Um *Scorecard* Operacional para Métricas de Segurança e Resiliência em Sistemas de Energia Baseados em IoT *

Lucas S. Oliveira[1], **Gabriel S. B. Alves**[1], **Thiago C. Jesus**[1,2]

[1]Programa de Pós-Graduação em Ciência da Computação (PGCC)
Universidade Estadual de Feira de Santana (UEFS)
Avenida Transnordestina, s/n, CEP: 44036-900, Feira de Santana – BA – Brazil

[2]Departamento de Tecnologia – Universidade Estadual de Feira de Santana (UEFS)
Avenida Transnordestina, s/n, CEP: 44036-900, Feira de Santana – BA – Brazil

lucassdeoliveira@outlook.com.br, gabrielalves@ecomp.uefs.br, tcjesus@uefs.br

Resumo. *A digitalização dos sistemas energéticos amplia a superfície de ataque e a dependência de componentes IoT/OT, ao mesmo tempo em que requisitos regulatórios como NIS2, CRA, LGPD e PNCiber, conjugados a exigências operacionais, demandam medições comparáveis e auditáveis de segurança e resiliência. Para responder a essa necessidade, este trabalho propõe um* scorecard *operacional composto por 15 submétricas distribuídas em 7 dimensões orquertradas por regras de* gating *que tornam dimensões críticas não compensáveis. A metodologia é validada em três cenários contrastantes derivados de premissas explícitas, a saber, um sistema doméstico de gerenciamento de energia, uma plataforma de comunidade de energia renovável e uma microrrede hospitalar, avaliados sob quatro perfis de ponderação. Os* scores *resultantes evidenciam capacidade discriminativa ao longo de todo o espectro de maturidade das aplicações, e a metodologia mantém-se robusta a variações dos pesos.*

Abstract. *The digitalisation of energy systems widens the attack surface and the dependence on IoT/OT components, while regulatory requirements such as NIS2, CRA, LGPD and PNCiber, combined with operational demands, call for comparable and auditable security and resilience measurements. To address this need, this work proposes an operational* scorecard *composed of 15 submetrics distributed across 7 dimensions and orchestrated by* gating *rules that render critical dimensions non-compensable. The methodology is validated on three contrasting scenarios derived from explicit assumptions, namely a domestic Home Energy Management System, a Renewable Energy Community platform and a hospital microgrid, evaluated under four weighting profiles. The resulting* scores *show discriminative capacity across the full maturity spectrum of the applications, and the methodology remains robust under weight perturbations.*

1. Introdução

A digitalização dos sistemas de energia tem reconfigurado a forma como a eletricidade é gerada, monitorada, distribuída e consumida. Nesse cenário, a *Internet of Things* (IoT)

*Este trabalho foi apoiado em parte pela Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB), auxílio nº 2465/2025, e pelo Programa Interno de Auxílio Financeiro aos Programas de Pós-Graduação Stricto Sensu (AUXPPG) da UEFS e pelo Programa de Apoio à Pós-Graduação (PROAP) da CAPES.

deixa de ser apenas uma camada auxiliar de aquisição de dados e passa a compor a própria infraestrutura operacional das redes inteligentes, conectando ativos físicos, sistemas de controle, consumidores, agregadores e operadores em arquiteturas ciberfísicas distribuídas [Achaal et al. 2024]. No Brasil, esse processo dialoga com a expansão da micro e minigeração distribuída, com a digitalização dos serviços de distribuição e com a necessidade de coordenar diferentes atores no contexto dos novos modelos de serviços energéticos regulados pela Agência Nacional de Energia Elétrica (ANEEL) e pelo marco legal da geração distribuída. Como consequência, os sistemas de energia tornam-se mais observáveis, automatizados e responsivos, mas também mais dependentes de conectividade, software embarcado, serviços digitais, interfaces remotas e cadeias de fornecimento tecnológicas complexas.

Ao mesmo tempo, essa digitalização amplia as possibilidades de ataque dos sistemas elétricos e torna a segurança uma condição para a confiabilidade, a continuidade e a resiliência do fornecimento de energia. Dispositivos IoT de baixo custo operam frequentemente com recursos limitados, ciclos de atualização irregulares, credenciais frágeis e interfaces expostas, enquanto sistemas legados de tecnologia operacional (OT) passam a interagir com ambientes de tecnologia da informação (IT) e dados operacionais, comerciais e pessoais tornam-se insumos críticos para supervisão, controle e tomada de decisão [Parsons et al. 2023, Mishchenko et al. 2024]. Diferentemente de aplicações puramente digitais, falhas de confidencialidade, integridade ou disponibilidade em sistemas de energia baseados em IoT (IoT+Energia) podem produzir efeitos físicos e socioeconômicos, afetando estados de equipamentos, estimação de estado, resposta da demanda, consumidores e infraestruturas críticas [Achaal et al. 2024]. Garantir segurança nesses sistemas é particularmente difícil devido à heterogeneidade de equipamentos, protocolos e fabricantes, à convergência IT/OT, às restrições de recursos em ativos de campo, à dependência de fornecedores externos e à necessidade de manter disponibilidade operacional contínua [Mishchenko et al. 2024].

Uma das dificuldades centrais nesse contexto é mensurar o nível de segurança ou, de forma complementar, o nível de vulnerabilidade, exposição, risco e resiliência de uma solução IoT+Energia. Embora existam normas, recomendações e arcabouços de gestão de risco, a comparação objetiva entre soluções, projetos-piloto, arquiteturas de comunicação ou plataformas de fornecedores ainda é limitada pela ausência de métricas operacionais padronizadas, auditáveis e suficientemente simples para uso em processos de projeto, aquisição, implantação e acompanhamento. Avaliações qualitativas são úteis, mas nem sempre permitem identificar lacunas prioritárias, comparar alternativas ou justificar decisões técnicas com base em evidências. Por outro lado, avaliações altamente intrusivas, baseadas em ensaios laboratoriais complexos ou testes de penetração completos, podem ser inviáveis em fases iniciais de projeto ou em ambientes operacionais sensíveis [Parsons et al. 2023].

Essa dificuldade torna-se ainda mais relevante quando os sistemas precisam atender simultaneamente a requisitos regulatórios, contratuais e normativos, sendo que o cumprimento regulatório não implica, por si só, comparabilidade técnica entre soluções. Por exemplo, dois fornecedores podem declarar aderência a requisitos semelhantes, mas implementá-los com diferentes níveis de maturidade, cobertura, rastreabilidade e efetividade. A lacuna entre “estar conforme” e “ser mensuravelmente seguro” exige, portanto,

instrumentos que traduzam obrigações normativas e boas práticas em indicadores verificáveis e comparáveis. Este trabalho propõe um conjunto de métricas e índices de Segurança e Resiliência para Sistemas de Energia baseados em IoT, estruturado como um *Scorecard de Segurança e Resiliência* para soluções IoT+Energia. A proposta privilegia métricas mensuráveis com baixo atrito, ou seja, indicadores que possam ser obtidos sem interromper a operação, sem exigir acesso irrestrito ao código dos fabricantes e sem depender, em uma primeira etapa, de ensaios intrusivos ou infraestrutura laboratorial complexa. Esse indicadores pode derivar de fontes como revisão documental, inventário de ativos, análise de arquitetura, políticas de atualização, varreduras não destrutivas, telemetria, logs operacionais, documentação de fornecedores e evidências de conformidade. Essa abordagem busca viabilizar avaliações repetíveis em fases de projeto, contratação, implantação, auditoria leve e melhoria contínua, preservando a possibilidade de complementação por testes mais profundos quando necessário.

As métricas propostas mantêm alinhamento explícito com obrigações regulatórias e normativas, mapeando dimensões técnicas para requisitos mínimos de diferentes legislações, normas e boas práticas. Em vez de propor um índice puramente abstrato, o *scorecard* organiza a avaliação em dimensões como governança e conformidade, gestão de ativos, identidade e controle de acesso, segurança de comunicação, ciclo de vida, monitoramento e detecção, continuidade e recuperação, proteção de dados e resiliência operacional. Para evitar que bons resultados em uma dimensão mascarem falhas críticas em outra, a agregação é transparente e segue regras de *gating*: fórmulas auditáveis, pesos declarados, análise de sensibilidade e limiares explícitos impedem compensações perigosas.

As principais contribuições deste artigo são: (i) um catálogo de submétricas operacionais para avaliar segurança e resiliência em sistemas IoT+Energia; (ii) um algoritmo de *scoring* em escala 0–100, com agregação por dimensão e regras explícitas de *gating*; (iii) o mapeamento das métricas para requisitos regulatórios e normativos aplicáveis a infraestruturas energéticas digitalizadas, com paralelos entre o contexto europeu e o brasileiro; (iv) a validação da metodologia em cenários contrastantes derivados de premissas explícitas, abrangendo diferentes níveis de maturidade; e (v) uma análise de sensibilidade e testes de estresse do mecanismo de agregação, verificando a robustez do índice diante de variações de pesos e falhas críticas. Com isso, o trabalho busca oferecer um instrumento prático, auditável e reprodutível para comparar soluções, apoiar decisões de projeto e implantação e contribuir para a melhoria contínua da segurança e resiliência de sistemas de energia cada vez mais dependentes de IoT.

2. Trabalhos Relacionados

A avaliação de segurança e resiliência em sistemas de energia baseados em IoT está apoiada hoje em um repertório consolidado de *frameworks* normativos, métricas de vulnerabilidade e modelos de resiliência ciberfísica. *Frameworks* de referência como o *Cybersecurity Framework* (CSF) do *National Institute of Standards and Technology* (NIST), o ISA/IEC 62443 [ISA/IEC 2024], a série IEC 62351 [International Electrotechnical Commission 2024], o NISTIR 7628 [NIST Smart Grid Interoperability Panel – Cyber Security Working Group 2014], o NIST SP 800-82r3 [Stouffer et al. 2023], o NIST SP 800-213 [Fagan et al. 2021] e o IEEE Std 1547.3-2023 organizam capacidades em funções, níveis de segurança ou requisitos por tipo de ativo, e são fundamentais para uniformizar a linguagem de *bench-*

marking OT/IoT. Em paralelo, instrumentos normativos recentes estabelecem obrigações mínimas de gestão de risco, gestão de vulnerabilidades, notificação de incidentes e proteção de dados pessoais. São exemplos a Diretiva *Network and Information Security 2* (NIS2), o *Cyber Resilience Act* (CRA), a Lei Geral de Proteção de Dados Pessoais (LGPD), o Decreto que institui a Política Nacional de Cibersegurança (PNCiber) e a ABNT NBR ISO/IEC 27001/27002:2022. Trabalhos como [Jara et al. 2024] discutem como traduzir os requisitos do CRA e da NIS2 em práticas concretas de engenharia em IoT, enquanto [Horálek and Sobeslav 2023] mapeia controles para subestações alinhados a ISO 27001 e à NIS2. Em todos esses casos, contudo, o foco é prescritivo, ou seja, define-se o que precisa existir, mas não se estabelece um índice agregável e comparável entre soluções concretas. O próprio relatório pioneiro da Agência da União Europeia para Cibersegurança (ENISA) sobre métricas de resiliência [ENISA 2011] já observava que poucos *frameworks* são agregáveis, diagnóstico ainda válido no panorama setorial recente.

No plano das métricas, o *Common Vulnerability Scoring System* (CVSS) [FIRST.org 2019] é o instrumento dominante para comunicar a severidade de vulnerabilidades individuais, mas o próprio guia explicita que o *Base Score* não deve ser usado isoladamente para avaliar risco, que depende de contexto, exposição e impacto [Linkov et al. 2013] – e, em energia, de modos de operação ilha, efeitos em cascata e requisitos de *safety* [U.S. Department of Energy 2024]. O NIST SP 800-55v2 [Schroeder et al. 2024] estabelece princípios para programas de medição de segurança orientados à decisão organizacional, princípios que adotamos neste trabalho, mas sem prescrever um modelo concreto para o domínio energético. Em uma direção complementar, métricas operacionais de resiliência ciberfísica vêm sendo propostas no domínio de *smart grids*. Em [Sarker et al. 2022] é proposta uma métrica de resiliência para sistemas de distribuição com IoT que combina um *IoT Trustability Score* agregado por tomada de decisão multicritério difusa (*Fuzzy Multi-Criteria Decision Making*, MCDM) e otimização por análise envoltória de dados (*Data Envelopment Analysis*, DEA) com teoria dos jogos. Já em [Zografopoulos et al. 2021] é apresentado um *framework* amplo de modelagem de ameaças, avaliação de risco e métricas para sistemas ciberfísicos de energia (*Cyber-Physical Energy Systems*, CPES), validado em *testbeds*. Os autores em [Coppolino et al. 2023] propõem monitorização cibernética baseada em *Digital Twins* alinhada à NIS2, enquanto que em [Aghazadeh Ardebili et al. 2025] são instrumentados indicadores-chave de desempenho (*Key Performance Indicators*, KPIs) de resiliência em tempo real sobre *Digital Twins* de infraestrutura crítica. A metodologia *i-TRACE* para gestão de energia e *connected sites*, integrando KPIs e *ledgers* distribuídos, é proposta em [Mehmood et al. 2023]. Esses trabalhos avançam a compreensão de *como* medir resiliência sob ataque, mas as suas métricas tendem a ser ancoradas em simulação, telemetria operacional contínua ou *testbeds* de co-simulação, focam predominantemente no eixo físico-operacional da resiliência e não articulam dimensões organizacionais de governança, ciclo de vida e cadeia de suprimentos a um índice comparativo único.

Artigos de revisão recentes sobre *Smart Grid 2.0* [Nguyen et al. 2024] e sobre segurança em sistemas ciberfísicos (*Cyber-Physical Systems*, CPS) [Kim et al. 2022] reforçam que ameaças cibernéticas precisam ser tratadas como vetores de degradação ao lado de falhas físicas, mas não fornecem instrumentos quantitativos que operadores possam aplicar diretamente em decisões de aquisição ou implantação. A análise

abrangente em [Ebad 2023], ao classificar 46 métricas de segurança para IoT, expõe a fragmentação do estado da arte e identifica lacunas explícitas em métricas que cubram simultaneamente as camadas técnicas, dimensões regulatórias e capacidade de validação prática. No contexto brasileiro, vários trabalhos abordam pilares complementares deste problema, como detecção de intrusão em *smart grids* [Quincozes et al. 2025], gestão de identidade e acesso para IoT em redes elétricas [Abreu Jr. et al. 2021] e modelagem declarativa de risco em IoT [Lento et al. 2023], sem, no entanto, propor um instrumento agregado de avaliação alinhado ao quadro regulatório nacional (LGPD, PNCiber, ANEEL e Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – PRODIST). Por fim, a tradição de dependabilidade em redes de sensores e sistemas ciberfísicos [Da Silva et al. 2023]fornece modelos sólidos para quantificar cobertura e segurança sob falhas de causa comum, mas, historicamente, não trata controles de segurança como barreiras de defesa cuja ausência, por si só, configura uma falha de causa comum sobre múltiplas capacidades.

O conjunto desses trabalhos delimita a lacuna específica que este artigo endereça. Embora existam *frameworks* normativos abrangentes, métricas de vulnerabilidade consolidadas, métricas de resiliência ciberfísica sofisticadas e revisão explícita do estado da arte em métricas de IoT, ainda não há um instrumento operacional que reúna, de forma simultânea: (i) submétricas mensuráveis com baixo atrito, obteníveis por revisão documental, inventário e telemetria, sem dependência de *testbed* ou ensaios intrusivos; (ii) agregação ponderada transparente em um índice 0–100 com regras explícitas de *gating* que tornam dimensões críticas não compensáveis; (iii) mapeamento direto às obrigações regulatórias aplicáveis a sistemas IoT+Energia tanto no contexto europeu (NIS2, CRA) quanto no brasileiro (LGPD, PNCiber, ANEEL/PRODIST, Lei 14.300/2022); e (iv) validação cruzada em cenários de maturidade contrastante, acompanhada de análise de sensibilidade a pesos e teste de estresse do mecanismo de agregação. É essa lacuna que o *scorecard* proposto procura preencher, posicionando-se como instrumento prático e auditável, complementar — e não substituto — dos *frameworks* normativos e das métricas de resiliência ciberfísica já estabelecidos.

3. Metodologia Proposta: *Scorecard* de Segurança e Resiliência

Um *scorecard* é um instrumento estruturado de avaliação que traduz evidências heterogêneas (documentais, técnicas e operacionais) em um índice comparável, organizando indicadores em dimensões temáticas, com fórmulas de normalização, pesos e regras de agregação declarados e auditáveis. Aplicado à segurança e à resiliência, ele consolida controles, maturidade e exposição em um valor numérico que apoia decisões de projeto, comparação entre soluções e diálogo com obrigações regulatórias, complementando, sem substituir, avaliações intrusivas, como testes de penetração ou auditorias aprofundadas. O *scorecard* proposto neste trabalho é guiado por três princípios de desenho. O primeiro é a mensurabilidade com baixo atrito, privilegiando indicadores obteníveis por revisão documental, inventário, varreduras de configuração e telemetria, sem dependência de *testbed* ou ensaios intrusivos. O segundo é o alinhamento com obrigações regulatórias, mapeando as dimensões para requisitos mínimos de NIS2, CRA, LGPD e PNCiber. O terceiro é a agregação transparente com *gating*, ou seja, fórmulas auditáveis, sensibilidade a pesos conhecida e regras explícitas que impedem compensações perigosas entre dimensões.

A operacionalização do *scorecard* envolve três blocos metodológicos articulados:

(i) um catálogo de submétricas distribuídas em sete dimensões temáticas; (ii) um procedimento de normalização que converte cada medição bruta em um *score* comparável na faixa $[0, 100]$; e (iii) uma agregação ponderada complementada por regras de *gating*, que produzem o índice final e a sua classificação em três faixas. O catálogo está sintetizado na Tabela 1 e é composto por 15 indicadores que refletem categorias mínimas regulatórias e boas práticas em OT e IoT. Para cada submétrica, a tabela registra o identificador, a dimensão à qual pertence, a definição operacional, o tipo de normalização aplicado e os limiares de qualidade de referência (L_{bom} e L_{mau}), cuja calibração é justificada adiante.

Tabela 1. Catálogo de submétricas do *scorecard* (15 métricas em 7 dimensões).

ID	Dim.	Submétrica	Tipo	$L_{\text{bom}}/L_{\text{mau}}$
G1	GOV	Avaliação de risco (recência + âmbito)	Meses (↓)	6 / 36
G2	GOV	*Accountability* da gestão	Nível 0–3	—
A1	ASSET	Inventário completo	% (↑)	30 / 95
A2	ASSET	*Baseline* segura (*hardening*)	% (↑)	20 / 90
I1	ID	MFA em contas privilegiadas	% (↑)	50 / 98
I2	ID	Autenticação mútua M2M	% (↑)	20 / 90
L1	LIFE	Latência de *patch* crítico	Dias (↓)	30 / 180
L2	LIFE	Cobertura SBOM	% (↑)	10 / 85
L3	LIFE	Gestão de vulnerabilidades	Nível 0–3	—
N1	NET	Cifragem em trânsito	% (↑)	40 / 98
N2	NET	Segmentação de rede	Nível 0–3	—
M1	MON	*Logging* centralizado	% (↑)	20 / 90
M2	MON	MTTD (tempo médio de detecção)	Horas (↓)	1 / 720
R1	RES	Testes de restauração/ano	Contagem (↑)	4
R2	RES	*Fail-safe* / modo manual	Nível 0–3	—

As sete dimensões organizam as submétricas por afinidade temática e cobertura regulatória. **Governança e Risco (GOV)** reúne as práticas organizacionais de avaliação, tratamento e *accountability* de risco, refletindo a maturidade institucional do programa de segurança. **Ativos e Configuração (ASSET)** cobre a visibilidade do inventário de equipamentos, *firmware* e *software* e a aderência a configurações seguras de referência (*hardening*). **Identidade e Acesso (ID)** trata da autenticação de usuários e de máquinas, com ênfase em autenticação multifator (*Multi-Factor Authentication*, MFA) para contas privilegiadas e em autenticação máquina a máquina (*Machine-to-Machine*, M2M) para integrações automatizadas. **Ciclo de Vida e Cadeia de Suprimentos (LIFE)** abrange o tratamento de vulnerabilidades, a latência de aplicação de correções críticas e a cobertura do inventário de componentes de *software* (*Software Bill of Materials*, SBOM) ao longo do ciclo de vida do produto. **Rede e Proteção de Dados (NET)** agrupa controles de cifragem em trânsito e de segmentação de rede, mitigando exposição lateral e escuta em comunicações OT/IT. **Monitorização e Resposta (MON)** reúne os indicadores de coleta centralizada de *logs* e o tempo médio de detecção (*Mean Time to Detect*, MTTD), que sustentam a capacidade de notificação tempestiva. Por fim, **Resiliência e Privacidade (RES)** avalia a capacidade de recuperar a operação após eventos adversos, incluindo a regularidade dos testes de restauração e a existência de modos de operação *fail-safe* ou manual.

Cada submétrica produz um *score* $s \in [0, 100]$ a partir de uma medição bruta. Para métricas em que "menos é melhor", aplica-se uma normalização linear por partes (*piecewise linear*), definida na Equação 1. Para métricas de percentagem em que "mais é melhor", adota-se a normalização da Equação 2, em que p é a percentagem observada e $p_{\min}$, $p_{\max}$ são os limiares de qualidade. As métricas de nível discreto (0–3) são convertidas por $s = 100 \cdot \text{nível}/3$, com os níveis ancorados em rubricas explícitas: 0 corresponde à ausência completa do controle, 1 a controle informal sem rastreabilidade, 2 a controle formalizado, mas com cobertura parcial, e 3 a controle formalizado, monitorado e com cobertura completa.

$$s = \begin{cases} 100 & \text{se } L \le L_{\text{bom}} \\ 0 & \text{se } L \ge L_{\text{mau}} \\ \dfrac{100 \cdot (L_{\text{mau}} - L)}{L_{\text{mau}} - L_{\text{bom}}} & \text{c.c.} \end{cases} \quad (1) \qquad s = \text{clip}\left(\frac{100 \cdot (p - p_{\min})}{p_{\max} - p_{\min}},\ 0,\ 100 \right) \quad (2)$$

Os limiares L_{bom} e L_{mau} da Tabela 1 foram calibrados a partir de requisitos explícitos de instrumentos regulatórios (NIS2 e CRA), de recomendações operacionais consolidadas em normas técnicas (família ISO/IEC 27000, série NIST SP 800, IEC 62351 e *CIS Benchmarks*), e de referências quantitativas em relatórios setoriais (ENISA, CISA e DOE). Quando um instrumento normativo fixa um valor de referência, ele é adotado diretamente; quando o requisito é modulado por cláusulas do tipo *where appropriate* – como ocorre em diversas alíneas do art. 21(2) da NIS2 –, adota-se a interpretação consolidada pela ENISA e por autoridades nacionais para entidades essenciais e importantes, na qual a aplicabilidade do controle é assumida como regra para acessos e ativos de maior criticidade. Em M2 (MTTD), $L_{\text{bom}} = 1\,\text{h}$ é compatível com o prazo do art. 23(4)(a) da NIS2 para emissão do alerta inicial em até 24 h após a tomada de conhecimento de um incidente significativo, prazo que pressupõe capacidade de detecção subordinada a essa janela. $L_{\text{mau}} = 720\,\text{h}$ (30 dias) corresponde ao limite de descoberta tardia reportado por levantamentos setoriais de incidentes. Em L1 (latência de aplicação de correção crítica), $L_{\text{bom}} = 30$ dias adota um baseline industrial consolidado para vulnerabilidades críticas — mais permissivo que o prazo de 14 dias do BOD 22-01 da CISA para itens recém-incluídos no *Known Exploited Vulnerabilities* (KEV), porém alinhado a práticas comerciais correntes em IoT/OT —, enquanto $L_{\text{mau}} = 180$ dias representa defasagem dificilmente compatível com as obrigações genéricas de tratamento de vulnerabilidades durante o período de suporte previstas no art. 13 e no Anexo I, Parte II, do CRA. Em G1, $L_{\text{bom}} = 6$ meses reflete a prática de revisão semestral de riscos recomendada para infraestruturas críticas, e $L_{\text{mau}} = 36$ meses corresponde a três ciclos anuais sem reavaliação. Em R1, $L_{\text{bom}} = 4$ testes de restauração por ano traduz um regime de testes trimestrais parciais, consistente com a orientação do NIST SP 800-34 de combinar testes anuais completos com testes parciais mais frequentes em sistemas de impacto moderado a alto. Para submétricas cuja unidade natural é cobertura percentual de um controle qualitativo (A1, A2, L2, N1 e M1), adota-se uma heurística uniforme: L_{bom} próximo da cobertura plena do controle ($\ge 85\%$) e L_{mau} em valor que sinaliza cobertura insuficiente para produzir efeito prático ($\le 30\%$). As exceções são I1 (MFA em contas privilegiadas), com $L_{\text{bom}} = 98\%$ porque o art. 21 da NIS2 inclui expressamente o uso de soluções de autenticação multifator ou de autenticação contínua no rol mínimo de medidas de gestão de risco, com a ressalva *sempre que apropriado*, e N1 (cifragem em trânsito), com $L_{\text{bom}} = 98\%$ alinhado

ao baseline criptográfico da série IEC 62351 e ao art. 21 da NIS2, que arrola políticas e procedimentos sobre o uso de criptografia e, *sempre que apropriado*, de cifragem entre as medidas mínimas.

A agregação ocorre em duas etapas. Primeiro, o *score* de cada dimensão S_d é definido como a média aritmética das submétricas dessa dimensão, com pesos intra-dimensão uniformes. Essa é uma escolha conservadora que evita introduzir hipóteses adicionais sobre a relevância relativa de submétricas dentro de uma mesma dimensão e que pode ser refinada por evidência empírica em trabalhos futuros. Em seguida, o *score* global é calculado conforme a Equação 3, em que W_d é o peso atribuído à dimensão d e D é o conjunto das sete dimensões.

$$S_{\text{total}} = \sum_{d \in D} W_d \cdot S_d, \qquad \sum_{d \in D} W_d = 1. \tag{3}$$

O perfil *baseline* adotado atribui W_d igual a 0,14 (GOV), 0,10 (ASSET), 0,14 (ID), 0,16 (LIFE), 0,14 (NET), 0,16 (MON) e 0,16 (RES). Estes valores resultam de uma hierarquia explícita de criticidade ancorada nas obrigações regulatórias mais impositivas em sistemas IoT+Energia. O peso máximo ($W_d = 0{,}16$) é atribuído a LIFE, MON e RES, dimensões cuja ausência tem consequência regulatória ou operacional direta (tratamento de vulnerabilidades, prazos de notificação e continuidade em ambientes OT críticos). O peso intermediário ($W_d = 0{,}14$) recai sobre GOV, ID e NET, medidas preventivas previstas no rol mínimo do art.21 da NIS2 que, por seu caráter de mitigação, não disparam isoladamente obrigação imediata de notificação. O menor peso ($W_d = 0{,}10$) cabe a ASSET, reconhecendo seu papel fundacional, mas com impacto mais indireto sobre a resposta a incidentes.

O *score* global obtido pela Equação 3 é classificado em três faixas calibradas pela severidade regulatória esperada e por convenções consolidadas em modelos de maturidade. A faixa **Verde** ($S \geq 80$) corresponde a uma postura compatível com auditorias estendidas e a uma posição de excelência relativa à média setorial. A faixa **Âmbar** ($60 \leq S < 80$) indica operação aceitável sob obrigação regulatória, porém com lacunas que demandam plano de remediação. E a faixa **Vermelho** ($S < 60$) sinaliza incapacidade de cumprir requisitos mínimos das principais legislações analisadas e exige remediação prioritária. Sobre essa pontuação agregada sobrepõem-se três regras de *gating* que tornam certas dimensões críticas não compensáveis pelas demais, impedindo que pontuações elevadas em controles periféricos mascarem ausências estruturais. Cada regra R_i fixa um teto τ_i quando a sua submétrica disparadora atinge *score* nulo, e o *score* ajustado S_{aj} é o mínimo entre S_{total} e os tetos ativos, conforme as Equações 4 e 5.

$$S_{\text{aj}} = \min\big(S_{\text{total}},\ \tau_1,\ \tau_2,\ \tau_3\big) \tag{4}$$

$$\tau_1 = \begin{cases} 55 & \text{se } s_{M2} = 0 \\ 100 & \text{c.c.} \end{cases}, \quad \tau_2 = \begin{cases} 50 & \text{se } s_{L1} = 0 \\ 100 & \text{c.c.} \end{cases}, \quad \tau_3 = \begin{cases} 65 & \text{se } s_{M1} = 0 \\ 100 & \text{c.c.} \end{cases} \tag{5}$$

Os três tetos foram calibrados para se ancorar nas fronteiras das faixas e na severidade regulatória da capacidade ausente. A regra R1 ($\tau_1 = 55$) trata a ausência total de capacidade de detecção como incompatível com o prazo de 24 h para o alerta inicial previsto na NIS2, forçando o sistema para a faixa Vermelha. A regra R2 ($\tau_2 = 50$), mais severa, reflete que a inexistência de via autenticada de correção crítica dificilmente se

concilia com as obrigações de tratamento de vulnerabilidades do CRA durante o período de suporte, configurando uma faixa Vermelha estrutural. A regra R3 ($\tau_3 = 65$) reconhece que a ausência de *logging* centralizado compromete detecção, resposta e análise forense, mas não anula *a priori* os demais controles preventivos. Assim o sistema é mantido na faixa Âmbar, próximo do seu limite inferior, sinalizando remediação urgente sem reclassificar para Vermelho. Tomados em conjunto, esses três blocos – catálogo de submétricas, normalização e agregação ponderada com *gating* – definem um procedimento determinístico que, dada a evidência observada em um sistema concreto, produz um *score* global ajustado e a sua classificação Verde, Âmbar ou Vermelho.

4. Metodologia de Validação

A validação da metodologia proposta considera três cenários contrastantes: um sistema residencial de gerenciamento de energia (*Home Energy Management System*, HEMS), uma plataforma de Comunidade de Energia Renovável (*Renewable Energy Community*, REC) e uma microrrede hospitalar. Estes foram escolhidos para cobrir o espectro de maturidade observado em sistemas IoT+Energia e, assim, ilustrar a capacidade analítica do *scorecard* ao longo desse espectro. Para cada cenário é aplicado o cálculo dos *scores* sob o perfil *Baseline* de ponderação definido na Seção 3. A partir daí uma análise de sensibilidade é realizada sob três perfis alternativos. Um com *Ênfase em Resiliência* ($W_{\text{RES}} = 0{,}24$; $W_{\text{MON}} = 0{,}18$), outro com *Ênfase em Supply Chain* ($W_{\text{LIFE}} = 0{,}24$) e por fim um perfil com *Ênfase em Monitorização* ($W_{\text{MON}} = 0{,}28$), cada um redistribuindo o peso e mantendo soma unitária. Ainda é realizada uma análise de prioridades de remediação e um teste de estresse do mecanismo de *gating*. Os três cenários são caracterizados a seguir:

Cenário A — HEMS Doméstico. Instalação residencial em 2026 composta por *smart meter*, inversor fotovoltaico, bateria doméstica e aplicativo em nuvem do fornecedor. Assume-se um sistema com usuário residencial sem operador dedicado a segurança. Fornecedores aplicam *Transport Layer Security* (TLS) para comunicações em nuvem ($\sim$75%), mas a rede local frequentemente está sem cifragem. MFA é opcional na conta em nuvem ($\sim$35% de adesão típica). A atualização automática do fornecedor tem cadência irregular (mediana de 75 dias). Não apresenta SBOM, nem registro centralizado de eventos (*logging*) e nem testes de restauração. Esse cenário reflete a realidade de milhões de instalações onde a segurança depende essencialmente das capacidades do fornecedor.

Cenário B — Plataforma REC. Plataforma na União Europeia (UE) em 2026 operando como agregador/empresa de serviços de energia (*Energy Service Company*, ESCO) comunitária no modelo *Software as a Service* (SaaS) *multi-tenant*, agregando $\sim$500 *prosumidores* e sujeita à NIS2 como entidade essencial. Equipe pequena (5–10 engenheiros), com centro de operações de segurança (*Security Operations Center*, SOC) contratado em horário comercial. A REC conta com avaliação anual de risco com cobertura de $\sim$70%. Possui base de gestão de configuração (*Configuration Management Database*, CMDB) para infraestrutura própria, mas com $\sim$30% dos dispositivos de borda fora. MFA aplicada na maioria dos administradores. Segmentação forte em nuvem, mas redes de borda mais planas. Tem SBOM próprio com cobertura parcial de fornecedores ($\sim$25%). MTTD de 24h (alertas fora do horário comercial em fila). Esse cenário representa o ponto típico de maturidade para pequenas e médias empresas (PMEs) sob obrigação regulatória recente. No Brasil, é diretamente comparável às Comunidades

Compartilhadas de Geração Distribuída amparadas pela Lei 14.300/2022 (marco legal da microgeração e minigeração distribuída) e pelo PRODIST.

Cenário C — Microrrede Hospitalar. Microrrede crítica em um hospital regional UE/BR com controlador central, geração distribuída (fotovoltaica, gerador e bateria), modo ilha obrigatório e regulação setorial estrita (Código de Rede de Cibersegurança – *Network Code on Cybersecurity*, NCCS – na UE, e ANEEL e Operador Nacional do Sistema Elétrico – ONS – no Brasil). Considere-se que a avaliação semestral da cobre 85% do escopo OT+IT+IoT. Tem CMDB completo com zonas IEC 62443 [ISA/IEC 2024]. MFA aplicada, mesmo com algumas contas de serviço herdadas isentas. SOC opera 24/7 com MTTD de 4h. Realização de testes de restauração 3×/ano. O modo ilha é testado mensalmente. O SBOM, contudo, é parcial, exigido em novas aquisições, mas inexistente no legado OT (problema estrutural reconhecido na literatura OT [Stouffer et al. 2023, NTIA 2021]).

5. Resultados e Discussões

A aplicação da metodologia aos três cenários parte dos valores brutos consolidados na Tabela 2, que sumariza as 15 medições atribuídas a cada arquitetura conforme as premissas declaradas na Seção 4. Esses valores, uma vez processados de acordo com a metodologia proposta na Seção 3, geram os *scores* por dimensão e a classificação global apresentados na Tabela 3, cuja leitura comparativa é sintetizada no radar da Figura 1.

Tabela 2. Valores brutos das 15 submétricas em cada cenário. Para G1, o valor entre parênteses é o fator de âmbito multiplicativo definido na Seção 3.

Cenário	**G1**	**G2**	**A1**	**A2**	**I1**	**I2**	**L1**	**L2**	**L3**	**N1**	**N2**	**M1**	**M2**	**R1**	**R2**
unid.	meses	0–3	%	%	%	%	dias	%	0–3	%	0–3	%	h	t/ano	0–3
HEMS	30 (0,30)	0	40	20	35	25	75	0	1	75	1	0	720	0	1
REC	12 (0,70)	2	70	60	80	50	60	25	2	88	2	65	24	2	2
Microrrede	6 (0,85)	3	90	75	92	65	45	35	3	85	3	80	4	3	3

Os três cenários ocupam faixas distintas e produzem uma progressão clara entre Vermelho, Âmbar e Verde. O HEMS atinge *score* ajustado de 16,4 pontos e mantém cinco dimensões abaixo de 10, o que reflete ausência estrutural de governança, identidade, monitorização e resiliência. As poucas dimensões em que pontua acima da média do cenário (LIFE=34,4 pela atualização automática do fornecedor e NET=46,8 pelo uso de TLS na nuvem) correspondem a capacidades fornecidas pelo fabricante, e não a escolhas do operador. A Plataforma REC, com 63,5 pontos, ocupa o ponto de inflexão típico de PMEs sob pressão regulatória recente, exibindo dimensões de proteção (NET=74,7) e detecção (MON=80,5) razoáveis enquanto governança (61,3), identidade (52,7) e *supply chain* (55,6) permanecem imaturas. A Microrrede Hospitalar, com 85,3 pontos, demonstra postura forte em todas as dimensões e tem o *supply chain* (LIFE=74,4) como única zona ainda em Âmbar, refletindo um desafio estrutural conhecido em ambientes OT e legados, em que a documentação de componentes é tipicamente incompleta.

O detalhamento submétrico, apresentado como *heatmap* na Figura 2, revela três padrões importantes para além da agregação por dimensão. Em primeiro lugar, L2 (cobertura SBOM) é a única submétrica em zona crítica para os três cenários (HEMS=0,

Tabela 3. *Scores* por dimensão e classificação global (perfil *Baseline*).

Dimensão	HEMS	REC	Microrrede
Governança e Risco (GOV)	3,0	61,3	92,5
Ativos e Configuração (ASSET)	7,7	59,3	85,4
Identidade e Acesso (ID)	3,6	52,7	75,9
Ciclo de Vida e *Supply Chain* (LIFE)	34,4	55,6	74,4
Rede e Proteção de Dados (NET)	46,8	74,7	88,8
Monitorização e Resposta (MON)	0,0	80,5	92,6
Resiliência e Privacidade (RES)	16,7	58,3	87,5
Score Global (ajustado)	**16,4**	**63,5**	**85,3**
Classificação	**VERMELHO**	**ÂMBAR**	**VERDE**

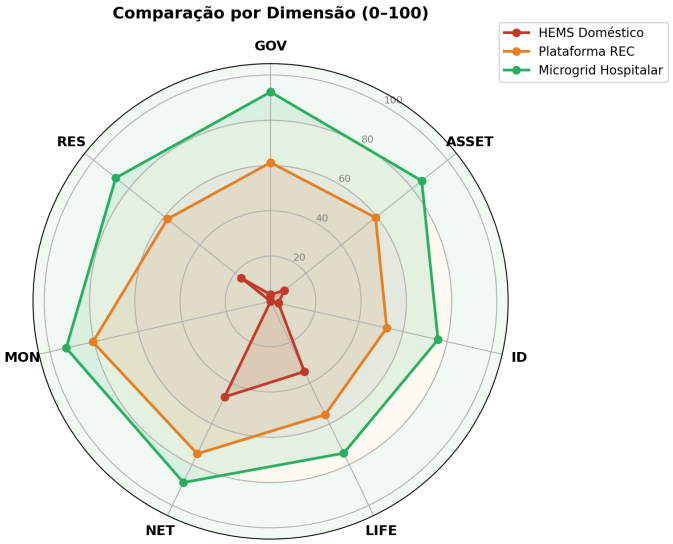

Figura 1. Comparação das dimensões do *scorecard* entre os três cenários.

REC=20 e Microrrede=33,3), o que confirma uma realidade do mercado em que o SBOM ainda é exceção mesmo onde o CRA o exige [NTIA 2021]. Em segundo lugar, L1 (latência de aplicação de *patch*) escala de forma não linear com a maturidade (70, 80 e 90 pontos nos três cenários), efeito direto da normalização *piecewise* adotada, em que o ganho marginal entre 60 e 45 dias é menor do que entre 75 e 60 dias. Em terceiro lugar, a REC apresenta L1=80 superior à expectativa intuitiva porque os fornecedores predominantes no mercado cumprem ciclos mensais, mas exibe I2=43 baixo porque a autenticação mútua TLS (*mutual TLS*, mTLS) verdadeira permanece exceção em integrações multifornecedor.

A robustez do ranqueamento é examinada pela análise de sensibilidade da Tabela 4, que compara os *scores* sob os quatro perfis de ponderação descritos na Seção 4. Nenhum cenário muda de faixa sob qualquer dos perfis testados, e a variação máxima é de apenas 4,2 pontos no HEMS, 2,9 na REC e 1,9 na Microrrede. A Microrrede perde 1,0 ponto sob ênfase em *Supply Chain* ($W_{\text{LIFE}} = 0{,}24$) por conta da sua lacuna real em SBOM, enquanto a REC ganha 2,3 pontos sob ênfase em Monitorização porque MON=80,5 é a sua dimensão mais forte, e o HEMS também ganha 2,3 pontos sob ênfase em *Supply*

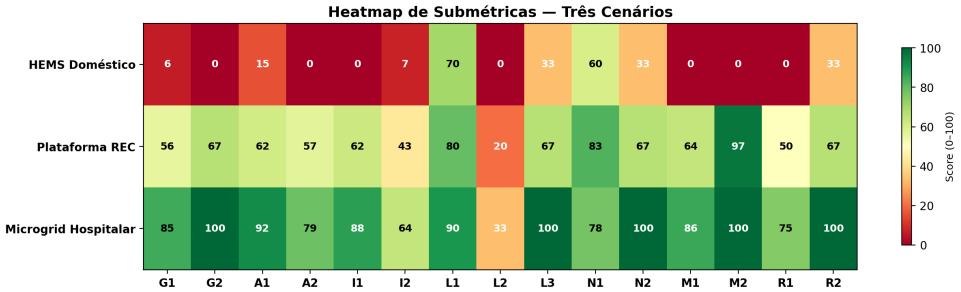

Figura 2. *Heatmap* de submétricas (gradiente vermelho-amarelo-verde, 0–100).

Chain porque L1=70 é, em termos relativos, o seu controle menos catastrófico. Esse comportamento sustenta com segurança a leitura de que a REC ocupa uma posição intermediária genuína de maturidade, pois não migra para Verde nem mesmo sob o perfil mais favorável (65,8 ainda abaixo de 80) e tampouco regride para Vermelho sob o menos favorável (62,9 acima de 60). Essa estabilidade é relevante para a utilidade prática do instrumento, pois pequenas mudanças nos pesos não reclassificam um sistema, o que reduz a margem para manipulação ou debate improdutivo e decorre de duas escolhas de desenho: pesos *baseline* relativamente uniformes (variação 0,10–0,16) e a estrutura linear por partes adotada nas Equações 1 e 2, que evita amplificações descontroladas próximas aos limiares.

Tabela 4. *Score* global ajustado sob quatro perfis de ponderação.

Perfil de Pesos	**HEMS**	**REC**	**Microrrede**
Baseline	16,4	63,5	85,3
Ênfase Resiliência	15,8	63,7	85,8
Ênfase *Supply Chain*	18,7	62,9	84,3
Ênfase Monitorização	14,5	65,8	86,2
Variação máxima	**4,2**	**2,9**	**1,9**

A priorização de ações de remediação é calculada como $\text{impacto} = (100 - \text{score}) \times w_{\text{ef}}$, em que score é o *score* normalizado da submétrica e $w_{\text{ef}} = w_{\text{dim}}/n_{\text{métricas na dim}}$ é o seu peso efetivo, obtido pela distribuição uniforme do peso W_d da dimensão (definido na Seção 3) entre as suas submétricas. Conforme a Figura 3, o HEMS exibe um perfil estrutural dominado por ausências completas (M1, M2 e R1 com impacto 8,0; G2 e I1 com 7,0), exigindo construção fundacional indiferenciada; a REC concentra prioridade em *supply chain* (L2 com 4,3), autenticação M2M (I2 com 4,0), testes de restauração (R1 com 4,0) e avaliação de risco (G1 com 3,1), perfil orientado a refinamento de capacidades já existentes; e a Microrrede mostra impactos absolutos baixos, dominados por SBOM (L2 com 3,6) e mTLS M2M (I2 com 2,5), próprios de um sistema maduro em otimização. Essa heterogeneidade qualitativa — recomendações fundacionais, de refinamento ou de otimização conforme a maturidade — evidencia que o instrumento captura informação útil para decisão, e não apenas diferenças numéricas.

Para verificar se o mecanismo de *gating* efetivamente desempenha o papel a que se destina, simula-se uma falha plausível na Microrrede Hospitalar, na qual o SOC contra-

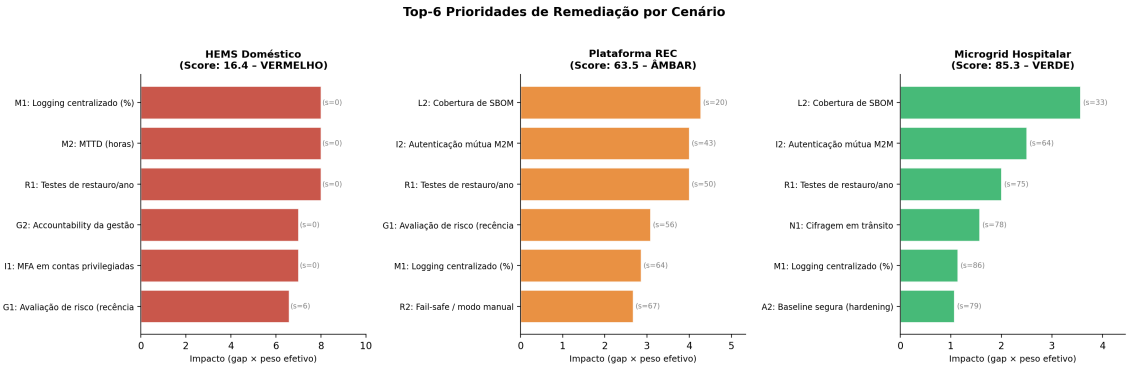

Figura 3. *Top*-6 prioridades de remediação por cenário.

tado torna-se indisponível por incidente operacional e M2 (MTTD) é levado efetivamente a infinito (720 h), permanecendo as outras 14 submétricas nos valores originais. O resultado é apresentado na Figura 4. Sem *gating*, o *score* bruto cai apenas de 85,3 para 77,3 e permanece na faixa Âmbar, o que seria enganoso porque o sistema apareceria como estando apenas pouco abaixo do nível de excelência. Com o *gating* ativado, S_{aj} é limitado a 55,0 e o sistema é classificado como Vermelho, refletindo corretamente que, sem MTTD operacional, o sistema não tem condições de cumprir o prazo de 24 h para o alerta inicial previsto na NIS2 nem o subsequente prazo de 72 h para a notificação de incidente, o que compromete sua capacidade fundamental de proteção. A diferença de 22,3 pontos entre o *score* bruto e o ajustado quantifica exatamente o efeito do *gating*, que é impedir que excelência em outras áreas mascare uma falha estrutural em uma capacidade não compensável.

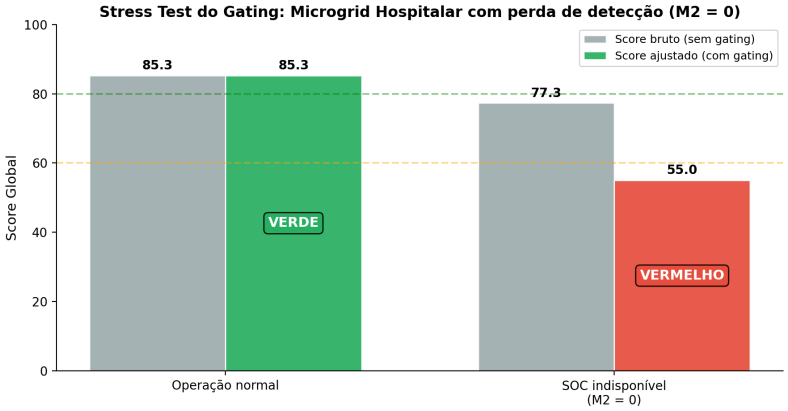

Figura 4. Comportamento do *gating* com perda de capacidade de detecção.

Embora o instrumento tenha sido construído com mapeamento explícito para NIS2 e CRA, a sua aplicabilidade ao quadro regulatório brasileiro é direta. As dimensões de gestão de identidade e acesso (*Identity and Access Management*, IAM), materializadas em I1 e I2, mapeiam as medidas técnicas e organizacionais de proteção de dados exigidas pela LGPD, tendo os controles da ABNT NBR ISO/IEC 27001/27002:2022 como referência operacional adotada. No plano das infraestruturas críticas de energia, o Decreto 11.856/2023 (PNCiber) enquadra requisitos análogos aos da NIS2, enquanto a Resolução

ANEEL n. 1.000/2021, conjugada ao PRODIST, introduz exigências para medição inteligente e geração distribuída, de modo que cenários como o da Plataforma REC têm equivalentes diretos nas Comunidades Compartilhadas de Geração Distribuída amparadas pela Lei 14.300/2022 (marco legal da microgeração e minigeração distribuída). Soma-se a essas frentes a expansão recente de microrredes para resiliência pós-desastre em regiões sujeitas a eventos climáticos extremos, contexto em que instrumentos práticos de avaliação aplicáveis por operadores e reguladores sem conhecimento técnico especializado tornam-se particularmente úteis [U.S. Department of Energy 2024]. A vitalidade dessa agenda nacional é confirmada por trabalhos brasileiros recentes em sistemas de detecção de intrusão (*Intrusion Detection Systems*, IDS), IAM e gestão de riscos para IoT e *smart grid* [Quincozes et al. 2025, Abreu Jr. et al. 2021, Lento et al. 2023].

6. Conclusões e Trabalho Futuro

O instrumento desenvolvido neste trabalho responde a uma lacuna concreta no estado da arte, qual seja, a ausência de um índice operacional que reúna, ao mesmo tempo, mensurabilidade com baixo atrito, mapeamento explícito às obrigações regulatórias mais relevantes para sistemas IoT em energia e robustez a escolhas razoáveis de ponderação. A validação por cenários contrastantes evidencia que a metodologia não apenas classifica diferentes sistemas, mas também produz recomendações qualitativamente distintas para cada nível, o que constitui o tipo de informação efetivamente útil para decisões de projeto, contratação e auditoria. A metodologia é transparente e modular, permitindo que diferentes *stakeholders*, com mandatos regulatórios, contratuais ou operacionais distintos, reexecutem a avaliação sob suas próprias premissas sem reabrir o debate sobre a metodologia. Além disso, a opção por evidências documentais e telemetria abre caminho para integração do *scorecard* em processos já existentes de auditoria e diligência prévia de fornecedores, sem exigir infraestrutura intrusiva. Por fim, a leitura por dimensão preserva o diálogo com normas técnicas estabelecidas, como ISO/IEC 27001, IEC 62351 e ISA/IEC 62443, de modo que o *scorecard* se posiciona como complemento, e não substituto, dos instrumentos já utilizados pela comunidade.

Apesar dos resultados promissores, o trabalho apresenta limitações que orientam a sua continuidade. Os cenários foram derivados de premissas de literatura, e não de medições em sistemas reais, o que motiva a validação do instrumento com operadores reais de HEMS, RECs e microrredes, por exemplo. O catálogo de 15 submétricas pode ser compacto para detalhar aplicações mais complexa, que necessitem de incorporação de privacidade granular e maior detalhe na cadeia de suprimentos, o que pode alterar prioridades em cenários específicos. Como o *scorecard* mede maturidade e controles, e não exposição real, ele não substitui testes de intrusão, caça a ameaças ou análise de vulnerabilidades ativa, mantendo-se como instrumento complementar a essas avaliações. Os resultados do teste de estresse, embora pedagogicamente claros, derivam de uma única perturbação, ficando testes mais amplos baseados em simulações de Monte Carlo sobre múltiplas perturbações simultâneas como extensão futura. Soma-se a essas frentes o desenvolvimento de uma ferramenta *web* de avaliação assistida com captura estruturada de evidências.

Referências

Abreu Jr., V., Santin, A. O., Viegas, E. K., Vicentini, C. J. A., and da Silva, M. N. (2021). Gestão de identidade e acesso para dispositivos IoT na Smart Grid. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021)*, pages 1–14, Belém, PA.

Achaal, B., Adda, M., and Berger, M. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity*, 7(1).

Aghazadeh Ardebili, A. et al. (2025). IoT-driven resilience monitoring: Case study of a cyber-physical system. *Applied Sciences*, 15(1):55.

Coppolino, L., D'Antonio, S., Mazzeo, G., and Romano, L. (2023). Building cyber-resilient smart grids with digital twins and data spaces. *Applied Sciences*, 13(24):13060.

Da Silva, G. F. P., Costa, D. G., and De Jesus, T. C. (2023). A secure OTA approach for flexible operation of emergency detection units in smart cities. In *2023 IEEE International Smart Cities Conference (ISC2)*, pages 01–07.

Ebad, S. A. (2023). Quantifying IoT security parameters: An assessment framework. *IEEE Access*, 11:101087–101097.

ENISA (2011). Resilience metrics and measurements: Technical report. Technical report, European Network and Information Security Agency, Heraklion, Greece.

Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K., and Herold, R. (2021). IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements. NIST Special Publication 800-213, National Institute of Standards and Technology, Gaithersburg, MD.

FIRST.org (2019). *Common Vulnerability Scoring System v3.1: Specification Document*. Forum of Incident Response and Security Teams.

Horálek, J. and Sobeslav, V. (2023). Security baseline for substation automation systems. *Sensors*, 23(16):7125.

International Electrotechnical Commission (2007–2024). *IEC 62351 — Power Systems Management and Associated Information Exchange: Data and Communications Security*. IEC TC57 WG15.

ISA/IEC (2018–2024). *ISA/IEC 62443 — Security for Industrial Automation and Control Systems*. ISA / IEC TC65/SC65A.

Jara, A. J. et al. (2024). CyberSecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2. In *2024 IEEE Smart Cities Futures Summit (SCFC)*. IEEE.

Kim, S., Park, K.-J., and Lu, C. (2022). A survey on network security for cyber-physical systems: From threats to resilient design. *IEEE Communications Surveys & Tutorials*, 24(3):1534–1573.

Lento, L. O. B., Patinho, P., and Abreu, S. (2023). Um modelo declarativo para gestão de riscos em IoT. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2023)*, pages 570–575, Juiz de Fora, MG.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., and Kott, A. (2013). Resilience metrics for cyber systems. *Environ. Systems and Decisions*, 33(4):471–476.

Mehmood, A., Epiphaniou, G., and Maple, C. (2023). A hybrid methodology to assess cyber resilience of IoT in energy management and connected sites. *Sensors*, 23(21):8720.

Mishchenko, D., Oļeiņikova, I., and Erdődi, L. (2024). Multidomain cyber-physical testbed for power system vulnerability assessment. *IEEE Access*, 12:38135–38149.

Nguyen, L.-H., Nguyen, V.-L., Hwang, R.-H., Kuo, J.-J., Lai, Y.-W., and Lee, Y.-C. (2024). Toward secured smart grid 2.0: Exploring security threats, protection models, and challenges. *IEEE Communications Surveys & Tutorials*.

NIST Smart Grid Interoperability Panel – Cyber Security Working Group (2014). Guidelines for smart grid cybersecurity. NISTIR 7628 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD.

NTIA (2021). The minimum elements for a software bill of materials (SBOM). Technical report, National Telecommunications and Information Administration, U.S. Department of Commerce. Pursuant to Executive Order 14028.

Parsons, E. K., Panaousis, E., and Loukas, G. (2023). A survey on cyber risk management for the internet of things. *Applied Sciences*, 13(15):9032.

Quincozes, V. E., Quincozes, S. E., Albuquerque, C., Passos, D., and Mossé, D. (2025). Uma avaliação estendida do impacto da seleção e enriquecimento de features em sistemas de detecção de intrusão para Smart Grids. In *Simpósio Brasileiro de Cibersegurança (SBSeg 2025)*, pages 905–920.

Sarker, P. S., Sadanandan, S. K., and Srivastava, A. K. (2022). Resiliency metrics for monitoring and analysis of cyber-power distribution system with IoTs. *IEEE Internet of Things Journal*, 9(10):7826–7837.

Schroeder, K., Souppaya, M., and Pillitteri, V. (2024). Measurement guide for information security: Volume 2 — developing an information security measurement program. NIST Special Publication 800-55 Vol. 2, National Institute of Standards and Technology, Gaithersburg, MD.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., and Thompson, M. (2023). Guide to operational technology (OT) security. NIST Special Publication 800-82 Rev. 3, National Institute of Standards and Technology, Gaithersburg, MD.

U.S. Department of Energy (2024). Microgrid overview. Fact Sheet 46060, Grid Deployment Office, U.S. Department of Energy.

Zografopoulos, I., Ospina, J., Liu, X., and Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 9:29775–29818.