (Withall, 2007), adaptada ao contexto de segurança em sistemas IoT.

4.2.1 Template do Requirement Pattern Group

O RPG representa o nível mais abstrato do catálogo STRIDE-IoT. Ele define o propósito central de um conjunto de requisitos de segurança e atua como um modelo genérico, sobre o qual os FRPs e NFRPs são derivados.

Na prática, o RPG funciona como um agrupador conceitual — estabelece diretrizes, princípios e escopo de aplicação, mas não se manifesta diretamente como um padrão de requisito. Seu papel é organizar e dar coesão aos FRPs que tratam de um mesmo tipo de ameaça STRIDE.

Cada RPG contém três campos principais:

- Descrição: Explica o objetivo e a natureza do grupo de requisitos;
- Racional: Justifica sua importância dentro do domínio de segurança;
- Aplicabilidade: Indica em quais contextos o grupo deve ser utilizado.

Exemplo de um RPG do catálogo STRIDE-IoT no Quadro 6 a seguir:

Quadro 6 - RPG-SEC-S01: Autenticação & Verificação de Identidade

RPG-SEC-S01: Autenticação & Verificação de Identidade
Descrição
Define os princípios de autenticação e verificação de identidade em sistemas IoT, assegurando que apenas entidades legítimas — usuários, dispositivos ou serviços — possam acessar recursos e interagir de forma segura.

Racional
A autenticação inadequada permite que atacantes falsifiquem identidades e comprometam o ecossistema IoT. Este grupo estabelece diretrizes para fortalecer a validação de identidade, reduzir o uso de credenciais inseguras e garantir confiança entre componentes conectados.
Aplicabilidade
Utilizado em sistemas e dispositivos que exigem autenticação de usuários, administradores ou comunicações entre dispositivos (M2M).

Fonte: Elaborado pelo autor

O template do RPG permite definir o propósito conceitual de cada categoria de segurança, servindo como ponto de partida para a derivação de padrões de requisitos (FRPs). Essa estrutura ajuda a manter consistência e coerência entre os domínios STRIDE e suas respectivas especializações.

4.2.2 Template do Functional Requirement Pattern

O FRP é a unidade concreta do catálogo. Cada FRP traduz um objetivo de segurança em um requisito observável, aplicável e verificável, derivado de um RPG e instanciado para o contexto IoT.

O template do FRP foi desenvolvido para manter equilíbrio entre clareza descritiva e aplicabilidade técnica, permitindo que analistas o utilizem diretamente na especificação de sistemas, validação de conformidade ou auditorias de segurança.

Cada FRP contém os seguintes campos:

- Identificador e Título: Código único e nome descritivo do requisito.
- Criticidade (CVSS 4.0): Pontuação entre 0.0 e 10.0 baseada no *Common Vulnerability Scoring System* versão 4.0, calculada conforme o impacto potencial da ausência do requisito.
- Descrição: Define o comportamento esperado do sistema.
- Racional: Explica a importância e o risco de não implementação.
- Exemplos de Requisitos: Detalha as ações, mecanismos ou políticas que materializam o requisito.

- Exemplos de Aplicação: Descreve cenários práticos de uso.
- Considerações de Implementação e Teste: Recomenda práticas, técnicas ou validações associadas.

Esse template foi utilizado para a definição de todos os padrões de requisitos, o que ajuda a manter a coerência documental, permitindo uma leitura modular do.

Exemplo de padrão de requisito do catálogo STRIDE-IoT, no Quadro 7 a seguir:

Quadro 7 - FRP-SEC-059: Monitoramento Ativo de Dispositivos IoT

FRP-SEC-059: Monitoramento Ativo de Dispositivos IoT
CVSS: 10.0 — Crítico
Descrição
O sistema deve implementar monitoramento ativo e contínuo de dispositivos IoT, registrando atividades e detectando comportamentos suspeitos em tempo real, para garantir visibilidade, rastreabilidade e resposta rápida a incidentes de segurança.
Racional
Sem monitoramento ativo, é impossível garantir a detecção de anomalias ou ataques em dispositivos IoT, comprometendo a capacidade de auditoria, atribuição de responsabilidades e prevenção de ameaças.
Exemplos de Requisitos
● Implementar monitoramento contínuo de desempenho e segurança. ● Aplicar técnicas de detecção de anomalias e análise comportamental. ● Centralizar logs e auditorias em repositório seguro. ● Emitir alertas em tempo real sobre incidentes. ● Manter políticas de segurança atualizadas conforme normas e boas práticas.
Exemplos de Aplicação
● Gateways IoT com monitoramento centralizado de logs e alertas automáticos de intrusão. ● Plataformas industriais com análise de comportamento anômalo em sensores conectados.
Considerações de Implementação e Teste

- Implementação: integração com sistemas SIEM, uso de IDS/IPS, técnicas de machine learning para detecção de anomalias e dashboards centralizados de monitoramento.
- Teste: simulação de incidentes para validação de alertas, auditoria de logs de dispositivos e testes de correlação de eventos em ambientes de sandbox.

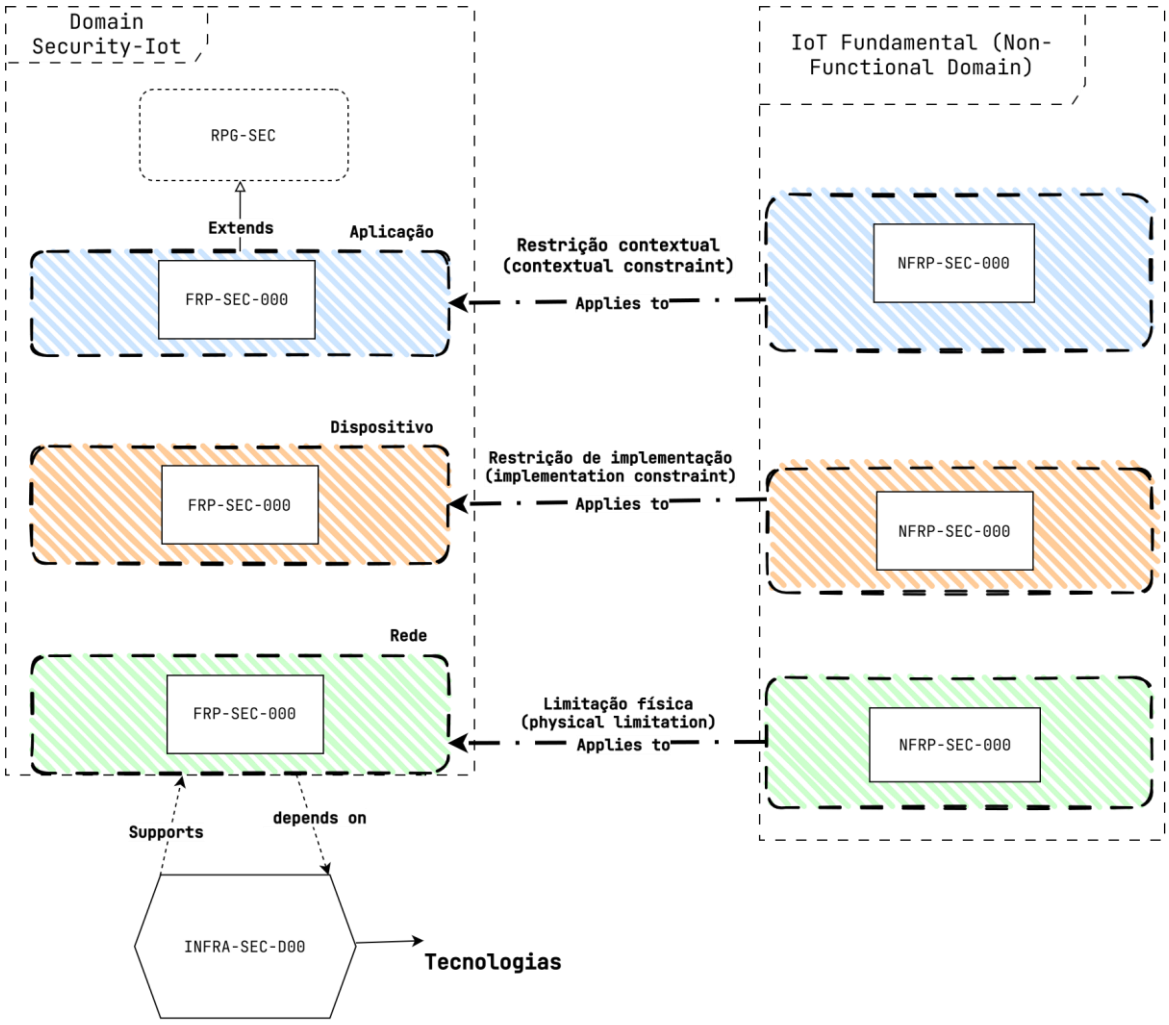
Fonte: Elaborado pelo autor

4.3 Modelo Visual do Catálogo STRIDE-IoT

A estrutura visual do catálogo foi desenvolvida para tornar explícitas as relações entre os diferentes tipos de padrões — conceituais, concretos, infraestruturais e não funcionais, seguindo o modelo de representação sugerido por (Withall, 2007). Mais detalhes sobre essas estruturas visuais estão no Apêndice A. A partir dessa abordagem gráfica, é possível compreender, em uma única visão, como os requisitos são organizados por domínio STRIDE, como cada padrão se relaciona com os demais, e quais elementos tecnológicos dão suporte à sua implementação.

A Figura 5, apresenta a visão geral do modelo adotado neste trabalho. O diagrama sintetiza a hierarquia entre NFRPs, RPGs, FRPs e infraestruturas IoT, organizados segundo as três camadas típicas de sistemas IoT (aplicação, dispositivo e rede).

Figura 5 - Visão Geral do Modelo STRIDE-IoT



Fonte: Elaborado pelo autor

À direita da representação principal (*Domain Security-IoT*), localiza-se o IoT *Fundamental Domain*, composto pelos NFRPs responsáveis por impor restrições transversais a todos os domínios STRIDE. Essas restrições são expressas visualmente pelas conexões do tipo *Applies to* e influenciam a implementação dos requisitos funcionais em três níveis distintos:

- Camada de Aplicação, limitando lógica de negócio. Como frequência de autenticação, complexidade criptográfica e padrões de troca de mensagens.

- Camada de Dispositivo, abrangendo limitações de *hardware*, energia, armazenamento, processamento e interfaces de acesso.

- Camada de Rede, representando fatores como alcance, interferência, variação de sinal, disponibilidade do enlace e a natureza inerente das redes sem fio utilizadas por dispositivos IoT.

Acima dos FRPs, o diagrama posiciona os RPGs, que realizam a organização conceitual dos requisitos por categoria de ameaça STRIDE. Cada RPG opera como um agrupamento abstrato que descreve a intenção e o escopo dos requisitos daquele domínio. Os FRPs, distribuídos nas camadas IoT, representam os padrões funcionais concretos, e todos eles estendem (*Extends*) o RPG de origem — relação indicada pela linha sólida. Essa estrutura expressa a herança semântica entre padrões: o FRP transforma a intenção abstrata do RPG em um padrão de requisito funcional.

Na base de cada domínio STRIDE aparece um losango, que representa a Infraestrutura IoT de Suporte. Essa infraestrutura funciona como uma interface tecnológica necessária para viabilizar os FRPs, oferecendo mecanismos e capacidades que permitam sua implementação. A dependência entre domínio e infraestrutura é representada pela linha tracejada grossa *Supports* e *depends on*, indicando que os requisitos daquele domínio dependem dessa base tecnológica para serem executáveis.

Essas camadas e relações formam um modelo integrado que evidencia como restrições fundamentais, padrões conceituais, requisitos concretos, infraestruturas tecnológicas e arquitetura IoT se articulam na construção do catálogo.

4.4 Organização por Domínios STRIDE

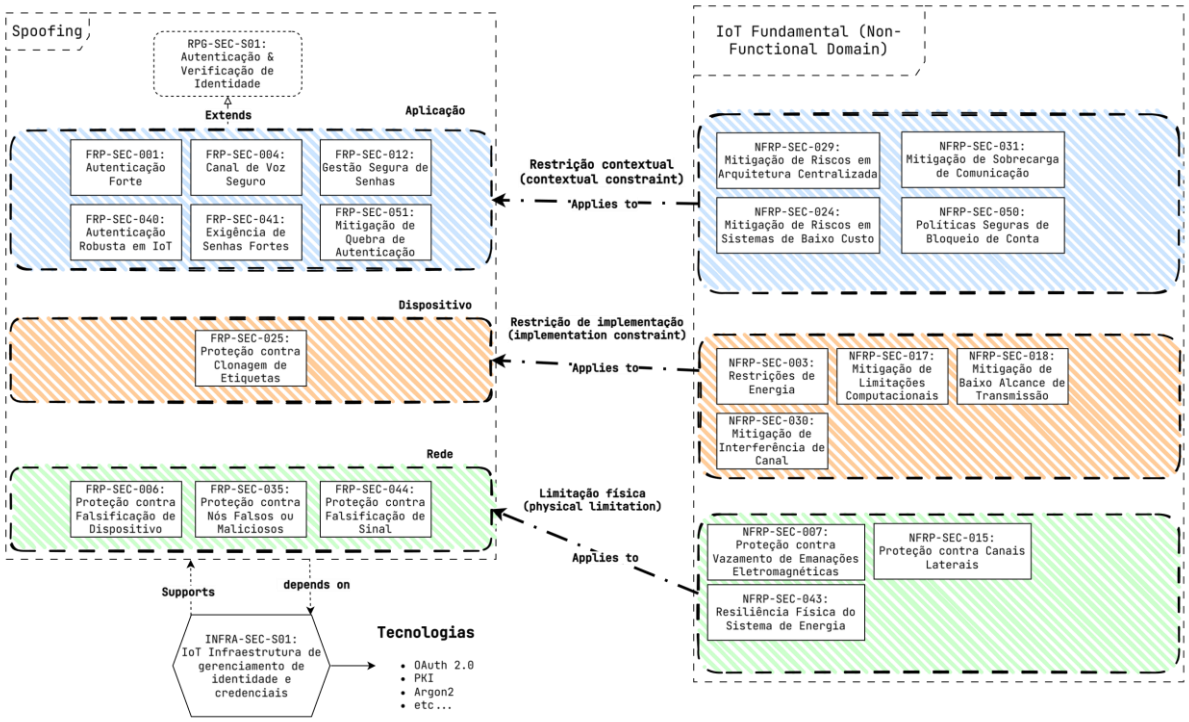
O Catálogo STRIDE-IoT é estruturado em seis domínios, correspondentes às classes de ameaça do modelo STRIDE. Cada domínio reúne um conjunto próprio de padrões de requisitos. Esses domínios aplicam a estrutura conceitual descrita nas seções anteriores — RPG, FRP, NFRP, infraestrutura e restrições transversais — de forma especializada para cada tipo de ameaça. A seção seguinte apresenta cada

domínio STRIDE, acompanhado de seu diagrama, padrões associados e relações internas.

4.4.1 Spoofing

A Figura 6, apresenta a organização do domínio *Spoofing* dentro do catálogo, destacando seu RPG central, seus FRPs associados e a infraestrutura que o suporta. Esse domínio abrange ataques em que um agente mal-intencionado tenta assumir a identidade de outro usuário, dispositivo ou serviço, explorando falhas de autenticação e mecanismos frágeis de verificação de identidade. Em sistemas IoT, onde entidades frequentemente se comunicam de forma autônoma e distribuída, ataques dessa natureza podem comprometer desde a privacidade do usuário até a integridade de serviços críticos.

Figura 6 - Estrutura do Domínio Spoofing no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

O **RPG-SEC-S01: Autenticação & Verificação de Identidade**, define que os princípios conceituais necessários para garantir que apenas entidades legítimas

possam acessar recursos e interagir com a infraestrutura IoT. Esse RPG define características para validação de identidade, prevenção de credenciais inseguras e fortalecimento da confiança entre componentes — humanos ou não — conectados ao ecossistema.

A partir desse RPG, são definidos os **FRPs**, que especializam essas diretrizes e as convertem em requisitos funcionais concretos aplicáveis às diferentes camadas IoT. Entre eles, destacam-se:

- **FRP-SEC-041 – Exigência de Senhas Fortes**, que estabelece critérios rigorosos de criação e manutenção de senhas;
- **FRP-SEC-004 – Canal de Voz Seguro**, aplicável a dispositivos com interfaces de áudio suscetíveis a falsificação de comandos;
- **FRP-SEC-012 – Gestão Segura de Senhas**, que detalha práticas de gerenciamento, armazenamento e renovação de credenciais;
- **FRP-SEC-040 – Autenticação Robusta em IoT**, voltado à verificação forte de dispositivos, usuários e serviços;
- **FRP-SEC-051 – Mitigação de Quebra de Autenticação**, que trata da proteção contra ataques ao processo de autenticação;
- **FRP-SEC-025 – Proteção contra Clonagem de Etiquetas**, voltado a dispositivos com RFID/NFC;
- **FRP-SEC-006 – Proteção contra Falsificação de Dispositivo**, que reforça o controle de identidade de dispositivos na rede;
- **FRP-SEC-035 – Proteção contra Nós Falsos ou Maliciosos**, que impede a inserção de dispositivos ilegítimos na malha IoT;
- **FRP-SEC-044 – Proteção contra Falsificação de Sinal**, garantindo que apenas transmissões autênticas sejam aceitas.

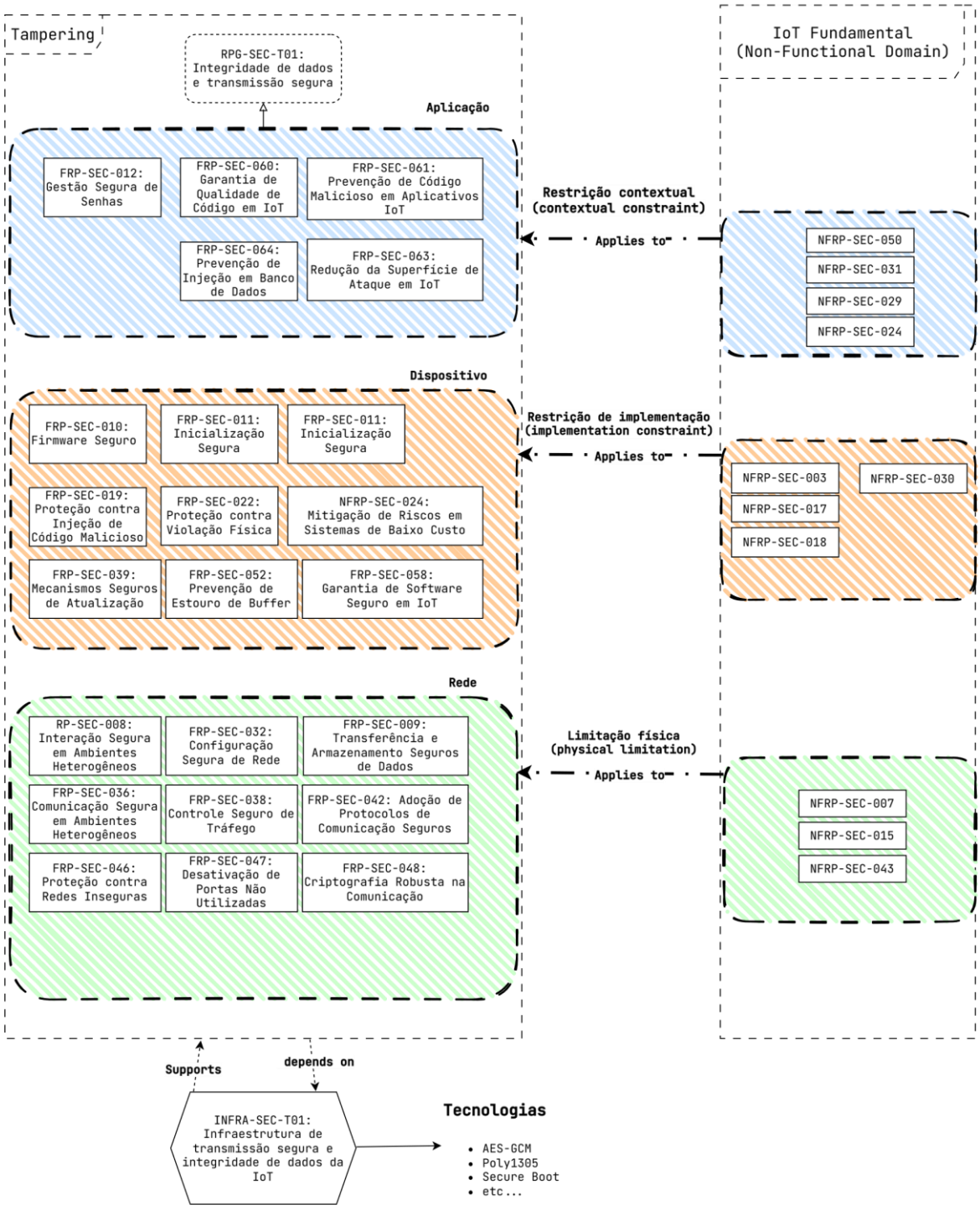
Esses FRPs especializam o RPG por meio da relação **Extends**, incorporando seus princípios e os transformando em FRP aplicáveis às camadas de aplicação, dispositivo e rede, conforme o escopo de cada padrão. A Figura 6 evidencia também

a hierarquia e destaca as restrições transversais provenientes do IoT Fundamental Domain.

4.4.2 Tempering

A Figura 7, apresenta a organização do domínio **Tampering** (Manipulação de Dados). Esse domínio abrange ameaças em que um atacante modifica, insere ou corrompe informações — seja em repouso, em trânsito ou durante processos de atualização — comprometendo a confiabilidade, a rastreabilidade e a tomada de decisão baseada nesses dados.

Figura 7 - Estrutura do Domínio Tampering no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

O domínio é estruturado pelo **INFRA-SEC-T01: Infraestrutura de transmissão segura e integridade de dados da IoT**, que define os princípios conceituais para garantir que informações coletadas, processadas e transmitidas

permaneçam autênticas, íntegras e protegidas contra adulteração. Esse RPG orienta a proteção do ciclo de vida completo dos dados, incluindo armazenamento, *firmware*, *software* e comunicação entre dispositivos, *gateways* e serviços em nuvem.

A partir desse RPG, são definidos os FRPs que especializam essas diretrizes e as convertem em padrões requisitos funcionais concretos aplicáveis às diferentes camadas IoT. Dentre os principais FRPs associados ao domínio, destacam-se:

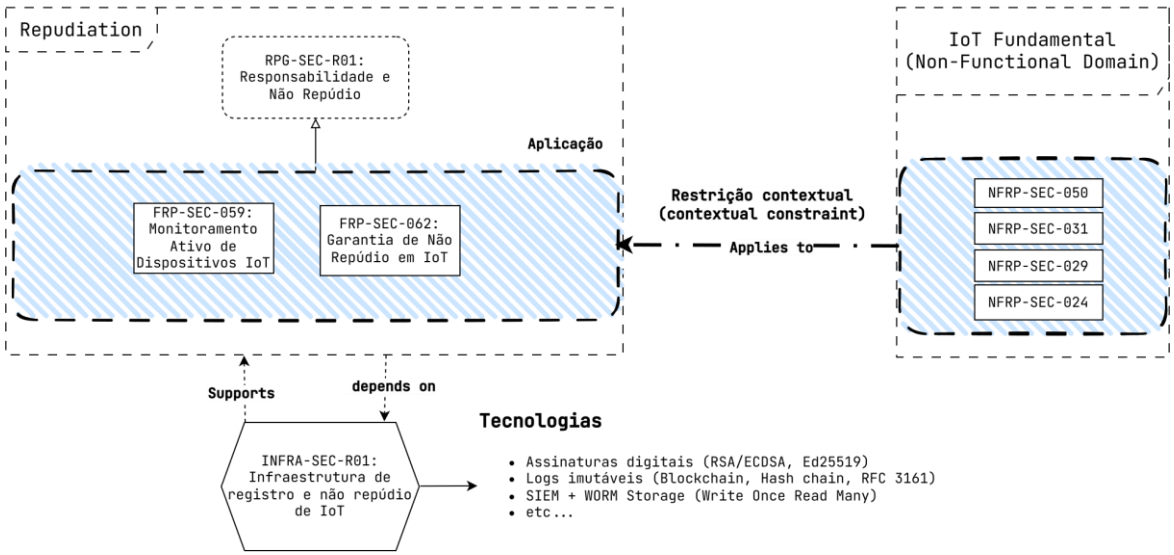
- **FRP-SEC-053 – Garantia de Consistência de Dados**, que estabelece mecanismos de validação, redundância e monitoramento contínuo para evitar inconsistências e corrupção de dados;
- **FRP-SEC-060 – Garantia de Qualidade de Código em IoT**, voltado a práticas de desenvolvimento seguro, revisão de código e testes de segurança para reduzir vulnerabilidades que possam levar à adulteração de dados;
- **FRP-SEC-061 – Prevenção de Código Malicioso em Aplicativos IoT**, que restringe a introdução e execução de software não confiável;
- **FRP-SEC-064 – Prevenção de Injeção em Banco de Dados**, que protege contra injeções e manipulação maliciosa de consultas;
- **FRP-SEC-010 – Firmware Seguro** e **FRP-SEC-011 – Inicialização Segura**, que abordam a integridade do firmware e do processo de boot em dispositivos IoT;
- **FRP-SEC-039 – Mecanismos Seguros de Atualização**, que garantem que atualizações de firmware e software sejam autenticadas, íntegras e protegidas contra adulteração;
- **FRP-SEC-052 – Prevenção de Estouro de Buffer**, que reduz riscos de corrupção de memória e, consequentemente, de manipulação de dados e fluxo de execução.

Na base do domínio encontra-se a interface, responsável por fornecer os mecanismos técnicos necessários à execução desses requisitos, como suporte a verificação de integridade, canais de comunicação confiáveis, validação de *firmware* e proteção de armazenamento.

4.4.3 Repudiation

A Figura 8, apresenta a organização do domínio *Repudiation* (Negação de Ações). Esse domínio abrange ameaças em que usuários, dispositivos ou serviços tentam negar a autoria de comandos, operações ou registros, mesmo após tê-los executado. Em sistemas IoT, essa ameaça é crítica, pois compromete diretamente a responsabilidade técnica, a auditabilidade e a confiabilidade das decisões automatizadas.

Figura 8 - Estrutura do Domínio Repudiation no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

No catálogo, o domínio é estruturado pelo **RPG-SEC-R01: Responsabilidade e Não Repúdio**, que define os princípios conceituais que garantem que ações realizadas no sistema possam ser autenticadas, registradas, verificadas e, sobretudo, não possam ser posteriormente negadas. Esse RPG consolida diretrizes de registro seguro, assinatura digital, preservação de evidências e fortalecimento da rastreabilidade em ambientes distribuídos.

A partir desse RPG, são definidos os **FRPs** que especializam suas diretrizes e as convertem em padrões de requisitos funcionais concretos aplicáveis às camadas de aplicação, dispositivo e rede. Entre os principais FRPs do domínio, conforme documentado no catálogo, destacam-se:

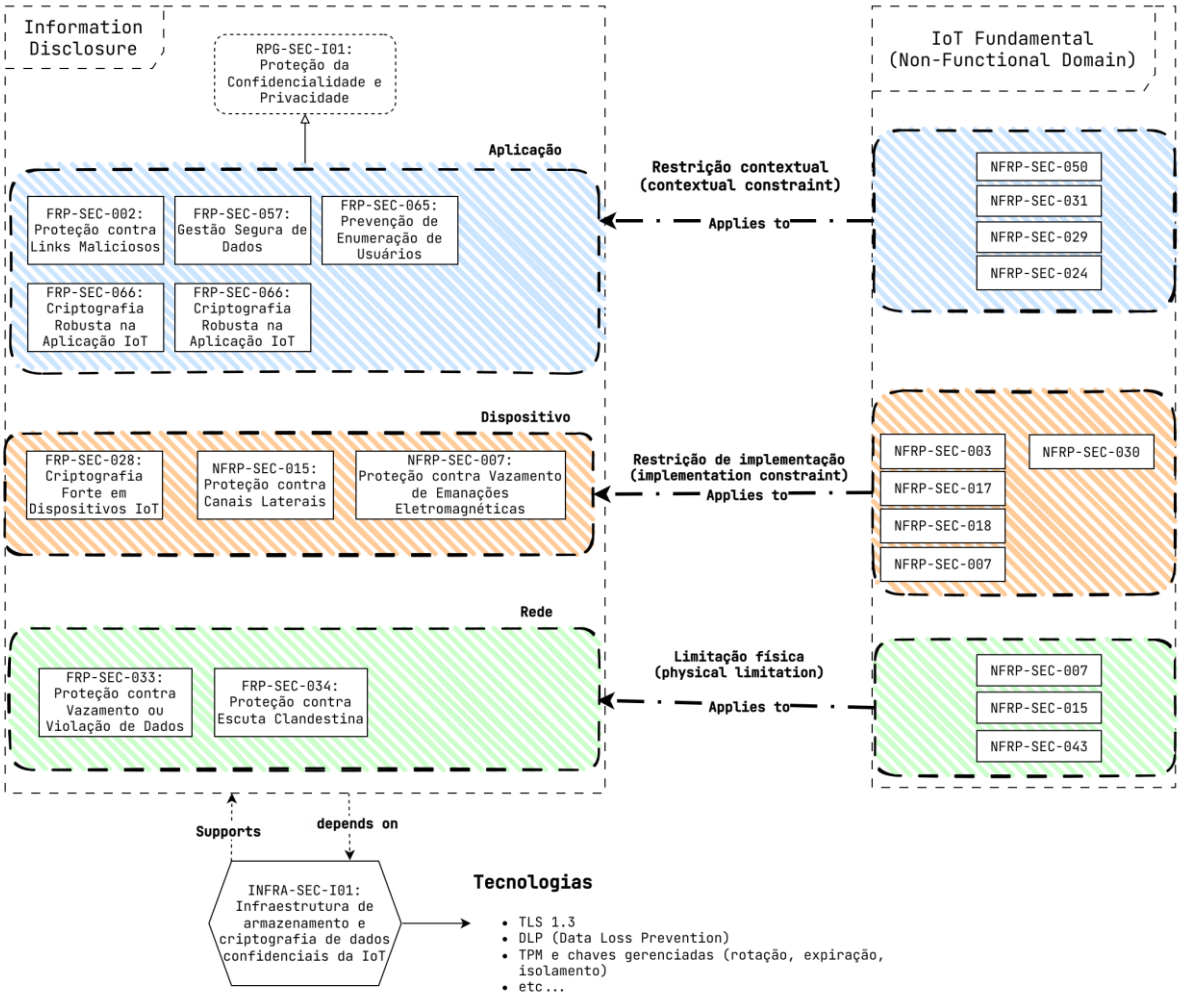
- **FRP-SEC-059 – Monitoramento Ativo de Dispositivos IoT**, que garante rastreabilidade contínua ao registrar atividades, detectar comportamentos suspeitos e manter visibilidade operacional;
- **FRP-SEC-062 – Garantia de Não Repúdio em IoT**, que exige assinatura digital, autenticação forte e comunicação segura para impedir a negação de ações;
- **FRP-SEC-065 – Assinatura de Comandos**, que assegura autenticidade, integridade e atribuição inequívoca da origem de comandos enviados a dispositivos;
- **FRP-SEC-070 – Preservação de Evidências de Auditoria**, que mantém registros protegidos contra adulteração e com validade jurídica;
- **FRP-SEC-048 – Registro Seguro de Eventos**, voltado à criação de logs robustos, íntegros e resistentes a manipulação;
- **FRP-SEC-082 – Controle de Acesso Baseado em Ações Registradas**, que associa permissões ao histórico verificável das atividades realizadas.

A infraestrutura associada, **INFRA-SEC-R01: Infraestrutura de registro e não repúdio de IoT**, fornece os mecanismos técnicos necessários para viabilizar os FRPs, incluindo trilhas imutáveis de auditoria, autenticação forte, carimbos de tempo confiáveis, sincronização segura de logs e suporte a assinaturas digitais.

4.4.4 Information Disclosure

A Figura 9, apresenta a estrutura do domínio *Information Disclosure* (Exposição de Informação). Esse domínio abrange ameaças relacionadas à exposição, interceptação ou obtenção indevida de informações sensíveis — tanto em repouso quanto em trânsito — comprometendo a privacidade, a segurança operacional e a conformidade regulatória dos sistemas IoT.

Figura 9 - Estrutura do Domínio Information Disclosure no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

O domínio é estruturado pelo **RPG-SEC-I01: Proteção da Confidencialidade e Privacidade**, que consolida os princípios conceituais necessários para garantir que dados sensíveis sejam protegidos ao longo de todo o ciclo de vida. Esse RPG reúne diretrizes relacionadas à criptografia, proteção de dados pessoais, controle de acesso,

limitação de coleta, prevenção a vazamentos e monitoramento de práticas de privacidade.

A partir desse RPG, derivam-se os **FRPs,** distribuídos nas camadas de aplicação, dispositivo e rede. Entre os principais FRPs associados ao domínio, destacam-se:

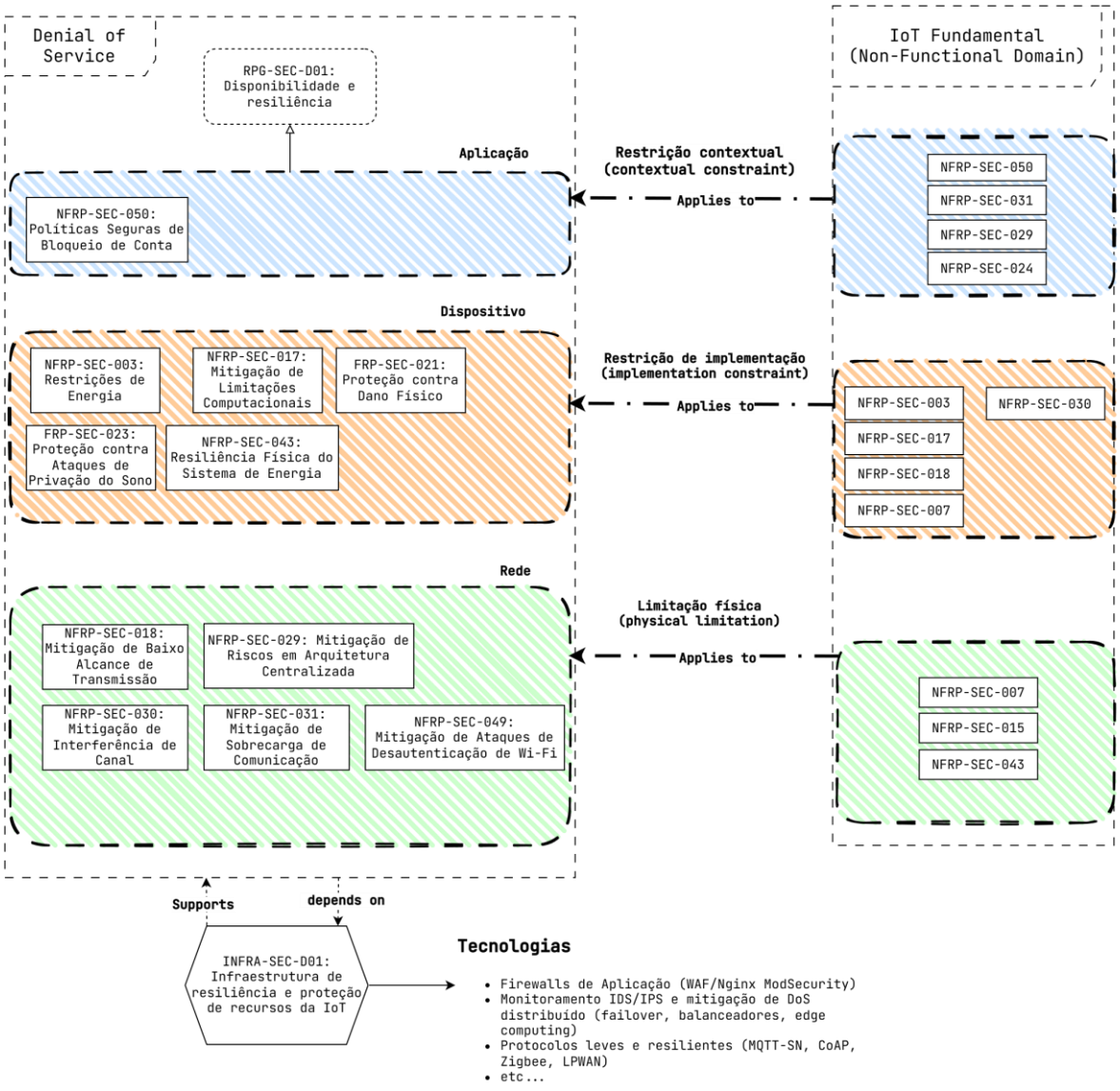
- **FRP-SEC-091 – Criptografia em Repouso e Trânsito**, que define requisitos para proteger dados armazenados e transmitidos, evitando acesso indevido mesmo em caso de interceptação;
- **FRP-SEC-092 – Minimização de Dados**, que exige a coleta apenas do estritamente necessário, reduzindo superfícies de exposição;
- **FRP-SEC-041 – Proteção contra Vazamento de Dados**, que estabelece mecanismos preventivos e corretivos para evitar exfiltração de informações;
- **FRP-SEC-053 – Gestão de Dados Pessoais em IoT**, que orienta o tratamento seguro e consentido de informações sensíveis;
- **FRP-SEC-063 – Controle de Acesso Baseado em Papeis**, que assegura que usuários e dispositivos acessem somente o necessário;
- **FRP-SEC-014 – Canal Seguro entre Dispositivos**, que garante comunicação autenticada e criptografada na malha IoT;
- **FRP-SEC-057 – Detecção de Vazamento de Dados**, que estabelece mecanismos de monitoramento e resposta a incidentes de privacidade.

A infraestrutura que sustenta esse domínio, representada pela **INFRA-SEC-I01: Infraestrutura de armazenamento e criptografia de dados confidenciais da IoT**, provê os mecanismos técnicos necessários para implementação dos FRPs. Ela inclui serviços de criptografia, armazenamento protegido, gerenciamento de chaves, controles de acesso e mecanismos de prevenção a vazamentos.

4.4.5 Denial of Service

A Figura 10, apresenta a organização do domínio *Denial of Service* (Negação de Serviço - DoS). O domínio abrange ameaças cujo objetivo é interromper ou degradar serviços IoT por meio do esgotamento de recursos computacionais, energéticos ou de comunicação. Em sistemas distribuídos, a indisponibilidade gerada por ataques DoS pode comprometer operações, causar falhas e prejudicar a confiabilidade global da arquitetura.

Figura 10 - Estrutura do Domínio Denial of Service no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

No catálogo, o domínio é estruturado pelo **RPG-SEC-D01: Disponibilidade e resiliência**, que define os princípios conceituais necessários para manter a continuidade operacional de dispositivos, redes e serviços IoT. Seu racional enfatiza a necessidade de arquiteturas resilientes, mecanismos de recuperação rápida e defesas contra indisponibilidades causadas por sobrecarga, interferência de canal, falhas físicas ou esgotamento energético.

A partir desse RPG, derivam-se os **FRPs (*Functional Requirement Patterns*)** que especializam suas diretrizes e as convertem em requisitos funcionais concretos aplicáveis às camadas de aplicação, dispositivo e rede. Com base no catálogo, destacam-se:

- **FRP-SEC-021 – Proteção contra Dano Físico**, que busca prevenir indisponibilidade causada por vandalismo, impactos ambientais ou manipulação física de dispositivos;
- **FRP-SEC-023 – Proteção contra Ataques de Privação do Sono**, que impede que dispositivos a bateria sejam mantidos permanentemente ativos por tráfego malicioso, evitando esgotamento energético;
- **NFRP-SEC-049 – Mitigação de Ataques de Desautenticação Wi-Fi**, que protege dispositivos contra desconexões forçadas na camada de rede, preservando disponibilidade e conectividade.

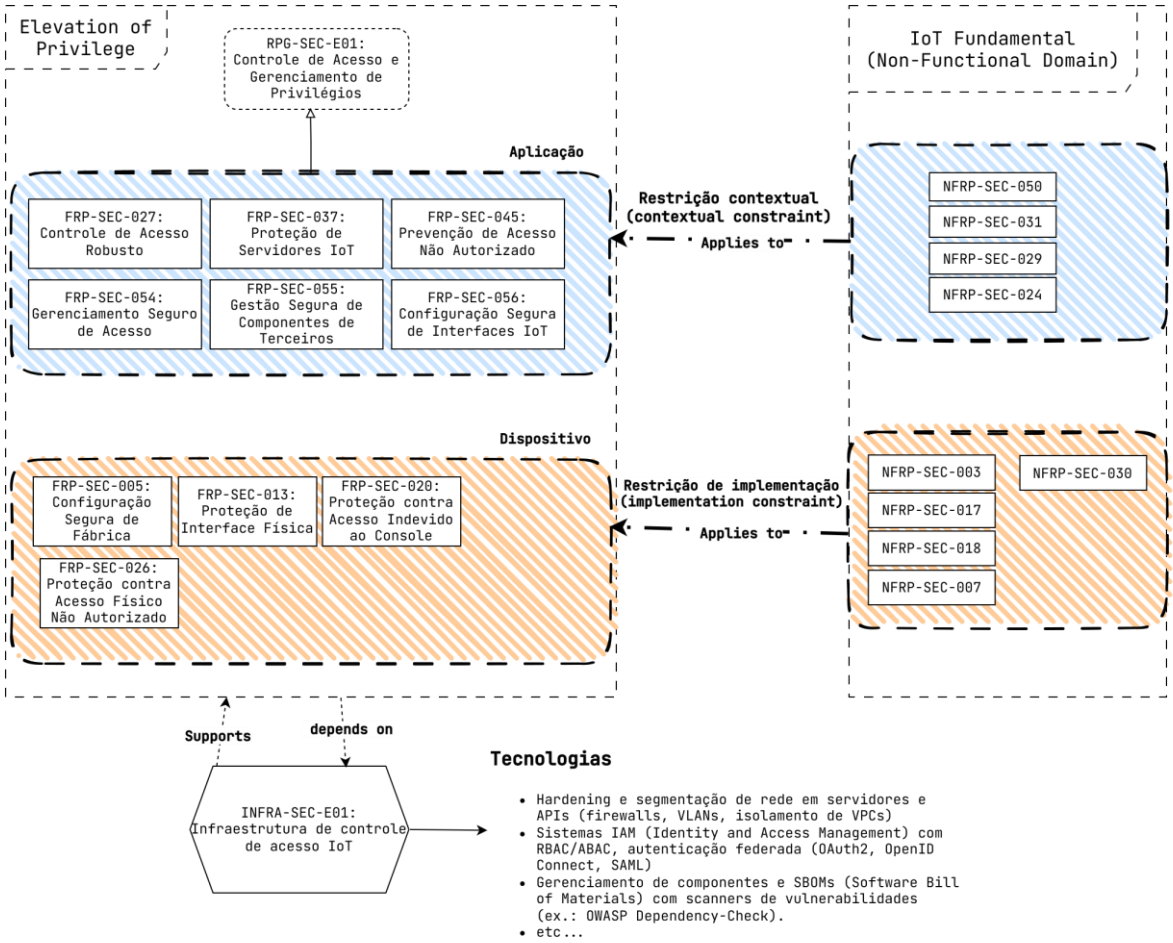
A infraestrutura associada ao domínio, **INFRA-SEC-D01: Infraestrutura de resiliência e proteção de recursos da IoT**, fornece os recursos técnicos necessários para que os FRPs possam ser implementados de forma eficaz. Ela engloba mecanismos de proteção física, sistemas de energia resilientes, detecção de tráfego anômalo, políticas de gerenciamento de energia e controles que evitem o esgotamento de recursos.

4.4.6 Elevation of Privilege

A Figura 11, apresenta a organização do domínio *Elevation of Privilege* (Elevação de Privilégio). Esse domínio abrange situações em que um atacante, inicialmente com permissões limitadas, obtém acesso a níveis superiores de privilégio, passando a executar ações reservadas a operadores ou administradores. Em

sistemas IoT, esse tipo de elevação indevida permite manipular dispositivos, alterar configurações sensíveis, acessar dados confidenciais e comprometer serviços.

Figura 11 - Estrutura do Domínio Elevation of Privilege no Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

Na estrutura do catálogo, esse domínio é representado pelo **RPG-SEC-E01: Controle de Acesso e Gerenciamento de Privilégios**, que consolida os princípios conceituais para assegurar que cada entidade — humana, lógica ou física — opere estritamente dentro do seu escopo autorizado. O RPG define diretrizes relacionadas à segregação de funções, limitação de privilégios, revisão periódica de permissões e prevenção de acessos indevidos, servindo como base conceitual para os padrões desse domínio.

A partir desse RPG, um conjunto de ***Functional Requirement Patterns*** **(FRPs)** especializa essas diretrizes e as converte em requisitos funcionais concretos aplicáveis às diferentes camadas do ecossistema IoT. Entre os principais FRPs, destacam-se:

- **FRP-SEC-071 – Princípio do Menor Privilégio**, que estabelece que cada entidade deve operar apenas com as permissões estritamente necessárias às suas funções;
- **FRP-SEC-073 – Gestão de Sessões, Tokens e Revogação**, que trata do ciclo de vida de sessões ativas, tokens de acesso e revogação de privilégios;
- **FRP-SEC-083 – Monitoramento e Resposta a Incidentes**, voltado à detecção, registro e bloqueio de tentativas de escalonamento de privilégios;
- **FRP-SEC-027 – Controle de Acesso Robusto**, que integra autenticação forte e autorização granular;
- **FRP-SEC-054 – Gerenciamento Seguro de Acesso**, que define políticas de concessão, revisão e remoção de permissões;
- **FRP-SEC-055 – Gestão Segura de Componentes de Terceiros**, prevenindo a introdução de caminhos de privilégio indevido por bibliotecas ou serviços externos;
- **FRP-SEC-056 – Configuração Segura de Interfaces IoT**, que protege consoles, APIs e interfaces administrativas contra uso abusivo;
- **FRP-SEC-005, FRP-SEC-013, FRP-SEC-020 e FRP-SEC-026**, que abordam riscos associados ao acesso físico como vetor para elevação de privilégios.

Na base do domínio encontra-se a **INFRA-SEC-E01: Infraestrutura de controle de acesso IoT**, responsável por fornecer os mecanismos técnicos necessários para aplicar políticas de autorização, validar identidades, gerenciar sessões e isolar funções críticas.

4.5 Desenvolvimento e Disponibilização do Catálogo

Considerando que catálogos tradicionais frequentemente apresentam baixa navegabilidade e dificuldade de consulta, optou-se por desenvolver uma plataforma própria, organizada segundo o modelo STRIDE e alinhada às camadas funcionais da arquitetura IoT.

4.5.1 Ferramentas

A documentação e o versionamento do catálogo foram realizados utilizando as ferramentas:

- GitHub (para versionamento e rastreabilidade do desenvolvimento)
- Markdown (para estruturação textual e legibilidade);
- Mkdocs (para converte arquivos escritos em formato Markdown para um site HTML)
- ReadTheDocs (para publicação e consulta online);
- Draw.io (para modelagem visual das relações RPG–FRP–Infra–NFRP);
- Calculadora CVSS 4.0 (para avaliação da criticidade de cada requisito, com pontuação entre 0.0 e 10.0).

4.5.2 Implementação do Catálogo

A Figura 12, apresenta a tela inicial do Catálogo de Padrões de Requisitos de Segurança para Sistemas IoT.

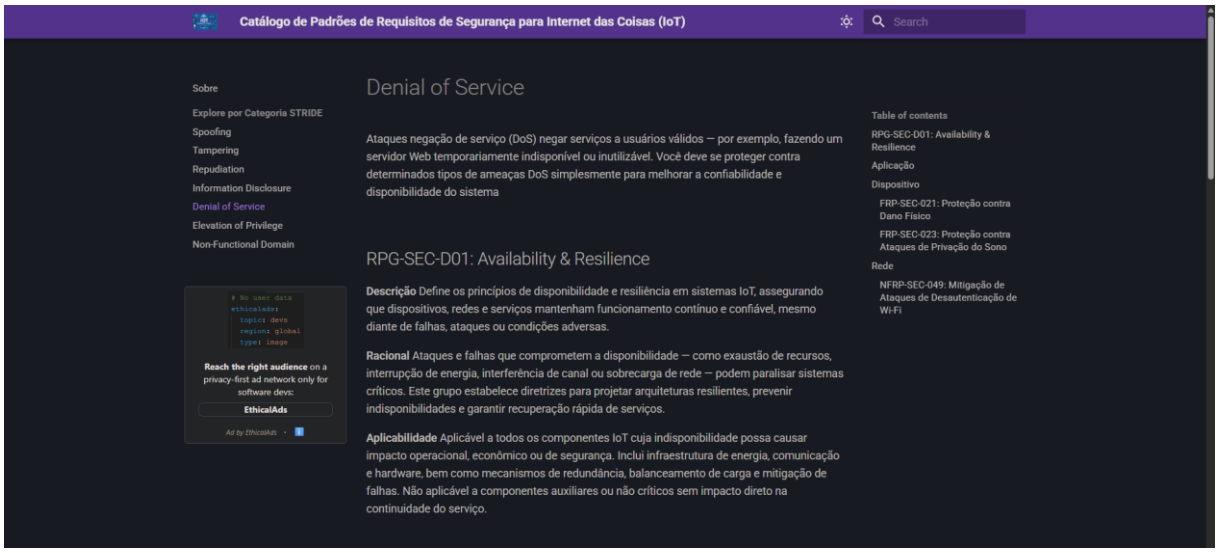
Figura 12 - Catálogo de Padrões de Requisitos de Segurança para Sistemas IoT

Fonte: Elaborado pelo autor

Ao acessar a plataforma, o usuário encontra o menu lateral esquerdo, estão listadas as categorias STRIDE para exploração, ao centro, uma área de apresentação destacando o escopo do catálogo, à direita, um painel de *Table of Contents* que permite navegação pelos tópicos da página.

Ao selecionar uma categoria do menu lateral — por exemplo*, Denial of Service* — a plataforma apresenta todos os elementos pertencentes a esse domínio. No topo da página, o usuário encontra **a definição do domínio STRIDE**, descrevendo o tipo de ameaça abordada e seu impacto em sistemas IoT.

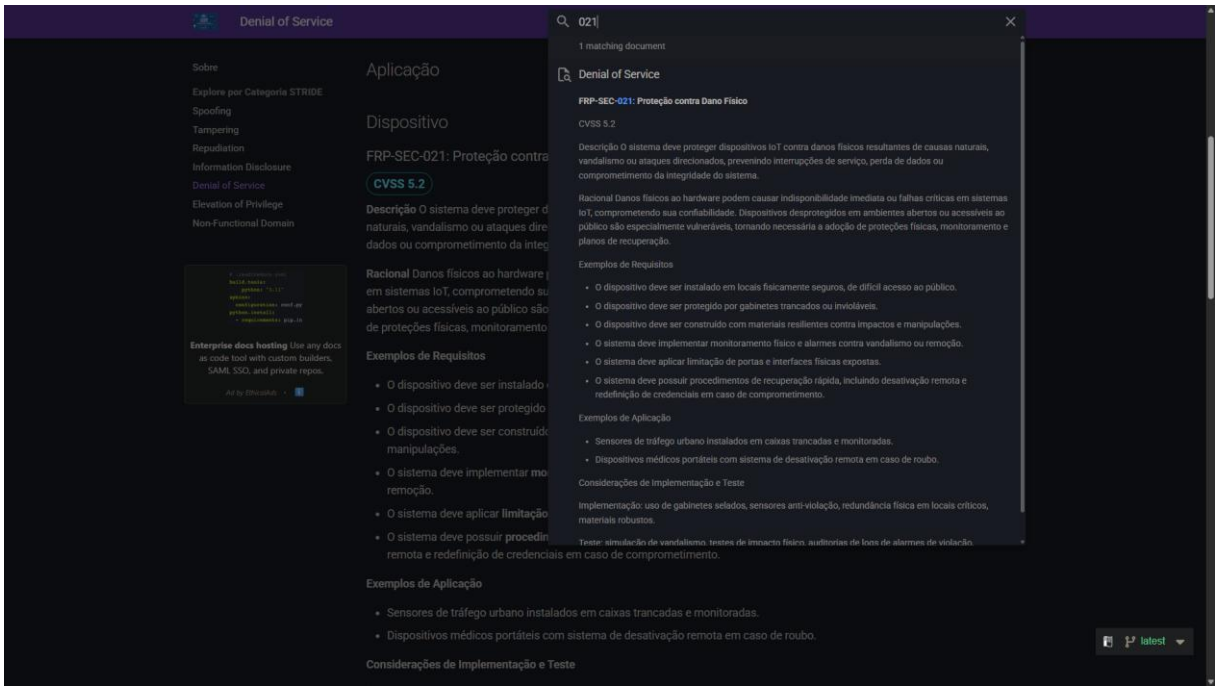
Figura 13 - Página do Domínio DoS



Fonte: Elaborado pelo autor

Em seguida, a plataforma lista os *Functional Requirement Patterns* **(FRPs)** associados ao RPG, organizados por camadas da arquitetura IoT (Aplicação, Dispositivo, Rede). Cada FRP aparece com seu identificador, título e pontuação CVSS, e ao selecionar um deles, o usuário é direcionado a uma seção detalhada contendo descrição, racional, exemplos de requisitos, exemplos de aplicação e considerações de implementação e teste.

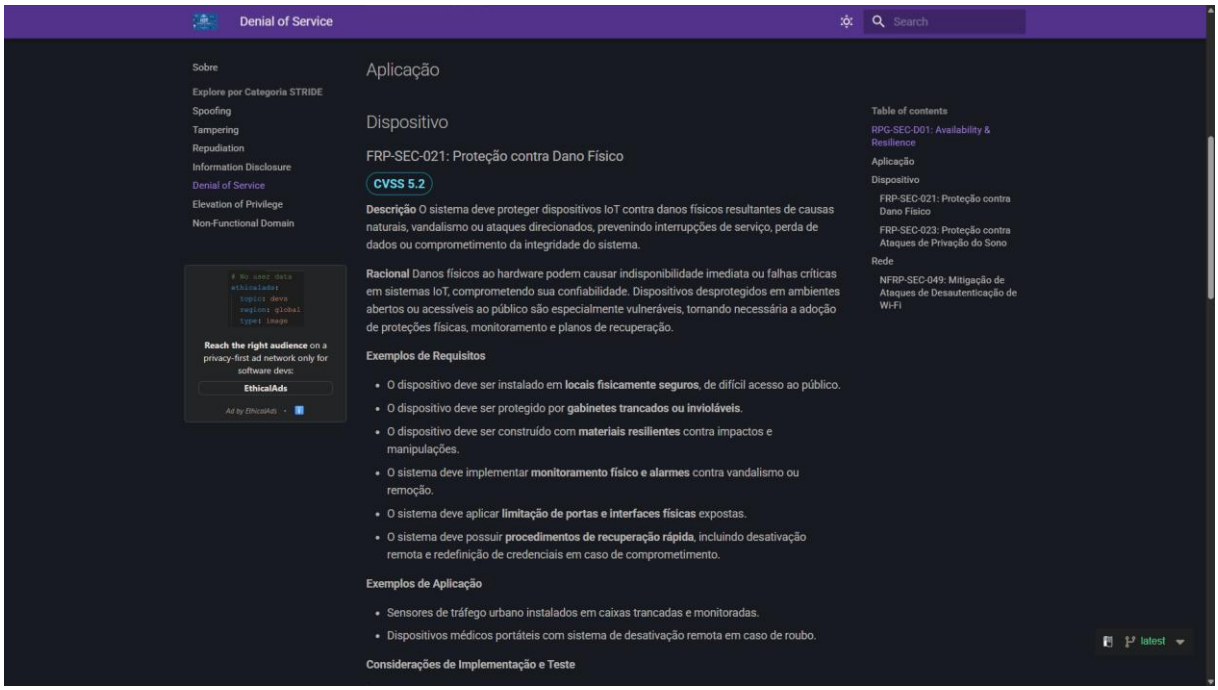
Figura 14 - Fazendo uma busca na plataforma



Fonte: Elaborado pelo autor

Além da navegação pelas categorias STRIDE, a ferramenta também permite pesquisar diretamente qualquer padrão do catálogo por meio do campo de busca localizado no topo da interface. Ao digitar parte do identificador ou do nome de um FRP — por exemplo, “021” para encontrar o *FRP-SEC-021: Proteção contra Dano Físico* — a plataforma apresenta imediatamente o padrão correspondente permitindo localizar requisitos específicos sem a necessidade de percorrer manualmente todas as categorias.

Figura 15 - FRP-SEC-021 – Proteção contra Dano Físico



Fonte: Elaborado pelo autor

Outra funcionalidade importante da plataforma é que, ao clicar em qualquer FRP exibido na interface, o usuário é direcionado para uma seção específica dedicada exclusivamente àquele padrão. Cada FRP possui um *link* único (URL própria), permitindo que o padrão seja compartilhado diretamente com outras pessoas ou equipes, sem a necessidade de percorrer toda a estrutura do catálogo. Dessa forma, um analista pode, por exemplo, enviar apenas o link do FRP-SEC-023 ou FRP-SEC-021 para outro membro da equipe, o que facilita a colaboração e torna o catálogo mais eficiente durante atividades de análise de risco ou definição de requisitos.

A disponibilização foi realizada por meio da plataforma *Read the Docs*, que hospeda gratuitamente a versão mais recente do catálogo. O código do catálogo está disponível no GitHub.

Documentação:

https://iot-security-catalog-requirements.readthedocs.io/pt-br/latest/

Repositório do projeto:

https://github.com/HigorAnjos/iot-security-catalog-requirements

A disponibilização aberta do código do Catálogo STRIDE-IoT garante que ele possa ser acessado, visionado e expandido continuamente, acompanhando a evolução das demandas e ameaças presentes no ecossistema de Internet das Coisas.

4.6 Aplicação Demonstrativa do Catálogo STRIDE-IoT

Para ilustrar o uso prático do catálogo, considere o seguinte cenário. Uma casa inteligente composta por três dispositivos IoT integrados a um *gateway* residencial.

Nesse ambiente, os dispositivos realizam funções automatizadas e comunicam-se entre si e com serviços externos, formando um ecossistema típico de IoT doméstico.

Casa Inteligente com Três Dispositivos IoT

- **Assistente de voz**
    - Dispositivo responsável por interpretar comandos verbais, controlar outros equipamentos da casa e enviar informações para serviços em nuvem.
- **Fechadura inteligente**
    - Dispositivo de controle de acesso à residência, operado por aplicativo, autenticação digital ou comandos via assistente de voz.
- **Sensor de presença conectado ao gateway**

- Dispositivo responsável por detectar movimento e enviar notificações ao sistema central.

A partir da análise do ambiente, podem ser identificadas categorias e ameaças relevantes:

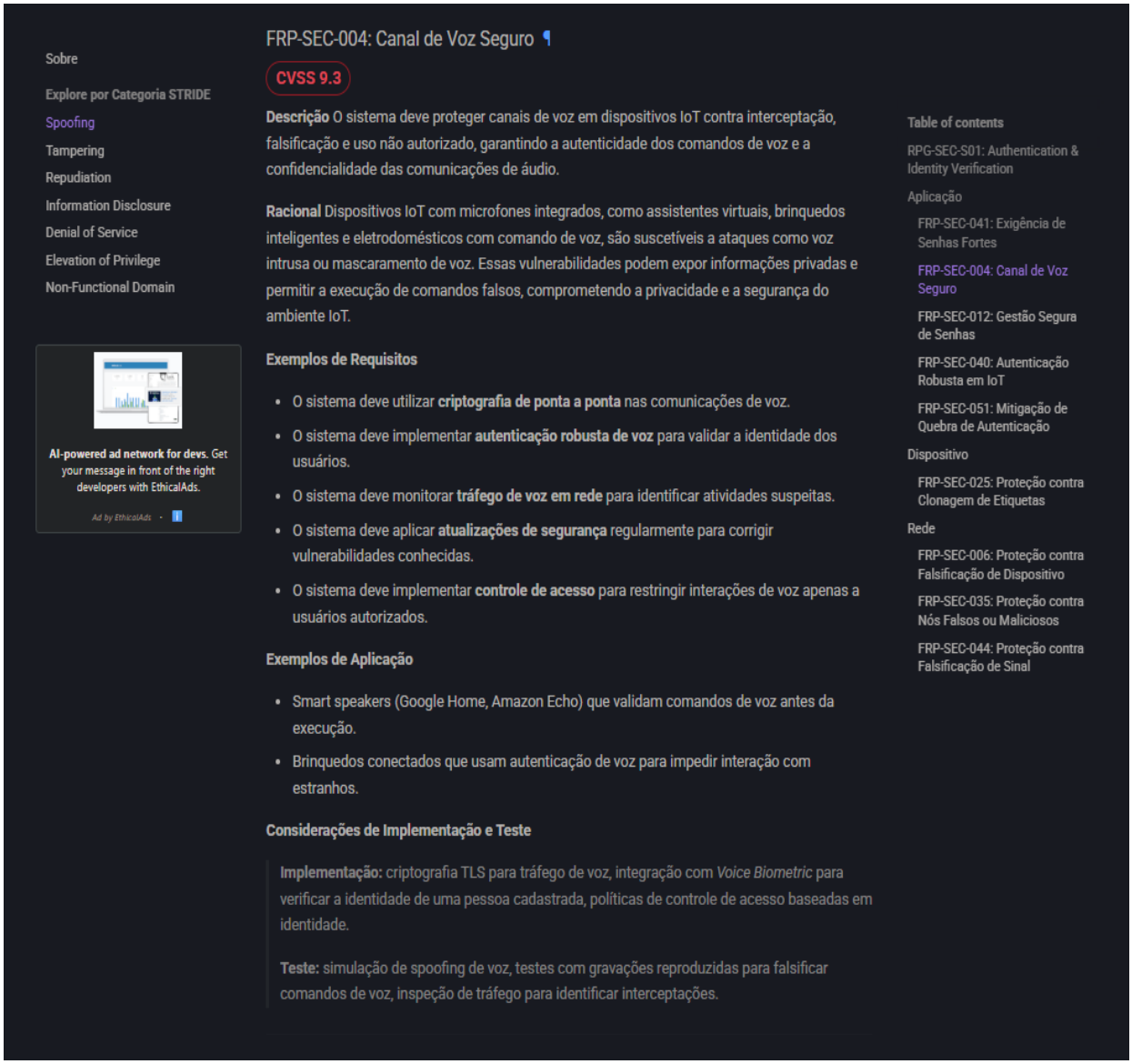
- *Spoofing*: Tentativa de falsificação de comandos de voz ou acesso à fechadura.
- *Tampering*: Adulteração de mensagens enviadas pelo sensor.
- *Information Disclosure*: Interceptação de dados transmitidos pelo *gateway*.
- *Denial of Service*: Sobrecarga do assistente de voz ou do *gateway*.

Com base nas vulnerabilidades identificadas, é possível navegar pelo catálogo e selecionar os padrões de requisitos mais adequados para cada dispositivo. A seguir, apresentam-se exemplos derivados diretamente dos FRPs selecionados.

Assistente de Voz – Canal de Voz Seguro

Esse padrão de requisito trata da proteção dos canais de comunicação baseados em voz, assegurando que os comandos recebidos sejam autênticos e provenientes de usuários legítimos antes de serem executados.

Figura 16 - FRP-SEC-004: Canal de Voz Seguro



Fonte: Elaborado pelo autor

A partir do padrão FRP-SEC-004, podem ser elaborados os seguintes requisitos específicos:

Requisito — Detecção de Voz Falsificada

O sistema deve analisar padrões acústicos em tempo real para identificar tentativas de uso de gravações, vozes sintéticas ou comandos reproduzidos por alto-falantes.

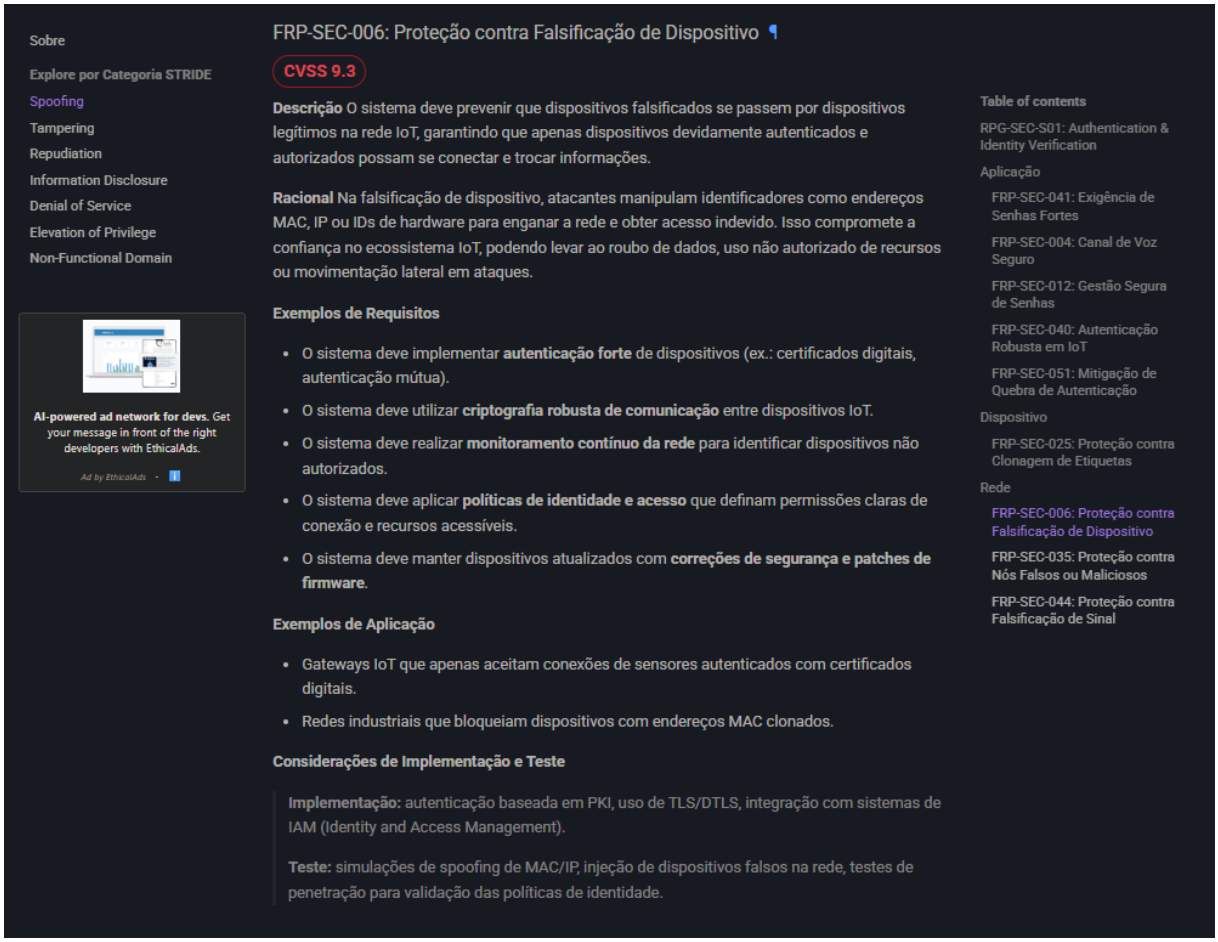
Requisito — Autenticação Biométrica de Voz

O sistema deve empregar autenticação biométrica de voz (*Voice Biometric*) para validar a identidade dos usuários antes da execução de comandos sensíveis.

4.6.1 Fechadura Inteligente – Proteção contra Falsificação de Dispositivo

Este padrão de requisito trata da prevenção contra dispositivos falsificados que tentam se passar por dispositivos legítimos na rede, o que é especialmente relevante no caso de uma fechadura inteligente.

Figura 17 - FRP-SEC-061: Prevenção de Código Malicioso em Aplicativos IoT



Fonte: Elaborado pelo autor

A partir do padrão FRP-SEC-061, podem ser definidos os seguintes requisitos específicos:

Requisito — Comunicação Segura entre Fechadura e Gateway

As comunicações devem utilizar criptografia robusta (TLS, DTLS ou curvas elípticas), prevenindo interceptação e adulteração de mensagens.

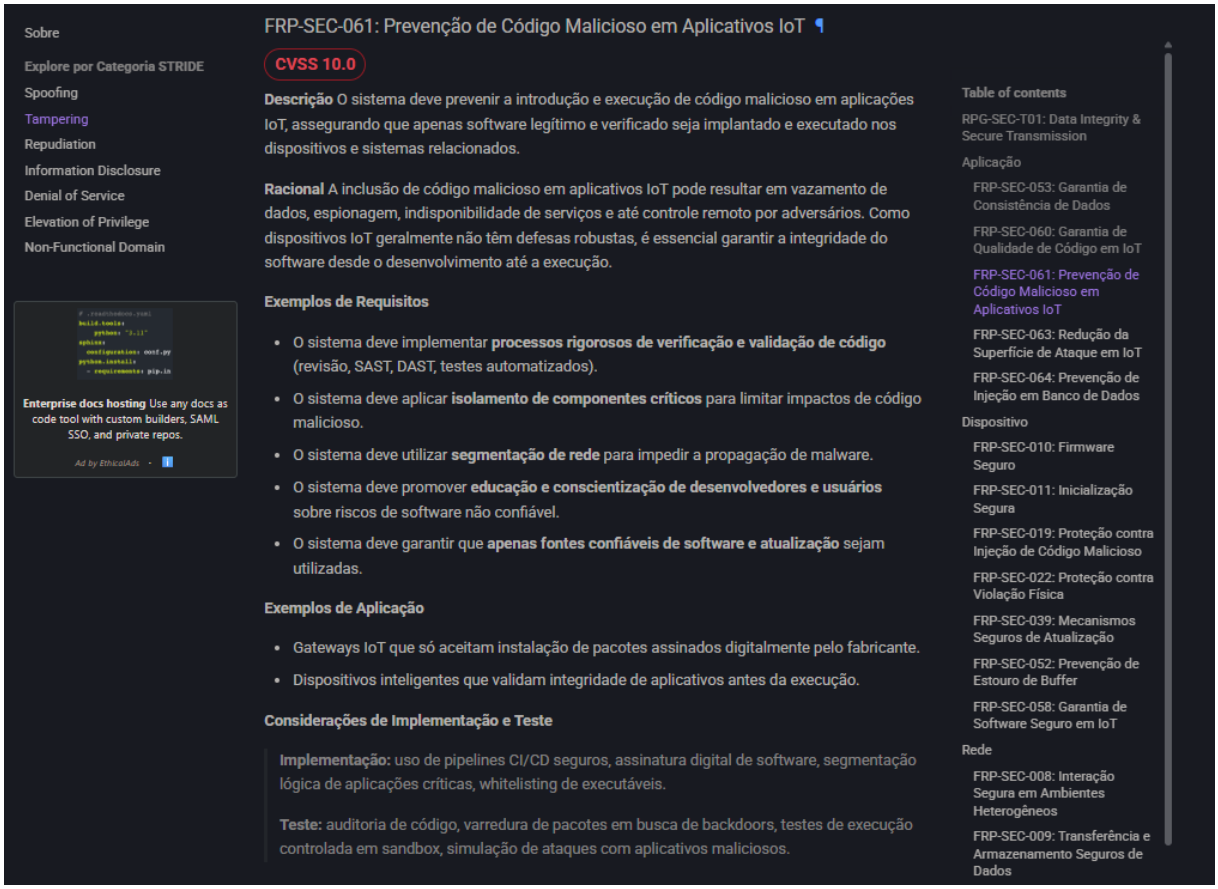
Requisito — Detecção de Dispositivos Não Autorizados

O sistema deve identificar e bloquear tentativas de conexão de dispositivos não autorizados, clonados ou com identificadores falsificados (ex.: MAC *spoofing* ou IDs alterados).

4.6.2 Sensor de Presença – Garantia de Integridade de Dados

Este padrão de requisito trata da prevenção à execução de código malicioso no dispositivo, visando garantir a integridade dos dados produzidos pelo sensor.

Figura 18 - FRP-SEC-061: Prevenção de Código Malicioso em Aplicativos IoT



Fonte: Elaborado pelo autor

A partir do padrão **FRP-SEC-061**, podem ser elaborados os seguintes requisitos específicos:

Requisito — Validação de Integridade de Firmware

O sensor deve validar a integridade do *firmware* antes de inicializar, rejeitando versões não assinadas ou com inconsistências de *hash*.

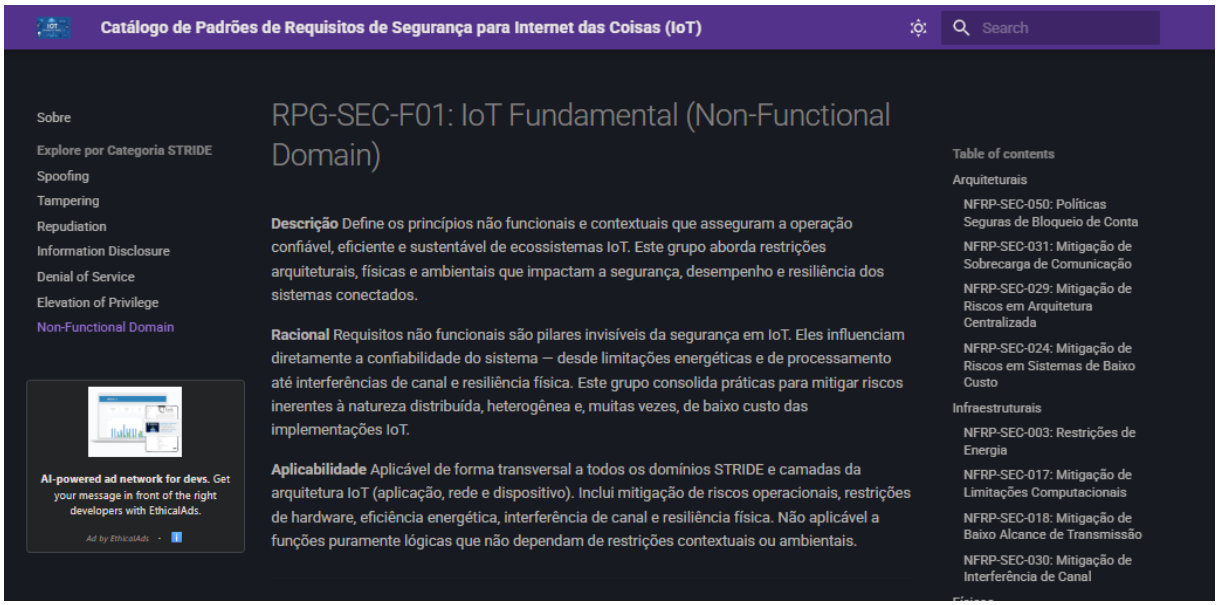
Requisito — Execução Restrita a Software Autorizado

O dispositivo deve executar apenas *software* oriundo de fontes confiáveis e assinadas digitalmente, prevenindo inserção de código malicioso.

4.6.3 A todos os dispositivos – Non-Functional Domain

E, de forma transversal, aplicam-se também os NFRPs relacionados à mitigação de interferências, às restrições de energia e às limitações de processamento.

Figura 19 - RPG-SEC-F01: IoT Fundamental (Non-Functional Domain)



Fonte: Elaborado pelo autor

O exemplo demonstra que o catálogo possibilita identificar, justificar e estruturar requisitos de segurança com base nas ameaças analisadas, oferecendo um suporte

metodológico consistente para o levantamento e a priorização de requisitos em contextos IoT.

5 CONCLUSÃO

Este capítulo resume a proposta e os resultados do Catálogo STRIDE-IoT, apresenta suas principais contribuições, reconhece limitações da pesquisa e indica caminhos para sua validação e evolução futura.

5.1 Considerações Finais

O desenvolvimento do Catálogo STRIDE-IoT representou uma forma prática de aproximar dois mundos de forma estruturada. O domínio conceitual da segurança da informação e o domínio aplicado da engenharia de requisitos. Partindo da tríade CIA e do modelo de ameaças STRIDE, o trabalho propôs uma forma sistemática de converter ameaças em requisitos de segurança documentados, rastreáveis e reutilizáveis.

O catálogo resultante organiza os padrões de requisitos em níveis conceituais (RPGs), concretos (FRPs) e transversais (NFRPs), permitindo que engenheiros e arquitetos compreendam a segurança como um sistema coerente, e não como um conjunto disperso de práticas isoladas.

Parte das falhas de segurança em IoT não decorre apenas da ausência de controles técnicos, mas da falta de linguagem comum entre equipes de desenvolvimento, arquitetura e negócio. O catálogo atua justamente sobre esse ponto, oferecendo uma estrutura conceitual e técnica que traduz ameaças em requisitos claros, apoiando o diálogo entre o risco, a tecnologia e o valor do sistema.

5.2 Contribuições

As principais contribuições deste trabalho são:

Definição da estrutura do catálogo

Definição de uma arquitetura de catálogo baseada em *Requirement Patterns* (Withall, 2007), adaptada ao contexto IoT e composta por RPGs, FRPs e NFRPs. Essa estrutura hierárquica facilita a reutilização, a coerência e a rastreabilidade entre ameaça, requisito e tecnologia.

Integração entre modelos

Integração entre o modelo STRIDE e a engenharia de requisitos, permitindo representar categorias de ameaça como domínios de especificação de segurança. Com isso, cada ameaça passa a ter um conjunto sistemático de contramedidas, facilitando o raciocínio arquitetural.

Desenvolvimento do catálogo

Desenvolvimento e disponibilização do catálogo em formato navegável (via **Read The Docs** e GitHub), assegurando acesso público, colaboração e evolução contínua, transformando o catálogo em um recurso aberto de engenharia de segurança aplicada à IoT.

5.3 Limitações da Pesquisa

O trabalho possui algumas limitações que devem ser consideradas:

- Ausência de validação empírica: devido às restrições de tempo e escopo, não foi possível aplicar o catálogo em projetos reais ou validar sua usabilidade com especialistas.
- Foco conceitual: a ênfase esteve na estruturação e documentação dos padrões, sem comparação qualitativa com outros *frameworks* existentes.
- Escopo tecnológico limitado: embora tecnologias de suporte sejam mencionadas (PKI, TLS 1.3, Argon2, OAuth 2.0), não foram exploradas implementações técnicas completas ou simulações de desempenho.

5.4 Trabalhos Futuros

O Catálogo STRIDE-IoT abre novas frentes de desenvolvimento. Entre as principais perspectivas e desafios futuros, destacam-se:

Validação prática

Aplicar o catálogo em projetos reais de IoT, avaliando sua aplicabilidade em diferentes cenários (residenciais, industriais, hospitalares, urbanos). Estudos de caso poderiam medir a eficácia dos requisitos na mitigação de ameaças e identificar ajustes necessários para contextos específicos.

Análise qualitativa com outros frameworks existentes

Fazer uma análise qualitativa do catálogo com e normas como o NISTIR 8259 e o ETSI EN 303 645 (que estabelecem, respectivamente, requisitos fundamentais para fabricantes de dispositivos IoT e diretrizes de segurança para dispositivos de consumo). Em síntese, o STRIDE-IoT deve ser visto como um ponto de partida, e não como um fim.

Atualizar catálogo atual com novos padrões

Propósito é evoluir junto com o ecossistema IoT, consolidando-se como um modelo prático de engenharia de segurança orientada a ameaças, capaz de transformar a análise de riscos em projetos seguros, verificáveis e sustentáveis.

REFERÊNCIAS

ABDULHAMID, Alhassan *et al.* An Overview of Safety and Security Analysis Frameworks for the Internet of Things. **Electronics**, v. 12, n. 14, p. 3086, 16 jul. 2023.

AGUILAR-CALDERÓN, José-Alfonso *et al.* Requirements Engineering for Internet of Things (IoT) Software Systems Development: A Systematic Mapping Study. **Applied Sciences**, v. 12, n. 15, p. 7582, 28 jul. 2022.

ALOTAIBI, Bandar. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. **Sensors**, v. 23, n. 17, p. 7470, 28 ago. 2023.

BARCELOS, Leonardo Vieira. **ESPECIFICAÇÃO DE REQUISITOS NO DOMÍNIO DE SISTEMAS DE INFORMAÇÃO COM O USO DE PADRÕES**. 2016. Dissertação de Pós-graduação.

CARNEIRO, Cinara. **Um Catálogo de Padrões de Requisitos de Privacidade Baseado na Lei Geral de Proteção de Dados Pessoais**. 2024.

CETINTAV, Isil; TAHIR SANDIKKAYA, Mehmet. A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs. **IEEE Access**, v. 13, p. 37703–37723, 2025.

CORDEIRO, André; VASCONCELOS, André; CORREIA, Miguel. **A Catalog of Security Patterns**. v. 0, n. 0, 2022. Dissertação de Mestrado.

DA SILVA, Danyllo. **RETIoT - Tecnologia de Software para Apoiar a Engenharia de Requisitos de Sistemas de Software IoT**. 2021. Dissertação de Mestrado.

DEATH, Darren. **Information security handbook: develop a threat model and incident response strategy to build a strong information security framework**. 1st ed ed. Place of publication not identified: Packt Publishing, 2017.

KUDO, Taciana Novo. **Um metamodelo para alinhamento de padrões de requisitos e padrões de testes e um framework para avaliação de metamodelos**. 2021. Dissertação de Pós-graduação.

MOTTA, Rebeca Campos; DE OLIVEIRA, Káthia Marçal; TRAVASSOS, Guilherme Horta. Towards a Roadmap for the Internet of Things Software Systems Engineering. *In*: MEDES ’20: 12TH INTERNATIONAL CONFERENCE ON MANAGEMENT OF DIGITAL ECOSYSTEMS. **Proceedings of the 12th International Conference on Management of Digital EcoSystems**. Virtual Event United Arab Emirates: ACM, 2 nov. 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3415958.3433100>. Acesso em: 10 nov. 2025

PAPOUTSAKIS, Manos *et al.* Towards a Collection of Security and Privacy Patterns. **Applied Sciences**, v. 11, n. 4, p. 1396, 4 fev. 2021.

PESSOA, Clinton. **CATÁLOGO DE VULNERABILIDADES DE SEGURANÇA EM SISTEMAS DE SOFTWARE IOT**. **06/2025**, jun. 2025. Dissertação de Mestrado.

SEBESTYEN, Hannelore; POPESCU, Daniela Elena; ZMARANDA, Rodica Doina. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. **Computers**, v. 14, n. 2, p. 61, 11 fev. 2025.

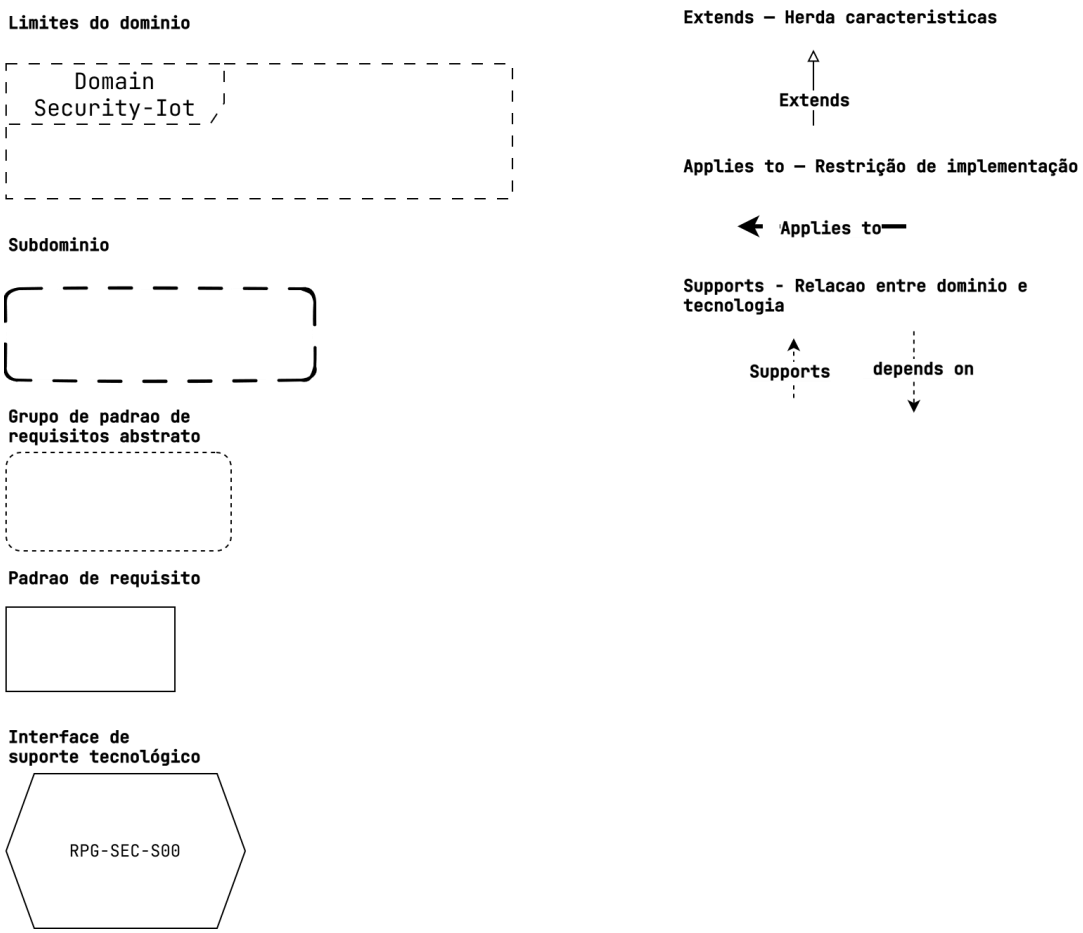
SHOSTACK, Adam. **Threat modeling: designing for security**. Indianapolis, IN: Wiley, 2014.

WITHALL, Stephen. **Software Requirement Patterns**. 2007.

APÊNDICE A - Elementos do Diagrama e Relações entre Padrões

A Figura 20, apresenta a legenda visual utilizada ao longo do catálogo, definindo os elementos estruturais e as relações entre padrões, grupos e infraestruturas.

Figura 20 - Notação e Elementos Gráficos do Catálogo STRIDE-IoT



Fonte: Elaborado pelo autor

Elementos Estruturais do Diagrama:

- Limites do Domínio (Domain): Representa a fronteira conceitual que agrupa RPGs.
- Subdomínio: Utilizado para separar grupos internos.
- RPG (Grupo de padrão de requisito): Agrupamento abstrato que define o objetivo de segurança.

- FRP (Padrão de requisito): Padrão funcional concreto derivado de um RPG e aplicável a uma das camadas IoT.
- Infraestrutura (Interface de suporte tecnológico): Viabiliza a implementação dos FRPs.

Tipos de Relação

- ***Extends***: Indica que o FRP especializa e concretiza o RPG.
- ***Applies to***: Indica que um NFRP do IoT Fundamental se aplica transversalmente aos domínios STRIDE, impondo restrições.
- ***Supports / Depends on***: Indica dependência técnica entre o domínio e sua infraestrutura.