



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO, DE CIÊNCIAS EXATAS E EDUCAÇÃO
DEPARTAMENTO DE ENG. DE CONTROLE, AUTOMAÇÃO E COMPUTAÇÃO
CURSO DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Rodrigo Eduardo Laffront

**UTILIZAÇÃO DE GÊMEO DIGITAL E APRENDIZADO DE MÁQUINA
PARA DETECÇÃO DE ATAQUES CIBERNÉTICOS EM REDES
ELÉTRICAS INTELIGENTES: REVISÃO DA LITERATURA**

Blumenau
2025

Rodrigo Eduardo Laffront

**UTILIZAÇÃO DE GÊMEO DIGITAL E APRENDIZADO DE MÁQUINA
PARA DETECÇÃO DE ATAQUES CIBERNÉTICOS EM REDES
ELÉTRICAS INTELIGENTES: REVISÃO DA LITERATURA**

Trabalho de Conclusão de Curso de Graduação em Engenharia de Controle e Automação do Centro Tecnológico, de Ciências Exatas e Educação da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Engenheiro de Controle e Automação.

Orientador: Prof. Dr. Tiago Davi Curi Busarello

Blumenau

2025

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Laffront, Rodrigo Eduardo

Utilização de gêmeo digital e aprendizado de máquina
para detecção de ataques cibernéticos em redes elétricas
inteligentes : revisão da literatura / Rodrigo Eduardo
Laffront ; orientador, Tiago Davi Curi Busarello, 2025.
87 p.

Trabalho de Conclusão de Curso (graduação) -
Universidade Federal de Santa Catarina, Campus Blumenau,
Graduação em Engenharia de Controle e Automação, Blumenau,
2025.

Inclui referências.

1. Engenharia de Controle e Automação. 2. Gêmeo digital
e aprendizado de máquina. 3. Redes elétricas inteligentes.
4. Cibersegurança. 5. Descarbonização. I. Busarello, Tiago
Davi Curi. II. Universidade Federal de Santa Catarina.
Graduação em Engenharia de Controle e Automação. III. Título.

Rodrigo Eduardo Laffront

**UTILIZAÇÃO DE GÊMEO DIGITAL E APRENDIZADO DE MÁQUINA
PARA DETECÇÃO DE ATAQUES CIBERNÉTICOS EM REDES
ELÉTRICAS INTELIGENTES: REVISÃO DA LITERATURA**

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de “Engenheiro de Controle e Automação” e aprovado em sua forma final pelo Curso de Graduação em Engenharia de Controle e Automação.

Blumenau, 09 de Dezembro de 2025.

Banca Examinadora:



Documento assinado digitalmente
Tiago Davi Curi Busarello
Data: 17/12/2025 15:23:26-0300
CPF: ***.950.098-**
Verifique as assinaturas em <https://v.ufsc.br>

Prof. Tiago Davi Curi Busarello, Dr.
Universidade Federal de Santa Catarina



Documento assinado digitalmente
Ciro Andre Pitz
Data: 17/12/2025 15:25:20-0300
CPF: ***.728.089-**
Verifique as assinaturas em <https://v.ufsc.br>

Prof. Ciro André Pitz, Dr.
Universidade Federal de Santa Catarina



Documento assinado digitalmente
Mauri Ferrandin
Data: 17/12/2025 15:24:36-0300
CPF: ***.580.869-**
Verifique as assinaturas em <https://v.ufsc.br>

Prof. Mauri Ferrandin, Dr.
Universidade Federal de Santa Catarina

AGRADECIMENTOS

Agradeço a Deus por ter me dado sabedoria e saúde para chegar até aqui, e por ter me guiado ao longo deste caminho.

Agradeço à minha família, em especial ao meu pai e à minha irmã, Jorge Eduardo Laffront e Flávia de Freitas Laffront, por terem me ensinado pelo exemplo e por serem uma parte significativa da pessoa que sou hoje.

Agradeço a todos os meus amigos da graduação que fizeram parte desta jornada de alguma forma, em especial aos meus amigos Jorge Luiz Satler Coltro e Vinicius Afonso Heinen, pelas discussões intermináveis sobre diversos assuntos e por terem tornado essa trajetória ainda melhor.

Agradeço à minha namorada, Ádria Cypriano, por ser quem ela é, por ter me apoiado no desenvolvimento deste trabalho, e por ter sido minha parceira em diversos momentos, inclusive na mudança para outro país durante a graduação.

Agradeço a todos os professores pelos ensinamentos, em especial ao meu orientador, Tiago Davi Curi Busarello, pelo suporte e pela excelente palestra sobre *Smart Grids*, que foi um dos fatores que motivaram a escolha do tema deste trabalho.

Por fim, agradeço à UFSC por ter me permitido aprender com excelentes professores, pela educação de excelente qualidade, pela estrutura fornecida e pelo universo de possibilidades oferecidas ao longo da graduação.

*“The world hates change, yet it is the only thing
that has brought progress.” (Kettering, Charles)*

RESUMO

Nos últimos anos, gêmeos digitais têm sido aplicados em diversos segmentos, como construção, manufatura, sistemas de saúde, logística e sistemas de energia. O aprendizado de máquina, por sua vez, tem ganhado mais evidência à medida que a inteligência artificial se torna cada vez mais popular, sendo também aplicado em diversas áreas. A combinação dessas duas tecnologias pode, portanto, trazer benefícios significativos para diferentes campos. Em sistemas de energia, especialmente diante da tendência de incorporar tecnologias que transformem esses sistemas em estruturas inteligentes, a utilização de gêmeos digitais em conjunto com aprendizado de máquina pode desempenhar um papel fundamental na supervisão e no controle das redes. Ao mesmo tempo, diversos ciberataques foram registrados nos últimos anos, inclusive contra sistemas de energia, e a integração de dispositivos de tecnologia da informação aumenta a superfície de ataque, tornando a cibersegurança uma preocupação crescente. Nesse contexto, este trabalho foca na revisão do uso de gêmeos digitais em conjunto com aprendizado de máquina para a identificação de ataques cibernéticos em redes elétricas inteligentes. Para isso, foi realizada uma revisão detalhada da literatura abordando a necessidade de implementação das redes elétricas inteligentes, o conceito e a aplicação dos gêmeos digitais, os fundamentos do aprendizado de máquina e suas principais abordagens, e, por fim, como esses componentes podem ser utilizados de forma integrada e quais benefícios essa combinação oferece. Além disso, ao final deste trabalho, são apresentadas as tendências futuras relacionadas a essa integração.

Palavras-chave: Redes Elétricas Inteligentes; Gêmeos Digitais; Aprendizado de Máquina; Ataques cibernéticos.

ABSTRACT

In recent years, digital twins have been applied across several sectors, including construction, manufacturing, healthcare, logistics, and energy systems. In the same time, machine learning has gained increasing prominence as artificial intelligence becomes more widespread, and it is also applied across various fields. Combining these two technologies can therefore bring significant benefits to various fields. In energy systems, particularly given the trend toward incorporating technologies that transform these systems into intelligent infrastructures, the use of digital twins together with machine learning can play a key role in the supervision and control of electrical networks. At the same time, numerous cyberattacks have been recorded in recent years, including attacks targeting energy systems, and the integration of information technology devices increases the attack surface, making cybersecurity an increasingly critical concern. In this context, this work focuses on reviewing the use of digital twins combined with machine learning for the detection of cyberattacks in smart grids. To this end, a detailed literature review was conducted, addressing the need for implementing smart grids, the concept and applications of digital twins, the foundations of machine learning and its main approaches, and finally how these components can be used together and what benefits they offer. Additionally, this work highlights the future trends associated with this integration.

Keywords: Smart Grids; Digital Twins; Machine Learning; Cyber attacks.

LISTA DE FIGURAS

Figura 1 – Evolução anual do número de publicações para <i>Cybersecurity</i> e <i>Smart Grids</i>	17
Figura 2 – Estrutura do trabalho.	19
Figura 3 – Evolução da renda por pessoa antes e após a Revolução Industrial. . .	24
Figura 4 – Estrutura de um sistema de energia convencional.	27
Figura 5 – Classificação dos recursos naturais.	28
Figura 6 – Evolução da geração de energia renovável no mundo.	32
Figura 7 – Modelo SGAM.	34
Figura 8 – Modelo NIST.	35
Figura 9 – Produção média de energia solar e eólica ao longo de uma semana na Alemanha durante o ano de 2025.	36
Figura 10 – Sistemas de armazenamento de energia.	37
Figura 11 – Estrutura de um sistema de energia inteligente.	42
Figura 12 – Tipos de fluxos de dados em um gêmeo digital.	45
Figura 13 – Gêmeo digital aplicado em eletrônica de potência.	46
Figura 14 – Gêmeo digital aplicado em um sistema mecânico.	47
Figura 15 – Arquitetura de um gêmeo digital com seis camadas.	48
Figura 16 – Arquitetura de um gêmeo digital com sete camadas.	49
Figura 17 – Algoritmos de classificação binária, classificação múltipla e de regressão.	53
Figura 18 – Estrutura de uma Rede Neural Artificial.	55
Figura 19 – Conjunto e subconjuntos do aprendizado de máquina.	56
Figura 20 – Técnicas de inteligência artificial para as diferentes categorias de gêmeos digitais.	57
Figura 21 – Classificação dos ataques cibernéticos de acordo com a tríade Integridade, Confiabilidade e Disponibilidade.	63
Figura 22 – Classificação dos ataques cibernéticos de acordo com as camadas do modelo OSI.	64
Figura 23 – Arquitetura de integração dos gêmeos digitais com inteligência artificial em uma rede elétrica.	69
Figura 24 – Arquitetura para utilização de gêmeos digitais com aprendizado de máquina em redes elétricas inteligentes.	74

LISTA DE QUADROS

Quadro 1 – Artigos utilizados.	21
--	----

LISTA DE TABELAS

Tabela 1 – Protocolos de comunicação em redes inteligentes.	41
Tabela 2 – Comparação entre as redes elétricas inteligentes e as redes elétricas tradicionais.	43
Tabela 3 – Descrição dos ataques cibernéticos contra infraestruturas de energia no século XXI.	60
Tabela 4 – Descrição dos tipos de ataques cibernéticos.	65

LISTA DE ABREVIATURAS E SIGLAS

BIM	<i>Building Information Modeling</i>
CLP	Controladores Lógicos Programáveis
CoAP	<i>Constrained Application Protocol</i>
DNP3	<i>Distributed Network Protocol 3</i>
DTC	<i>Digital Twin Construction</i>
EHR	Registros Eletrônicos de Saúde
ERP	Planejamento de Recursos Empresariais
GPS	Sistema de Posicionamento Global
IA	Inteligência Artificial
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IoT	<i>Internet of Things</i>
kWh	Quilowatt-hora
LSTM	<i>Long Short-Term Memory</i>
MQTT	<i>Message Queuing Telemetry Transport</i>
MWh	Megawatt-hora
NASA	<i>National Aeronautics and Space Administration</i>
NIST	<i>National Institute of Standards and Technology</i>
ODS	Objetivos de Desenvolvimento Sustentável
ONU	Organização das Nações Unidas
OPEP	Organização dos Países Exportadores de Petróleo
PEDG	<i>Power Electronics-Dominated Grid</i>
PMU	<i>Phasor Measurement Unit</i>
PROFIBUS	<i>Process Field Bus</i>
RFID	Identificação por Rádio Frequência
RNA	Redes Neurais Artificiais
S7Comm	<i>S7 Communication</i>
SCADA	<i>Supervisory Control and Data Acquisition</i>
SGAM	<i>Smart Grid Architecture Model</i>
V2G	<i>Vehicle-to-Grid</i>

SUMÁRIO

1	INTRODUÇÃO	15
1.1	JUSTIFICATIVA	16
1.2	OBJETIVOS	17
1.2.1	Objetivo geral	17
1.2.2	Objetivos específicos	18
1.3	ESTRUTURA DO TRABALHO	18
2	METODOLOGIA	20
3	REVISÃO DA LITERATURA	23
3.1	SISTEMAS DE DISTRIBUIÇÃO DE ENERGIA	23
3.1.1	Utilização dos combustíveis fósseis	23
3.1.2	Sistema de distribuição de energia atual	25
3.1.3	Crescimento Populacional e Mudanças Climáticas	27
3.1.4	A rede elétrica do futuro	32
3.2	REDES ELÉTRICAS INTELIGENTES	33
3.2.1	Definição e características	33
<i>3.2.1.1</i>	<i>Sistemas de Armazenamento de Energia</i>	<i>36</i>
<i>3.2.1.2</i>	<i>Microrredes</i>	<i>38</i>
<i>3.2.1.3</i>	<i>Dispositivos IoT</i>	<i>39</i>
<i>3.2.1.4</i>	<i>Tecnologias de comunicação</i>	<i>40</i>
<i>3.2.1.5</i>	<i>Vantagens e limitações das redes inteligentes</i>	<i>42</i>
3.3	GÊMEOS DIGITAIS	44
3.3.1	Definição e características	44
3.3.2	Implementação de gêmeos digitais	45
3.3.3	Aplicações de gêmeos digitais	49
<i>3.3.3.1</i>	<i>Aplicação de gêmeos digitais para construção</i>	<i>50</i>
<i>3.3.3.2</i>	<i>Aplicação de gêmeos digitais para sistemas de saúde</i>	<i>50</i>
<i>3.3.3.3</i>	<i>Aplicação de gêmeos digitais para manufatura inteligente</i>	<i>50</i>
<i>3.3.3.4</i>	<i>Aplicação de gêmeos digitais para gerenciamento de cadeia de suprimentos</i>	<i>51</i>
3.4	INTELIGÊNCIA ARTIFICIAL	51
3.4.1	Definição e características	51
3.4.2	Aprendizado de máquina	52
3.4.3	Integração de aprendizado de máquina com gêmeos digitais .	56
3.5	ATAQUES CIBERNÉTICOS EM REDES ELÉTRICAS INTELIGENTES	58
3.6	INTEGRAÇÃO DE GÊMEOS DIGITAIS E APRENDIZADO DE MÁ- QUINA NA DETECÇÃO DE ATAQUES CIBERNÉTICOS EM RE- DES ELÉTRICAS INTELIGENTES	67
4	SÍNTESE E TENDÊNCIAS	71

5	CONCLUSÃO	76
	REFERÊNCIAS	77

1 INTRODUÇÃO

A geração convencional de energia elétrica por meio de combustíveis fósseis, como carvão, petróleo e gás natural, foi essencial para o desenvolvimento econômico e tecnológico nos últimos 200 anos. Por outro lado, o uso dessas fontes de energia não é sustentável e constitui um dos principais, senão o maior, fatores responsáveis pelas atuais mudanças climáticas, devido à emissão de CO₂ na atmosfera. Para reduzir essas emissões, a matriz energética mundial precisa ser composta, ao menos em sua maioria, por fontes de energia renováveis. Alguns acordos internacionais, como o Acordo de Paris e a Agenda 2030, propõem metas para que a transição energética ocorra de forma rápida e colaborativa; entretanto, a infraestrutura atual dos sistemas de energia representa um obstáculo significativo para que essa transição se concretize.

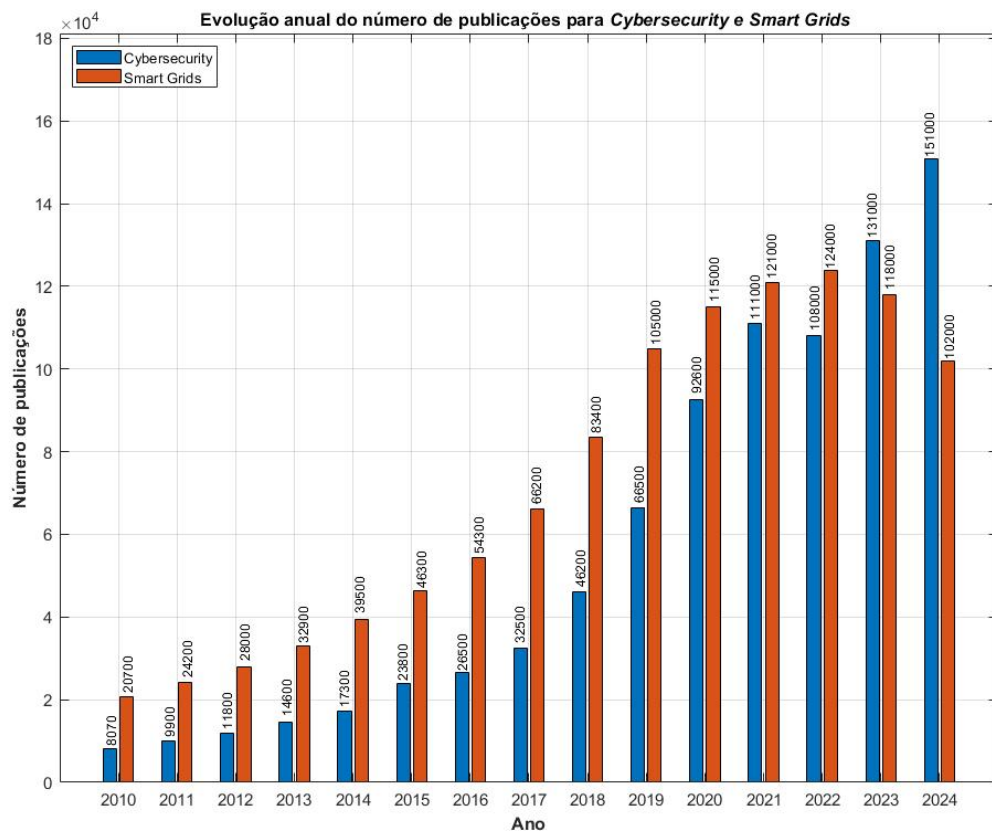
Ao mesmo tempo, as Redes Elétricas Inteligentes, conhecidas como *Smart Grids*, surgem como uma alternativa para integrar a geração distribuída de energia, facilitando o uso de fontes renováveis, como a solar e a eólica. Além disso, utilizam dispositivos de comunicação para a coleta de dados em toda a rede e sistemas de armazenamento de energia, tornando-a mais eficiente e preparada para atender às demandas globais atuais. Paralelamente, preocupações relacionadas à cibersegurança das *Smart Grids* ganham destaque, uma vez que é necessário manter a integridade dos usuários conectados à rede, tanto em termos de segurança física quanto de privacidade, bem como garantir a confiabilidade das redes e a disponibilidade ininterrupta dos sistemas de energia. Ao integrarmos os mundos da tecnologia da informação e da tecnologia da operação, a necessidade de assegurar proteção cibernética torna-se um dever essencial.

Paralelamente, o mundo presencia a ascensão da IA (Inteligência Artificial), cuja aplicação se estende a praticamente todos os setores da indústria. No contexto das redes elétricas inteligentes, a IA, em especial com o aprendizado de máquina, tem o potencial de analisar padrões e identificar comportamentos anômalos nas redes, atuando como um sistema de controle capaz de garantir que a complexidade das *Smart Grids* e os ataques cibernéticos que essas redes podem sofrer não se tornem um problema.

Entretanto, a IA por si só não é suficiente. Dispositivos IoT (*Internet of Things*) são necessários para a ampla coleta de dados em toda a rede, enquanto os gêmeos digitais, conhecidos como *Digital Twins*, têm sido amplamente aplicados em diversos setores da indústria, inclusive no setor energético. Eles se mostram promissores por permitirem a simulação e o monitoramento em tempo real das redes elétricas inteligentes, integrando sua complexidade e comportamento dinâmico de maneira eficiente e previsível, além de servirem como ferramenta para prever comportamentos e realizar simulações relacionadas a ciberataques.

1.1 JUSTIFICATIVA

Haja vista a crescente demanda por energia elétrica e as mudanças climáticas causadas pela vasta utilização de combustíveis fósseis e pela ineficiente utilização da energia, é fundamental discutir as melhores formas de implementar as redes elétricas inteligentes e reforçar os benefícios que podem ser alcançados com sua adoção. Ao analisar o número de publicações relacionadas às redes elétricas inteligentes, especialmente desde o início da década passada, percebe-se a relevância que esse tema adquiriu na literatura. Ao mesmo tempo, a sociedade presencia o avanço acelerado de tecnologias nos últimos anos, sobretudo da IA e dos dispositivos IoT, refletindo a tendência de termos cada vez mais sistemas considerados inteligentes, ou seja, sistemas conectados e digitais. O termo digitalização, inclusive, é amplamente discutido tanto por pesquisadores quanto pela indústria como uma etapa necessária para diversos setores. Paralelamente, o tema da segurança cibernética torna-se cada vez mais evidente à medida que sistemas digitais são implementados em larga escala. De acordo com a Insight (2025), empresa do mercado financeiro, o mercado global de segurança cibernética foi avaliado em US\$ 193,73 bilhões em 2024, com previsão de crescimento para US\$ 218,98 bilhões em 2025 e para US\$ 562,77 bilhões em 2032, demonstrando a força e a perspectiva positiva que a área de cibersegurança apresenta para os próximos anos. Na literatura, os temas *Smart Grids* e *Cybersecurity* evidenciam uma clara evolução no número de trabalhos publicados ao longo dos anos, como mostrado na Figura 1.

Figura 1 – Evolução anual do número de publicações para *Cybersecurity* e *Smart Grids*.

Fonte: Elaborado pelo autor com dados do Google Scholar.

Dessa forma, a relevância deste trabalho consiste na necessidade de compreender como as tecnologias emergentes têm potencial para suprir a demanda por um sistema de energia mais resiliente, eficiente e sustentável, ao mesmo tempo em que previnem possíveis interrupções, danos e invasões causadas por ataques cibernéticos.

1.2 OBJETIVOS

Nas seções abaixo estão descritos o objetivo geral e os objetivos específicos deste Trabalho de Conclusão de Curso.

1.2.1 Objetivo geral

Descrever a tecnologia de gêmeos digitais e investigar o seu potencial de aplicação em conjunto com aprendizado de máquina na detecção de ataques cibernéticos em redes elétricas inteligentes.

1.2.2 Objetivos específicos

1. Analisar a literatura científica sobre redes elétricas inteligentes, destacando seu papel na descarbonização e eletrificação do setor energético, bem como suas principais aplicações e os desafios relacionados à sua implementação.
2. Descrever e investigar as potenciais aplicações de gêmeos digitais em sistemas industriais e energéticos.
3. Explorar os benefícios do uso de técnicas de aprendizado de máquina na detecção de ataques cibernéticos em sistemas elétricos, considerando diferentes abordagens disponíveis na literatura.
4. Examinar o estado da arte sobre a aplicação conjunta de gêmeos digitais e aprendizado de máquina para a detecção de ataques cibernéticos em redes elétricas inteligentes, avaliando as abordagens existentes, suas vantagens e limitações.

1.3 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em cinco capítulos principais. O Capítulo 2 descreve a metodologia utilizada para a elaboração do trabalho, detalhando os critérios de seleção das fontes, o tipo de revisão da literatura adotada e os procedimentos realizados para análise e organização das informações obtidas.

O Capítulo 3 corresponde à revisão da literatura, dividida em cinco seções temáticas. A primeira seção introduz o leitor à utilização de combustíveis fósseis e apresenta um resumo sobre a criação da primeira usina de energia. A segunda seção aborda os principais conceitos relacionados às redes elétricas inteligentes, seus fundamentos, aplicações e desafios. Em seguida, a terceira seção trata dos gêmeos digitais, explorando suas definições, características, aplicações e os desafios envolvidos em sua implementação. A quarta seção apresenta a inteligência artificial e o aprendizado de máquina, incluindo conceitos, técnicas e aplicações, além de sua integração com gêmeos digitais. Na quinta seção, é apresentado um panorama sobre o potencial danoso de ataques cibernéticos em uma rede elétrica, bem como os ataques registrados na história contra infraestruturas de energia, os tipos de ciberataques e suas classificações. Por fim, essa seção examina a integração entre gêmeos digitais e aprendizado de máquina na detecção de ataques cibernéticos, sistematizando os estudos encontrados na literatura quanto às abordagens utilizadas, arquiteturas propostas, desafios e benefícios dessa integração.

O Capítulo 4 apresenta uma síntese de todo o trabalho, bem como a opinião do autor em relação à revisão da literatura apresentada e às tendências futuras para a integração entre gêmeos digitais e aprendizado de máquina na detecção de ataques cibernéticos em redes elétricas inteligentes.

O Capítulo 5 apresenta a conclusão, na qual são destacados os resultados do trabalho e suas contribuições.

A seguir, na Figura 2, é apresentado um panorama da estrutura do trabalho.

Figura 2 – Estrutura do trabalho.



Fonte: Elaborado pelo autor.

2 METODOLOGIA

A metodologia deste trabalho consistiu em uma revisão sistemática da literatura, utilizando principalmente quatro bases de dados para a pesquisa (Elsevier, IEEE, MDPI e Springer). Além disso, foram utilizados sites de notícias e bases de dados confiáveis para a fundamentação de eventos recentes que ainda não se encontram na literatura, bem como para a apresentação de dados atualizados. Para a pesquisa, foram utilizadas palavras-chave que se correlacionassem com o objetivo geral e objetivos específicos deste trabalho, como “*smart grids*”, “*digital twins*”, “*machine learning*” e “*cyber attacks in smart grids*”, bem como seus correspondentes em português: “redes elétricas inteligentes”, “gêmeos digitais”, “aprendizado de máquina”, “ataques cibernéticos em redes elétricas inteligentes”, respectivamente.

Para a classificação e seleção dos trabalhos encontrados nas áreas de redes elétricas inteligentes, aprendizado de máquina e gêmeos digitais, aplicou-se filtros para a publicação a partir de 2020. Junto com isso, para o desenvolvimento deste trabalho e realização dos objetivos propostos, foram aplicadas as seguintes perguntas de pesquisa no momento da revisão da literatura:

1. O que são as redes elétricas inteligentes e no que se diferem em relação as redes elétricas tradicionais?
2. Quais as vantagens e perspectivas futuras que as redes elétricas inteligentes oferecem?
3. O que são os ataques cibernéticos, sobretudo em infraestruturas de energia, e qual a importância de detectá-los?
4. O que são os gêmeos digitais, suas aplicações, arquiteturas e desafios para implementação?
5. O que é aprendizado de máquina e quais são suas abordagens?
6. Como utilizar gêmeo digital em conjunto com aprendizado de máquina para detecção de falhas em redes elétricas inteligentes?

A partir dessas perguntas, foram definidas as referências utilizadas para a realização deste trabalho, totalizando 102 referências. No Quadro 1, são apresentadas as informações das vinte referências que tiveram maior contribuição para o desenvolvimento desta revisão da literatura, organizadas por ano de publicação, incluindo título, autores, ano de publicação e quais perguntas de pesquisa cada trabalho responde.

Quadro 1 – Artigos utilizados.

Nº	Título	Autor(es)	Ano	Resp. a pergunta
1	<i>Characterising the Digital Twin: A systematic literature review</i>	David Jones, Chris Snider, Aydin Nassehi, Jason Yon, Ben Hicks	2020	4
2	<i>Digital twin technology</i>	Zongyan Wang	2020	4
3	<i>Smart grid anomaly detection using a deep learning digital twin</i>	William Danilczyk, Yan Sun, Haibo He	2021	6
4	<i>Recent advancement in smart grid technology: Future prospects in the electrical power network</i>	Osama Butt, Muhammad Zulqarnain, Tallal Butt	2021	1, 2
5	<i>A survey on IoT-enabled smart grids: technologies, architectures, applications, and challenges</i>	Sheeraz Kirmani, Abdul Mazid, Irfan Khan, Manaullah Abid	2022	1, 2, 3
6	<i>A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions</i>	Tala Khoei, Hadjar Slimane, Naima Kaabouch	2022	1, 2, 6
7	<i>Overview of smart grid implementation: Frameworks, impact, performance and challenges</i>	Malik Judge, Asif Khan, Awais Manzoor, Hasan Khattak	2022	1, 2
8	<i>Gridattackanalyzer: A cyber attack analysis framework for smart grids</i>	Tan Le, Mengmeng Ge, Adnan Anwar, Seng Loke, Razvan Beuran, Robin Doss, Yasuo Tan	2022	1, 3, 6
9	<i>Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods</i>	Tehseen Mazhar, Hafiz Irfan, Sunawar Khan, Inayatul Haq, Inam Ullah, Muhammad Iqbal, Habib Hamam	2023	1, 2, 3, 6
10	<i>Digital Twin: Benefits, use cases, challenges, and opportunities</i>	Mohsen Attaran, Bilge Celik	2023	4
11	<i>Artificial intelligence and the digital twin: an essential combination</i>	Roberto Minerva, Noel Crespi, Reza Farahbakhsh, Faraz Awan	2023	4, 5, 6
12	<i>Machine learning and deep learning: A review of methods and applications</i>	Koosha Sharifani, Mahyar Amini	2023	5

13	<i>A cyber-physical-social perspective on future smart distribution systems</i>	Yi Wang, Chien-Fei Chen, Peng-Yong Kong, Husheng Li, Qingsong Wen	2022	1, 4
14	<i>A review on the evaluation of feature selection using machine learning for cyber-attack detection in smart grid</i>	Saad Mohammed, Abdulmajeed Al-Jumaily, Mandeep Singh, Victor Jiménez, Aqeel Jaber, Yaseein Hussein, Mudhar Al-Najjar, Dhiya Al-Jumeily	2024	3, 5
15	<i>Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies</i>	Bishowjit Paul, Auvizit Sarker, Sarafat Abhi, Sajal Das, Firoj Ali, Manirul Islam, Robiul Islam, Sumaya Moyeen, Faisal Badal, Hafiz Ahamed	2024	1, 2, 3, 6
16	<i>Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation</i>	Doney Abraham, Siv Houmb, Laszlo Erdodi	2025	3, 6
17	<i>Security of smart grid: cybersecurity issues, potential cyberattacks, major incidents, and future directions</i>	Mohammad Alomari, Mohammed Al-Andoli, Mukhtar Ghaleb, Reema Thabit, Gamal Alkawsi, Jamil Alsayaydeh, AbdulGuddoos Gaid	2025	1, 2, 3, 6
18	<i>A Comprehensive Review of Solar PV Integration with Smart-Grids: Challenges, Standards, and Grid Codes</i>	Gowthamraj Rajendran, Reiko Raute, Cedric Caruana	2025	1, 2, 4, 6
19	<i>Leveraging digital twin and machine learning techniques for anomaly detection in power electronics dominated grid</i>	Ildar Idrisov, Divine Okeke, Abdullatif Albaser, Mohamed Abdallah, Federico Ibanez	2025	3, 6
20	<i>Electric power system basics for the nonelectrical professional</i>	Steven Blume	2025	1, 2

3 REVISÃO DA LITERATURA

3.1 SISTEMAS DE DISTRIBUIÇÃO DE ENERGIA

3.1.1 Utilização dos combustíveis fósseis

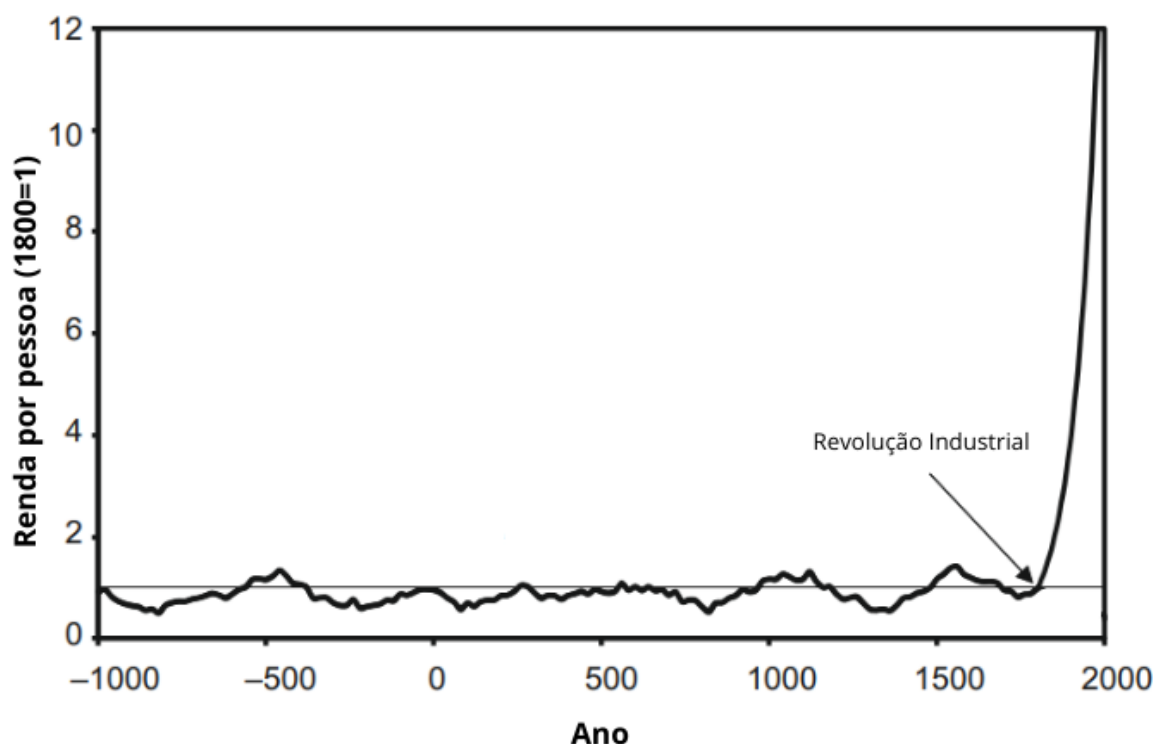
A Primeira Revolução Industrial é considerada, sob diversos aspectos, um dos marcos mais importantes da história da humanidade, não apenas pelo impacto imediato em seu período, mas também por ainda influenciar e moldar o mundo contemporâneo. Seu conceito central é relativamente simples: consistiu na aplicação de novas fontes de energia ao processo produtivo, que passaram a substituir, em parte, a força de trabalho humana e animal (STEARNs, 2020).

Não há uma data ou local exatos que determinem seu início e, para muitos que a vivenciaram, essa transformação pode até ter passado despercebida. No entanto, a Revolução alterou profundamente a forma como as pessoas viviam, se comportavam e se relacionavam. Assim, a história da Primeira Revolução Industrial é, essencialmente, a análise de todos os impactos positivos e negativos decorrentes desse processo de transformação (STEARNs, 2020).

As máquinas a vapor desempenharam um papel central na Primeira Revolução Industrial, sendo responsáveis por impulsionar a produção em larga escala e pela transformação dos meios de transporte (DICKINSON, 2022). Para viabilizar esse processo, um minério que até hoje permanece dominante na matriz energética global passou a ser utilizado de forma intensiva: o carvão mineral. Composto majoritariamente por carbono e hidrocarbonetos, o carvão apresenta elevada concentração de energia, liberada por meio de sua combustão. No contexto da Primeira Revolução Industrial, essa energia foi convertida em movimento, alimentando motores industriais e possibilitando o surgimento de novos meios de transporte, como locomotivas e navios a vapor, que revolucionaram a mobilidade e a logística mundial (GASPAROTTO; MARTINELLO, 2021).

De acordo com Clark (2014), a Revolução Industrial foi responsável por um acentuado desenvolvimento econômico e tecnológico entre os anos 1800 e 2000, como apresentado na Figura 3. Pode-se afirmar, inclusive, que a sociedade contemporânea só existe em razão dos desdobramentos desse período histórico. A necessidade de mão de obra atraiu milhares de pessoas das áreas rurais para os centros industriais, o que resultou no adensamento populacional e em condições caóticas nas cidades. Do ponto de vista econômico, essa transformação e a utilização do carvão como fonte primária de energia foram revolucionárias, mas as consequências ambientais permanecem perceptíveis até hoje (GASPAROTTO; MARTINELLO, 2021).

Figura 3 – Evolução da renda por pessoa antes e após a Revolução Industrial.



Fonte: Adaptado de Clark (2014).

Apesar de o carvão ainda ser uma das principais fontes de energia, o petróleo e o gás natural constituem outros combustíveis fósseis amplamente utilizados. O petróleo, enquanto combustível fóssil, foi desenvolvido muito depois do carvão mineral, mas sua existência já era conhecida na antiguidade, como nos depósitos de betume utilizados por sumérios, assírios e babilônios em construções, impermeabilizações e até em práticas médicas. Entretanto, foi apenas no século XIX que o petróleo começou a ser extraído comercialmente, com Edwin Drake sendo creditado como o pioneiro desse processo. No século XX, a produção de petróleo se intensificou, especialmente após a Segunda Guerra Mundial, período em que a demanda por automóveis, eletrodomésticos e outros bens derivados do petróleo cresceu significativamente. Nessa época, os Estados Unidos se tornaram o maior consumidor de petróleo do mundo. Na década de 1960, o país passou a importar petróleo para suprir sua demanda, até o ponto em que um terço de seu consumo era atendido por importações. Entretanto, em 1973, os países árabes membros da OPEP (Organização dos Países Exportadores de Petróleo) impuseram um embargo às nações que apoiaram Israel na Guerra do Yom Kippur, especialmente os Estados Unidos, levando o petróleo a enfrentar sua primeira grande crise (SOEDER, 2022).

Similarmente ao petróleo, o gás natural também já era conhecido desde os povos antigos, como os da região da Pérsia, que interpretavam as chamas provenientes de vaza-

mentos de gás como fenômenos divinos ou sobrenaturais. Entretanto, o valor energético do gás começou a ser reconhecido na China, onde também foi perfurado o primeiro poço de gás natural, em 211 a.C. Os chineses construíram tubulações de bambu para transportar o gás e utilizá-lo na dessalinização da água do mar. Entretanto, o primeiro uso comercial do gás natural a partir de sua extração subterrânea ocorreu em 1821, quando William Hart perfurou o primeiro poço na América do Norte, em Fredonia (SPEIGHT, 2018). Ao longo do século XX, novas tecnologias passaram a permitir o transporte do gás sob alta pressão e em grandes volumes, expandindo sua utilização. No entanto, foi a crise do petróleo nas décadas de 1960 e 1970 que impulsionou sua adoção global, consolidando o gás natural como uma importante alternativa energética (MOKHATAB; POE; MAK, 2018).

3.1.2 Sistema de distribuição de energia atual

A invenção da lâmpada incandescente por Thomas Edison representou um marco para a história da engenharia elétrica. Sua descoberta, datada no ano de 1879, foi essencial não apenas por oferecer uma fonte confiável e eficiente de luz artificial, mas também por ter conduzido, nos anos seguintes, à criação da primeira central elétrica do mundo, a *Pearl Street Station* (MILLER; PASERBA, 2024; ISRAEL, 2024). Quando registrou a patente da lâmpada, Edison já demonstrava a idealização de uma estação de energia ao declarar:

"O objetivo desta invenção é organizar um sistema para a geração, fornecimento e consumo de eletricidade, seja para iluminação, para força motriz, ou para ambos, de modo que todas as operações relacionadas, que exijam cuidados especiais, atenção ou conhecimento técnico, sejam realizadas para muitos consumidores em estações centrais, deixando aos consumidores apenas a tarefa de ligar ou desligar o fornecimento."

A *Pearl Street Station* foi inaugurada em 1882 e responsável por gerar e distribuir energia elétrica para um distrito de Nova York, com área aproximada de 0,65 km², que incluía escritórios, lojas e residências. O minério utilizado na *Pearl Street Station* para produzir vapor e alimentar os motores que geravam energia em corrente contínua é o mesmo apresentado anteriormente e que permanece dominante na matriz energética mundial: o carvão mineral. Edison, à época, tinha em mente a criação de um sistema de distribuição capaz de atender um bairro inteiro e todos os potenciais usos da eletricidade (MILLER; PASERBA, 2024).

Apesar da eficiência do modelo proposto por Edison, que incluía inclusive um avançado controle de tensão para a época, a proposta de corrente alternada, defendida por George Westinghouse e Nikola Tesla, acabou prevalecendo. Esse sistema, baseado no uso de alta voltagem para a transmissão de energia a longas distâncias, reduzia significativamente as perdas no transporte e constitui, até hoje, a base do sistema de distribuição elétrica moderno (BALOH, 2024).

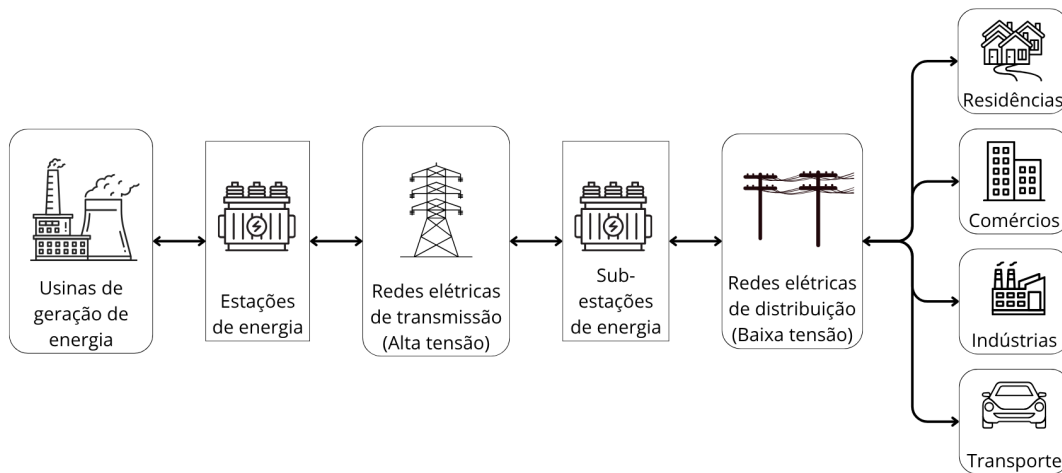
Dessa forma, o sistema de distribuição de energia atual é composto, principalmente, pelas etapas de geração, transmissão e distribuição. Na etapa de geração, a energia elétrica

é produzida a partir de diferentes fontes, como carvão, petróleo, gás natural, nuclear, hidráulica, eólica, solar e geotérmica, entre outras, e fornecida aos usuários finais por meio de uma rede com fluxo unidirecional. Uma importante característica desse tipo de sistema é que não há armazenamento de energia, dessa forma, ele opera em tempo real, gerando e transmitindo eletricidade no exato momento em que, por exemplo, o interruptor de uma lâmpada é acionado. Para realizar o controle da geração de energia, dois parâmetros são utilizados: frequência e tensão. Quando o consumo de energia elétrica aumenta, é detectada uma pequena variação na frequência da rede, ajustando-se a geração para equilibrar produção e consumo. Paralelamente, a tensão na rede é controlada para garantir estabilidade nos barramentos e gerenciamento da potência reativa, oferecendo energia de melhor qualidade e evitando perdas (BLUME, 2025).

Na fase de transmissão, considerada a espinha dorsal do sistema de energia, a energia é convertida em alta tensão por meio de transformadores elevadores, com o objetivo de aumentar a eficiência do transporte, sendo então conduzida até as estações de distribuição. Nessa etapa, encontram-se diversos equipamentos de proteção e um gerenciamento totalmente centralizado da energia (BLUME, 2025).

Por fim, na etapa de distribuição, a energia elétrica é novamente transformada em baixa tensão e entregue aos consumidores finais. Nesse processo, técnicas de controle e dispositivos de proteção, como fusíveis, relés eletromecânicos e religadores eletromecânicos, são aplicados em pontos específicos para garantir o funcionamento do sistema. Entretanto, como o fluxo é unidirecional, as redes de distribuição tradicionais não recebem resposta imediata do consumidor final, fazendo com que as decisões de controle sejam majoritariamente baseadas em estimativas (NDAHEPELE; CHOWDHURY, 2020). Na Figura 4, é apresentada a estrutura base de um sistema de energia tradicional.

Figura 4 – Estrutura de um sistema de energia convencional.



Fonte: Elaborado pelo autor.

Esse tipo de rede funcionou de forma eficaz e atendeu às necessidades da sociedade por mais de 100 anos, mas duas tendências têm impactado os sistemas de energia e gerado debates sobre a necessidade de sua adequação: crescimento da demanda por energia e mudanças climáticas.

3.1.3 Crescimento Populacional e Mudanças Climáticas

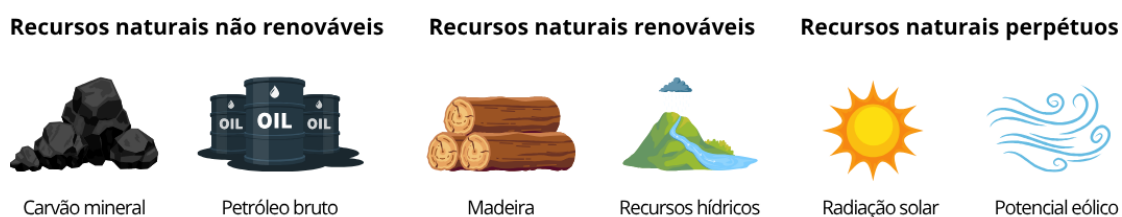
A população mundial continua a crescer a cada ano, tendo atingido o patamar de 7 bilhões de habitantes em 2010, com projeção de alcançar 10 bilhões até o final do século XXI. Considerando que a energia elétrica se tornou essencial para a humanidade e é utilizada em diversos setores do cotidiano, como transporte, agricultura e indústria, o aumento populacional está diretamente associado ao crescimento da demanda por eletricidade (MAJA; AYANO, 2021). Entretanto, o aumento do consumo e do número de usuários conectados à rede eleva a complexidade dos sistemas de energia, pois intensifica a necessidade de recursos para garantir confiabilidade, eficiência e segurança em toda a rede, impondo novos desafios ao gerenciamento centralizado das redes tradicionais. Vale ressaltar que, apesar do expressivo crescimento da demanda, não foram realizadas mudanças significativas nas infraestruturas elétricas, ao mesmo tempo que os objetivos operacionais tradicionais das concessionárias de energia sempre foram fornecer eletricidade confiável ao menor custo possível, mantendo tensão e frequência constantes, garantindo segurança

e estabilidade adequadas, além de mitigar impactos negativos à população e ao meio ambiente, bem como reduzir perdas de energia (BELU, 2022).

Além de impor novos desafios de segurança aos sistemas de distribuição, o crescimento populacional representa uma das preocupações mais críticas do mundo moderno, especialmente devido ao aumento do consumo de recursos naturais não renováveis e aos impactos ambientais associados. Um recurso natural é, por definição, "uma fonte material de riqueza que ocorre em estado natural e tem valor econômico", apresentando três características principais: 1) provém da Terra; 2) existe independentemente da ação humana; e 3) possui utilidade. O termo utilidade refere-se ao valor que o recurso natural tem para a humanidade, podendo variar ao longo do tempo, de acordo com as necessidades humanas, além de ser relativo entre diferentes sociedades (JAIN *et al.*, 2025).

Os recursos naturais, conforme apresentado na Figura 5, podem ser classificados em não renováveis, renováveis e perpétuos. Os recursos não renováveis são materiais finitos que não podem ser repostos e cujo uso excessivo pode ser prejudicial ao meio ambiente, como combustíveis fósseis, minerais e metais. Os recursos renováveis possuem capacidade de regeneração quando utilizados de forma sustentável, mas podem se tornar escassos caso a exploração supere seu ritmo de reposição, como madeira, solo fértil e recursos hídricos. Por fim, os recursos perpétuos são renováveis e não se esgotam independentemente do uso humano, como a radiação solar e o potencial eólico (JAIN *et al.*, 2025).

Figura 5 – Classificação dos recursos naturais.



Fonte: Elaborado pelo autor.

Fontes de energia primária provenientes de recursos naturais não renováveis, sobretudo os combustíveis fósseis, como carvão, petróleo e gás natural, desempenharam um papel fundamental para a sociedade ao impulsionar a industrialização, como visto anteriormente, e, conseqüentemente, o crescimento econômico. A presença abundante e acessível desses recursos foi a base do crescimento de diversos países em áreas-chave para a sociedade, como manufatura, transporte e construção, além de fomentar o desenvolvimento tecnológico em muitos aspectos. Em uma mensagem ao Congresso dos Estados Unidos, Kennedy (1961) destacou a importância dos recursos naturais:

“Desde o início da civilização, a riqueza e o progresso fundamentais de cada nação derivaram, em grande medida, de seus recursos naturais. Esta nação tem sido, e continua a ser, especialmente afortunada pelas bênçãos que herdamos. Toda a nossa sociedade se baseia — e depende — de nossas águas, nossas terras, nossas florestas e nossos minerais. A forma como utilizamos esses recursos influencia nossa saúde, segurança, economia e bem-estar.”

Ainda hoje, aproximadamente 68,3% da energia produzida mundialmente provém de fontes não renováveis (ENERDATA, 2025). Entretanto, as fontes de energia não renováveis, apesar da eficiência, acarretam diversos impactos negativos ao meio ambiente, como contaminação do ar e da água, prejuízos à saúde humana, perda de habitats naturais e de vida selvagem devido à exploração, e aquecimento global (PARAMATI; SHAHZAD; DOĞAN, 2022; KHAN *et al.*, 2022).

Ao mesmo tempo, as fontes de energia renováveis, provenientes de recursos naturais renováveis ou perpétuos, surgem como uma alternativa eficiente para a substituição das fontes não renováveis, uma vez que sua disponibilidade na natureza também é abundante (ou infinita, no caso dos recursos perpétuos) e seu uso é sustentavelmente menos danoso, apresentando emissões de carbono mínimas ou até mesmo nulas, auxiliando na mitigação das mudanças climáticas. Além dos fatores mencionados, a adoção das fontes de energia renováveis também se alinha com os objetivos sustentáveis de acordos internacionais, como o Acordo de Paris e a Agenda 2030 (IWUANYANWU *et al.*, 2022).

O Acordo de Paris é um acordo mundial sobre mudanças climáticas assinado em 2015, que visa a adoção de medidas sustentáveis para a mitigação das mudanças climáticas. Nesse acordo, representantes de 196 países concordaram em reduzir suas emissões de gases de efeito estufa para assegurar um meio ambiente mais seguro e estável. Em resumo, o Acordo de Paris busca proteger as gerações presentes e futuras de um ambiente incerto e potencialmente perigoso, garantindo o direito de viver em um ambiente saudável e livre de poluentes, sem os impactos negativos das mudanças climáticas (NATIONS, 2015a; MAKKA; ALABID, 2022).

A Agenda 2030 foi publicada pela ONU (Organização das Nações Unidas) em 2015 e contém 17 ODS (Objetivos de Desenvolvimento Sustentável) a serem alcançados até 2030. Esse documento, também elaborado em conjunto com diversos países, tem como lema “Ninguém será deixado para trás”, e possui cinco grandes áreas principais: pessoas, planeta, prosperidade, paz e parcerias. Segundo a Nations (2015b), trata-se de um plano de ação para o planeta e suas populações, com foco na colaboração entre diferentes nações para a realização dos 17 ODS, visando um mundo mais resiliente e sustentável.

Entre os 17 ODS, o ODS 7 define o acesso à energia como um direito humano fundamental e estabelece a meta de garantir que todas as pessoas tenham acesso confiável, moderno e a preços acessíveis à energia até 2030. O ODS 7 prevê aumentar substancialmente a participação de energias renováveis na matriz energética global, além de dobrar a taxa mundial de melhoria da eficiência energética. Também estabelece a necessidade de

cooperação internacional para impulsionar o desenvolvimento de pesquisas e tecnologias relacionadas à energia limpa, bem como promover o investimento em infraestrutura e tecnologias sustentáveis, expandindo e modernizando os sistemas de fornecimento de energia para torná-los mais acessíveis e sustentáveis para todos. A Nations (2015b) descreve os objetivos do ODS 7 nos seguintes tópicos:

7.1 Até 2030, garantir o acesso universal a serviços de energia acessíveis, confiáveis e modernos.

7.2 Até 2030, aumentar substancialmente a participação de energias renováveis na matriz energética global.

7.3 Até 2030, dobrar a taxa global de melhoria da eficiência energética.

7.a Até 2030, fortalecer a cooperação internacional para facilitar o acesso à pesquisa e às tecnologias de energia limpa, incluindo energias renováveis, eficiência energética e tecnologias avançadas e mais limpas de combustíveis fósseis, além de promover o investimento em infraestrutura de energia e em tecnologias de energia limpa.

7.b Até 2030, expandir a infraestrutura e modernizar a tecnologia para o fornecimento de serviços de energia modernos e sustentáveis para todos nos países em desenvolvimento, em especial nos países menos desenvolvidos, nos pequenos Estados insulares em desenvolvimento e nos países em desenvolvimento sem litoral, de acordo com seus respectivos programas de apoio.

Instituições governamentais em todo o mundo têm demonstrado comprometimento com a modernização das redes de energia, necessária para viabilizar o uso de fontes renováveis e para o cumprimento do Acordo de Paris e da Agenda 2030 (DI FOGGIA, 2020). Entre as fontes de energia renováveis disponíveis, destacam-se: energia solar, eólica, geotérmica, hidráulica e de biomassa. Cada uma oferece benefícios e apresenta desafios específicos, sendo a escolha da fonte energética dependente de considerações econômicas, geográficas e ambientais (SINSEL; RIEMKE; HOFFMANN, 2020).

A energia solar é uma das fontes renováveis mais significativas atualmente. Ela converte a luz solar em eletricidade por meio do efeito fotovoltaico e se destaca pela flexibilidade de instalação, podendo ser implementada inclusive em residências (MAKA; ALABID, 2022). O custo de produção dos painéis fotovoltaicos tem diminuído progressivamente, tornando essa fonte de energia mais acessível e, em alguns casos, a alternativa menos onerosa, com vida útil aproximada de 30 anos. Entretanto, o desempenho dos sistemas solares depende de fatores como localização geográfica, condições climáticas e orientação dos painéis, que influenciam diretamente a produção total de energia (IWUANYANWU *et al.*, 2022).

A energia eólica é obtida a partir da força do vento por meio de aerogeradores que convertem a energia cinética em eletricidade. Trata-se de uma das fontes que mais crescem globalmente, principalmente devido à eficiência e ao baixo impacto ambiental. Turbinas de geração eólica são instaladas em parques eólicos de grande escala, mas também podem ser aplicadas, com turbinas de menor escala, em residências e comércios, configurando uma fonte de energia descentralizada. Entretanto, a geração depende da intensidade e

constância dos ventos, além de ainda apresentar problemas em ambientes urbanos, como ruído, estética e impactos na fauna local (IWUANYANWU *et al.*, 2022).

A energia geotérmica é obtida a partir do calor interno da Terra, aproveitado por meio de reservatórios subterrâneos de vapor ou água quente. Esse calor pode ser usado para geração de eletricidade em usinas geotérmicas ou para aquecimento direto em residências, estufas e indústrias, estando disponível continuamente. É considerada, inclusive, a primeira fonte de energia utilizada pela humanidade. Entretanto, seu acesso é limitado e requer alto investimento, fazendo com que a utilização geotérmica dependa do nível de desenvolvimento do país, além de sua disponibilidade não ser uniforme globalmente (DINCER; OZTURK, 2021; IWUANYANWU *et al.*, 2022).

A energia de biomassa envolve o uso de materiais orgânicos para produzir energia, incluindo plantas e resíduos animais. A forma mais comum é a proveniente de culturas agrícolas, mas também inclui resíduos florestais e esterco animal. Esses materiais são queimados para gerar eletricidade ou aquecimento (IWUANYANWU *et al.*, 2022).

A energia hidráulica converte a queda de grandes volumes de água em eletricidade, transformando a energia potencial em energia cinética, que é então convertida em eletricidade através de turbinas e alternadores. Para potencializar a geração, são construídas represas e reservatórios para regulação do fluxo de água. A energia hidráulica é a fonte renovável mais utilizada globalmente, mas exige alto investimento inicial e pode causar alagamentos, perda de biodiversidade e alterações nos ecossistemas locais ao ser instalada (KAMRAN; FAZAL, 2021).

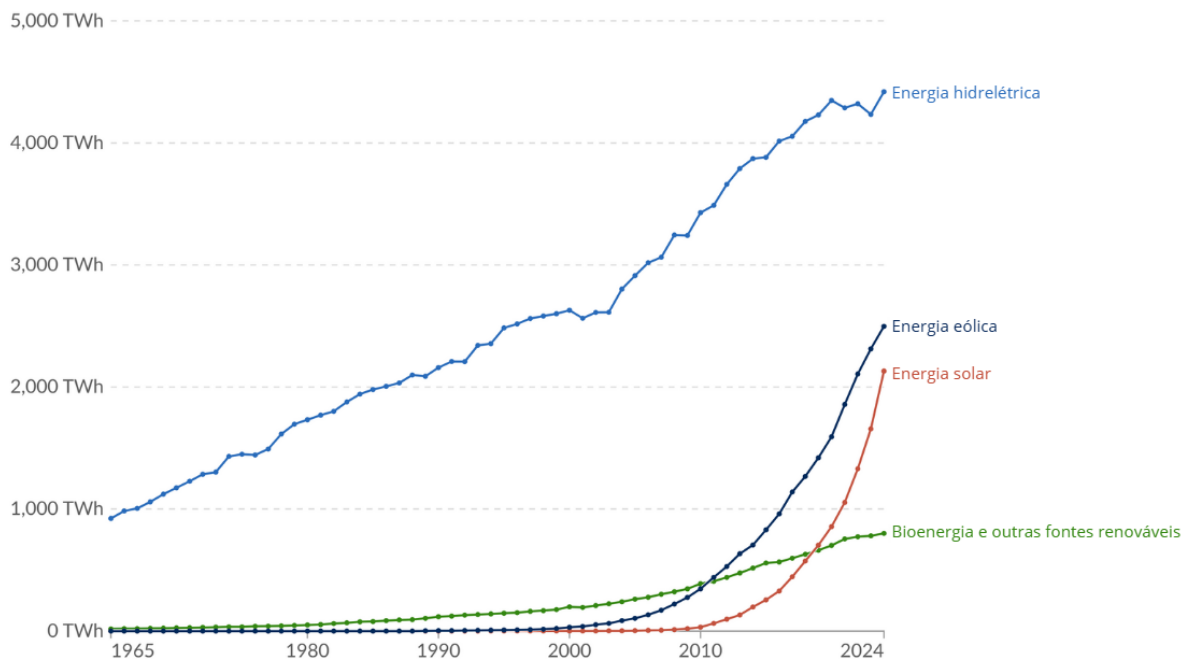
Diante das mudanças climáticas provocadas pelo uso de combustíveis fósseis, a utilização de fontes renováveis tem crescido, especialmente energia solar e eólica, com quotas globais de 6% e 8% na capacidade instalada e aumentos médios anuais de 19,84% e 10,63%, respectivamente, de 2019 a 2024 (DATA, 2025). Na Figura 6, observa-se a crescente demanda por essas fontes de energia.

Figura 6 – Evolução da geração de energia renovável no mundo.

Geração de energia renovável por fonte no mundo

Medido em terawatts-hora

Our World
in Data



Fonte: Ember (2025); Energy Institute - Statistical Review of World Energy (2025)

Nota: "Outras fontes renováveis" incluem energia geotérmica, das ondas e das marés

OurWorldinData.org/renewable-energy | CC BY

Fonte: Adaptado de Data (2025).

Entretanto, a integração em larga escala de fontes renováveis, especialmente de geração descentralizada, traz novos desafios para a operação e controle das redes de energia, podendo afetar sua confiabilidade, qualidade e estabilidade, tornando necessária, mais uma vez, a adequação da infraestrutura atual (AHMED *et al.*, 2020; NDAHEPELE; CHOWDHURY, 2020).

3.1.4 A rede elétrica do futuro

Em resumo, nos sistemas de energia tradicionais, a energia é consumida a partir de grandes centros centralizados de geração, sem monitoramento avançado e com controle de malha aberta (WANG, Y. *et al.*, 2022). Esse tipo de rede funcionou de forma eficaz por mais de 100 anos, como discutido anteriormente, mas a crescente demanda por energia e a dificuldade para integração das fontes renováveis tem se tornado um desafio tanto para a produção quanto para a distribuição aos usuários finais. Para um funcionamento mais eficiente das redes de energia nesse novo cenário, é necessária a incorporação de novas tecnologias às redes de energia que possibilitem a coleta de dados e o fluxo bidirecional de informações, que permitiria a aplicação de técnicas avançadas de processamento e controle, como o uso de inteligência artificial, resultando na criação de um sistema de energia

inteligente (BELLIZIO *et al.*, 2022; BUTT, O. M.; ZULQARNAIN; BUTT, T. M., 2021). Nesse novo sistema de energia, considerada a rede elétrica do futuro, três características se destacam: digitalização, descentralização e descarbonização (WANG, Y. *et al.*, 2022).

O termo digitalização consiste na integração de tecnologias digitais, tanto de software quanto de hardware, que permitem ampla coleta de dados, possibilitando o monitoramento e o controle em tempo real, e que maximizam o uso da energia elétrica (JUDSON; FITCH-ROY; SOUTAR, 2022). A descentralização refere-se à incorporação de novas fontes geradoras de energia à rede elétrica, como geração solar e geração eólica, e a utilização de centros de armazenamento de energia. Este último possibilita que o excedente produzido em períodos de baixa demanda seja armazenado e utilizado em momentos de maior consumo, promovendo maior eficiência na utilização da energia, além de integrar de maneira eficiente toda a energia gerada na rede elétrica (AZAD, 2020). A descarbonização, por sua vez, é consequência direta dos processos de digitalização e descentralização, haja vista que a adoção de tecnologias de monitoramento torna o uso da energia mais eficiente, reduzindo desperdícios, enquanto a descentralização da geração promove maior flexibilidade nos sistemas de transmissão, viabilizando a redução das emissões de carbono.

O conceito de rede elétrica do futuro, que a torna inteligente e capaz de lidar com o aumento da demanda ao mesmo tempo em que garante confiabilidade, segurança e eficiência, além de possibilitar a utilização de energia renovável gerada de forma descentralizada, é conhecido como *Smart Grids*, ou Redes Elétricas Inteligentes (BUTT, O. M.; ZULQARNAIN; BUTT, T. M., 2021).

3.2 REDES ELÉTRICAS INTELIGENTES

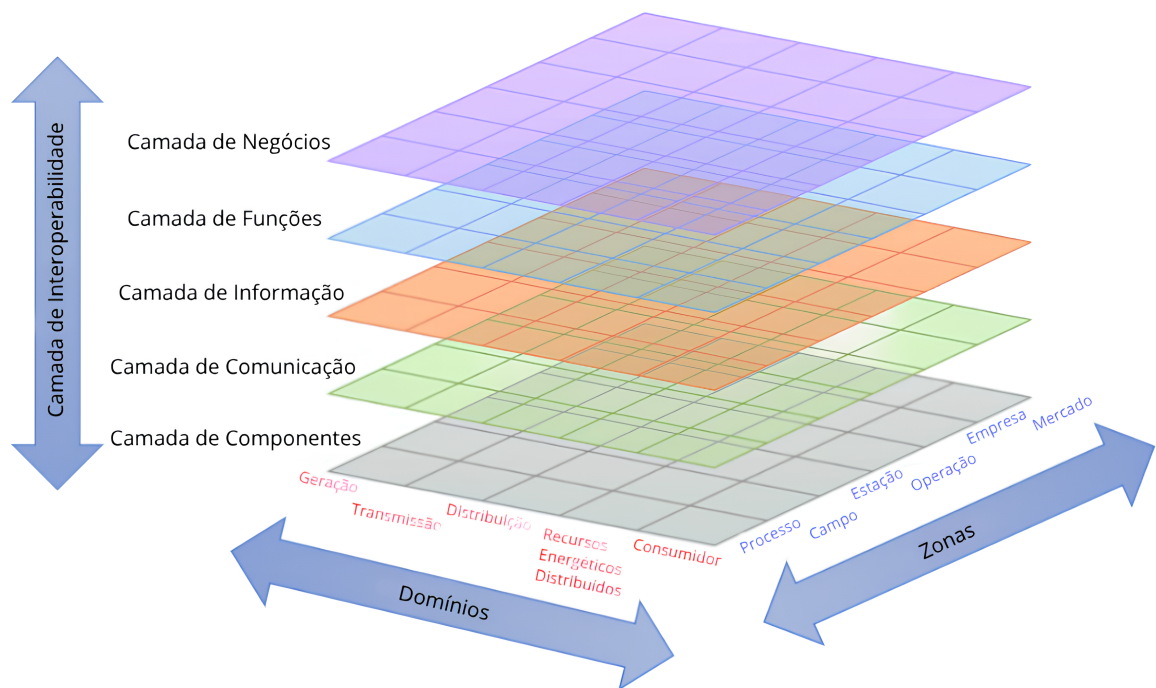
3.2.1 Definição e características

As Redes Elétricas Inteligentes, de acordo com Judge *et al.* (2022), representam uma evolução às redes elétricas tradicionais, em que é possível coletar dados de todos os usuários conectados à essa rede, sejam eles consumidores ou geradores, para entregar energia de maneira mais econômica, segura e sustentável. Além disso, em uma Rede Elétrica Inteligente, são oferecidos controles abrangentes de tensão e frequência, e um gerenciamento mais inteligente da energia em toda a rede elétrica, com fluxo de eletricidade bidirecional e fluxo de informações constante, que permitem criar uma rede de distribuição de eletricidade automática e distribuída (MUQEET *et al.*, 2023).

Dessa forma, as Redes Elétricas Inteligentes tem como objetivo garantir a máxima eficiência, segurança e qualidade de uma rede elétrica, enquanto incorpora tecnologias digitais avançadas de controle, sensoriamento, tecnologia da informação e automação, sendo uma peça chave também para a transição energética visto a maior facilidade para integração de energias renováveis com fontes de energia convencionais, além de possibilitar uma utilização mais eficiente da energia (CAMPANA *et al.*, 2025).

Na literatura, diferentes arquiteturas foram propostas para a estruturação das redes elétricas inteligentes, como o modelo SGAM (*Smart Grid Architecture Model*), arquitetura padronizada europeia, e o modelo NIST (*National Institute of Standards and Technology*), arquitetura padronizada dos Estados Unidos. O modelo SGAM, apresentado na Figura 7 fornece uma abordagem para o desenvolvimento da arquitetura das redes inteligentes, sendo composto por cinco camadas, que são negócios, funções, informação, comunicação e componentes, conhecidas como camadas de interoperabilidade. Além das camadas, há os domínios, que representam os serviços presentes na rede elétrica, como geração, transmissão, distribuição, recursos energéticos distribuídos e consumidores, e também as zonas, que correspondem aos níveis hierárquicos de gestão dos sistemas de energia. O principal objetivo desse modelo é mostrar quais domínios interagem entre si e por meio de quais zonas de gerenciamento da informação, além de definir um padrão para o desenvolvimento de redes elétricas inteligentes, permitindo identificar em que parte do modelo, ou seja, em qual domínio, zona e camada, uma função deve existir na rede elétrica.

Figura 7 – Modelo SGAM.

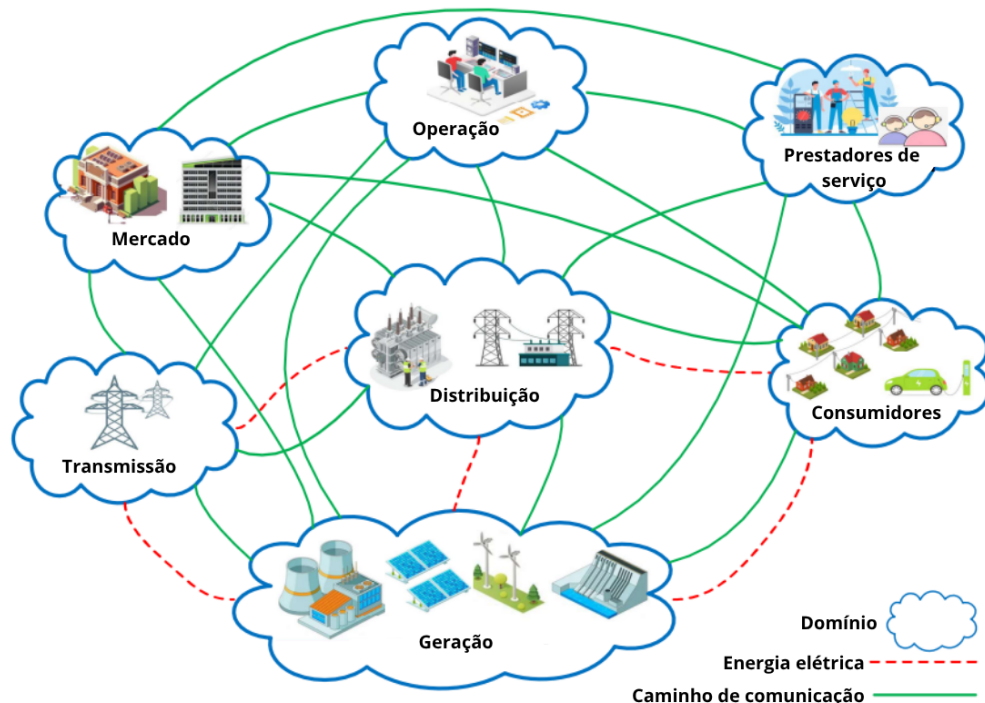


Fonte: Adaptado de Kirmani *et al.* (2022).

De acordo com o NIST (*National Institute of Standards and Technology*), as redes elétricas inteligentes são divididas em sete domínios: geração, transmissão, distribuição, consumidores, prestadores de serviço, mercados e operações, em contraposição aos três

domínios das redes tradicionais. Os domínios de geração, transmissão e distribuição funcionam de maneira similar aos das redes tradicionais, mas incorporam fontes de energia renováveis, sistemas de armazenamento de energia e tecnologias digitais para monitoramento avançado. O domínio dos prestadores de serviço refere-se às empresas responsáveis por gerenciar a entrega de energia, faturamento, consumo e serviços relacionados. O domínio dos consumidores compreende os usuários finais da energia, incluindo residências, comércios e indústrias, nos quais os consumidores podem não apenas consumir energia, mas também produzi-la e armazená-la, além de participar da gestão do lado da demanda, ajustando o uso de energia com base em sinais de preço ou nas necessidades do sistema. O domínio de mercado refere-se aos facilitadores do mercado de energia, que incentivam ações para melhorar o desempenho do sistema elétrico, como incentivos para quem gera ou economiza energia. Nesse domínio também se encontram plataformas de comércio de energia, precificação em tempo real e supervisão regulamentada. Por fim, o domínio de operação tem como objetivo controlar e otimizar a rede, incluindo sistemas de operação e controle avançados, algoritmos de otimização e medidas de cibersegurança (ALOMARI *et al.*, 2025; MORENO ESCOBAR *et al.*, 2021). Na Figura 8, são apresentados os domínios de uma rede elétrica inteligente de acordo com o modelo NIST.

Figura 8 – Modelo NIST.

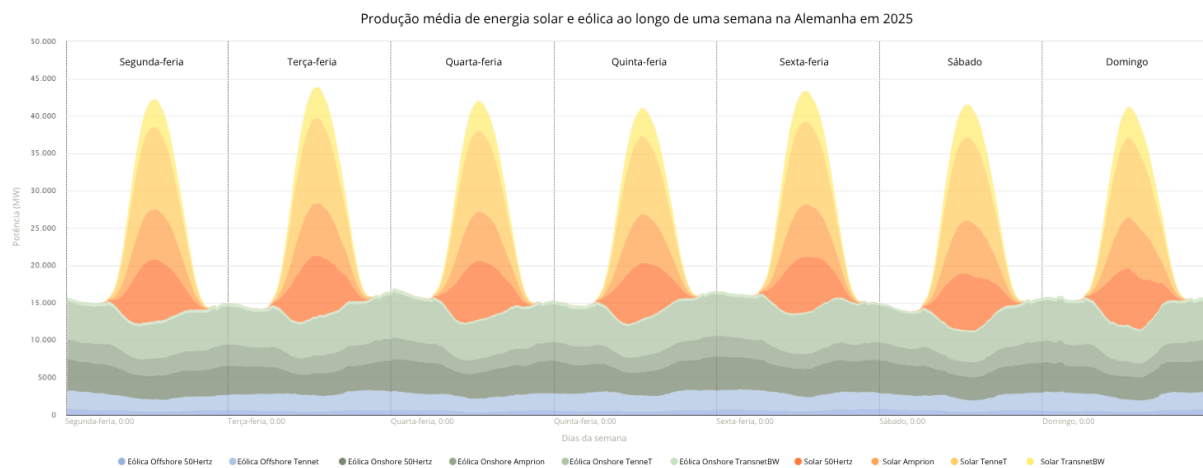


Fonte: Adaptado de Alomari *et al.* (2025).

3.2.1.1 Sistemas de Armazenamento de Energia

Em uma rede elétrica inteligente, a integração de fontes de energia renováveis é facilitada e considerada uma demanda crítica, haja vista que essas fontes são abundantes, sustentáveis, escaláveis e aplicáveis a diversos setores, como industrial, comercial, residencial e agrícola. Entretanto, a geração de energia renovável, especialmente a proveniente de radiação solar, não é linear, apresentando picos de produção durante o dia e baixa geração durante a noite (ABDALLA *et al.*, 2021). Na Figura 9, são mostrados dados de produção média de energia solar e eólica ao longo de uma semana na Alemanha durante o ano de 2025, nos quais é possível observar esses picos de produção.

Figura 9 – Produção média de energia solar e eólica ao longo de uma semana na Alemanha durante o ano de 2025.

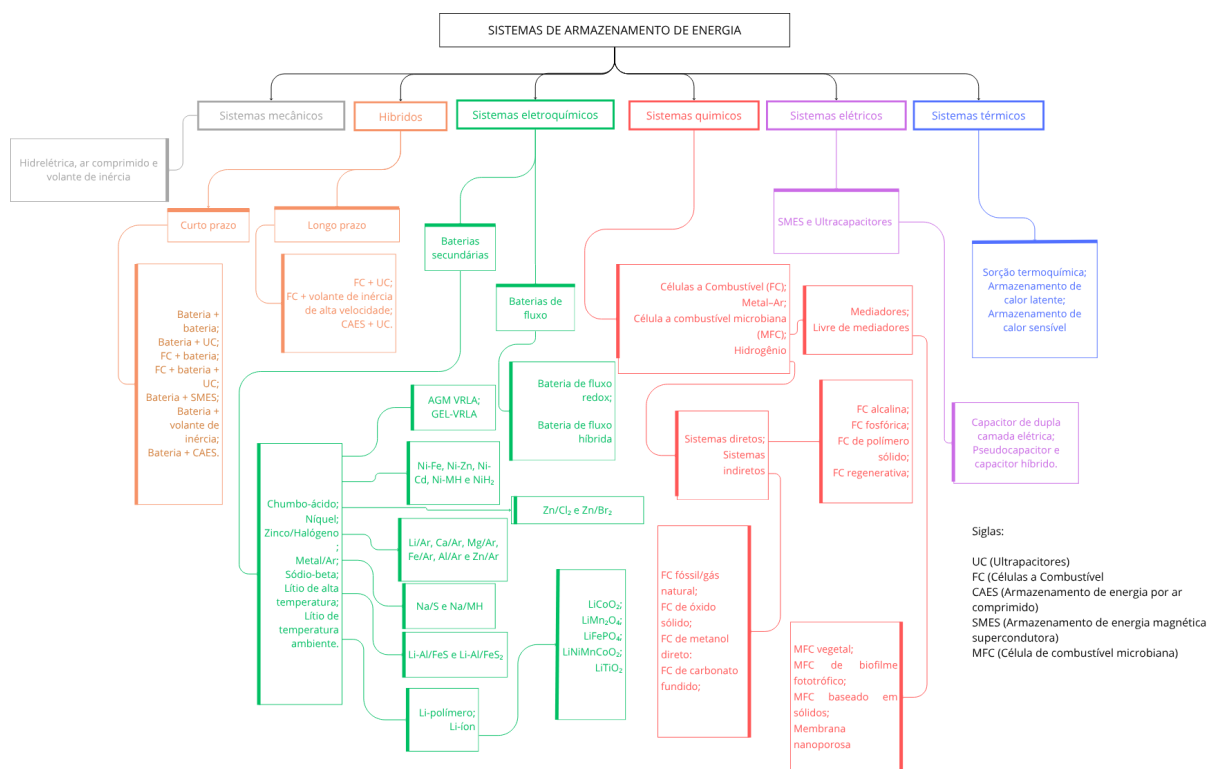


Fonte: Adaptado de (ENERGY-CHARTS, 2025)

Dessa forma, a implementação de sistemas de armazenamento de energia torna-se essencial para superar essa limitação, ao possibilitar o estoque de energia durante períodos de produção excessiva. Além disso, de acordo com Tan *et al.* (2021), diversos outros benefícios são adicionados às redes elétricas quando sistemas de armazenamento são integrados, trazendo vantagens para todas as etapas do setor elétrico. Para os operadores da rede, desde a geração até a distribuição, o uso de sistemas de armazenamento permite a redução de custos operacionais, auxilia no equilíbrio entre oferta e demanda e melhora a qualidade e a confiabilidade do fornecimento de energia. Para os consumidores, sejam eles industriais, comerciais ou residenciais, esses sistemas possibilitam a redução dos custos com eletricidade, a disponibilidade de energia durante eventos climáticos adversos e apagões, bem como a oportunidade de gerar receita por meio da participação no mercado de energia, vendendo excedentes, oferecendo serviços à rede para regulação de tensão e frequência e participando de programas de resposta à demanda.

Os sistemas de armazenamento de energia são divididos em seis categorias: sistemas mecânicos, eletroquímicos, elétricos, térmicos, químicos e híbridos. Entre essas categorias, encontram-se diferentes tecnologias, como baterias, supercapacitores, armazenamento por ar comprimido, armazenamento hidrelétrico por bombeamento, sistemas de hidrogênio, volantes de inércia, armazenamento de energia magnética supercondutora e até mesmo veículos elétricos (TAN *et al.*, 2021; AHMAD; KHALID; PANIGRAHI, 2021; ABDALLA *et al.*, 2021). Na Figura 10, é apresentado um panorama de todas as tecnologias utilizadas em sistemas de armazenamento de energia.

Figura 10 – Sistemas de armazenamento de energia.



Fonte: Elaborado pelo autor com base em Ahmad, Khalid e Panigrahi (2021).

A escolha do sistema de armazenamento a ser utilizado depende de diversos fatores, sendo os principais a quantidade de energia que o sistema consegue armazenar, o tempo de resposta, a potência de descarga, além da eficiência necessária para a aplicação e da vida útil. Por exemplo, para a integração de fontes renováveis, é necessário um tempo de resposta muito rápido, na ordem de milissegundos, com potências variando de dezenas de quilowatts até cerca de 10 megawatts, capacidade entre 10 kWh (Quilowatt-hora) e 200 MWh (Megawatt-hora), alta eficiência e longa vida útil. Para o nivelamento da demanda, exige-se potência em escala de megawatts e capacidade energética que pode alcançar milhares de MWh, porém com tempo de resposta mais lento. Para fornecimento de energia de backup em caso de interrupção do suprimento, é necessário tempo de resposta

quase imediato, potência em megawatts e capacidade também na ordem de milhares de MWh, sendo aceitável uma eficiência média. Para qualidade de energia, requer-se resposta muito rápida, inferior a 20 milissegundos, com potências menores e atuação de curta duração, capacidade entre 50 kWh e 500 kWh, eficiência menos elevada e vida útil reduzida (ATTEYA *et al.*, 2016).

3.2.1.2 Microrredes

Microrredes, conhecidas como *microgrids*, são redes elétricas de menor escala que podem operar em conjunto com as redes de grande porte ou de forma independente. No primeiro caso, as microrredes podem enviar ou receber energia elétrica da rede principal de acordo com a demanda, enquanto, no segundo caso, operam de maneira totalmente autônoma por meio da geração descentralizada de energia. Nesse tipo de rede, a energia é produzida principalmente a partir de fontes renováveis, como painéis solares, turbinas eólicas e sistemas de mini-hidrelétricas. Para o seu funcionamento adequado, quatro componentes são considerados essenciais: fontes e geradores de energia, sistemas de armazenamento de energia, infraestrutura de distribuição de energia e sistema de controle (RAJENDRAN; RAUTE; CARUANA, 2025).

As fontes e geradores de energia dizem respeito à geração primária de energia dentro da microrrede. Nesse caso, utilizam-se principalmente as fontes renováveis, mas também podem ser empregados geradores a diesel, gás natural ou biomassa, dependendo se a microrrede opera de forma isolada ou integrada à rede principal. Os sistemas de armazenamento de energia permitem acumular o excedente produzido durante períodos de maior geração, quando a geração solar e eólica atinge seu pico, para utilização em momentos de baixa disponibilidade. A infraestrutura de distribuição de energia é responsável por transportar e distribuir a energia proveniente tanto da geração distribuída quanto dos sistemas de armazenamento até os consumidores, podendo ainda ser conectada à rede elétrica principal. Por fim, o sistema de controle é encarregado de gerenciar a geração, o armazenamento e a distribuição de energia na microrrede, assegurando maior eficiência e estabilidade (RAJENDRAN; RAUTE; CARUANA, 2025).

Além disso, por operarem de forma independente, as microrredes podem manter o fornecimento de energia elétrica mesmo em caso de falha na rede principal, assegurando a continuidade do abastecimento por meio da geração descentralizada de energia. Ao mesmo tempo, a microrrede pode ser isolada em caso de falha interna, prevenindo efeitos em cascata e apagões generalizados. Quando operando de forma isolada, conforme Bressanini *et al.* (2023), a microrrede deve garantir a estabilidade de tensão e frequência em toda a rede, respeitando as características previamente definidas de seus componentes internos, como consumidores e geradores distribuídos. Já quando conectada à rede principal, a microrrede deve monitorar os valores de tensão e frequência fornecidos por esta e, caso identifique alguma anomalia, alterar automaticamente para o modo isolado.

3.2.1.3 Dispositivos IoT

O conceito de IoT (*Internet of Things*) refere-se à conexão de diferentes dispositivos à Internet, com o objetivo principal de possibilitar o acesso e a transferência de dados entre objetos físicos e o mundo virtual (ARSHI *et al.*, 2024). Segundo Hassan (2025), a IoT pode ser analisada sob duas perspectivas: a primeira, voltada ao consumidor, engloba dispositivos como celulares, smart TVs e automóveis, enquanto a segunda, de caráter industrial, inclui redes de distribuição e usinas de geração de energia, transporte, turbinas eólicas e equipamentos industriais. No setor de energia, a IoT tem o potencial de transformar a forma como os sistemas geram, distribuem e consomem eletricidade, permitindo o monitoramento em tempo real para controle e otimização desses sistemas, oferecendo vantagens tanto para os consumidores quanto para as indústrias. Dessa forma, a IoT torna-se uma ferramenta essencial para o aprimoramento da eficiência energética (ARSHI *et al.*, 2024).

Entre os dispositivos IoT utilizados no gerenciamento de redes de energia, destacam-se os sensores inteligentes, visto que a geração de dados é uma funcionalidade essencial dos sistemas de energia inteligentes para possibilitar o controle adequado desses sistemas (RIND *et al.*, 2023). Um sensor inteligente, tipicamente, é composto por módulos de medição, computação e comunicação, permitindo medir, processar e enviar dados por meio de protocolos de comunicação para outros dispositivos ou até para uma central de controle (ARSHI *et al.*, 2024). Em uma rede elétrica inteligente, o sensor mais amplamente utilizado é o medidor inteligente de energia, uma evolução do medidor elétrico tradicional, popularmente conhecido como “medidor de luz”. Os medidores inteligentes são instalados em residências e indústrias para coletar dados de consumo de diferentes equipamentos, sendo capazes de analisar o uso de energia, fornecer informações relevantes às concessionárias e aos operadores do sistema elétrico, além de facilitar o acesso do público aos dados de consumo. Conectados à infraestrutura da rede inteligente, esses medidores também permitem a transferência de energia, o fluxo bidirecional de informações e possibilitam o desligamento remoto do fornecimento de energia, bem como a regulação do consumo máximo em pontos específicos da rede (PAUL *et al.*, 2024).

O PMU (*Phasor Measurement Unit*) é um dispositivo utilizado para estimar a magnitude e o ângulo de fase de uma grandeza fasorial elétrica, geralmente tensão ou corrente, na rede elétrica, empregando uma fonte de tempo comum para sincronização. Essa sincronização precisa do tempo é normalmente obtida por meio do GPS (Sistema de Posicionamento Global), o que permite a obtenção e comparação dos ângulos de fasores distribuídos em uma ampla região. Dessa forma, as PMU oferecem uma vantagem significativa às redes elétricas, possibilitando o monitoramento do estado operacional e da estabilidade da rede, a detecção de falta de sincronismo entre diferentes pontos, a identificação de eventos críticos e a análise da qualidade da energia (ANDRESEN *et al.*, 2018).

Os sistemas SCADA (*Supervisory Control and Data Acquisition*) referem-se a sistemas de controle amplamente utilizados para o gerenciamento de processos industriais, com aplicações que vão desde a integração de sensores e controladores em fábricas para o monitoramento e controle de linhas de produção, até o monitoramento avançado em edifícios, na agricultura e em usinas de energia. Dessa forma, os sistemas SCADA têm como objetivo fundamental possibilitar a transferência de dados úteis entre objetos do mundo real, amplamente incorporados e percebidos por dispositivos sensores, e os sistemas de controle, onde esses dados são analisados para a tomada de decisões. Em uma rede elétrica inteligente, as medições realizadas pelos sensores inteligentes e pelas PMU são coletadas pelos sistemas SCADA, possibilitando o gerenciamento, o monitoramento e o controle das redes elétricas (ALOMARI *et al.*, 2025; PAUL *et al.*, 2024).

3.2.1.4 Tecnologias de comunicação

Uma rede de comunicação estável é essencial para que a troca de informações entre os componentes da rede elétrica inteligente ocorra de forma eficiente. Entre as principais funções dos protocolos de comunicação estão a capacidade de transmitir a vasta quantidade de dados gerada por medidores inteligentes, PMU e demais dispositivos IoT presentes na rede, permitir o controle de dispositivos desde a geração até a distribuição, proteger a infraestrutura contra ataques por meio de uma comunicação robusta e possibilitar a integração contínua e ininterrupta de todos os componentes da rede (KUZLU; PIPATTANASOMPOM; RAHMAN, 2017).

Os medidores inteligentes, por exemplo, são considerados equipamentos-chave nas redes inteligentes, e diversos protocolos garantem seu funcionamento adequado, como Zigbee, IEC 62056-21 e MQTT (*Message Queuing Telemetry Transport*). Para redes residenciais, destacam-se protocolos como Zigbee, MQTT, Z-Wave, Bluetooth e CoAP (*Constrained Application Protocol*). Protocolos como Modbus, PROFIBUS (*Process Field Bus*), S7Comm (*S7 Communication*) e IEC 60870 são amplamente utilizados em automação industrial, com forte presença em subestações, plantas industriais e salas de controle no contexto das redes elétricas inteligentes. Em redes geograficamente extensas, que incluem usinas, centros de operação e subestações, encontram-se protocolos como DNP3 (*Distributed Network Protocol 3*), IEC 60870, IEC 61400-25 e Modbus. Entre os protocolos citados, destaca-se o DNP3, amplamente utilizado em sistemas SCADA no setor elétrico, sobretudo para telemetria e telecontrole em redes de transmissão e distribuição. O IEC 61850 também é muito empregado nas redes elétricas, especialmente para proteção, controle e monitoramento de subestações, permitindo a troca de mensagens em tempo real. Por fim, destaca-se a IEC 62056-21, um protocolo dominante para medidores inteligentes, utilizado para leitura, parametrização e comunicação desses dispositivos com concentradores de dados, sendo responsável por viabilizar a conexão dos consumidores às distribuidoras, a tarifação dinâmica e o monitoramento em tempo real (KUZLU; PIPATTANASOMPOM;

RAHMAN, 2017; LE *et al.*, 2022; KHOEI; SLIMANE; KAABOUC, 2022; KIRMANI *et al.*, 2022; RIND *et al.*, 2023). Na Tabela 1, apresenta-se um resumo dos protocolos mais utilizados em redes inteligentes, conforme identificado na literatura.

Tabela 1 – Protocolos de comunicação em redes inteligentes.

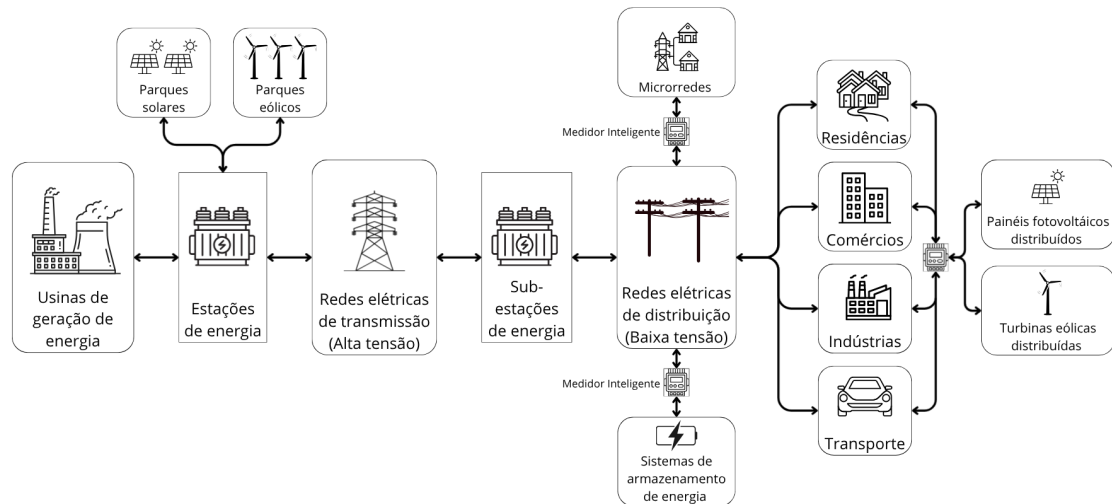
Protocolo	Descrição	Área de aplicação
MQTT	Protocolo de mensagens para comunicação entre dispositivos inteligentes	Dispositivos para automação residencial, sistemas de gerenciamento de dados, sensoriamento remoto
Modbus	Protocolo de comunicação industrial para controladores lógicos programáveis	Dispositivos para automação industrial, como CLP e sensores
Z-Wave	Protocolo utilizado para conectar e controlar dispositivos inteligentes residenciais em curto alcance	Automação residencial, eficiência energética
Zigbee	Protocolo sem fio de baixo consumo usado para conectar medidores inteligentes, sensores e atuadores em redes residenciais e industriais	Medidores inteligentes, monitoramento de energia, automação residencial
Bluetooth	Protocolo sem fio de curto alcance e baixo consumo de energia	Automação residencial
DNP3	Protocolo para automação de processos em SCADA, utilizado por empresas de energia para telemetria e telecontrole	Sistemas SCADA para usinas e estações de energia, dispositivos RTU
S7Comm	Protocolo proprietário da Siemens para controladores lógicos programáveis	Dispositivos para automação industrial, como CLP e controladores industriais
Profibus	Protocolo para comunicação em barramento de campo, nas variantes DP e PA, sendo o primeiro usado para operar sensores e atuadores por meio de um controlador centralizado, e o segundo para monitorar equipamentos de medição	Dispositivos de campo, como controladores, sensores e atuadores
IEC 61400-25	Protocolo para usinas de geração eólica e sistemas de controle	Pequenas turbinas eólicas, turbinas eólicas offshore, usinas de geração eólica, sistemas de controle para geração eólica
IEC 60870	Protocolo para telecontrole, utilizado em sistemas SCADA e RTU	Sistemas SCADA, dispositivos RTU
IEC 62056-21	Protocolo para medidores de energia, usado para leitura, parametrização e testes de medidores	Medidores inteligentes, concentradores de dados
CoAP	Protocolo leve para comunicação e controle de dispositivos IoT	Dispositivos inteligentes das redes elétricas inteligentes, sistemas de controle

Fonte: Elaborado pelo autor com base em Kuzlu, Pipattanasompom e Rahman (2017), Le *et al.* (2022), Khoei, Slimane e Kaabouch (2022), Kirmani *et al.* (2022) e Rind *et al.* (2023).

Com isso, na Figura 11 é apresentada uma representação de uma rede elétrica inteligente, cuja base estrutural é semelhante à das redes tradicionais, porém com a

adição de tecnologias que possibilitam a integração dos recursos de energia renovável distribuídos, o fluxo bidirecional de energia e de informações, a incorporação de sistemas de armazenamento de energia, e dos demais sistemas que tornam a rede mais eficiente.

Figura 11 – Estrutura de um sistema de energia inteligente.



Fonte: Elaborado pelo autor.

3.2.1.5 Vantagens e limitações das redes inteligentes

Quando comparadas às redes elétricas tradicionais, as redes elétricas inteligentes apresentam uma série de vantagens em termos de eficiência energética, qualidade da energia, resiliência e redução de impactos ambientais. O monitoramento em tempo real do consumo de energia, por exemplo, permite aos consumidores ajustar seu consumo conforme o preço da energia ou as necessidades do sistema, e até vender energia excedente para a rede, tornando-os mais participativos no mercado de energia, como visto anteriormente. As diversas tecnologias da informação aplicadas às redes também as tornam menos suscetíveis a falhas, devido ao monitoramento de ponta a ponta, além de possibilitarem o atendimento à crescente demanda por energia sem a necessidade de grandes expansões na infraestrutura, visto que o monitoramento e o controle avançados da rede facilitam essa integração. Por outro lado, embora representem uma evolução necessária e significativa em relação às redes de energia tradicionais, as redes elétricas inteligentes também apresentam limitações e vulnerabilidades que precisam ser superadas. O custo de implementação de uma rede elétrica inteligente, por exemplo, embora vantajoso em uma perspectiva de longo prazo, ainda constitui uma barreira relevante para a sua aceitação.

Além disso, desafios relacionados à segurança e à privacidade, uma vez que a integração de sistemas de informação às redes elétricas inteligentes as torna vulneráveis a possíveis ataques cibernéticos, representam uma das maiores preocupações quanto à aceitação e à implementação dessas redes. (KIRMANI *et al.*, 2022). Na Tabela 2, é apresentada uma comparação entre as redes elétricas tradicionais e as redes inteligentes.

Tabela 2 – Comparação entre as redes elétricas inteligentes e as redes elétricas tradicionais.

	Redes elétricas inteligentes	Redes elétricas tradicionais
Principal característica	Rede elétrica digital, com integração de tecnologias da informação e comunicação	Rede elétrica eletromecânica, com baixa automação e comunicação limitada
Geração	Distribuída, permitindo a inserção de múltiplas fontes de energia	Centralizada, dependendo sobretudo de grandes usinas
Comunicação	Comunicação bidirecional, com monitoramento em tempo real por meio de sensores e sistemas de dados	Comunicação unidirecional, sem monitoramento em tempo real
Restauração em caso de falhas	Capacidade de autorrecuperação	Restauração manual, dependendo de intervenção humana
Controle	Controle abrangente	Controle limitado
Confiabilidade	Alta confiabilidade e resiliência	Menor confiabilidade e maior suscetibilidade a falhas
Operação e manutenção	Baseadas em dados e manutenção preditiva	Baseadas em inspeções físicas e manutenção corretiva
Interação com os usuários	Interação ativa, com os consumidores se tornando ativos no mercado de energia	Interação passiva, com os consumidores apenas consumindo energia das grandes usinas
Eficiência energética	Alta eficiência, com redução de perdas	Baixa eficiência
Integração de energias renováveis	Elevada, suportando fontes como solar, eólica e biomassa	Limitada
Armazenamento de energia	Capacidade de integração com sistemas de armazenamento	Capacidade limitada ou inexistente
Cibersegurança	Maior vulnerabilidade a ataques cibernéticos	Menor vulnerabilidade a ataques cibernéticos
Custo	Investimento inicial elevado, mas menor custo operacional e maior eficiência no longo prazo	Investimento inicial menor, porém custos operacionais mais altos a longo prazo
Sustentabilidade	Mais sustentável, sobretudo devido à facilidade de integração de fontes renováveis e à maior eficiência energética	Menos sustentável, sobretudo devido à utilização majoritária de combustíveis fósseis para a geração de energia

Fonte: Elaborado pelo autor com base em Le *et al.* (2022) e Khoei, Slimane e Kaabouch (2022).

3.3 GÊMEOS DIGITAIS

3.3.1 Definição e características

A definição de gêmeos digitais, segundo David Jones *et al.* (2020), ainda é tema de discussões, mas as duas definições mais aceitas foram estabelecidas por Grieves e pela NASA (*National Aeronautics and Space Administration*). A NASA definiu os gêmeos digitais, no contexto aeroespacial, como “uma simulação multifísica, multiescala e probabilística integrada de um veículo ou sistema construído que utiliza os melhores modelos físicos disponíveis, atualizações de sensores, histórico da frota, entre outros, para espelhar a vida útil do seu gêmeo voador correspondente” (JONES, D. *et al.*, 2020). Posteriormente, Michael Grieves conceituou os gêmeos digitais como uma cópia digital de um ou de um conjunto de dispositivos específicos, capaz de representar, de forma abstrata, um dispositivo real, podendo ser utilizada como base para testes em situações reais ou simuladas (WANG, Z., 2020).

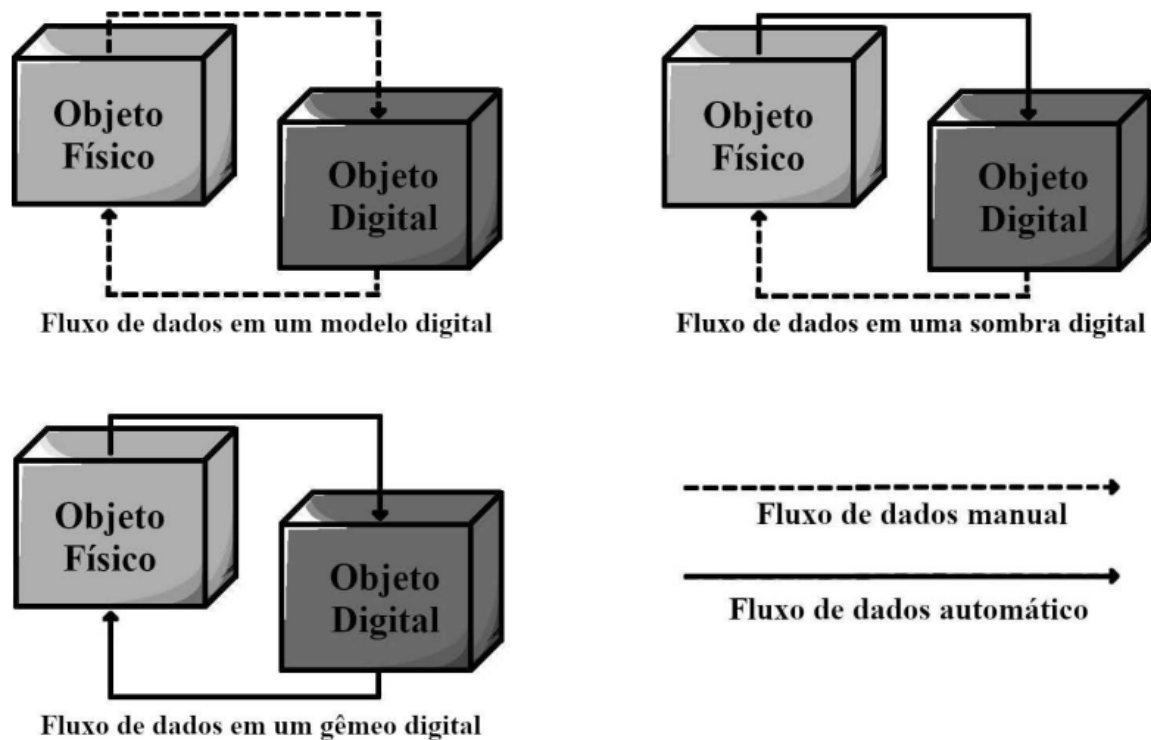
Ainda segundo David Jones *et al.* (2020), o conceito de gêmeos digitais é composto por três elementos principais: um produto físico, muito encontrado na literatura com o nome “entidade física”, uma representação virtual desse produto e uma conexão bidirecional de dados que transmite informações do sistema físico para o sistema digital, bem como dados e processos do sistema digital para o sistema físico.

De acordo com San (2021), um gêmeo digital pode ser definido como um modelo digital que evolui ao longo do tempo para representar de maneira fiel a estrutura, o comportamento e o contexto de um sistema físico único, que pode ser um simples dispositivo, um sistema composto por múltiplos dispositivos ou um processo. Dessa forma, o gêmeo digital é capaz de atuar como uma interface entre o ser humano e o sistema físico, facilitando o monitoramento e a análise do estado deste sistema. Entretanto, um gêmeo digital pode ser utilizado não apenas para o monitoramento de um sistema físico, mas também para a realização de testes e simulações que permitam explorar e prever comportamentos em um sistema desconhecido. Além disso, apesar de serem conceitos semelhantes, o gêmeo digital não é uma simulação, mas sim uma representação em tempo real do sistema físico (WANG, Z., 2020).

Segundo Passos (2024), Attaran e Celik (2023) e OLIVEIRA (2025), o tipo de fluxo de dados nos gêmeos digitais é dividido em três categorias: modelo digital, sombra digital e gêmeo digital, dependendo do nível de integração. Em um modelo digital, as alterações realizadas no sistema físico ou no sistema digital não são refletidas automaticamente, sendo necessária a intervenção manual para efetuar qualquer modificação (PASSOS, 2024; ATTARAN; CELIK, 2023; OLIVEIRA, 2025). Em uma sombra digital, quaisquer alterações do sistema físico para o sistema digital são transferidas automaticamente, exigindo, porém, intervenção manual para aplicar mudanças do sistema digital ao sistema físico (PASSOS, 2024; ATTARAN; CELIK, 2023; OLIVEIRA, 2025). O gêmeo digital, por sua

vez, apresenta um fluxo de dados bidirecional, de modo que quaisquer modificações realizadas, tanto no sistema físico quanto no digital, são refletidas automaticamente em ambos (PASSOS, 2024; ATTARAN; CELIK, 2023; OLIVEIRA, 2025). Na figura 12, são apresentados os diferentes tipos de fluxo de dados.

Figura 12 – Tipos de fluxos de dados em um gêmeo digital.



Fonte: Elaborado pelo autor.

3.3.2 Implementação de gêmeos digitais

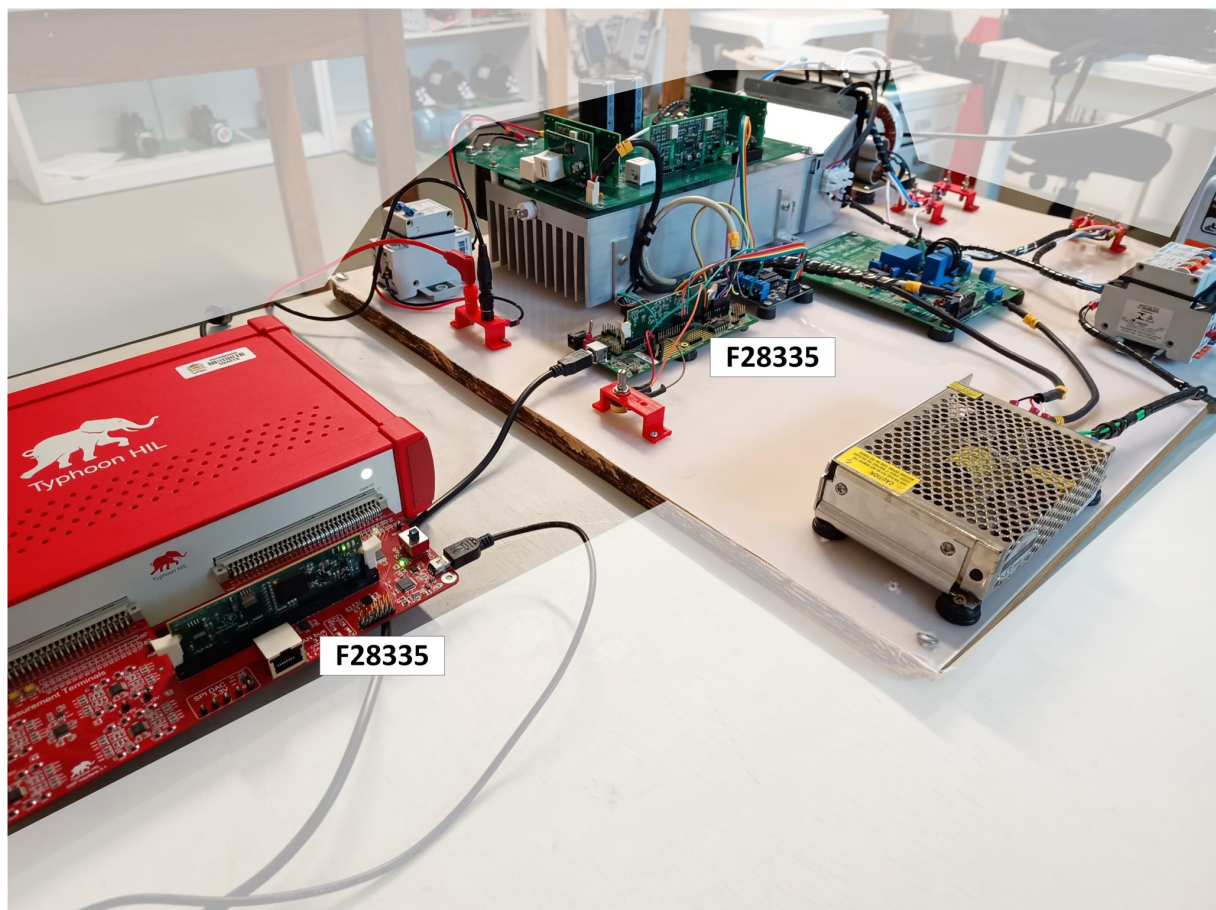
É notório que a indústria, de forma geral, está passando por um processo de transformação digital e, nesse contexto, os gêmeos digitais alinham-se à ideia de digitalização e Indústria 4.0. Entretanto, para a implementação dessa tecnologia, é fundamental garantir que os objetivos a serem alcançados estejam claramente definidos, identificar o sistema físico a ser controlado, criar a respectiva representação digital e estabelecer as conexões de dados necessárias para atingir o objetivo previamente estabelecido (VANDERHORN; MAHADEVAN, 2021).

De acordo com Coppolino *et al.* (2023a) e Yang *et al.* (2024), a criação de um gêmeo digital envolve quatro fases principais: aquisição de dados, modelagem do gêmeo digital, simulação e implementação. A etapa de aquisição de dados consiste na coleta de informações em tempo real do sistema físico, realizada por meio de uma rede de sensores. A etapa de modelagem utiliza esses dados para construir uma representação fiel do sistema

físico, permitindo simular seu comportamento. A etapa de simulação consiste em testar o comportamento do modelo digital em diferentes condições, com o objetivo de avaliar a acurácia e precisão do modelo construído. Por fim, a etapa de implementação corresponde à integração do gêmeo digital com o sistema físico real.

Na Figura 13, é apresentado um exemplo de gêmeo digital aplicado em eletrônica de potência. À direita, encontra-se o sistema físico real, composto por um inversor conectado à rede com filtro LCL, controlado pelo microcontrolador F28335. À esquerda, está o simulador responsável por reproduzir, em tempo real, o comportamento do sistema físico, utilizando o mesmo microcontrolador. Nessa configuração, segundo Busarello (2024), é possível testar novos algoritmos de controle e repetir experimentos em um curto intervalo de tempo por meio do gêmeo digital, sem afetar o sistema físico.

Figura 13 – Gêmeo digital aplicado em eletrônica de potência.

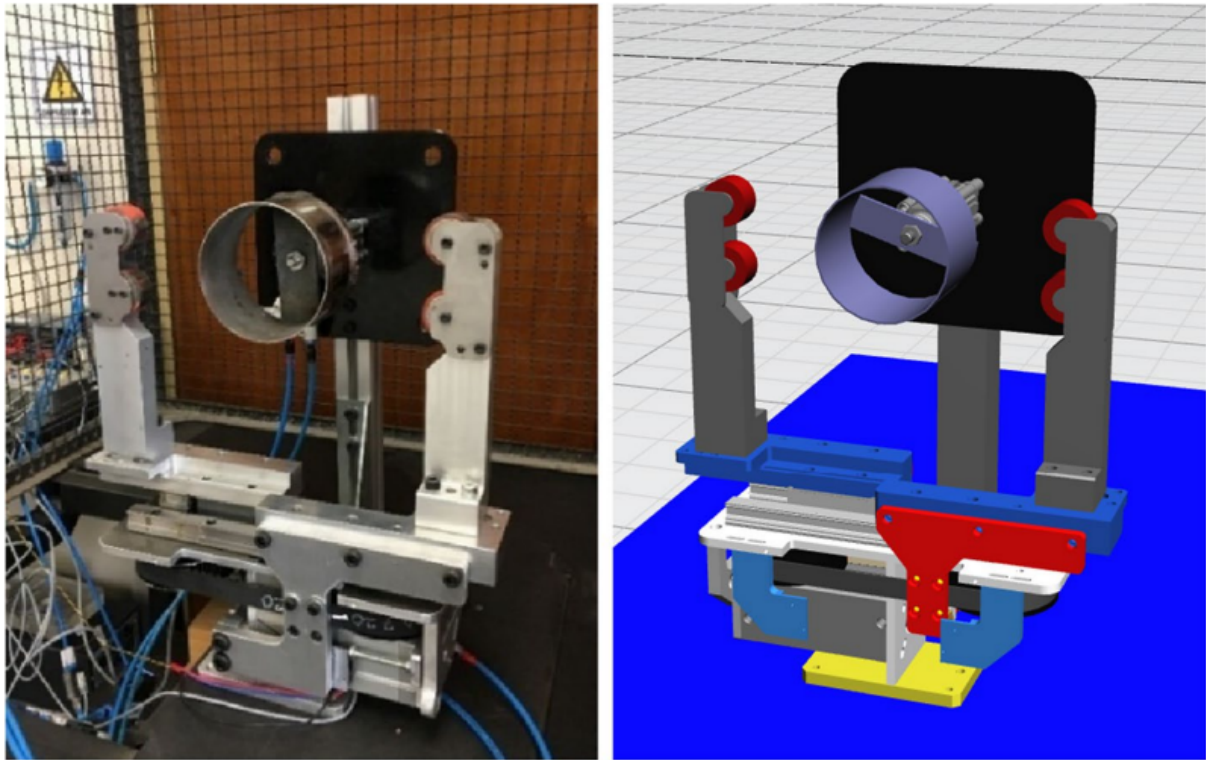


Fonte: (BUSARELLO, 2024).

No trabalho de Redelinghuys, Basson e Kruger (2020), é apresentado o desenvolvimento de uma arquitetura para aplicação de gêmeos digitais na área de manufatura e, para validar essa arquitetura, foi criado o gêmeo digital de uma garra pneumática industrial, utilizada para o monitoramento remoto do gêmeo físico, diagnóstico de falhas e simulação

de comportamento. Por se tratar de um sistema mecânico, a modelagem utilizou um modelo em CAD do sistema físico em conjunto com o software de simulação Tecnomatix PS, permitindo simular com precisão os movimentos do sistema real. Na Figura 14, é apresentado o sistema físico real à esquerda e o gêmeo digital à direita.

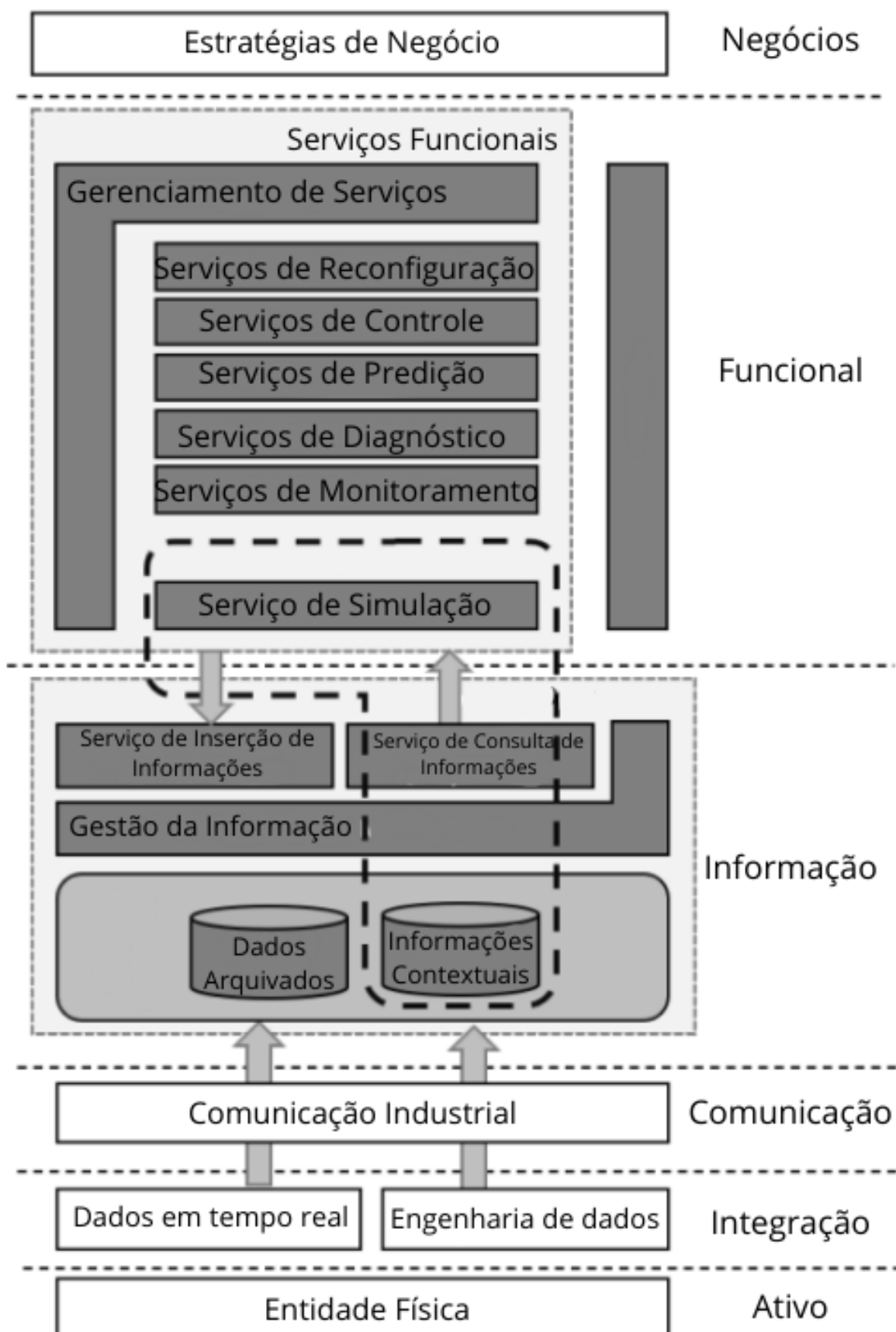
Figura 14 – Gêmeo digital aplicado em um sistema mecânico.



Fonte: (REDELINGHUY; BASSON; KRUGER, 2020)

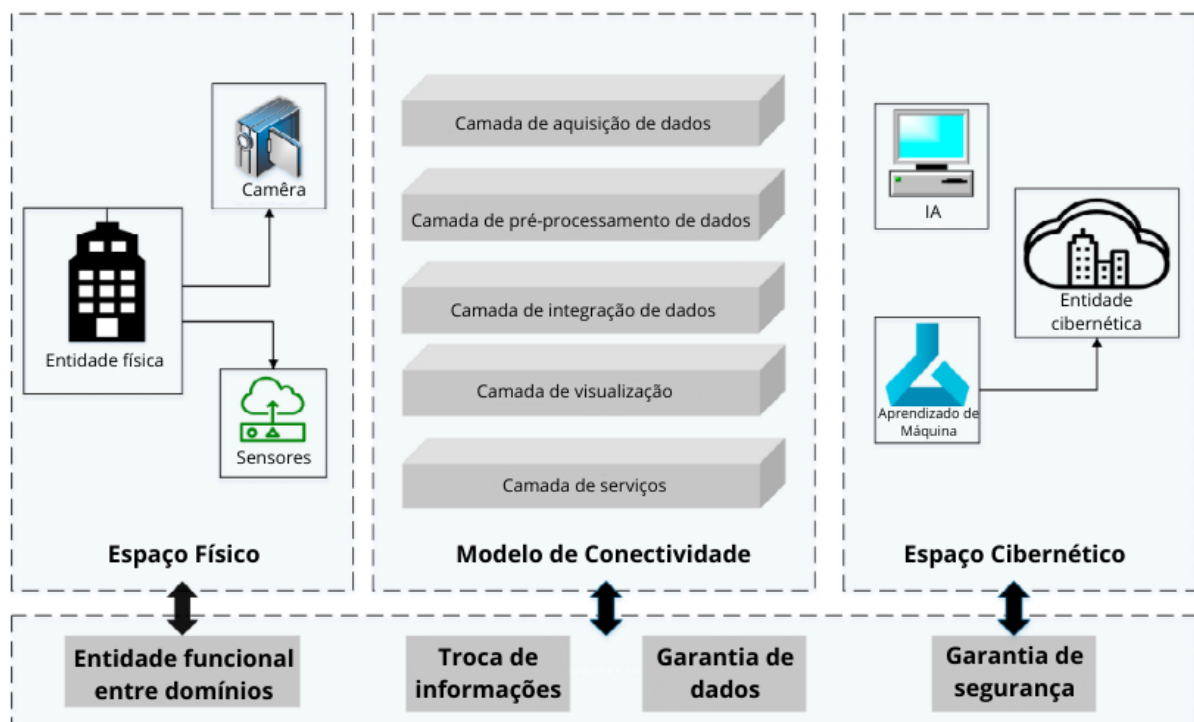
Na literatura, são apresentadas diferentes arquiteturas para gêmeos digitais. No trabalho Steindl *et al.* (2020), é proposta uma arquitetura de gêmeos digitais voltada para sistemas de energia, estruturada em seis camadas, conforme apresentado na Figura 15. A primeira camada corresponde à entidade física, ou seja, o sistema físico real. A segunda camada refere-se à integração, na qual os mundos físico e digital são conectados pela coleta de dados em tempo real. A terceira camada, denominada camada de comunicação industrial, representa os protocolos utilizados para essa integração. Em seguida, a camada de informação corresponde ao armazenamento e gerenciamento dos dados do sistema. A quinta camada, chamada camada funcional, concentra as atividades principais do gêmeo digital, como simulação, visualização, monitoramento, diagnósticos, previsões, controle e reconfiguração. Por fim, a camada de negócios refere-se aos objetivos operacionais definidos para o sistema real e à coordenação de múltiplos gêmeos digitais.

Figura 15 – Arquitetura de um gêmeo digital com seis camadas.



O trabalho de Yang *et al.* (2024) apresenta uma arquitetura baseada em três partes principais: o espaço físico, onde se encontra o sistema real, o espaço de conectividade, responsável por realizar a ligação entre o mundo físico e o mundo virtual, e o espaço virtual, no qual está localizado o gêmeo digital desenvolvido. Entretanto, a arquitetura completa é composta por um total de sete camadas, com o espaço de conectividade abrangendo as camadas de aquisição de dados, pré-processamento de dados, integração de dados, visualização e serviço, conforme apresentado na Figura 16.

Figura 16 – Arquitetura de um gêmeo digital com sete camadas.



Fonte: Adaptado de Yang *et al.* (2024).

3.3.3 Aplicações de gêmeos digitais

Em Attaran e Celik (2023), os autores citam a pandemia de Covid-19 como responsável por acelerar o desenvolvimento e a aplicação de gêmeos digitais em diversas áreas nos últimos anos, incluindo setores como saúde e energia. Além disso, mencionam a expectativa de que muitos países e indústrias passem a implementar gêmeos digitais como parte de suas estratégias econômicas, especialmente para otimizar processos operacionais. No trabalho de San (2021) é destacado que a crescente tendência de implementação de gêmeos digitais se deve, em grande parte, à ampla disponibilidade de sensores de baixo custo, à robustez das tecnologias de comunicação, ao avanço do aprendizado de máquina e da inteligência artificial, bem como aos novos desenvolvimentos nas áreas de hardware e computação em nuvem. Por outro lado, é apontado que a modelagem de sistemas complexos

ainda representa um desafio significativo para a implementação de alguns modelos digitais, especialmente aqueles que dependem de modelos matemáticos robustos para garantir equivalência com o sistema físico real. Segundo Qi *et al.* (2021), a crescente popularidade dos gêmeos digitais reflete a tendência mundial de conexão entre o mundo físico e o mundo virtual. Por conta disso, diversos segmentos têm desenvolvido soluções inteligentes para sua aplicação, e o uso dessa tecnologia tem se expandido gradualmente para diferentes campos, níveis de usuários e tipos de negócios (JONES, D. *et al.*, 2020). Além disso, os atrativos para o mercado na adoção de gêmeos digitais são múltiplos, como a necessidade de monitoramento remoto em tempo real, flexibilidade operacional, manutenção preditiva e programação, melhor administração de ativos, gerenciamento de cenários e riscos, maior sinergia e colaboração intra e interequipes, bem como a personalização de produtos e serviços (SAN, 2021). Com isso, a seguir, são apresentadas algumas aplicações de gêmeos digitais encontradas na literatura.

3.3.3.1 Aplicação de gêmeos digitais para construção

Em Sacks *et al.* (2020), os autores apresentam o conceito de DTC (*Digital Twin Construction*) como um novo modelo de gerenciamento em construções, integrando o BIM (*Building Information Modeling*), *lean construction*, gêmeos digitais para monitoramento em tempo real e inteligência artificial. Nesse contexto, o gêmeo digital utiliza tecnologias de monitoramento como GPS (Sistema de Posicionamento Global), sensores inteligentes, visão computacional, *laser scanning* e RFID (Identificação por Rádio Frequência), e permite a visualização digital e automática, de forma constante, tanto do produto (a obra em execução) quanto do processo em andamento.

3.3.3.2 Aplicação de gêmeos digitais para sistemas de saúde

No trabalho Vallée (2023), os autores propõem a utilização da tecnologia de gêmeos digitais para permitir que profissionais de saúde reúnam e analisem grandes volumes de dados de pacientes provenientes de diversas fontes, incluindo EHR (Registros Eletrônicos de Saúde), dispositivos vestíveis e dispositivos médicos. Isso possibilita a criação de modelos personalizados para apoiar diagnósticos, monitoramento contínuo, predição da progressão de doenças e intervenções preventivas. Além disso, propõe-se o uso de gêmeos digitais como ferramenta educacional e de treinamento para médicos, com potencial de melhorar significativamente o atendimento e a eficiência nos sistemas de saúde.

3.3.3.3 Aplicação de gêmeos digitais para manufatura inteligente

Em Soori, Arezoo e Dastres (2023), propõe-se a aplicação de gêmeos digitais para a integração, monitoramento e otimização de todo o ciclo produtivo, abrangendo desde o design até a manutenção, no contexto da manufatura inteligente. Com a utilização de

sensores e redes de manufatura inteligentes para coleta de dados, são empregados modelos virtuais detalhados de produtos, máquinas e processos, permitindo a simulação de cenários, a prevenção de falhas e o ajuste automático de parâmetros operacionais.

3.3.3.4 Aplicação de gêmeos digitais para gerenciamento de cadeia de suprimentos

Em uma cadeia de suprimentos (*Supply Chain*), sobretudo em um ambiente globalizado, o gerenciamento de estoque, transporte, produção e demanda é sempre um desafio e requer uma análise cuidadosa. Em Lu Wang *et al.* (2022), os autores propõem a aplicação de gêmeos digitais para a gestão da cadeia de suprimentos, utilizando sensores, sistemas de ERP (Planejamento de Recursos Empresariais) e IoT para criar réplicas virtuais dinâmicas de toda a cadeia, possibilitando a simulação de cenários e análises preditivas para a mitigação de riscos. Nesse trabalho, destaca-se a utilização dos modelos digitais como facilitadores para a tomada de decisão.

3.4 INTELIGÊNCIA ARTIFICIAL

3.4.1 Definição e características

Para falar sobre aprendizado de máquina, é necessário introduzir um pouco sobre o que é a IA. A IA vem, a cada dia, ganhando popularidade e se difundindo nas principais atividades humanas, seja em aplicativos de celular ou em máquinas industriais. No entanto, o seu conceito há muito tempo gera esforços significativos para ser definido. Ao buscar uma definição de IA, é necessário ao máximo evitar redundâncias. Na literatura, alguns autores defendem que uma forma razoável de começar a defini-la seria entender o significado das palavras que a compõem separadamente. Por exemplo, artificial pode ser considerado como aquilo que é feito pelo ser humano, e não gerado pela natureza, mesmo que muitas vezes inspirado nela. Já inteligência está relacionada à habilidades cognitivas, como aprender, pensar, tomar decisões e resolver problemas. Assim, ao unir os dois termos, chega-se à ideia de uma inteligência criada, capaz de simular aspectos do raciocínio humano (ABBASS, 2021).

A IA não se trata de um produto pronto e acabado, mas sim de um campo de conhecimento pertencente à ciência da computação, cujo objetivo é desenvolver sistemas inteligentes capazes de realizar tarefas complexas. Essas tarefas abrangem diversas áreas do conhecimento humano, como manufatura, educação, saúde e política, entre outras, nas quais normalmente seria necessário algum tipo de raciocínio humano (KISSINGER; SCHMIDT; HOTTENLOCHER, 2021). A IA pode ser vista como uma área focada no desenvolvimento de sistemas que pensam e agem como humanos, que conseguem analisar dados, aprender e tomar decisões. Assim, de maneira simples, a IA pode ser definida como uma simulação da inteligência humana (GÖDE; KALKAN, 2023).

As ideias relacionadas à IA já vinham aparecendo desde a década de 1920, sobretudo em obras de ficção científica e em reflexões filosóficas sobre máquinas pensantes. Um exemplo marcante é a peça R.U.R. (Rossum's Universal Robots), escrita por Karel Čapek em 1923, na qual surgiu pela primeira vez o termo “robô” (MOSTENSKA *et al.*, 2025; GÖDE; KALKAN, 2023). Contudo, foi após a Segunda Guerra Mundial, com o avanço dos computadores, que pesquisadores passaram a estudar de forma sistemática a possibilidade de desenvolver máquinas capazes de “pensar” e imitar ações humanas. Estes pesquisadores se reuniram em 1956 durante a conferência de Dartmouth College, em New Hampshire, nos Estados Unidos. Durante esta conferência, o termo Inteligência Artificial foi registrado como um campo de conhecimento pela primeira vez (CASTRO BARBOSA, 2020).

3.4.2 Aprendizado de máquina

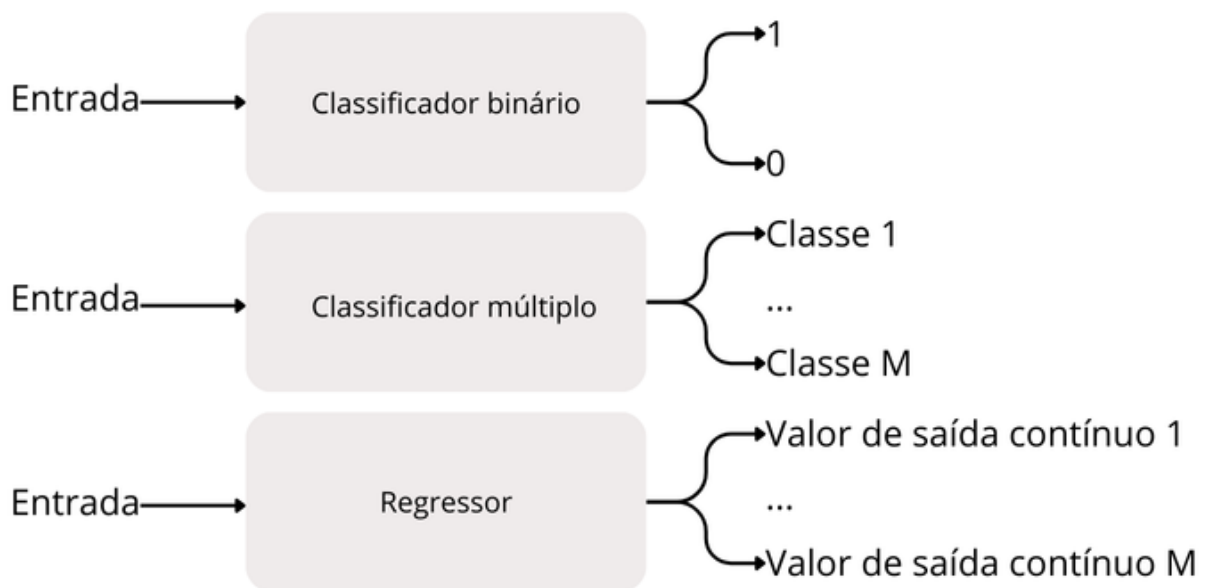
Aprendizado de máquina, embora muitas vezes seja confundido com a própria IA, refere-se a uma subárea da IA, baseada em algoritmos que permitem aos computadores aprender de forma automática a partir de dados e de poder computacional, extraíndo padrões complexos dos dados fornecidos (SHARIFANI; AMINI, 2023). Segundo Janiesch, Zschech e Heinrich (2021), o objetivo central do aprendizado de máquina é automatizar a construção de modelos analíticos para a realização de tarefas cognitivas, por meio da aplicação de algoritmos que aprendem iterativamente a partir de dados de treinamento específicos do problema, permitindo que os modelos descubram informações ocultas e padrões complexos sem serem diretamente programados para isso.

Os algoritmos de aprendizado de máquina são, de modo geral, classificados em três categorias: aprendizado supervisionado, aprendizado não supervisionado e aprendizado por reforço. No aprendizado supervisionado, o modelo é treinado a partir de entradas e saídas conhecidas, em que cada entrada já está associada a uma saída. Dessa forma, o modelo identifica os padrões entre entradas e saídas e, durante o treinamento, busca prever as saídas de novas entradas, comparando os resultados obtidos com os dados previamente fornecidos, a fim de minimizar os erros. No aprendizado não supervisionado, o modelo não possui informações prévias, de modo que tenta compreender, de forma autônoma durante o treinamento, as similaridades e diferenças entre os dados fornecidos. Por fim, no aprendizado por reforço, o modelo é treinado com base em um sistema de recompensas e penalidades, distinguindo-se das abordagens supervisionada e não supervisionada por empregar agentes inteligentes capazes de interagir com o ambiente e otimizar, continuamente, a função de recompensa ao longo do tempo (JANIESCH; ZSCHECH; HEINRICH, 2021; SHARIFANI; AMINI, 2023).

Na literatura, diferentes algoritmos de aprendizado de máquina são encontrados, desde aqueles aplicados a tarefas simples até aqueles utilizados em problemas mais complexos. Um algoritmo simples de aprendizado de máquina, por exemplo, é o algoritmo de classificação binária, no qual o modelo deve classificar um item em um grupo A ou B. Já

o algoritmo de classificação múltipla realiza a mesma tarefa, porém considerando vários grupos possíveis. O algoritmo de regressão, por sua vez, fornece um valor contínuo na saída em vez de um valor discreto e, assim, ao fornecer entradas ao modelo, o usuário recebe como saída um valor dentro de um intervalo específico (JO, 2021; PANESAR, 2020). Na Figura 17, é apresentada uma visualização do funcionamento desses três algoritmos em um exemplo de classificação de casas.

Figura 17 – Algoritmos de classificação binária, classificação múltipla e de regressão.



Fonte: Elaborado pelo autor com base em Jo (2021).

Em seguida, falando sobre algoritmos mais elaborados, os algoritmos de árvores de decisão podem ser resumidos pela lógica de que, caso uma condição seja verdadeira, uma determinada saída será escolhida, seguindo nessa estrutura até o fim da árvore, quando não há mais ramificações. São amplamente utilizados para classificação e podem fornecer tanto valores discretos quanto contínuos, sendo vistos como uma evolução dos algoritmos de classificação múltipla e de regressão. Entretanto, o seu desempenho tende a ser melhor em conjuntos de dados menores. Os algoritmos de florestas aleatórias, por outro lado, são formados pelo treinamento de diversas árvores de decisão, e a saída final é determinada pela média ou pela maioria das previsões feitas por cada árvore. A vantagem das florestas aleatórias está na possibilidade de treinar múltiplas árvores a partir de subconjuntos diferentes de dados, aumentando a acurácia do modelo (JO, 2021; PANESAR, 2020).

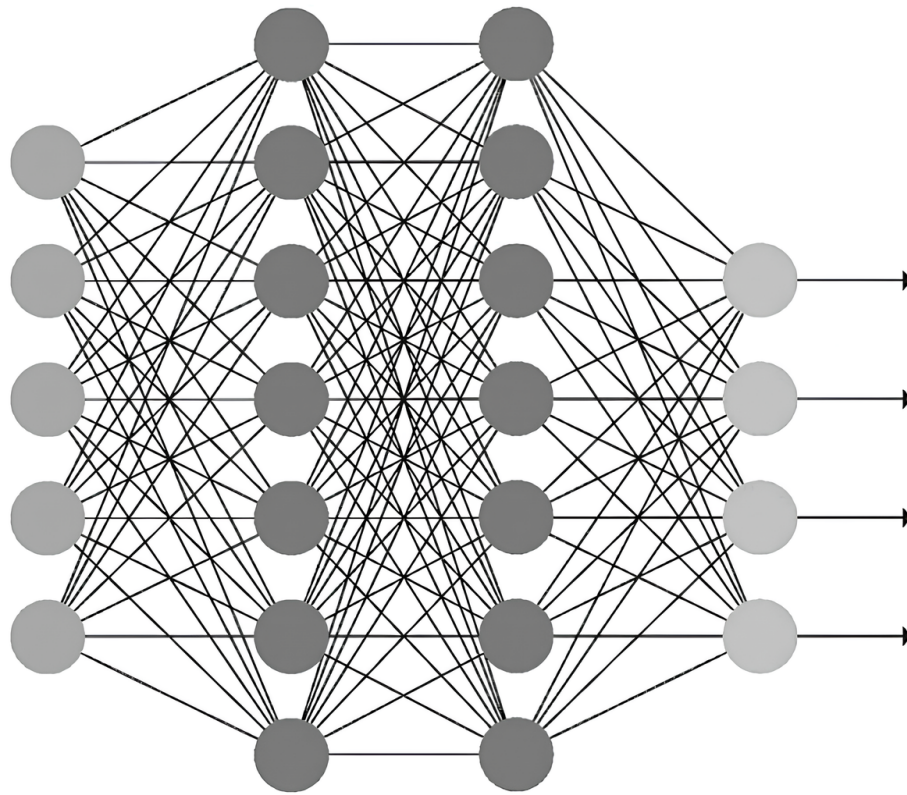
Os algoritmos de Máquinas de Vetores de Suporte (SVM) são métodos de classificação linear binária não probabilísticos, podendo ser aplicados tanto em tarefas de classificação quanto de regressão. Segundo o autor Panesar (2020), os algoritmos SVM são frequentemente utilizados em conjunto com métodos de Processamento de Linguagem Natural, como análise de textos, além de serem amplamente aplicados no reconhecimento

de imagens. O funcionamento das SVM consiste em encontrar um hiperplano ótimo que separe duas classes, sendo esse hiperplano determinado pelos vetores de suporte, que são os pontos mais próximos da fronteira entre as classes. Caso esses vetores sejam removidos, o hiperplano também é alterado, o que evidencia como esses pontos influenciam diretamente a classificação (JO, 2021; PANESAR, 2020; HASSANIEN; CHANG; MINCONG, 2021).

Os algoritmos Naive Bayes são úteis para grandes quantidades de dados e recebem esse nome por tratarem as variáveis como independentes entre si, o que pode ser visto como uma suposição “ingênua”, já que nem sempre corresponde à realidade dos problemas. O termo “Bayes” refere-se à aplicação do teorema de Bayes, que calcula a probabilidade de um evento ocorrer com base em outro evento já observado. Para utilizar esse algoritmo, os dados precisam ser discretizados, ou seja, convertidos para valores ou estados binários. O processo de aprendizado envolve, considerando apenas duas classes e as denominando de classes A e B, a análise das probabilidades das classes A e B acontecerem, seguida do cálculo da probabilidade de cada atributo pertencer a cada uma das classes. A partir dessas informações, o modelo estima a probabilidade de um novo atributo pertencer a A ou B. Apesar da simplicidade, modelos baseados em Naive Bayes são conhecidos por alcançar resultados robustos, muitas vezes superando algoritmos muito sofisticados (JO, 2021; PANESAR, 2020; HASSANIEN; CHANG; MINCONG, 2021).

As RNA (Redes Neurais Artificiais) são modelos computacionais e matemáticos que simulam o funcionamento do cérebro humano, imitando a forma como ele processa dados e cria conhecimento. São consideradas um subconjunto dos algoritmos de aprendizado de máquina, sendo a maioria treinada pelo método de retropropagação. Entre os tipos de redes neurais, encontram-se autoencoders, redes convolucionais, redes recorrentes, redes totalmente conectadas e muitas outras (JO, 2021; DASTRES; SOORI, 2021). Essas redes são organizadas de maneira semelhante às redes neurais biológicas, com nós interconectados distribuídos em camadas de entrada, uma ou mais camadas ocultas e uma camada de saída, como mostrado na Figura 18.

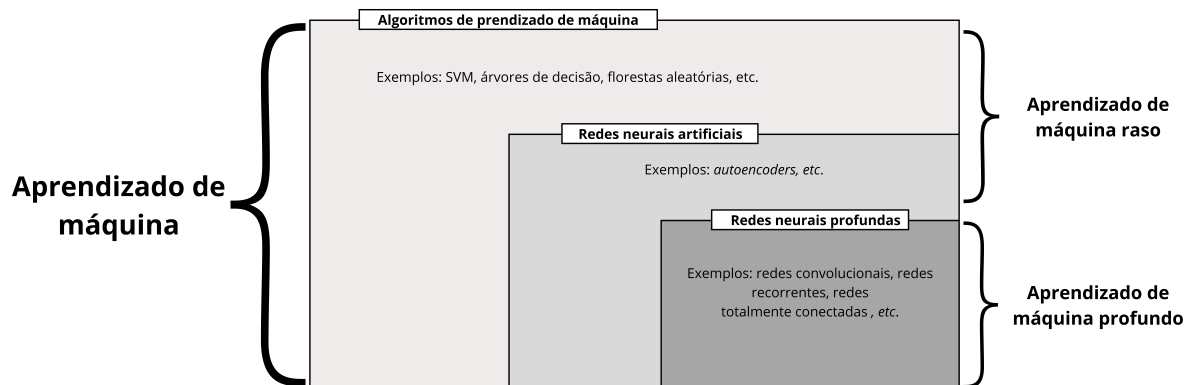
Figura 18 – Estrutura de uma Rede Neural Artificial.



Fonte: (JO, 2021).

Com o avanço da computação, outras abordagens têm se tornado mais frequentes, como o aprendizado de máquina profundo, conhecido como *Deep Learning*. De maneira simplificada, o *Deep Learning* pode ser definido como uma rede neural artificial mais profunda, com múltiplas camadas entre a entrada e a saída, sendo ideal para extrair padrões complexos e uma grande quantidade de características a partir de dados não estruturados. O treinamento desses modelos demanda maior tempo e maior poder computacional quando comparado a algoritmos tradicionais de aprendizado de máquina. Seu funcionamento consiste em passar os dados por diversas camadas, sendo que cada uma delas extrai características progressivamente, com as primeiras camadas capturando informações de baixo nível, enquanto as camadas mais profundas formam representações abstratas de nível maior (JO, 2021; HASSANIEN; CHANG; MINCONG, 2021; JANIESCH; ZSCHECH; HEINRICH, 2021). Na Figura 19, são apresentados o conjunto e subconjuntos do aprendizado de máquina.

Figura 19 – Conjunto e subconjuntos do aprendizado de máquina.



Fonte: Elaborado pelo autor com base em Janiesch, Zschech e Heinrich (2021).

3.4.3 Integração de aprendizado de máquina com gêmeos digitais

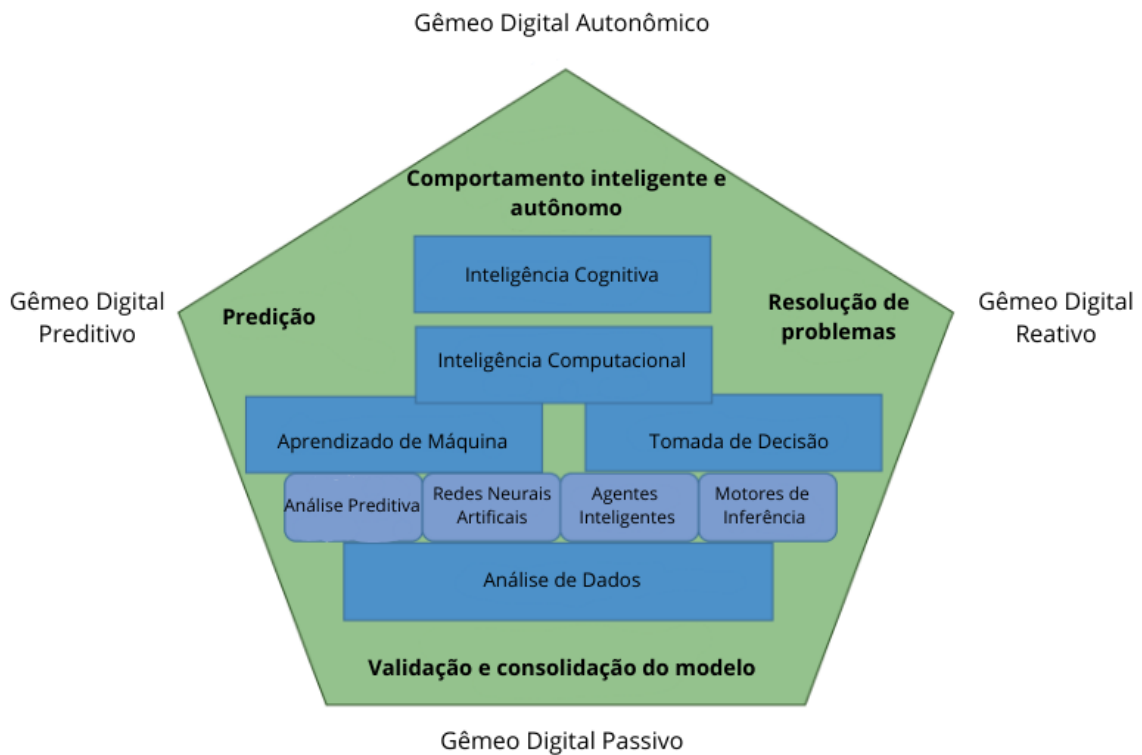
Considerando que tanto o aprendizado de máquina quanto os gêmeos digitais dependem de dados para operar, integrá-los pode ser visto como uma consequência lógica, conforme defendem os autores Kreuzer, Papapetrou e Zdravkovic (2024). O aprendizado de máquina pode exercer um papel fundamental quando utilizado em conjunto com gêmeos digitais, uma vez que pode atuar na atualização automática dos modelos, aumentando a fidelidade do gêmeo digital em relação ao sistema físico real, além de permitir a execução de simulações com dados que contemplam desde o estado inicial da entidade física até informações sobre como essa entidade afeta e interage com o ambiente ao seu redor, bem como oferecer suporte à tomada de decisões automatizada (JYENISKHAN *et al.*, 2023).

No trabalho de Minerva *et al.* (2023), os autores apresentam uma classificação de gêmeos digitais dividida em quatro categorias, definidas de acordo com o nível de autonomia que a inteligência artificial pode fornecer a esses sistemas. A primeira, denominada gêmeo digital passivo, diz respeito ao gêmeo digital que apenas busca representar o estado do sistema físico real, além de realizar simulações. A segunda categoria, denominada gêmeo digital preditivo, está relacionada ao uso de gêmeos digitais para prever o comportamento futuro do sistema físico real. Em seguida, o gêmeo digital reativo é aquele capaz de tomar decisões por conta própria, realizando as modificações que considerar necessárias na entidade física. Por fim, os gêmeos digitais autônômicos, embora mencionados pelos autores como a categoria menos pesquisada na literatura, representam o nível mais avançado, sendo capazes de aprender de maneira autônoma, prever comportamentos futuros e tomar decisões sem qualquer intervenção humana (MINERVA *et al.*, 2023).

Para todas as quatro diferentes categorias, diversas técnicas de IA podem ser utilizadas. Nos gêmeos digitais preditivos, algoritmos de aprendizado de máquina e redes neurais artificiais podem ser empregados por meio da análise de dados históricos do sistema, oferecendo suporte à previsão de eventos futuros na entidade física. Para os

gêmeos digitais reativos, árvores de decisão, florestas aleatórias e agentes inteligentes podem ser utilizados para auxiliar a tomada de decisão automática, podendo o gêmeo digital implementar uma ou mais dessas técnicas para a mesma entidade física. No caso dos gêmeos digitais passivos, abordagens de inteligência artificial voltadas à análise de dados podem ser empregadas para validar e ajustar o modelo do gêmeo digital. Por fim, para os gêmeos digitais autônômicos, redes neurais profundas podem ser utilizadas para fornecer a capacidade de raciocínio necessária para esse tipo de gêmeo digital (MINERVA *et al.*, 2023). Na Figura 20, é apresentada uma representação das técnicas de IA associadas a cada tipo de gêmeo digital.

Figura 20 – Técnicas de inteligência artificial para as diferentes categorias de gêmeos digitais.



Fonte: Adaptado de Minerva *et al.* (2023).

A utilização de aprendizado de máquina para realizar previsões, simulações e intervenções em entidades físicas representadas por gêmeos digitais tem sido estudada e aplicada por diversos pesquisadores, e as possibilidades de aplicação são amplas (KREUZER; PAPAPETROU; ZDRAVKOVIC, 2024). Como um exemplo dessa utilização, para que fique claro, os autores Jyeniskhan *et al.* (2023) apresentam o uso de visão computacional associada e aprendizado de máquina para detecção de problemas durante o processo de impressão em uma impressora 3D, identificando anomalias como falhas e irregularida-

des estruturais por meio do aprendizado de máquina, bem como atualizando o modelo do gêmeo digital em tempo real durante a impressão. Além disso, o sistema automatiza a análise dos dados coletados para realizar a detecção de maneira rápida e automática, eliminando a necessidade de inspeção manual por um operador humano, podendo inclusive interromper a impressão caso necessário.

3.5 ATAQUES CIBERNÉTICOS EM REDES ELÉTRICAS INTELIGENTES

É fato que a energia elétrica constitui um pilar essencial da sociedade moderna, sendo responsável por abastecer residências, escolas, hospitais e empresas. Ao integrar toda a rede elétrica a um sistema computadorizado para supervisão e controle de maneira remota, o sistema de energia torna-se vulnerável a ataques cibernéticos, que podem afetar um país inteiro de diferentes maneiras. Um ataque cibernético que compromettesse a transmissão de energia poderia impactar a vida de milhões de pessoas, além de afetar gravemente a economia de um país. Em maio de 2025, de maneira repentina e sem causa aparente, milhões de pessoas ficaram sem energia por mais de 12 horas em Portugal e Espanha, causando impactos significativos tanto na indústria quanto na vida da população. Embora a hipótese de ataque cibernético tenha sido considerada, não foram encontradas evidências que confirmassem essa possibilidade. Ainda assim, o episódio evidenciou o potencial danoso que a vulnerabilidade da rede elétrica pode causar a um país (BLACKBURN, 2025b; JONES, S., 2025; BEATO, 2025).

Adicionalmente, ataques cibernéticos podem comprometer a infraestrutura da rede elétrica, causando danos a componentes como transformadores e geradores, o que acarretaria prejuízos não apenas do ponto de vista da segurança, mas também financeiros, já que a reparação desses equipamentos exige altos investimentos. Em 2011, um ataque cibernético à usina nuclear de Natanz, no Irã, uma instalação de enriquecimento de urânio, fez com que as centrífugas dos geradores operassem de forma descontrolada, resultando na destruição de mais de mil delas. Nesse ataque, os CLP (Controladores Lógicos Programáveis) e o sistema SCADA (*Supervisory Control and Data Acquisition*) de toda a planta industrial foram invadidos, que são tecnologias utilizadas há muitos anos para controle e automação industrial e que também são utilizados em uma rede elétrica inteligente. Esse ataque é considerado um divisor de águas por ter demonstrado o potencial de destruição que uma ofensiva cibernética pode causar (KRIVOHLAVA; CHREN; ROSSI, 2022)

Junto com isso, um ataque cibernético poderia representar uma ameaça à segurança nacional, uma vez que um país se torna altamente vulnerável diante de uma rede elétrica inoperante. Na guerra entre a Rússia e a Ucrânia, por exemplo, os ataques a sistemas energéticos têm sido uma estratégia de ambos os lados desde o início do conflito, com o objetivo de comprometer o fornecimento de energia elétrica e aquecimento (BLACKBURN, 2025a; RAINSFORD, 2024).

Além dos ataques mencionados anteriormente, diferentes ciberataques a sistemas

de energia foram registrados nos últimos anos. Na literatura, o primeiro ataque reportado no século XXI é o ataque à planta de Davis-Besse, nos Estados Unidos, no qual os sistemas SCADA foram o principal alvo e informações importantes de produção foram bloqueadas por aproximadamente cinco horas (ALOMARI *et al.*, 2025). Além do ataque à planta de Davis-Besse, alguns ataques se destacam na literatura por demonstrarem o potencial danoso dos ciberataques contra infraestruturas críticas. Em 2010, o ataque conhecido como Stuxnet, que posteriormente foi evoluído e utilizado para atacar a usina de Natanz em 2011, explorou vulnerabilidades dos sistemas SCADA e afetou cerca de quinze plantas industriais na Alemanha (ALOMARI *et al.*, 2025; PAUL *et al.*, 2024; ABRAHAM; HOUMB; ERDODI, 2025). Em 2015 e 2016, os ataques BlackEnergy e Industroyer atingiram infraestruturas de energia na Ucrânia. O primeiro desligou trinta subestações e interrompeu o fornecimento de energia para cerca de 230 mil consumidores por mais de seis horas, enquanto o segundo atacou os sistemas SCADA de gerenciamento de energia de Kiev, deixando a capital sem luz por uma hora (PAUL *et al.*, 2024; ABRAHAM; HOUMB; ERDODI, 2025; ALOMARI *et al.*, 2025; MOHAMMED *et al.*, 2024; ABRAHAM *et al.*, 2024). Em 2017, o ataque Triton foi registrado como o primeiro ataque direcionado a sistemas de segurança de uma planta industrial, não visando apenas o acesso a informações ou a interrupção de serviços, mas provocando danos físicos a equipamentos e representando risco a vidas humanas (PAUL *et al.*, 2024; ABRAHAM; HOUMB; ERDODI, 2025). Em seguida, , em 2021, o ataque realizado pelo grupo DarkSide contra o Oleoduto Colonial, nos Estados Unidos, bloqueou servidores e obrigou a empresa a interromper o fornecimento de combustível na costa leste do país para impedir que o ataque alcançasse outros sistemas da empresa (ABRAHAM; HOUMB; ERDODI, 2025; ALOMARI *et al.*, 2025). Em 2022, o ataque Industroyer2, uma evolução do Industroyer de 2016, comprometeu sistemas de controle de uma subestação de energia, provocando o corte do fornecimento elétrico. Em 2023, também na Ucrânia, um ataque contra a infraestrutura de aquecimento urbano teve como alvo dispositivos que utilizavam o protocolo Modbus, causando a interrupção dos serviços de aquecimento em uma região por cerca de 48 horas (ABRAHAM; HOUMB; ERDODI, 2025). Na Tabela 3, é apresentado um resumo dos ataques contra infraestruturas de energia registrados na literatura que ocorreram no século XXI.

Tabela 3 – Descrição dos ataques cibernéticos contra infraestruturas de energia no século XXI.

Ano	Nome do ataque	Alvo do ataque	País	Descrição do ataque
2003	s.n	Usina nuclear Davis-Besse	Estados Unidos	Ataque ao sistema SCADA da usina nuclear, bloqueando o acesso a informações operacionais por cerca de cinco horas
2007	s.n	Laboratório Nacional de Idaho	Estados Unidos	Teste controlado que demonstrou vulnerabilidades em sistemas SCADA, em que o código Aurora provocou a abertura e o fechamento repetido de disjuntores, causando danos físicos a um gerador elétrico
2007	s.n	Oleoduto Baku–Tbilisi–Ceyhan	Turquia	Ataque cibernético que inseriu dados falsos no sistema de controle do oleoduto BTC, causando superpressurização do duto e resultando em explosão e vazamento de óleo
2010	Stuxnet	Sistema WinCC SCADA	Alemanha	O malware Stuxnet explorou uma vulnerabilidade no Windows para comprometer o sistema SCADA WinCC, afetando cerca de 15 plantas industriais na Alemanha
2011	Stuxnet	Usina nuclear de Natanz	Irã	Ataque ao sistema SCADA da usina nuclear de Natanz, realizado por meio do malware Stuxnet, que obteve acesso aos controladores industriais responsáveis pelas centrífugas de enriquecimento de urânio, provocando danos físicos aos equipamentos e interrupções no processo de operação
2012	s.n	Aramco Oil & Gas	Arábia Saudita	Ataque que acessou e apagou dados de cerca de 30 mil computadores da Aramco, maior empresa de petróleo e gás do mundo, interrompendo as operações por duas semanas e causando prejuízos estimados em 15 milhões de dólares
2012	s.n	RasGas	Qatar	Ataque que acessou e apagou dados sensíveis dos servidores da empresa, paralisando a produção por várias semanas
2013	Havex	Infraestrutura de energia	Múltiplos países	Acesso e coleta de dados não autorizados através de software de Supply Chain
2014	Operation Cleaver	Infraestrutura de energia	Múltiplos países	Ataque voltado ao acesso não autorizado de sistemas sensíveis de energia, com potencial objetivo de sabotagem de infraestruturas críticas
2014	Energetic Bear	Infraestrutura de energia	Múltiplos países	Ataque aos sistemas SCADA do setor de energia conduzido pelo grupo Dragonfly, com o objetivo de espionar e obter acesso a informações confidenciais de empresas do setor de energia

2015	Black Energy	Infraestrutura de energia ucraniense	Ucrânia	Ataque ao sistema SCADA da rede elétrica, desligando 30 subestações e deixando 230 mil consumidores sem energia por mais de seis horas
2016	Industroyer	Infraestrutura de energia ucraniense	Ucrânia	Ataque aos sistemas SCADA de gerenciamento de energia de Kiev, deixando a capital ucraniana sem luz por aproximadamente uma hora
2017	Triton	Usina petroquímica saudita	Arábia Saudita	Ataque aos sistemas instrumentados de segurança de uma planta industrial na Arábia Saudita, explorando a segmentação inadequada entre as redes de tecnologia da informação e de operação. O incidente causou a interrupção das operações e danos físicos a equipamentos
2019	s.n	Setor de Energia Renovável da Norsk Hydro	Noruega	O malware LockerGoga foi disseminado por e-mails de phishing, bloqueando servidores e estações de trabalho, afetando 35 mil funcionários e causando prejuízos de 71 milhões de dolares
2021	s.n	Oleoduto Colonial	Estados Unidos	Ataque realizado pelo grupo DarkSide, que bloqueou servidores e interrompeu o fornecimento de combustível na costa leste dos Estados Unidos
2022	Industroyer2	Subestações de transmissão de energia ucraniense	Ucrânia	Ataque aos sistemas de controle de uma subestação de energia, em que foram abertos os disjuntores da subestação provocando o corte de energia elétrica
2023	s.n	Infraestrutura de aquecimento urbano ucraniense	Ucrânia	Ataque realizado pelo grupo FrostyGroup contra dispositivos que utilizavam o protocolo Modbus, resultando na interrupção dos serviços de aquecimento em cerca de 600 edifícios por 48 horas na Ucrânia

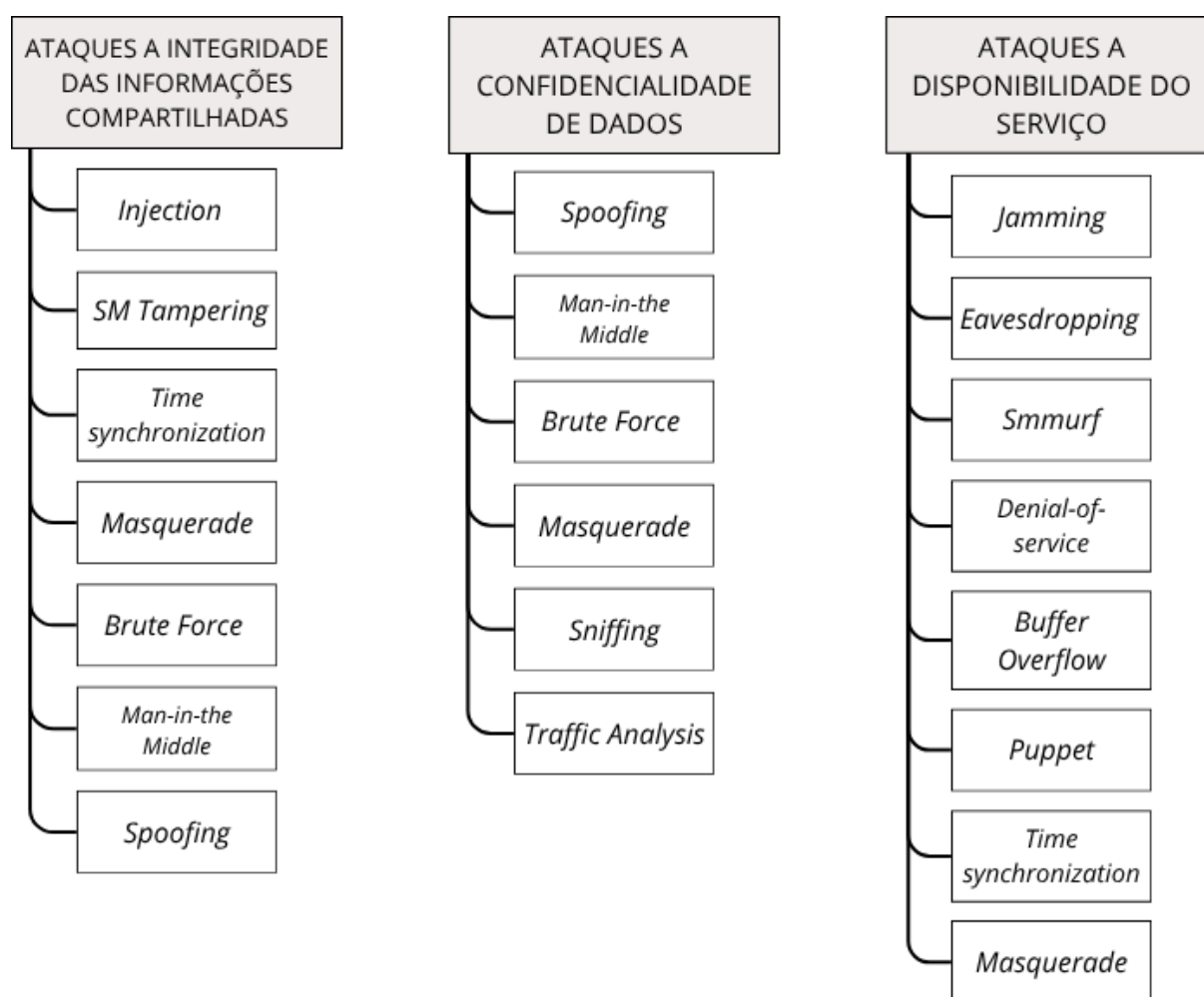
Fonte: Elaborado pelo autor com base em Alomari *et al.* (2025), Paul *et al.* (2024), Abraham, Houmb e Erdodi (2025), Mohammed *et al.* (2024) e Abraham *et al.* (2024).

Entre os desafios relacionados à contenção dos ataques cibernéticos está o fato de que eles podem ser lançados e operados de forma remota, além de assumirem diferentes formas e serem desenvolvidos especificamente para explorar vulnerabilidades do alvo. Esses ataques podem resultar em acesso a dados sensíveis, interrupção de serviços essenciais, danos a equipamentos de geração, transmissão e distribuição de energia, e até causar danos físicos a pessoas. Além disso, a complexidade no tratamento e na interceptação dos ciberataques aumenta, pois todos os componentes presentes em uma rede elétrica inteligente, sejam eles de software, hardware ou sistemas de transferência de dados, estão suscetíveis a invasões. Isso torna ainda mais necessária a adoção de tecnologias eficientes para prevenir e mitigar os impactos causados pelos ataques cibernéticos. Em infraestruturas críticas, como sistemas de geração, transmissão e distribuição de energia, um ataque pode

manipular dispositivos de campo, modificar configurações de firmware ou interromper processos de segurança, resultando em danos físicos reais e prejuízos significativos à operação do sistema elétrico (MOHAMMED *et al.*, 2024).

Ao classificar os ataques cibernéticos, diferentes abordagens podem ser utilizadas, como aquelas baseadas na camada de comunicação, nos requisitos de segurança, sendo eles integridade, confidencialidade e disponibilidade, nas redes envolvidas, no ciclo de ataque ou no tipo de rede de comunicação. No trabalho de Paul *et al.* (2024) e Alomari *et al.* (2025), os autores apresentam a classificação de acordo com a tríade Integridade, Confidencialidade e Disponibilidade, na qual os ataques são categorizados conforme o aspecto que buscam comprometer: a integridade das informações compartilhadas, a confidencialidade dos dados ou a disponibilidade do serviço. Assim, ataques que buscam modificar ou destruir dados em uma rede elétrica inteligente são classificados como ataques à integridade das informações. Ataques direcionados à confidencialidade dos dados têm como objetivo obter acesso não autorizado a informações sensíveis de indivíduos ou organizações conectadas à rede. Por fim, ataques que comprometem a disponibilidade do serviço são aqueles cujo objetivo é interromper, degradar ou tornar indisponível a rede, bem como impedir a transferência de dados entre seus componentes. Na Figura 21, é apresentada a classificação dos ataques cibernéticos de acordo com a tríade Integridade, Confidencialidade e Disponibilidade.

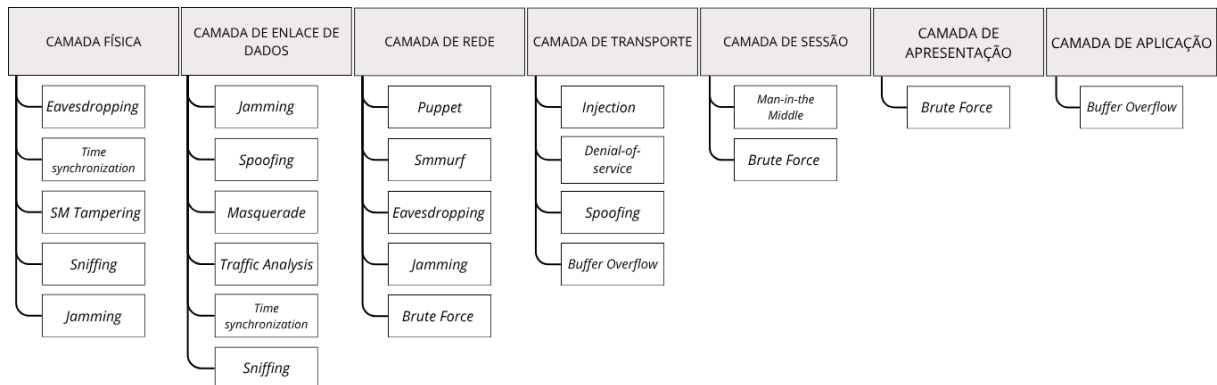
Figura 21 – Classificação dos ataques cibernéticos de acordo com a tríade Integridade, Confiabilidade e Disponibilidade.



Fonte: Elaborado pelo autor.

Nos trabalhos Mazhar *et al.* (2023) e Khoei, Slimane e Kaabouch (2022), é apresentada a classificação dos ciberataques de acordo com as camadas de comunicação do modelo OSI que esses ataques buscam comprometer, embora também seja mencionada a classificação baseada na tríade Integridade, Confiabilidade e Disponibilidade. Na Figura 22, é apresentada a classificação dos ciberataques conforme as camadas do modelo OSI. Observa-se que diferentes ataques podem visar a mesma camada do modelo simultaneamente.

Figura 22 – Classificação dos ataques cibernéticos de acordo com as camadas do modelo OSI.



Fonte: Elaborado pelo autor.

Em seguida, é importante entendermos os diferentes tipos de ataques cibernéticos existentes. Na literatura, são encontrados ciberataques considerados mais comuns em redes elétricas inteligentes, entre eles *Jamming*, *Spoofing*, *Injection*, *Man-in-the-middle*, *Eavesdropping* e *Denial-of-Service*. O ataque do tipo *Jamming* tem como objetivo afetar o envio e o recebimento de dados por meio do bloqueio de um ou mais nós da rede, transmitindo sinais contínuos ou aleatórios que mantêm esses nós ocupados. Esse ataque compromete as camadas física, de enlace de dados e de rede, podendo afetar diretamente a disponibilidade do sistema. O ataque do tipo *Spoofing* consiste em fazer com que o invasor se passe por um nó legítimo da rede, obtendo acesso não autorizado. Esse ataque representa risco à integridade da rede, à confiabilidade das informações e à disponibilidade do serviço, e pode atingir as camadas física, de enlace de dados, de rede e de transporte. O ataque do tipo *Injection* tem como objetivo inserir pacotes de dados falsos ou não confiáveis na rede, violando a integridade das informações e possibilitando o surgimento de nós ilegítimos. Esse ataque compromete as camadas de enlace de dados, de rede, de transporte e de aplicação. O ataque *Man-in-the-middle* afeta as camadas de enlace de dados, de rede e de sessão, além da integridade e confiabilidade das informações, ao interceptar o tráfego e inserir-se entre dois dispositivos autorizados. O invasor se conecta a ambos os dispositivos, retransmitindo as mensagens entre eles e fazendo com que pareça que a comunicação ocorre diretamente, enquanto, na realidade, o tráfego está sendo desviado e manipulado. O ataque *Eavesdropping* tem como objetivo obter e registrar a troca de dados entre dispositivos da rede, visando o acesso a informações sensíveis. Ele afeta principalmente as camadas física e de rede, além da confidencialidade dos dados. Por fim, o ataque *Denial-of-Service*, conhecido como DoS, busca tornar um serviço, sistema ou rede indisponível para usuários legítimos ao bloquear um ou mais nós, de forma semelhante ao ataque *Jamming*. Uma variação desse ataque, o *Distributed Denial-of-Service*, conhecido como DDoS, opera da mesma forma, porém de maneira mais intensa, com múltiplos ataques simultâneos

direcionados ao mesmo alvo.

No trabalho de Khoei, Slimane e Kaabouch (2022), são apresentados 18 tipos de ciberataques, enquanto em Mazhar *et al.* (2023) são identificados 11 tipos, em Paul *et al.* (2024) são listados 24 tipos e em Alomari *et al.* (2025) são descritos 23 tipos. Na tabela 4, é apresentada uma descrição dos ataques mais comuns encontrados na literatura, bem como a camada da rede que visam comprometer e o aspecto de segurança que buscam atingir.

Tabela 4 – Descrição dos tipos de ataques cibernéticos.

Ataque cibernético	Objetivo	Camadas-alvo	Requisito(s) de segurança afetado(s)
<i>Jamming</i>	Afetar o envio e o recebimento de dados através do bloqueio de um ou mais nós da rede	Camada Física Camada de Enlace de Dados Camada de Rede	Disponibilidade
<i>Spoofing</i>	Fingir ser um nó pertencente à rede para conseguir um acesso não autorizado	Camada Física Camada de Enlace de Dados Camada de Rede Camada de Transporte	Integridade, Confiabilidade, Disponibilidade
<i>Injection</i>	Inserir pacotes de dados falsos ou não confiáveis em uma rede	Camada de Enlace de Dados Camada de Rede Camada de Transporte Camada de Aplicação	Integridade
<i>Man-in-the-middle</i>	Alterar e modificar dados durante a transmissão pela rede	Camada de Enlace de Dados Camada de Rede Camada de Sessão	Integridade, Confiabilidade
<i>Eavesdropping</i>	Obter acesso e registrar (gravar) o fluxo de dados da rede entre dispositivos, acessando dados sensíveis	Camada Física Camada de Rede	Confiabilidade
<i>Brute force</i>	Conseguir acesso a nomes de usuário e senhas de acesso para obter acesso às contas de usuários	Camada de Rede Camada de Sessão Camada de Apresentação	Integridade, Confiabilidade
<i>Time synchronization</i>	Afetar a sincronização de tempo entre os nós de uma rede, afetando estimação de localização e detecção de falta de energia	Camada Física Camada de Enlace de Dados	Integridade, Disponibilidade

<i>Smart Meter (SM) Tampering</i>	Acessar os medidos inteligentes para alterar leituras, falsificar medições ou interromper o serviço	Camada Física	Integridade
<i>Masquerade</i>	Fingir ser um usuário para obter acesso não autorizado à rede	Camada de Enlace de Dados	Integridade, Confiabilidade, Disponibilidade
<i>Sniffing</i>	Analisar o tráfego de rede com a intenção de roubar informações, espionar comunicações ou obter credenciais	Camada Física	
Camada de Enlace de Dados	Confiabilidade	Camada de Rede Camada de Transporte Camada de Aplicação	Disponibilidade
<i>Buffer overflow</i>	Enviar muitos dados incorretos ou maiores do que o esperado para um sistema específico, a fim de comprometer sua memória	Camada de Transporte Camada de Aplicação	Disponibilidade
<i>Puppet</i>	Explorar nós legítimos da rede para gerar tráfego ou ações que degradam o serviço	Camada de Rede	Disponibilidade
<i>Smmurf</i>	Enviar requisições fingindo ser um usuário da rede, com o objetivo de causar sobrecarga que pode levar à saturação da largura de banda e à indisponibilidade dos serviços	Camada de Rede	Disponibilidade
<i>Traffic analysis</i>	Monitorar os dispositivos conectados à rede, detectando e analisando mensagens para obter informações sobre os padrões de comunicação entre os nós	Camada de Enlace de Dados	Confiabilidade

Fonte: Elaborado pelo autor com base em Khoei, Slimane e Kaabouch (2022), Mazhar *et al.* (2023), Paul *et al.* (2024) e Alomari *et al.* (2025).

3.6 INTEGRAÇÃO DE GÊMEOS DIGITAIS E APRENDIZADO DE MÁQUINA NA DETECÇÃO DE ATAQUES CIBERNÉTICOS EM REDES ELÉTRICAS INTELIGENTES

Quando falamos sobre a utilização de gêmeos digitais exclusivamente para garantir cibersegurança, é fato que eles podem ser uma ferramenta crucial para equipes de segurança na detecção e no combate a ameaças cibernéticas, sobretudo diante da intensificação dessas ameaças, que têm se tornado cada vez mais refinadas e robustas (HOMAEI *et al.*, 2024). Os gêmeos digitais podem atuar na prevenção desses ataques ao fornecer a capacidade de modelar e prever o comportamento dos sistemas físicos reais durante situações de invasão, além de ampliar a visibilidade e o entendimento do comportamento do sistema para as equipes de segurança cibernética (HOLMES *et al.*, 2021).

Entrando no campo das redes elétricas, no trabalho de Alomari *et al.* (2025), os autores mencionam que o crescimento populacional levou à expansão e ao surgimento de novas redes de energia, e que essa expansão representa atualmente uma dificuldade para o gerenciamento desses sistemas. Nesse contexto, os autores destacam que os gêmeos digitais podem ser utilizados como ferramenta para facilitar o gerenciamento de sistemas de energia em larga escala. Ademais, discutem a utilização dos gêmeos digitais no âmbito da cibersegurança em redes elétricas inteligentes e sugerem que essa tecnologia seja empregada para simular ações em caso de um ciberataque e, posteriormente, avaliar as consequências dessas ações sem interferir na rede real. Isso permite analisar a resposta das redes elétricas inteligentes sob diferentes condições e cenários e, a partir disso, desenvolver contramedidas eficazes (ALOMARI *et al.*, 2025).

Em Kandasamy *et al.* (2022), os autores desenvolvem um gêmeo digital de uma microrrede elétrica voltado para testes de cibersegurança, possibilitando simular ataques e defesas de maneira segura e econômica. O gêmeo digital desenvolvido reproduziu o comportamento de dispositivos conectados à microrrede, como controladores lógicos programáveis, sistemas SCADA e medidores inteligentes, durante um ataque do tipo *Man-in-the-Middle*, demonstrando de forma prática como os gêmeos digitais podem ser utilizados como alternativa para treinamento e pesquisa em cibersegurança de sistemas reais.

Em Coppolino *et al.* (2023b), os autores propõem uma arquitetura de monitoramento para cibersegurança em redes elétricas inteligentes que tem como peça central a utilização de um gêmeo digital do sistema real, com o objetivo de melhorar a detecção de anomalias e ameaças cibernéticas em infraestruturas críticas do setor de energia. Para validar o modelo proposto, a arquitetura foi aplicada em uma rede de distribuição elétrica real na vila de Kropa, na Eslovênia, monitorando o estado em tempo real de duas subestações, identificadas como T343 e T346, e injetando uma anomalia no sistema. Como resultado, observou-se que o gêmeo digital foi capaz de identificar a presença da anomalia em um curto intervalo de tempo, de aproximadamente 5 segundos, evidenciando seu potencial como ferramenta para resposta rápida a ciberataques.

O aprendizado de máquina, por sua vez, pode ser utilizado por meio de suas diferentes abordagens apresentadas anteriormente para aprimorar a eficiência e a confiabilidade das redes elétricas inteligentes, conforme defendem os autores Alomari *et al.* (2025). Seja com algoritmos de aprendizado supervisionado, não supervisionado ou por reforço, a inteligência artificial tem capacidade de processar e analisar grandes volumes de dados, tornando-se ideal para lidar com o monitoramento e o controle dinâmico dessas redes. Ademais, os autores afirmam que soluções baseadas em inteligência artificial para detecção de anomalias em redes elétricas tendem a se consolidar como mecanismos fundamentais de segurança nas redes elétricas inteligentes, dada sua capacidade de escanear continuamente a rede em busca de inconsistências e atividades suspeitas (ALOMARI *et al.*, 2025).

Em Xu *et al.* (2022), os autores argumentam que algoritmos de aprendizado de máquina podem estabelecer um mapeamento de relações entre entrada e saída para representar mecanismos complexos presentes nas redes elétricas inteligentes. Segundo os autores, entre os algoritmos mais utilizados e adequados para lidar com a complexidade dessas redes estão a regressão linear, SVM, os algoritmos de *clustering* e as árvores de decisão, devido à sua capacidade de realizar diagnóstico rápido de falhas, prever a utilização e a produção de recursos energéticos distribuídos e analisar a estabilidade das redes elétricas.

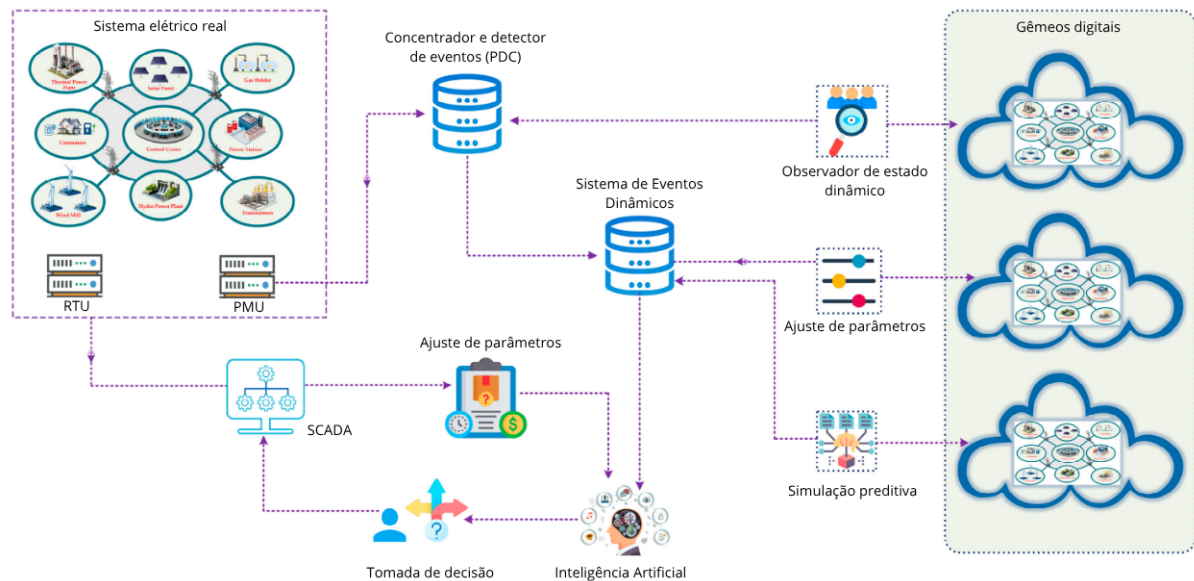
Em Onu, Mbohwa e Pradhan (2023), é apresentada a utilização de aprendizado de máquina para detecção e diagnóstico de falhas em redes elétricas inteligentes. Os autores destacam como aspectos positivos dessa integração a maior acurácia na detecção de falhas, decorrente da capacidade das técnicas do aprendizado de máquina de processar grandes volumes de dados e analisar as correlações complexas entre eles. Além disso, mencionam sua aplicação na manutenção preditiva, possibilitando a prevenção de falhas antes que ocorram, com o aprendizado de máquina sendo responsável por criar estratégias e até mesmo um planejamento estruturado para as manutenções ao longo da rede.

No trabalho de Danilczyk, Sun e He (2021), os autores apresentam a utilização de aprendizado profundo em conjunto com gêmeos digitais para detecção de anomalias em uma rede elétrica, mais especificamente danos ou falhas em equipamentos físicos. Embora o estudo não trate diretamente de cibersegurança e nem simule ataques, os autores desenvolvem um gêmeo digital como uma réplica virtual da rede de energia, capaz de coletar dados de PMU distribuídas pela rede e, através do algoritmo CNN, analisar os gráficos de tensão nos barramentos e identificar falhas existentes, bem como localizá-las. Para validação, foram utilizados dois modelos de rede, IEEE 9 Bus e IEEE 39 Bus, ambos contendo falhas inseridas em todos os barramentos. Como resultado, o sistema proposto obteve acurácia de 100% na detecção de falhas no modelo IEEE 9 Bus e acurácia de 94,9% na localização das falhas. Já para o modelo IEEE 39 Bus, a acurácia na detecção foi de 99,5%, enquanto a acurácia na localização das falhas atingiu 95,7%.

Em Rajendran, Raute e Caruana (2025), os autores abordam a utilização de gêmeos

digitais e inteligência artificial para o gerenciamento de uma rede elétrica, como ferramenta de monitoramento e para a sinalização de manutenção preventiva, aumentando consequentemente a eficiência desses sistemas, e apresentam uma arquitetura dessa utilização, como mostrado na Figura 23.

Figura 23 – Arquitetura de integração dos gêmeos digitais com inteligência artificial em uma rede elétrica.



Fonte: Adaptado de Rajendran, Raute e Caruana (2025).

Junto com isso, é mencionado que diversas empresas, como a General Electric e a Siemens, estão focadas no desenvolvimento de gêmeos digitais para redes de energia. Ao discutir o funcionamento dos gêmeos digitais e aprendizado de máquina em conjunto com as redes elétricas inteligentes, os autores Rajendran, Raute e Caruana (2025) destacam que:

“Essas réplicas digitais possibilitam monitoramento em tempo real, análise preditiva e otimização das operações da rede elétrica, contribuindo para maior eficiência, confiabilidade e resiliência. Ao aplicar a tecnologia de gêmeos digitais ao setor de energia, essas empresas estão estabelecendo as bases para redes elétricas mais inteligentes e adaptáveis, capazes de atender melhor às demandas da gestão energética moderna e aos objetivos de sustentabilidade. [...] A integração da tecnologia de gêmeos digitais com aprendizado de máquina facilita o monitoramento, a análise e a otimização em tempo real dos sistemas de energia, resultando em operações de rede aprimoradas e melhor gestão energética.”

Em Idrisov *et al.* (2025), os autores propõem a integração de gêmeos digitais e aprendizado de máquina para detectar anomalias e ciberataques em redes do tipo PEDG (*Power Electronics-Dominated Grid*), ou seja, redes com características semelhantes às redes elétricas inteligentes, por contarem com geração de energia renovável distribuída

e sistemas de armazenamento de energia. Os autores utilizam dois algoritmos de aprendizado de máquina, sendo eles florestas aleatórias e LSTM (*Long Short-Term Memory*), juntamente com o gêmeo digital para reproduzir o comportamento dos elementos da rede. Para a realização dos testes, foi utilizada uma bancada *hardware-in-the-loop* e a simulação de um ataque do tipo *man-in-the-middle*. Dois cenários foram analisados: no primeiro, apenas o aprendizado de máquina foi aplicado ao sistema físico real, e no segundo, o aprendizado de máquina atuou em conjunto com o gêmeo digital. Em seguida, avaliou-se a capacidade do sistema proposto de identificar o invasor na rede. Nos resultados obtidos, o modelo florestas aleatórias alcançou uma acurácia de aproximadamente 86,9% atuando em conjunto com o gêmeo digital na detecção do ataque cibernético, contra cerca de 74,3% atuando de maneira isolada, enquanto a LSTM atingiu cerca de 91,6% com gêmeo digital, em comparação a 86,9% sem gêmeo digital.

4 SÍNTESE E TENDÊNCIAS

A utilização de combustíveis fósseis marcou profundamente a história da humanidade e foi responsável por um acentuado desenvolvimento tecnológico. No entanto, a forte dependência desses recursos ao longo de muitos anos também incorporou novos desafios à sociedade, tornando urgente a transição para uma matriz energética mundial composta, ao menos em sua maioria, por fontes de energia renováveis. Diversos fatores explicam a demora dessa mudança, incluindo aspectos econômicos, como a elevada receita que alguns países ainda obtêm com combustíveis fósseis; aspectos financeiros, como os custos elevados da transição; e aspectos tecnológicos, como a maturidade limitada das energias renováveis há alguns anos. Acordos internacionais como o Acordo de Paris e a Agenda 2030, intermediados pela Organização das Nações Unidas e publicados em 2015, parecem finalmente impulsionar essa transição.

Nesse contexto, as redes elétricas inteligentes surgem como a espinha dorsal da transição e transformação energética, integrando tecnologias que permitem o monitoramento avançado das redes e a incorporação segura de fontes renováveis, inclusive de geração descentralizada. Além de proporcionar aos usuários uma rede elétrica mais limpa, segura e resiliente, a utilização de tecnologias de monitoramento nos sistemas elétricos traz, sobretudo, maior eficiência aos sistemas de potência, permitindo a máxima utilização dos recursos naturais. Em entrevista ao site *Manufacturing Digital*, Barbara Frei, vice-presidente executiva de automação industrial da Schneider Electric, empresa reconhecida como a mais sustentável do mundo nos anos de 2024 e 2025, afirmou:

“O que realmente me motiva é a crença de que a eficiência energética é fundamental para sermos verdadeiramente sustentáveis. E quando você olha para o problema das emissões de CO₂ como um todo, apenas 45% está na geração de energia, 55% está realmente em como você usa essa energia”.

Dessa forma, a incorporação de tecnologias para monitoramento, armazenamento, controle e maximização do uso da energia, bem como a adoção de uma nova rede em que os consumidores se tornam agentes ativos e participativos no mercado, torna-se essencial para os sistemas de energia. Por outro lado, outro tema que ganha força e tem sido amplamente pesquisado na última década é a cibersegurança. A crescente utilização de tecnologias da informação tem aumentado a conectividade e a digitalização dos sistemas, mas, ao mesmo tempo, cria novas portas de entrada para ataques cibernéticos, comprometendo a segurança, a privacidade e a integridade dos usuários. Nos últimos anos, os diversos ataques contra infraestruturas de energia demonstram não apenas o potencial danoso que um ataque cibernético pode causar, mas também sua capacidade de se reinventar e se tornar cada vez mais robusto, aumentando a probabilidade de sucesso dessas ofensivas.

Os gêmeos digitais, por sua vez, são uma tecnologia de simulação e controle de sistemas físicos reais que oferece diversas vantagens para a garantia de cibersegurança em redes elétricas. Nos últimos anos, avanços rápidos nas áreas de aprendizado de máquina

e dispositivos IoT têm impulsionado o desenvolvimento e a adoção dos gêmeos digitais, possibilitando aplicações em praticamente qualquer setor. O aprendizado de máquina, por sua vez, tem o papel de tornar o gêmeo digital ainda mais eficiente, permitindo a atualização automática dos modelos digitais, o apoio à tomada de decisão por meio da análise de dados e até mesmo a tomada de decisão automática, sem necessidade de intervenção humana. Tiago Busarello, professor e pesquisador da Universidade Federal de Santa Catarina na área de eletrônica de potência e membro sênior do IEEE (*Institute of Electrical and Electronics Engineers*), afirmou:

"Embora o conceito de gêmeos digitais na engenharia não seja novo, a capacidade de modificar automaticamente o modelo virtual sempre que ocorre qualquer alteração no sistema real está levando indústrias e academia a buscarem soluções novas, rápidas e mais confiáveis. A inteligência artificial é uma boa candidata para atender a essa demanda."

Pensando na utilização dessas tecnologias em redes elétricas inteligentes, os gêmeos digitais, em conjunto com o aprendizado de máquina, podem ser empregados de diferentes maneiras para otimização das redes. Na etapa de geração, o aprendizado de máquina pode utilizar os dados coletados pelos sensores inteligentes para otimizar a geração de energia, equilibrando produção e consumo por meio da previsão de carga a partir de dados históricos e de informações em tempo real provenientes de diferentes pontos da rede, além de dados de irradiação solar e vento, que influenciam diretamente a geração renovável. Em cenários de falha em equipamentos físicos, o aprendizado de máquina, combinado aos gêmeos digitais, pode detectar com precisão a localização da falha por meio da rede de sensores e ajustar o sistema de forma rápida em tempo real, isolando as áreas afetadas e reduzindo o impacto no fornecimento. A aplicação de aprendizado de máquina para manutenção preditiva também apresenta enorme potencial, contribuindo para aumentar a vida útil dos equipamentos distribuídos ao longo da rede, além de fornecer informações relevantes para os operadores por meio da análise de dados, servindo como apoio à tomada de decisão.

Na etapa de distribuição, que pode ser vista como a parte mais complexa das redes elétricas inteligentes, os medidores inteligentes fornecem informações valiosas para os gêmeos digitais, inclusive para a detecção de falhas, além de dados detalhados sobre perfis de consumo e variações horárias do consumo de energia. O aprendizado de máquina pode atuar em conjunto com os medidores inteligentes no mercado de energia, analisando o desempenho do sistema elétrico e sinalizando automaticamente aos consumidores a necessidade de economia de energia, além de contribuir para a precificação em tempo real em plataformas de comércio de energia. De forma complementar, também pode utilizar dados do estado de carga de sistemas de armazenamento de energia, como veículos elétricos e baterias, para melhorar a qualidade da energia na rede e equilibrar geração e consumo. No caso dos veículos elétricos, a literatura apresenta abordagens que propõem a utilização simultânea da energia proveniente da rede e da geração distribuída durante recargas

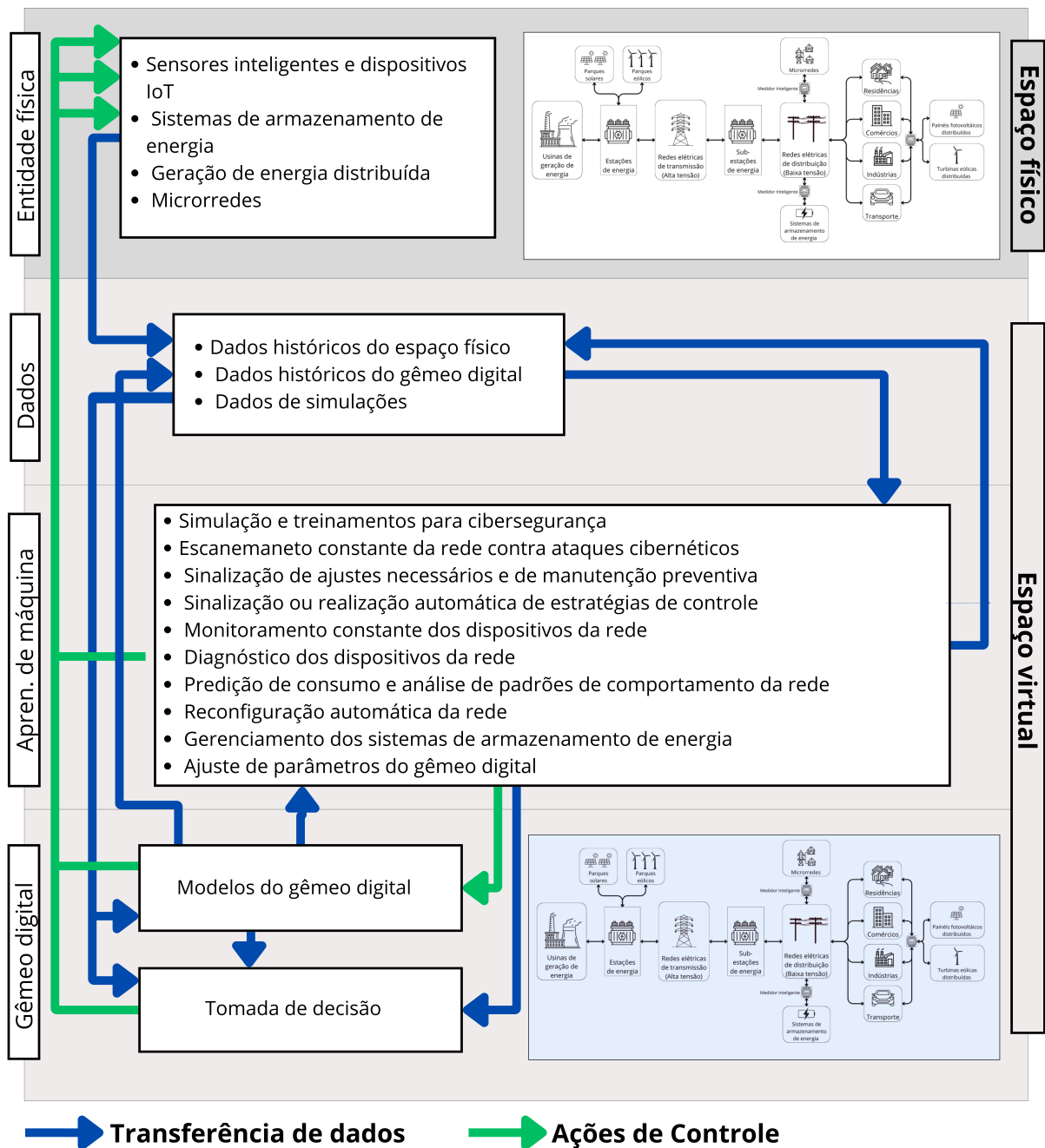
rápidas, mitigando possíveis instabilidades. Da mesma forma, o aprendizado de máquina pode analisar o estado de carga dos veículos e permitir a devolução de energia à rede, conceito conhecido como V2G (*Vehicle-to-Grid*), em momentos de maior necessidade.

Considerando o uso dos gêmeos digitais em conjunto com o aprendizado de máquina na detecção de ataques cibernéticos em redes elétricas inteligentes, o maior potencial dessa integração consiste na capacidade de realizar treinamentos com diferentes cenários, permitindo que o sistema aprenda a identificar anomalias decorrentes de diversos tipos de ataques, sem interferir no funcionamento da rede elétrica real. Ataques do tipo *Injection*, *Man-in-the-Middle* e *Smart Meter Tampering* podem ser simulados para injetar dados falsos ou alterar dados legítimos, como aumentos abruptos no consumo de energia ou falhas fictícias em equipamentos, permitindo que algoritmos como SVM distingam comportamentos normais de anormais. Ataques de *Brute Force*, *Masquerade* e *Spoofing*, que visam obter acesso não autorizado à dispositivos da rede, podem ser empregados para avaliar a detecção de padrões de comportamento incomuns, como tentativas repetidas de acesso, comportamentos não humanos e comandos suspeitos, sendo as redes neurais artificiais bastante úteis nesse contexto. Já para ataques como *Jamming*, *Time Synchronization Attacks* e *Denial-of-Service*, que visam interromper a comunicação entre nós ou tornar serviços indisponíveis, algoritmos de SVM e florestas aleatórias podem ser empregados para distinguir comportamentos normais de anômalos.

A partir dessas simulações e treinamentos, torna-se possível para as equipes de segurança cibernética avaliar o desempenho do modelo do gêmeo digital e das técnicas de proteção empregadas, além de desenvolver estratégias de controle e medidas de segurança com base nos resultados obtidos. A inteligência artificial, inclusive, pode fornecer informações valiosas sobre a causa raiz do ataque e sobre as características de comportamento de equipamentos específicos da rede sob diferentes condições de invasão, apoiando as equipes nesse desenvolvimento de novas medidas de segurança. Junto com isso, o aprendizado de máquina pode recomendar ou até realizar automaticamente os ajustes necessários na rede após os testes executados. Por fim, técnicas de aprendizado profundo podem ser utilizadas para identificar padrões complexos de comportamento em casos reais, permitindo que o sistema se adapte e responda aos ataques cibernéticos antes que causem danos ou interrupções nas redes elétricas, e sem depender de grandes volumes de dados previamente rotulados. Devido ao escaneamento constante da rede elétrica, os algoritmos de aprendizado profundo têm a capacidade de identificar anomalias mesmo sem treinamento prévio, além de serem capazes de compreender o comportamento dinâmico dos equipamentos presentes na rede e mudanças realizadas na rede, como a inserção de novas fontes de energia descentralizada, tornando-os essenciais no contexto de segurança cibernética em redes elétricas inteligentes. Na Figura 24, é apresentada uma arquitetura, desenvolvida pelo autor, para utilização de gêmeos digitais com aprendizado de máquina em redes elétricas inteligentes, tanto para otimização quanto para cibersegurança. Nessa arquitetura, composta por quatro camadas,

o sistema físico real, referenciado como entidade física, envia os dados coletados para a camada de dados, onde são armazenadas todas as informações do sistema. Esses dados são utilizados pela camada de aprendizado de máquina tanto para ajustar parâmetros nos modelos do gêmeo digital, presente na última camada, quanto para fornecer informações úteis para a tomada de decisão, também localizada na última camada, além de possibilitar a realização automática de ações de controle na entidade física.

Figura 24 – Arquitetura para utilização de gêmeos digitais com aprendizado de máquina em redes elétricas inteligentes.



Fonte: Elaborado pelo autor.

Para trabalhos futuros em relação aos analisados na literatura, entende-se que devem surgir mais pesquisas que apliquem gêmeos digitais com aprendizado de máquina para a detecção de ataques cibernéticos em redes de energia cada vez maiores, a fim de dimensionar adequadamente o potencial dessa combinação e sua acurácia em sistemas mais complexos. Também se espera a realização de estudos que incluam diferentes ataques de forma síncrona, sejam eles direcionados a linhas de transmissão, distribuição, medidores inteligentes ou sistemas SCADA, garantindo que a detecção seja eficaz mesmo em cenários de alta complexidade e ataques simultâneos em diversos pontos da rede. Além disso, devem ser desenvolvidos trabalhos que abordem também a prevenção de ataques cibernéticos focados no espaço virtual da rede elétrica inteligente, o qual igualmente pode ser alvo dessas ofensivas. Quanto às tendências futuras dessa aplicação, entende-se que a união entre gêmeos digitais e aprendizado de máquina será uma consequência natural do desenvolvimento contínuo dessas tecnologias, bem como da crescente adoção de dispositivos inteligentes, essenciais para essa integração. Na literatura, muitos autores destacam essa combinação como promissora, e a busca por redes de energia cada vez mais eficientes, no sentido de uso da energia, e mais seguras, no sentido de cibersegurança e prevenção contra ataques, reforça a importância do aprendizado de máquina para a máxima otimização dos sistemas das redes elétricas inteligentes.

5 CONCLUSÃO

Neste trabalho, foi conduzida uma revisão da literatura sobre o que são as redes elétricas inteligentes, sua importância, limitações e perspectivas para os próximos anos. Além disso, foram abordados os conceitos de gêmeos digitais e suas diferentes abordagens, o que é o aprendizado de máquina e seus principais algoritmos, bem como os ataques cibernéticos e os incidentes registrados na literatura contra infraestruturas de energia. Em seguida, discutiu-se como os gêmeos digitais podem ser utilizados em conjunto com o aprendizado de máquina para a detecção de ataques cibernéticos em redes elétricas inteligentes. A revisão contou com exemplos de aplicações encontrados na literatura, os resultados alcançados nesses trabalhos e as perspectivas futuras para a utilização de gêmeos digitais com aprendizado de máquina na detecção de ataques cibernéticos em redes inteligentes. De maneira geral, pode-se concluir que essa integração é promissora para garantir a integridade e a confidencialidade das redes, bem como o funcionamento ininterrupto, sobretudo em um cenário em que os ataques cibernéticos se tornam cada vez mais sofisticados.

REFERÊNCIAS

ABBASS, Hussein. What is artificial intelligence? **IEEE Transactions on Artificial Intelligence**, IEEE Computer Society, v. 2, n. 02, p. 94–95, 2021.

ABDALLA, Ahmed N; NAZIR, Muhammad Shahzad; TAO, Hai; CAO, Suqun; JI, Rendong; JIANG, Mingxin; YAO, Liu. Integration of energy storage system and renewable energy sources based on artificial intelligence: An overview. **Journal of Energy Storage**, Elsevier, v. 40, p. 102811, 2021.

ABRAHAM, Doney; HOUMB, Siv Hilde; ERDODI, Laszlo. Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation. **Applied Sciences**, MDPI, v. 15, n. 17, p. 9233, 2025.

ABRAHAM, Doney; TOFTEGAARD, Øyvind; DR, Binu Ben Jose; GEBREMEDHIN, Alemayehu; YILDIRIM YAYILGAN, Sule. Consequence simulation of cyber attacks on key smart grid business cases. **Frontiers in Energy Research**, Frontiers Media SA, v. 12, p. 1395954, 2024.

AHMAD, Furkan; KHALID, Mohd; PANIGRAHI, Bijaya Ketan. Development in energy storage system for electric transportation: A comprehensive review. **Journal of Energy Storage**, Elsevier, v. 43, p. 103153, 2021.

AHMED, Shakir D; AL-ISMAIL, Fahad SM; SHAFIULLAH, Md; AL-SULAIMAN, Fahad A; EL-AMIN, Ibrahim M. Grid integration challenges of wind energy: A review. **Ieee Access**, IEEE, v. 8, p. 10857–10878, 2020.

ALOMARI, Mohammad Ahmed; AL-ANDOLI, Mohammed Nasser; GHALEB, Mukhtar; THABIT, Reema; ALKAWSI, Gamal; ALSAYAYDEH, Jamil Abedalrahim Jamil; GAID, AbdulGuddoos SA. Security of smart grid: cybersecurity issues, potential cyberattacks, major incidents, and future directions. **Energies**, MDPI, v. 18, n. 1, p. 141, 2025.

ANDRESEN, Christian Andre; TORSÆTER, Bendik Nybakk; HAUGDAL, Hallvar; UHLEN, Kjetil. Fault detection and prediction in smart grids. *In*: IEEE. 2018 IEEE 9th international workshop on applied measurements for power systems (AMPS). [*S.l.*: *s.n.*], 2018. P. 1–6.

- ARSHI, Oroos; RAI, Akanksha; GUPTA, Gauri; PANDEY, Jitendra Kumar; MONDAL, Surajit. IoT in energy: a comprehensive review of technologies, applications, and future directions. **Peer-to-Peer Networking and Applications**, Springer, v. 17, n. 5, p. 2830–2869, 2024.
- ATTARAN, Mohsen; CELIK, Bilge Gokhan. Digital Twin: Benefits, use cases, challenges, and opportunities. **Decision Analytics Journal**, Elsevier, v. 6, p. 100165, 2023.
- ATTEYA, Inji; FAHMI, Nagi R; STRICKLAND, Danielle R; ASHOUR, HA. Utilization of battery energy storage systems (bess) in smart grid: A review. **Renewable Energy and Power Quality Journal**, European Association for the Development of Renewable Energies, Environment ..., v. 1, n. 14, p. 855–861, 2016.
- AZAD, Abul Kalam. **Advances in clean energy technologies**. [S.l.]: Academic Press, 2020.
- BALOH, Robert W. Electricity and the Nervous System. *In*: BRAIN Electricity: The Interwoven History of Electricity and Neuroscience. [S.l.]: Springer, 2024. P. 125–158.
- BEATO, Filipe. **Iberian blackout: Cyberattack is not to blame – but the threat to power grids is real**. Acessado em: 7 out. 2025. 2025. Disponível em: <https://www.weforum.org/stories/2025/05/spain-might-not-cyberattack-blackout-power-outage-electric-grids-vulnerable/>.
- BELLIZIO, Federica; XU, Wangkun; QIU, Dawei; YE, Yujian; PAPADASKALOPOULOS, Dimitrios; CREMER, Jochen L; TENG, Fei; STRBAC, Goran. Transition to digitalized paradigms for security control and decentralized electricity market. **Proceedings of the IEEE**, IEEE, v. 111, n. 7, p. 744–761, 2022.
- BELU, Radian. **Smart Grid Fundamentals: Energy Generation, Transmission and Distribution**. [S.l.]: CRC Press, 2022.
- BLACKBURN, Gavin. **Nova estratégia energética da Rússia empurra a Ucrânia para mais um inverno de apagões**. Acessado em: 25 out. 2025. 2025. Disponível em: <https://pt.euronews.com/2025/10/22/nova-estrategia-energetica-da-russia-empurra-a-ucrania-para-mais-um-inverno-de-apagoes>.

BLACKBURN, Gavin. **Spain says April's blackout was caused by multiple technical failures and rules out cyberattack**. Acessado em: 7 out. 2025. 2025. Disponível em: <https://www.euronews.com/my-europe/2025/06/17/spain-says-aprils-blackout-was-caused-by-multiple-technical-failures-and-rules-out-cyberat>.

BLUME, Steven W. **Electric power system basics for the nonelectrical professional**. [S.l.]: John Wiley & Sons, 2025.

BRESSANINI, Gabriel Lucas *et al.* Simulação de uma microrrede AC com controle centralizado, 2023.

BUSARELLO, Tiago. **Have you ever heard about Digital Twins?** Acessado em: 23 nov. 2025. 2024. Disponível em: <https://www.linkedin.com/feed/update/urn:li:activity:7239639220309372929/>.

BUTT, Osama Majeed; ZULQARNAIN, Muhammad; BUTT, Tallal Majeed. Recent advancement in smart grid technology: Future prospects in the electrical power network. **Ain Shams Engineering Journal**, Elsevier, v. 12, n. 1, p. 687–695, 2021.

CAMPANA, Paola; CENSI, Riccardo; RUGGIERI, Roberto; AMENDOLA, Carlo. Smart Grids and Sustainability: The Impact of Digital Technologies on the Energy Transition. **Energies**, MDPI, v. 18, n. 9, p. 2149, 2025.

CASTRO BARBOSA, Xênia de. Breve introdução à história da Inteligência Artificial. **Jamaxi**, v. 4, n. 1, 2020.

CLARK, Gregory. The industrial revolution. *In*: HANDBOOK of economic growth. [S.l.]: Elsevier, 2014. v. 2. P. 217–262.

COPPOLINO, Luigi; NARDONE, Roberto; PETRUOLO, Alfredo; ROMANO, Luigi. Building cyber-resilient smart grids with digital twins and data spaces. **Applied Sciences**, MDPI, v. 13, n. 24, p. 13060, 2023.

COPPOLINO, Luigi; NARDONE, Roberto; PETRUOLO, Alfredo; ROMANO, Luigi; SOUVENT, Andrej. Exploiting digital twin technology for cybersecurity monitoring in smart grids. *In*: PROCEEDINGS of the 18th international conference on availability, reliability and security. [S.l.: s.n.], 2023. P. 1–10.

- DANILCZYK, William; SUN, Yan Lindsay; HE, Haibo. Smart grid anomaly detection using a deep learning digital twin. *In: IEEE. 2020 52nd North American Power Symposium (NAPS)*. [S.l.: s.n.], 2021. P. 1–6.
- DASTRES, Roza; SOORI, Mohsen. Artificial neural network systems. **International Journal of Imaging and Robotics (IJIR)**, v. 21, n. 2, p. 13–25, 2021.
- DATA, Our World in. **Renewable Energy**. Accessed: 12 October 2025. 2025. Disponível em: <https://ourworldindata.org/renewable-energy>.
- DI FOGGIA, Giacomo. Smart Grid Technologies and the 2030 Agenda for Sustainable Development: Drivers for Innovation. **Preprints**, MDPI AG, 2020.
- DICKINSON, Henry Winram. **A short history of the steam engine**. [S.l.]: Routledge, 2022.
- DINCER, Ibrahim; OZTURK, Murat. **Geothermal energy systems**. [S.l.]: Elsevier, 2021.
- ENERDATA. **Share of renewables in electricity production**. Accessed: 12 October 2025. 2025. Disponível em: <https://yearbook.enerdata.net/renewables/renewable-in-electricity-production-share.html>.
- ENERGY-CHARTS. **Durchschnittliche öffentliche Nettostromerzeugung in einer Woche in Deutschland 2025**. Accessed: 16 November 2025. 2025. Disponível em: <https://www.energy-charts.info/charts/power/chart.htm?l=de&c=DE&source=sw&year=2025&week=-2>.
- GASPAROTTO, Juciano; MARTINELLO, Kátia Da Boit. Coal as an energy source and its impacts on human health. **Energy Geoscience**, Elsevier, v. 2, n. 2, p. 113–120, 2021.
- GÖDE, Aslı; KALKAN, Adnan. What is artificial intelligence. **A. Akpınar, Research on Mathematics and Science-IV**, p. 23–43, 2023.
- HASSAN, Qusay F. **Internet of things A to Z: technologies and applications**. [S.l.]: John Wiley & Sons, 2025.

HASSANIEN, Aboul-Ella; CHANG, Kuo-Chi; MINCONG, Tang. **Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2021**. [S.l.]: Springer Nature, 2021. v. 1339.

HOLMES, David; PAPATHANASAKI, Maria; MAGLARAS, Leandros; FERRAG, Mohamed Amine; NEPAL, Surya; JANICKE, Helge. Digital twins and cyber security—solution or challenge? *In*: IEEE. 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). [S.l.: s.n.], 2021. P. 1–8.

HOMAEI, Mohammadhossein; MOGOLLÓN-GUTIÉRREZ, Óscar; SANCHO, José Carlos; ÁVILA, Mar; CARO, Andrés. A review of digital twins and their application in cybersecurity based on artificial intelligence. **Artificial Intelligence Review**, Springer, v. 57, n. 8, p. 201, 2024.

IDRISOV, Ildar N; OKEKE, Divine; ALBASEER, Abdullatif; ABDALLAH, Mohamed; IBANEZ, Federico M. Leveraging digital twin and machine learning techniques for anomaly detection in power electronics dominated grid. **arXiv preprint arXiv:2501.13474**, 2025.

INSIGHT, Fortune Business. **Cybersecurity Market Size, Share Industry Analysis**. Acessado em: 23 nov. 2025. 2025. Disponível em: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>.

ISRAEL, Paul. **Thomas Edison: A Reference Guide to His Life and Works**. [S.l.]: Bloomsbury Publishing PLC, 2024.

IWUANYANWU, Obinna; GIL-OZOUDEH, Ifechukwu; OKWANDU, Azubuike Chukwudi; IKE, Chidiebere Somadina. The integration of renewable energy systems in green buildings: Challenges and opportunities. **Journal of Applied**, 2022.

JAIN, Udit; NAGRAMI, Faizan ul Haque; SHARMA, Barkha; PRIYAMBADA; PARUL; SHARMA, Uma. Natural Resources: Definition, Types, Examples, Uses, and Abuses. **Epidemiology and Environmental Hygiene in Veterinary Public Health**, Wiley Online Library, p. 329–338, 2025.

JANIESCH, Christian; ZSCHECH, Patrick; HEINRICH, Kai. Machine learning and deep learning. **Electronic markets**, Springer, v. 31, n. 3, p. 685–695, 2021.

JO, Taeho. Machine learning foundations. **Supervised, Unsupervised, and Advanced Learning**. Cham: Springer International Publishing, Springer, v. 6, n. 3, p. 8–44, 2021.

JONES, David; SNIDER, Chris; NASSEHI, Aydin; YON, Jason; HICKS, Ben. Characterising the Digital Twin: A systematic literature review. **CIRP journal of manufacturing science and technology**, Elsevier, v. 29, p. 36–52, 2020.

JONES, Sam. **Spanish minister rules out cyber-attack as cause of April blackout, after expert report**. Acessado em: 7 out. 2025. 2025. Disponível em: <https://www.theguardian.com/world/2025/jun/17/expert-report-rules-out-cyber-attack-for-spain-and-portugal-april-blackout>.

JUDGE, Malik Ali; KHAN, Asif; MANZOOR, Awais; KHATTAK, Hasan Ali. Overview of smart grid implementation: Frameworks, impact, performance and challenges. **Journal of Energy Storage**, Elsevier, v. 49, p. 104056, 2022.

JUDSON, Emily; FITCH-ROY, Oscar; SOUTAR, Iain. Energy democracy: A digital future? **Energy Research & Social Science**, Elsevier, v. 91, p. 102732, 2022.

JYENISKHAN, Nursultan; KEUTAYEVA, Aigerim; KAZBEK, Gani; ALI, Md Hazrat; SHEHAB, Essam. Integrating machine learning model and digital twin system for additive manufacturing. **IEEE Access**, IEEE, v. 11, p. 71113–71126, 2023.

KAMRAN, Muhammad; FAZAL, Muhammad Rayyan. **Renewable energy conversion systems**. [S.l.]: Academic Press, 2021.

KANDASAMY, Nandha Kumar; VENUGOPALAN, Sarad; WONG, Tin Kit; LEU, Nicholas Junming. An electric power digital twin for cyber security testing, research and education. **Computers and Electrical Engineering**, Elsevier, v. 101, p. 108061, 2022.

KENNEDY, John. **Special Message to the Congress on Natural Resources**. Acessado em: 10 out. 2025. 1961. Disponível em: <https://www.presidency.ucsb.edu/documents/special-message-the-congress-natural-resources>.

KHAN, Irfan; ZAKARI, Abdulrasheed; AHMAD, Munir; IRFAN, Muhammad; HOU, Fujun. Linking energy transitions, energy consumption, and environmental

sustainability in OECD countries. **Gondwana Research**, Elsevier, v. 103, p. 445–457, 2022.

KHOEI, Tala Talaei; SLIMANE, Hadjar Ould; KAABOUC, Naima. A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. **arXiv preprint arXiv:2207.07738**, 2022.

KIRMANI, Sheeraz; MAZID, Abdul; KHAN, Irfan Ahmad; ABID, Manaullah. A survey on IoT-enabled smart grids: technologies, architectures, applications, and challenges. **Sustainability**, MDPI, v. 15, n. 1, p. 717, 2022.

KISSINGER, Henry; SCHMIDT, Eric; HOTTENLOCHER, Daniel. **A era da inteligência artificial**. [S.l.]: Leya, 2021.

KREUZER, Tim; PAPAPETROU, Panagiotis; ZDRAVKOVIC, Jelena. Artificial intelligence in digital twins—A systematic literature review. **Data & Knowledge Engineering**, Elsevier, v. 151, p. 102304, 2024.

KRIVOHLAVA, Zuzana; CHREN, Stanislav; ROSSI, Bruno. Failure and fault classification for smart grids. **Energy Informatics**, Springer, v. 5, n. 1, p. 33, 2022.

KUZLU, M; PIPATTANASOMPOM, M; RAHMAN, S. A comprehensive review of smart grid related standards and protocols. *In: IEEE. 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG)*. [S.l.: s.n.], 2017. P. 12–16.

LE, Tan Duy; GE, Mengmeng; ANWAR, Adnan; LOKE, Seng W; BEURAN, Razvan; DOSS, Robin; TAN, Yasuo. Gridattackanalyzer: A cyber attack analysis framework for smart grids. **Sensors**, MDPI, v. 22, n. 13, p. 4795, 2022.

MAJA, Mengistu M; AYANO, Samuel F. The impact of population growth on natural resources and farmers' capacity to adapt to climate change in low-income countries. **Earth Systems and Environment**, Springer, v. 5, n. 2, p. 271–283, 2021.

MAKA, Ali OM; ALABID, Jamal M. Solar energy technology and its roles in sustainable development. **Clean Energy**, Oxford University Press UK, v. 6, n. 3, p. 476–483, 2022.

MAZHAR, Tehseen; IRFAN, Hafiz Muhammad; KHAN, Sunawar; HAQ, Inayatul; ULLAH, Inam; IQBAL, Muhammad; HAMAM, Habib. Analysis of cyber security

attacks and its solutions for the smart grid using machine learning and blockchain methods. **Future Internet**, MDPI, v. 15, n. 2, p. 83, 2023.

MILLER, Richard B; PASERBA, John. Pearl Street Station: Powering the First Distribution Network [History]. **IEEE Power and Energy Magazine**, IEEE, v. 22, n. 6, p. 134–140, 2024.

MINERVA, Roberto; CRESPI, Noel; FARAHBAKHS, Reza; AWAN, Faraz M. Artificial intelligence and the digital twin: an essential combination. *In: THE Digital Twin*. [S.l.]: Springer, 2023. P. 299–336.

MOHAMMED, Saad Hammood; AL-JUMAILY, Abdulmajeed; SINGH, Mandeep S Jit; JIMÉNEZ, Víctor P Gil; JABER, Aqeel S; HUSSEIN, Yaseen Soubhi; AL-NAJJAR, Mudhar Mustafa Abdul Kader; AL-JUMEILY, Dhiya. A review on the evaluation of feature selection using machine learning for cyber-attack detection in smart grid. **Ieee Access**, IEEE, v. 12, p. 44023–44042, 2024.

MOKHATAB, Saeid; POE, William A; MAK, John Y. **Handbook of natural gas transmission and processing: principles and practices**. [S.l.]: Gulf professional publishing, 2018.

MORENO ESCOBAR, Jesús Jaime; MORALES MATAMOROS, Oswaldo; TEJEIDA PADILLA, Ricardo; LINA REYES, Ixchel; QUINTANA ESPINOSA, Hugo. A comprehensive review on smart grids: Challenges and opportunities. **Sensors**, MDPI, v. 21, n. 21, p. 6978, 2021.

MOSTENSKA, Tatyana Genadiivna; CHEREP, Oleksandr Grigorovich; LESCHCHENKO, Anatoly Anatoliyovich; NAUMENKO, Yevhen Valentynovich; KALIUZHNA, Yuliia Viktorivna; MARKOVA, Svitlana Viktorivna; MASLAK, Maria Volodymyrivna. INNOVATIVE APPROACHES TO THE USE OF ARTIFICIAL INTELLIGENCE IN COUNTERING DISINFORMATION: EU EXPERIENCE AND PROSPECTS FOR UKRAINE. **Publishing House “Baltija Publishing”**, 2025.

MUQEET, Hafiz Abdul; LIAQAT, Rehan; JAMIL, Mohsin; KHAN, Asharf Ali. A state-of-the-art review of smart energy systems and their management in a smart grid environment. **Energies**, MDPI, v. 16, n. 1, p. 472, 2023.

NATIONS, United. **The Paris Agreement**. Accessed: 12 October 2025. 2015.

Disponível em: <https://www.un.org/en/climatechange/paris-agreement>.

NATIONS, United. **Transforming our world: the 2030 Agenda for Sustainable Development**. Accessed: 12 October 2025. 2015. Disponível em:

<https://sdgs.un.org/2030agenda>.

NDAHEPELE, L; CHOWDHURY, S. Impact of distributed generation on traditional protection in distribution and transmission systems: a review. **2020 IEEE PES/IAS PowerAfrica**, IEEE, p. 1–5, 2020.

OLIVEIRA, Savio Alves de. **Gemeos digitais para baterias de veiculos eletricos**. 2025. Diss. (Mestrado) – Universidade Federal de Campina Grande.

ONU, Peter; MBOHWA, Charles; PRADHAN, Anup. Machine Learning: A Comprehensive Exploration of Fault Detection and Diagnosis in Smart Grids. *In*: IEEE. 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). [S.l.: s.n.], 2023. P. 1–6.

PANESAR, Arjun. Machine learning algorithms. *In*: MACHINE learning and AI for healthcare: big data for improved health outcomes. [S.l.]: Springer, 2020. P. 85–144.

PARAMATI, Sudharshan Reddy; SHAHZAD, Umer; DOĞAN, Buhari. The role of environmental technology for energy demand and energy efficiency: Evidence from OECD countries. **Renewable and Sustainable Energy Reviews**, Elsevier, v. 153, p. 111735, 2022.

PASSOS, Fernanda Werlich dos. **Experimentacao com gemeos digitais aplicados ao ambiente construido: conceituacao, ferramentas e competencias**. 2024. Diss. (Mestrado) – Universidade Federal de Santa Catarina.

PAUL, Bishowjit *et al*. Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. **Heliyon**, Elsevier, v. 10, n. 19, 2024.

QI, Qinglin; TAO, Fei; HU, Tianliang; ANWER, Nabil; LIU, Ang; WEI, Yongli; WANG, Lihui; NEE, Andrew YC. Enabling technologies and tools for digital twin. **Journal of Manufacturing Systems**, Elsevier, v. 58, p. 3–21, 2021.

RAINSFORD, Sarah. **A estratégia militar da Rússia para deixar a Ucrânia sem energia elétrica**. Acessado em: 25 out. 2025. 2024. Disponível em: <https://www.bbc.com/portuguese/articles/cd18951159xo>.

RAJENDRAN, Gowthamraj; RAUTE, Reiko; CARUANA, Cedric. A Comprehensive Review of Solar PV Integration with Smart-Grids: Challenges, Standards, and Grid Codes. **Energies**, MDPI, v. 18, n. 9, p. 2221, 2025.

REDELINGHUYS, AJH; BASSON, Anton Herman; KRUGER, Karel. A six-layer architecture for the digital twin: a manufacturing case study implementation. **Journal of Intelligent Manufacturing**, Springer, v. 31, n. 6, p. 1383–1402, 2020.

RIND, Yousaf Murtaza; RAZA, Muhammad Haseeb; ZUBAIR, Muhammad; MEHMOOD, Muhammad Qasim; MASSOUD, Yehia. Smart energy meters for smart grids, an internet of things perspective. **Energies**, MDPI, v. 16, n. 4, p. 1974, 2023.

SACKS, Rafael; BRILAKIS, Ioannis; PIKAS, Ergo; XIE, Haiyan Sally; GIROLAMI, Mark. Construction with digital twin information systems. **Data-centric engineering**, Cambridge University Press, v. 1, e14, 2020.

SAN, Omer. The digital twin revolution. **Nature Computational Science**, Nature Publishing Group US New York, v. 1, n. 5, p. 307–308, 2021.

SHARIFANI, Koosha; AMINI, Mahyar. Machine learning and deep learning: A review of methods and applications. **World Information Technology and Engineering Journal**, v. 10, n. 07, p. 3897–3904, 2023.

SINSEL, Simon R; RIEMKE, Rhea L; HOFFMANN, Volker H. Challenges and solution technologies for the integration of variable renewable energy sources—a review. **renewable energy**, Elsevier, v. 145, p. 2271–2285, 2020.

SOEDER, Daniel. **Energy Futures**. [S.l.]: Springer, 2022.

SOORI, Mohsen; AREZOO, Behrooz; DASTRES, Roza. Digital twin for smart manufacturing, A review. **Sustainable Manufacturing and Service Economics**, Elsevier, v. 2, p. 100017, 2023.

SPEIGHT, James G. **Natural gas: a basic handbook**. [S.l.]: Gulf Professional Publishing, 2018.

- STEARNS, Peter N. **The industrial revolution in world history**. [S.l.]: Routledge, 2020.
- STEINDL, Gernot; STAGL, Martin; KASPER, Lukas; KASTNER, Wolfgang; HOFMANN, Rene. Generic digital twin architecture for industrial energy systems. **Applied Sciences**, MDPI, v. 10, n. 24, p. 8903, 2020.
- TAN, Kang Miao; BABU, Thanikanti Sudhakar; RAMACHANDARAMURTHY, Vigna K; KASINATHAN, Padmanathan; SOLANKI, Sunil G; RAVEENDRAN, Shangari K. Empowering smart grid: A comprehensive review of energy storage technology and application with renewable energy integration. **Journal of Energy Storage**, Elsevier, v. 39, p. 102591, 2021.
- VALLÉE, Alexandre. Digital twin for healthcare systems. **Frontiers in Digital Health**, Frontiers Media SA, v. 5, p. 1253050, 2023.
- VANDERHORN, Eric; MAHADEVAN, Sankaran. Digital Twin: Generalization, characterization and implementation. **Decision support systems**, Elsevier, v. 145, p. 113524, 2021.
- WANG, Lu; DENG, Tianhu; SHEN, Zuo-Jun Max; HU, Hao; QI, Yongzhi. Digital twin-driven smart supply chain. **Frontiers of Engineering Management**, Springer, v. 9, n. 1, p. 56–70, 2022.
- WANG, Yi; CHEN, Chien-Fei; KONG, Peng-Yong; LI, Husheng; WEN, Qingsong. A cyber–physical–social perspective on future smart distribution systems. **Proceedings of the IEEE**, IEEE, v. 111, n. 7, p. 694–724, 2022.
- WANG, Zongyan. Digital twin technology. *In*: INDUSTRY 4.0-impact on intelligent logistics and manufacturing. [S.l.]: IntechOpen, 2020.
- XU, Chongchong; LIAO, Zhicheng; LI, Chaojie; ZHOU, Xiaojun; XIE, Renyou. Review on interpretable machine learning in smart grid. **Energies**, MDPI, v. 15, n. 12, p. 4427, 2022.
- YANG, Zhou; TANG, Chao; ZHANG, Tongrui; ZHANG, Zhongjian; DOAN, Dat Tien. Digital twins in construction: Architecture, applications, trends and challenges. **Buildings**, MDPI, v. 14, n. 9, p. 2616, 2024.