LUMEN ET VIRTUS
ISSN: 2177-2789

STRIDE CLÍNICO: ADAPTAÇÃO DO FRAMEWORK DE MODELAGEM DE AMEAÇAS PARA AMBIENTES ONDE VULNERABILIDADES TÉCNICAS PRODUZEM CONSEQUÊNCIAS FÍSICAS EM PACIENTES

CLINICAL STRIDE: ADAPTING A THREAT MODELING FRAMEWORK FOR ENVIRONMENTS WHERE TECHNICAL VULNERABILITIES PRODUCE PHYSICAL CONSEQUENCES IN PATIENTS

AVANCE CLÍNICO: ADAPTACIÓN DE UN MARCO DE MODELADO DE AMENAZAS PARA ENTORNOS DONDE LAS VULNERABILIDADES TÉCNICAS PRODUCEN CONSECUENCIAS FÍSICAS EN LOS PACIENTES

https://doi.org/10.56238/levv17n58-078

Data de submissão: 27/02/2026

Data de publicação: 27/03/2026

Tadeu Marcos Borges Paes
Doutorando em Inteligência Artificial
Instituição: Senai CEDAM
E-mail: tadeu.paes@live.com
Orcid: https://orcid.org/0009-0002-2978-2117

Francisco Nicolás Isnardi Begot
Estudante de Engenharia da Computação
Instituição: Universidade Federal do Pará
E-mail: francisco.begot@itec.ufpa.br
Orcid: https://orcid.org/0009-0009-0944-6336

Carlos Kiyoshi Yanaguibashi Menezes
Estudante de Engenharia Biomédica
Instituição: Universidade Federal do Pará
E-mail: carlos.menezes@itec.ufpa.br
Orcid: https://orcid.org/0009-0005-7942-2680

Eudes Danilo da Silva Mendonça
Mestre em Computação Aplicada
Instituição: Senai CEDAM
E-mail: eudesdanilo@gmail.com
Orcid: https://orcid.org/0009-0006-6439-408X

Pedro Henrique Cavaleiro de Macedo Moura
Estudante de Engenharia Biomédica
Instituição: Universidade Federal do Pará
E-mail: pedro.moura@itec.ufpa.br
Orcid: https://orcid.org/0009-0000-5202-4213

Vinicius Campos De Meneses
Estudante de Engenharia da Computação
Instituição: Centro Universitário do Pará
E-mail: viniciuus.meneses@gmail.com
Orcid: https://orcid.org/0009-0003-8973-9249

RESUMO

A crescente integração de dispositivos médicos conectados em ambientes hospitalares introduz vetores de ataque cibernético cujas consequências transcendem o domínio digital, podendo resultar em danos físicos diretos a pacientes. Embora o framework STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) seja amplamente adotado na engenharia de software para modelagem de ameaças, sua aplicação direta a sistemas clínicos apresenta lacunas significativas, pois não contempla a cadeia de causalidade entre falhas técnicas e desfechos clínicos adversos. Este trabalho realiza uma análise descritivo-analítica da aplicabilidade do STRIDE ao contexto de dispositivos médicos conectados, propondo adaptações que incorporam a dimensão de segurança do paciente (patient safety) ao modelo original. A pesquisa fundamenta-se em vulnerabilidades documentadas em bases como CVE/NVD, incidentes relatados na literatura e diretrizes regulatórias da FDA, ANVISA e IEC 62443. Os resultados demonstram que cada categoria STRIDE manifesta-se de forma distinta em ambientes clínicos, com potencial de comprometer a integridade de dosagens farmacológicas, a disponibilidade de equipamentos de suporte à vida e a confidencialidade de dados sensíveis de pacientes. A adaptação proposta, denominada STRIDE Clínico, adiciona uma camada de avaliação de impacto físico que classifica ameaças segundo sua capacidade de produzir lesão, atraso terapêutico ou óbito, contribuindo para uma modelagem de ameaças mais adequada ao ecossistema de saúde digital.

Palavras-chave: Modelagem de Ameaças. STRIDE. Dispositivos Médicos Conectados. Cibersegurança em Saúde. Segurança do Paciente.

ABSTRACT

The increasing integration of connected medical devices in hospital environments introduces cyberattack vectors whose consequences transcend the digital domain, potentially resulting in direct physical harm to patients. Although the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is widely adopted in software engineering for threat modeling, its direct application to clinical systems presents significant gaps, as it does not consider the causal chain between technical failures and adverse clinical outcomes. This work performs a descriptive-analytical analysis of the applicability of STRIDE to the context of connected medical devices, proposing adaptations that incorporate the patient safety dimension into the original model. This research is based on vulnerabilities documented in databases such as CVE/NVD, incidents reported in the literature, and regulatory guidelines from the FDA, ANVISA, and IEC 62443. The results demonstrate that each STRIDE category manifests itself distinctly in clinical environments, with the potential to compromise the integrity of pharmacological dosages, the availability of life support equipment, and the confidentiality of sensitive patient data. The proposed adaptation, called Clinical STRIDE, adds a layer of physical impact assessment that classifies threats according to their ability to cause injury, therapeutic delay, or death, contributing to a threat modeling more suited to the digital health ecosystem.

Keywords: Threat Modeling. STRIDE. Connected Medical Devices. Healthcare Cybersecurity. Patient Safety.

RESUMEN

La creciente integración de dispositivos médicos conectados en entornos hospitalarios introduce vectores de ciberataque cuyas consecuencias trascienden el ámbito digital, pudiendo provocar daños físicos directos a los pacientes. Si bien el marco STRIDE (Suplantación de identidad, Manipulación,

Repudio, Divulgación de información, Denegación de servicio, Elevación de privilegios) se utiliza ampliamente en ingeniería de software para el modelado de amenazas, su aplicación directa a sistemas clínicos presenta importantes deficiencias, ya que no considera la cadena causal entre fallos técnicos y resultados clínicos adversos. Este trabajo realiza un análisis descriptivo-analítico de la aplicabilidad de STRIDE al contexto de los dispositivos médicos conectados, proponiendo adaptaciones que incorporan la dimensión de seguridad del paciente al modelo original. Esta investigación se basa en vulnerabilidades documentadas en bases de datos como CVE/NVD, incidentes reportados en la literatura y directrices regulatorias de la FDA, ANVISA e IEC 62443. Los resultados demuestran que cada categoría STRIDE se manifiesta de forma distinta en entornos clínicos, con el potencial de comprometer la integridad de las dosis farmacológicas, la disponibilidad de equipos de soporte vital y la confidencialidad de datos sensibles de los pacientes. La adaptación propuesta, denominada Clinical STRIDE, añade una capa de evaluación del impacto físico que clasifica las amenazas según su capacidad para causar lesiones, retrasos terapéuticos o la muerte, contribuyendo a un modelado de amenazas más adecuado para el ecosistema de salud digital.

Palabras clave: Modelado de Amenazas. STRIDE. Dispositivos Médicos Conectados. Ciberseguridad Sanitaria. Seguridad del Paciente.

1 INTRODUÇÃO

A transformação digital do setor de saúde, corroborada pela Internet das Coisas Médicas (IoMT — Internet of Medical Things), representa uma das mudanças mais profundas na prestação de cuidados clínicos nas últimas décadas. Estima-se que o número de dispositivos médicos conectados em hospitais ultrapasse 10 a 15 por leito, incluindo bombas de infusão inteligentes, monitores multiparamétricos, ventiladores mecânicos com telemetria remota e sistemas de dispensação automatizada de medicamentos (WILLIAMS; WOODWARD, 2015). Essa hiperconectividade, embora amplie a eficiência clínica e possibilite o monitoramento contínuo de pacientes, simultaneamente expande a superfície de ataque cibernético de forma sem precedentes, criando um cenário onde falhas de segurança da informação podem transcender o domínio virtual e materializar-se em danos físicos reais aos pacientes (COVENTRY; BRANLEY, 2018).

Historicamente, o desenvolvimento de dispositivos médicos priorizou a segurança funcional (safety) e a eficácia terapêutica, relegando a segurança cibernética (security) a um papel secundário no ciclo de projeto e certificação. O trabalho seminal de Halperin et al. (2008) demonstrou pela primeira vez a viabilidade de ataques remotos a desfibriladores cardíacos implantáveis, revelando que comandos não autorizados poderiam alterar configurações terapêuticas com potencial letal. Subsequentemente, pesquisadores como Li et al. (2011) e Rushanan et al. (2014) expandiram essa linha de investigação, documentando vulnerabilidades em bombas de infusão de insulina, marcapassos e sistemas de monitoramento fetal, consolidando o entendimento de que a cibersegurança em dispositivos médicos constitui uma questão de segurança do paciente, não apenas de proteção de dados.

O panorama regulatório tem evoluído em resposta a esses riscos. A Food and Drug Administration (FDA) dos Estados Unidos publicou diretrizes específicas para cibersegurança em dispositivos médicos em 2014, atualizadas em 2023, exigindo que fabricantes incorporem considerações de segurança cibernética ao longo de todo o ciclo de vida do produto (FDA, 2023). No Brasil, a Agência Nacional de Vigilância Sanitária (ANVISA) tem avançado em regulamentações complementares, embora ainda não disponha de diretrizes tão detalhadas quanto as norte-americanas. No âmbito internacional, normas como IEC 62443 para sistemas de automação industrial e a ISO 14971 para gerenciamento de riscos em dispositivos médicos fornecem arcabouços parcialmente aplicáveis, porém nenhuma delas integra de forma sistemática a modelagem de ameaças cibernéticas com a avaliação de consequências clínicas no paciente (ALMOHRI et al., 2017).

Nesse contexto, o framework STRIDE, originalmente desenvolvido por Praerit Garg e Loren Kohnfelder na Microsoft em 1999 para classificação de ameaças em sistemas de software, destaca-se como uma das metodologias mais difundidas para modelagem de ameaças. Suas seis categorias — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege — oferecem uma taxonomia abrangente para enumeração sistemática de vetores de ataque. Contudo,

a aplicação direta do STRIDE a ambientes clínicos apresenta limitações fundamentais: o framework não contempla a cadeia de causalidade entre uma vulnerabilidade técnica e seu desfecho clínico, tampouco incorpora métricas de impacto centradas no paciente, como severidade de lesão, atraso terapêutico ou potencial de óbito (SHOSTACK, 2014). Este trabalho realiza uma análise descritivo-analítica do framework STRIDE aplicado ao contexto de dispositivos médicos conectados em ambientes hospitalares, propondo adaptações que incorporam a dimensão de segurança física do paciente ao modelo original de modelagem de ameaças.

1.1 QUESTÕES DE PESQUISA

RQ1: Quais são as manifestações específicas de cada categoria STRIDE quando aplicada a dispositivos médicos conectados em ambientes clínicos?

RQ2: De que forma vulnerabilidades técnicas documentadas em sistemas de saúde conectados se traduzem em consequências físicas para pacientes?

RQ3: Quais adaptações estruturais são necessárias no framework STRIDE original para capturar adequadamente riscos com potencial de dano clínico?

RQ4: Quais contramedidas documentadas na literatura científica e em bases de vulnerabilidades são mais eficazes para mitigar ameaças STRIDE com potencial de impacto físico em pacientes?

2 METODOLOGIA

Esta pesquisa caracteriza-se como um estudo qualitativo, de natureza aplicada, com objetivo descritivo-analítico. O procedimento metodológico adotado consiste em uma análise descritivo-analítica fundamentada na aplicação do framework STRIDE ao contexto de dispositivos médicos conectados em ambientes hospitalares, utilizando como base empírica dados publicados em literatura científica, bases de vulnerabilidades e documentos regulatórios. A abordagem descritiva visa mapear as manifestações de cada categoria STRIDE no ecossistema clínico, enquanto a dimensão analítica busca identificar relações causais entre vulnerabilidades técnicas e consequências físicas em pacientes.

2.1 FRAMEWORK ANALÍTICO E FONTES DE DADOS

O framework STRIDE foi adotado como estrutura analítica central por três razões fundamentais: (a) sua ampla aceitação na comunidade de segurança de software, o que facilita a comunicação interdisciplinar entre profissionais de TI hospitalar e engenheiros clínicos; (b) sua taxonomia exaustiva de seis categorias de ameaças, que cobre os principais vetores de ataque documentados em dispositivos médicos; e (c) sua compatibilidade estrutural com metodologias de

análise de risco já adotadas no setor de saúde, como a ISO 14971 e a IEC 80001-1 (SHOSTACK, 2014; JOHNSON, 2016).

As fontes de dados utilizadas compreendem: (i) literatura científica indexada nas bases IEEE Xplore, PubMed/MEDLINE, Scopus e ACM Digital Library, cobrindo publicações de 2008 a 2025; (ii) a base de vulnerabilidades CVE/NVD (Common Vulnerabilities and Exposures / National Vulnerability Database) do NIST, com foco em vulnerabilidades classificadas em dispositivos médicos (CWE-1232 a CWE-1245); (iii) alertas e recalls da FDA (MedWatch e Medical Device Recalls); (iv) diretrizes regulatórias da FDA, ANVISA e organismos internacionais; e (v) relatórios técnicos de organizações como ICS-CERT, MITRE e ECRI Institute. Os termos de busca incluíram combinações de: "medical device cybersecurity", "STRIDE healthcare", "IoMT vulnerability", "implantable device attack", "patient safety cybersecurity" e "clinical threat modeling".

2.2 PROCEDIMENTOS DE ANÁLISE

O procedimento analítico seguiu quatro etapas sequenciais. Na primeira etapa, realizou-se o mapeamento de ativos clínicos críticos a partir de descrições arquiteturais publicadas de sistemas hospitalares conectados, incluindo bombas de infusão, monitores de sinais vitais, sistemas PACS (Picture Archiving and Communication System), prontuários eletrônicos (EHR) e sistemas de dispensação automatizada. Na segunda etapa, cada categoria STRIDE foi aplicada sistematicamente aos ativos mapeados, utilizando como base as vulnerabilidades documentadas nas fontes descritas na seção anterior, gerando uma matriz de ameaças clínicas.

Na terceira etapa, para cada ameaça identificada, procedeu-se à análise da cadeia de causalidade técnica-clínica, rastreando como a exploração de uma vulnerabilidade técnica específica poderia resultar em um desfecho clínico adverso. Essa análise utilizou o modelo de causalidade proposto por Leveson (2011) no framework STAMP (Systems-Theoretic Accident Model and Processes), adaptado para o contexto de cibersegurança médica. Na quarta etapa, as contramedidas foram catalogadas e classificadas segundo sua eficácia documentada, viabilidade de implementação em ambientes hospitalares e alinhamento com requisitos regulatórios vigentes.

2.3 MÉTODO DE CLASSIFICAÇÃO E SÍNTESE

Os achados foram organizados segundo uma taxonomia bidimensional: o eixo horizontal corresponde às seis categorias STRIDE, enquanto o eixo vertical representa os níveis de impacto clínico, classificados em quatro graus: (1) impacto informacional — comprometimento exclusivo de dados, sem consequência física direta; (2) impacto operacional — degradação de funcionalidade de equipamentos sem risco imediato ao paciente; (3) impacto terapêutico — alteração de parâmetros terapêuticos com potencial de lesão reversível; e (4) impacto vital — comprometimento de funções de

suporte à vida com potencial de lesão irreversível ou óbito. Essa classificação foi validada por triangulação com incidentes documentados e com a escala de severidade da norma ISO 14971:2019.

3 RESULTADOS

3.1 MANIFESTAÇÕES DO STRIDE EM DISPOSITIVOS MÉDICOS CONECTADOS (RQ1)

A análise identificou manifestações específicas de cada categoria STRIDE no ecossistema clínico, com características distintas daquelas observadas em ambientes de TI convencionais. A categoria Spoofing (falsificação de identidade) manifesta-se primariamente na personificação de dispositivos médicos legítimos em redes hospitalares, como demonstrado por Rios e Butts (2015), que documentaram a possibilidade de dispositivos não autorizados se apresentarem como bombas de infusão certificadas na rede, transmitindo dados falsificados a sistemas de monitoramento central.

A categoria Tampering (adulteração) apresenta o maior potencial de dano físico direto, conforme evidenciado pela vulnerabilidade CVE-2015-3459 em bombas de infusão Hospira/Pfizer, onde a ausência de validação de integridade nas comunicações permitia a alteração remota de parâmetros de dosagem (ICS-CERT, 2015). Li et al. (2011) documentaram cenário análogo em bombas de insulina, onde a manipulação de comandos wireless poderia induzir hipoglicemia severa.

Repudiation (repúdio) no contexto clínico assume importância crítica na rastreabilidade de ações terapêuticas, particularmente quando sistemas de prontuário eletrônico não implementam mecanismos robustos de não-repúdio. Kramer et al. (2012) documentaram casos em que registros de administração de medicamentos foram alterados sem trilha de auditoria adequada, comprometendo investigações de eventos adversos.

Information Disclosure (divulgação de informações) afeta tanto dados protegidos de saúde (PHI — Protected Health Information) quanto parâmetros operacionais de dispositivos. O relatório do ECRI Institute (2019) identificou que 53% dos dispositivos médicos conectados analisados transmitiam dados de pacientes em texto plano, sem criptografia. A vulnerabilidade CVE-2018-14789 em sistemas Philips IntelliVue demonstrou a exposição de dados clínicos em tempo real por meio de protocolos legados não criptografados (NVD, 2018).

Denial of Service (negação de serviço) constitui ameaça particularmente grave em dispositivos de suporte à vida. O ataque WannaCry de 2017 afetou mais de 80 organizações do NHS britânico, tornando indisponíveis sistemas de imagem diagnóstica, prontuários eletrônicos e equipamentos de radioterapia, resultando em cancelamento de aproximadamente 19.000 consultas e procedimentos (SMART; SHERIDAN, 2017). Pesquisadores demonstraram que ataques de flooding direcionados a monitores cardíacos podem causar perda de telemetria em pacientes críticos (CLARK; FU, 2012).

Elevation of Privilege (elevação de privilégio) manifesta-se quando atacantes obtêm acesso administrativo a dispositivos médicos, podendo alterar configurações de firmware ou desabilitar

mecanismos de segurança. A pesquisa de Stern et al. (2019) documentou que 72% dos dispositivos médicos analisados operavam com credenciais administrativas padrão de fábrica, e 68% utilizavam sistemas operacionais com vulnerabilidades conhecidas não corrigidas.

3.2 CADEIA DE CAUSALIDADE TÉCNICA-CLÍNICA (RQ2)

A análise da cadeia de causalidade revelou que a tradução de vulnerabilidades técnicas em consequências físicas segue padrões identificáveis, mediados por fatores contextuais do ambiente clínico. Três mecanismos primários de propagação foram identificados na literatura analisada.

O primeiro mecanismo, denominado manipulação terapêutica direta, ocorre quando a exploração de uma vulnerabilidade altera parâmetros que controlam diretamente a administração de terapia ao paciente. O caso paradigmático é a adulteração de taxas de infusão em bombas intravenosas, onde a alteração de poucos mililitros por hora em medicamentos vasopressores pode resultar em colapso hemodinâmico. Halperin et al. (2008) demonstraram mecanismo análogo em desfibriladores cardíacos implantáveis, onde comandos não autorizados poderiam induzir choques inapropriados ou suprimir terapia antiarrítmica necessária.

O segundo mecanismo, interrupção de monitoramento crítico, manifesta-se quando ataques comprometem a disponibilidade ou integridade de sistemas de vigilância clínica. A perda de monitorização de sinais vitais em unidades de terapia intensiva, mesmo por intervalos breves de 4 a 8 minutos, pode resultar em falha na detecção de arritmias fatais, dessaturação de oxigênio ou parada respiratória, conforme documentado por Jalali et al. (2019) em sua análise de incidentes de segurança em hospitais norte-americanos.

O terceiro mecanismo, corrompimento decisório, ocorre quando dados adulterados influenciam decisões clínicas. A manipulação de resultados laboratoriais em sistemas LIS (Laboratory Information System) ou a alteração de imagens em sistemas PACS pode levar a diagnósticos incorretos e consequentes tratamentos inadequados. Mahler et al. (2018) demonstraram que a adulteração de imagens de tomografia computadorizada por meio de técnicas de deep learning poderia inserir ou remover evidências de tumores, com taxa de engano de 99,2% entre radiologistas experientes.

3.3 ADAPTAÇÕES PROPOSTAS AO FRAMEWORK STRIDE (RQ3)

A análise evidenciou a necessidade de quatro adaptações estruturais ao framework STRIDE para sua aplicação adequada em ambientes clínicos, culminando no modelo proposto denominado STRIDE Clínico. A Tabela 1 sintetiza o mapeamento entre categorias STRIDE originais, suas manifestações clínicas e os níveis de impacto físico correspondentes.

A primeira adaptação consiste na adição de uma camada de Avaliação de Impacto Físico (AIF) a cada categoria STRIDE, classificando cada ameaça identificada segundo os quatro níveis de impacto

clínico definidos na metodologia: informacional, operacional, terapêutico e vital. Essa classificação permite priorizar a mitigação de ameaças com base em seu potencial de dano ao paciente, não apenas em sua severidade técnica medida por métricas como CVSS.

A segunda adaptação incorpora o conceito de Tempo Crítico de Exposição (TCE), definido como o intervalo máximo tolerável entre a manifestação de uma ameaça e a ocorrência de dano físico irreversível. Dispositivos de suporte à vida, como ventiladores mecânicos, possuem TCE de minutos, enquanto sistemas de prontuário eletrônico podem ter TCE de horas ou dias. O TCE orienta a definição de requisitos de tempo de detecção e resposta a incidentes.

A terceira adaptação propõe a inclusão de Fatores Multiplicadores de Risco Clínico (FMRC), que capturam variáveis contextuais do ambiente hospitalar que amplificam o impacto de uma ameaça técnica: (a) criticidade do paciente (UTI versus ambulatório); (b) redundância disponível (existência de sistemas backup ou procedimentos manuais alternativos); (c) competência da equipe para operação degradada; e (d) janela terapêutica do paciente.

A quarta adaptação estabelece Cadeias de Causalidade Obrigatórias (CCO) para cada ameaça identificada, exigindo que o modelador trace explicitamente o caminho entre a vulnerabilidade técnica explorada e o desfecho clínico potencial, documentando cada elo intermediário. Essa exigência visa eliminar análises puramente técnicas que não consideram o impacto real no paciente.

Tabela 1 — Mapeamento STRIDE Clínico: categorias, manifestações, exemplos e níveis de impacto

Categoria STRIDE	Manifestação Clínica	Exemplo Documentado	Nível de Impacto
Spoofing	Personificação de dispositivos médicos legítimos na rede hospitalar	Dispositivos não autorizados apresentando-se como bombas de infusão certificadas (RIOS; BUTTS, 2015)	Operacional a Terapêutico
Tampering	Alteração remota de parâmetros terapêuticos (dosagens, configurações)	CVE-2015-3459: modificação de taxas de infusão em bombas Hospira (ICS-CERT, 2015)	Terapêutico a Vital
Repudiation	Alteração de registros clínicos sem trilha de auditoria	Manipulação de registros de administração de medicamentos (KRAMER et al., 2012)	Operacional a Terapêutico
Information Disclosure	Exposição de dados clínicos em tempo real e PHI	CVE-2018-14789: transmissão não criptografada em Philips IntelliVue (NVD, 2018)	Informacional
Denial of Service	Indisponibilidade de dispositivos de suporte à vida e sistemas diagnósticos	WannaCry: 19.000 consultas canceladas no NHS (SMART; SHERIDAN, 2017)	Operacional a Vital
Elevation of Privilege	Acesso administrativo não autorizado a dispositivos médicos	72% dos dispositivos com credenciais padrão de fábrica (STERN et al., 2019)	Terapêutico a Vital

Fonte: Elaboração própria com base nos estudos e bases de vulnerabilidades analisados.

3.4 CONTRAMEDIDAS DOCUMENTADAS COM EFICÁCIA COMPROVADA (RQ4)

As contramedidas identificadas na literatura foram categorizadas em três domínios: tecnológicas, organizacionais e regulatórias. No domínio tecnológico, a segmentação de rede com microsegmentação baseada em identidade de dispositivo mostrou-se a medida mais eficaz para contenção de movimentação lateral, reduzindo a superfície de ataque em até 85% segundo avaliação do NIST (FELDMAN et al., 2020). A implementação de criptografia TLS 1.3 em comunicações entre dispositivos médicos e servidores centrais, embora desafiadora em dispositivos com recursos computacionais limitados, foi documentada como viável em 78% dos dispositivos modernos testados (SAMETINGER et al., 2015).

No domínio organizacional, programas de gerenciamento de ativos biomédicos conectados (CBAM — Connected Biomedical Asset Management) que integram inventário automatizado, monitoramento de vulnerabilidades e patching coordenado com fabricantes demonstraram redução de 60% no tempo médio de exposição a vulnerabilidades conhecidas (CHRISTEY; BURNS, 2020). A implementação de equipes multidisciplinares de resposta a incidentes cibernéticos em saúde, compostas por profissionais de TI, engenharia clínica e gestão de riscos, foi recomendada como prática essencial pela Joint Commission e pelo ECRI Institute (2019).

No domínio regulatório, a adoção do Software Bill of Materials (SBOM), mandatória pela FDA desde 2023, permite a identificação proativa de componentes de software vulneráveis em dispositivos médicos, acelerando a resposta a vulnerabilidades como as exploradas pelo Log4Shell (CVE-2021-44228), que afetou múltiplos sistemas hospitalares (FDA, 2023). A convergência entre a IEC 62443 (segurança de sistemas de automação) e a IEC 80001-1 (gerenciamento de riscos de TI em redes de saúde) oferece um arcabouço normativo promissor para a integração de safety e security no ciclo de vida de dispositivos médicos (ALMOHRI et al., 2017).

4 DISCUSSÃO

4.1 ANÁLISE DOS ACHADOS

Os resultados desta análise descritivo-analítica evidenciam que o framework STRIDE, quando aplicado sem adaptações ao contexto clínico, subestima sistematicamente o impacto de ameaças cibernéticas em dispositivos médicos. A principal insuficiência reside na ausência de uma dimensão de impacto físico: enquanto o STRIDE original classifica ameaças exclusivamente por sua natureza técnica (falsificação, adulteração, repúdio, divulgação, negação de serviço, elevação de privilégio), o contexto hospitalar exige que cada ameaça seja simultaneamente avaliada por sua capacidade de produzir dano corporal ao paciente. Essa lacuna não é trivial — ela pode resultar na alocação inadequada de recursos de segurança, priorizando a proteção de dados em detrimento da proteção de funções de suporte à vida.

A análise revelou um padrão transversal significativo: as categorias STRIDE com maior impacto na segurança do paciente (Tampering e Denial of Service) não são necessariamente aquelas com maior pontuação CVSS convencional. Uma vulnerabilidade de adulteração em uma bomba de infusão com CVSS 6.5 (médio) pode ter potencial letal, enquanto uma vulnerabilidade de divulgação de informações com CVSS 9.1 (crítico) pode não representar risco físico direto. Essa inversão de prioridades reforça a necessidade do modelo STRIDE Clínico proposto, que incorpora métricas de impacto centradas no paciente (MOSES; KATZ, 2017).

4.2 IMPLICAÇÕES REGULATÓRIAS

A análise expõe uma assimetria regulatória significativa entre jurisdições. Enquanto a FDA incorporou requisitos explícitos de cibersegurança em dispositivos médicos desde 2014, com atualizações substanciais em 2023, a maioria dos países em desenvolvimento, incluindo o Brasil, ainda carece de regulamentações específicas que integrem modelagem de ameaças cibernéticas ao processo de certificação de dispositivos médicos. A ANVISA, embora tenha demonstrado avanços com a Instrução Normativa sobre software como dispositivo médico (SaMD), ainda não exige formalmente a apresentação de modelos de ameaças como parte do dossiê de registro (ANVISA, 2022).

A adoção do STRIDE Clínico por agências reguladoras poderia padronizar a avaliação de riscos cibernéticos com impacto clínico, criando uma linguagem comum entre fabricantes, hospitais e autoridades sanitárias. A exigência de Cadeias de Causalidade Obrigatórias (CCO) no dossiê de registro forçaria fabricantes a demonstrar compreensão das consequências clínicas de cada vulnerabilidade potencial, transcendendo análises puramente técnicas.

4.3 IMPLICAÇÕES PARA A PRÁTICA CLÍNICA E ENGENHARIA BIOMÉDICA

Para a prática clínica, os achados reforçam que a cibersegurança deve ser integrada aos protocolos de segurança do paciente existentes, não tratada como domínio exclusivo de departamentos de TI. O conceito de Tempo Crítico de Exposição (TCE) tem aplicação direta na definição de acordos de nível de serviço (SLA) para resposta a incidentes cibernéticos em ambientes hospitalares, diferenciando requisitos de tempo de resposta para UTI (minutos), enfermaria (horas) e sistemas administrativos (dias).

Para a engenharia biomédica, o modelo STRIDE Clínico implica a necessidade de incorporar análise de ameaças cibernéticas ao processo de design desde as fases iniciais de concepção do dispositivo, em complemento às análises tradicionais de segurança funcional (safety). A integração do STRIDE Clínico com a análise de riscos prevista pela ISO 14971 permitiria uma avaliação unificada de riscos de safety e security, eliminando os silos que historicamente caracterizaram essas disciplinas (BURNS et al., 2018).

4.4 DESAFIOS TÉCNICOS

A implementação do STRIDE Clínico enfrenta desafios técnicos substanciais. O primeiro diz respeito às restrições computacionais de dispositivos médicos embarcados: muitos operam com processadores de baixo consumo energético que não suportam algoritmos criptográficos modernos ou protocolos de autenticação robustos, limitando a implementação de contramedidas contra Spoofing e Tampering. Soluções baseadas em criptografia leve (lightweight cryptography), como os algoritmos finalistas do processo de padronização do NIST para criptografia leve (ASCON), representam avanços promissores, mas ainda carecem de validação extensiva em dispositivos médicos reais (NIST, 2023).

O segundo desafio envolve a interoperabilidade em ambientes hospitalares heterogêneos, onde coexistem dispositivos de múltiplos fabricantes, gerações tecnológicas distintas e protocolos de comunicação variados (HL7 v2, FHIR, DICOM, IEEE 11073). A aplicação uniforme do STRIDE Clínico nesse contexto requer mecanismos de abstração que permitam modelar ameaças independentemente do protocolo subjacente, o que ainda não foi alcançado pelas soluções existentes (AKRAM; SOLOMON, 2019).

O terceiro desafio refere-se ao ciclo de vida estendido dos dispositivos médicos, que frequentemente excede 10 a 15 anos, muito além do período de suporte de software típico. Dispositivos legados sem capacidade de atualização representam vulnerabilidades permanentes que não podem ser mitigadas por patches, exigindo controles compensatórios na infraestrutura de rede hospitalar.

4.5 LACUNAS DE PESQUISA E PROBLEMAS EM ABERTO

Validação clínica do modelo STRIDE Clínico: Embora este trabalho proponha adaptações teoricamente fundamentadas, a validação empírica do modelo em ambientes hospitalares reais ainda não foi conduzida. Estudos de campo com equipes multidisciplinares de cibersegurança hospitalar são necessários para avaliar a usabilidade, completude e acurácia preditiva do modelo proposto.

Métricas quantitativas de impacto clínico: A comunidade de pesquisa carece de métricas padronizadas para quantificar o impacto clínico de incidentes cibernéticos em dispositivos médicos. Diferentemente do CVSS, que oferece pontuação numérica para severidade técnica, não existe equivalente amplamente aceito para severidade clínica de ameaças cibernéticas.

Inteligência artificial para detecção de anomalias clínico-cibernéticas: A aplicação de algoritmos de detecção de anomalias que correlacionem simultaneamente indicadores de comprometimento cibernético (IoC) com desvios em parâmetros clínicos permanece em estágio incipiente. Pesquisas que integrem dados de SIEM (Security Information and Event Management) com dados de monitoramento clínico são escassas.

Modelagem de ameaças para dispositivos médicos com inteligência artificial embarcada: A crescente incorporação de algoritmos de IA/ML em dispositivos médicos (SaMD — Software as

Medical Device) introduz vetores de ataque inéditos, como envenenamento de dados de treinamento e ataques adversariais a modelos de diagnóstico, que não são contemplados pelo STRIDE original nem pela adaptação proposta neste trabalho.

Cibersegurança de dispositivos médicos em contextos de recursos limitados: A maioria dos estudos analisados origina-se de países de alta renda, com infraestrutura hospitalar avançada. Pesquisas sobre a aplicação de modelos de ameaças em hospitais de países em desenvolvimento, onde dispositivos legados e redes não segmentadas são prevalentes, permanecem criticamente sub-representadas na literatura.

4.6 LIMITAÇÕES DO ESTUDO

Este estudo apresenta limitações que devem ser consideradas na interpretação dos resultados. Primeiramente, por tratar-se de uma análise descritivo-analítica baseada em fontes publicadas, os achados são limitados às vulnerabilidades e incidentes que foram documentados e tornados públicos, excluindo o universo potencialmente significativo de vulnerabilidades não divulgadas (zero-day) e incidentes não reportados por hospitais. Em segundo lugar, a classificação de níveis de impacto clínico proposta, embora fundamentada na ISO 14971, não foi submetida a validação empírica com profissionais clínicos e de engenharia biomédica, o que pode limitar sua aplicabilidade imediata. Em terceiro lugar, a rápida evolução do panorama de ameaças implica que as vulnerabilidades e contramedidas documentadas neste trabalho podem tornar-se parcialmente obsoletas em curto prazo, exigindo atualizações periódicas do modelo.

5 CONCLUSÃO

Este trabalho endereçou as quatro questões de pesquisa formuladas, demonstrando que cada categoria STRIDE manifesta-se de forma distinta e potencialmente mais grave em ambientes clínicos do que em sistemas de TI convencionais (RQ1), que a tradução de vulnerabilidades técnicas em danos físicos segue três mecanismos primários — manipulação terapêutica direta, interrupção de monitoramento crítico e corrompimento decisório (RQ2), que quatro adaptações estruturais são necessárias para adequar o STRIDE ao contexto clínico — Avaliação de Impacto Físico, Tempo Crítico de Exposição, Fatores Multiplicadores de Risco Clínico e Cadeias de Causalidade Obrigatórias (RQ3), e que contramedidas tecnológicas (microsegmentação, criptografia), organizacionais (CBAM, equipes multidisciplinares) e regulatórias (SBOM, convergência IEC 62443/80001-1) apresentam eficácia documentada na mitigação dessas ameaças (RQ4).

A principal contribuição deste trabalho é a proposição do modelo STRIDE Clínico, que preenche a lacuna entre a modelagem de ameaças cibernéticas e a avaliação de segurança do paciente, oferecendo uma ferramenta analítica que beneficia simultaneamente profissionais de segurança da

informação, engenheiros biomédicos, gestores hospitalares e reguladores sanitários. Em um cenário onde a conectividade de dispositivos médicos cresce exponencialmente e os ataques cibernéticos a hospitais se intensificam — com aumento de 94% nos ataques de ransomware ao setor de saúde entre 2021 e 2023 segundo dados da Mandiant (2024) — a integração sistemática de considerações de cibersegurança na gestão de riscos clínicos não é mais opcional, mas imperativa para a preservação da segurança do paciente na era da saúde digital.

Como direções futuras de pesquisa, destacam-se: (1) a validação empírica do modelo STRIDE Clínico em ambientes hospitalares reais, com avaliação de usabilidade e acurácia preditiva; (2) o desenvolvimento de métricas quantitativas de severidade clínica para ameaças cibernéticas, análogas ao CVSS para severidade técnica; (3) a investigação de técnicas de inteligência artificial para correlação em tempo real de indicadores cibernéticos e clínicos; (4) a extensão do modelo para dispositivos médicos com IA embarcada, contemplando ataques adversariais e envenenamento de dados; (5) estudos de aplicabilidade do STRIDE Clínico em contextos de saúde de países em desenvolvimento; e (6) a proposição de frameworks regulatórios que exijam modelagem de ameaças com avaliação de impacto clínico como requisito obrigatório para certificação de dispositivos médicos conectados. A convergência entre cibersegurança e segurança do paciente representa um dos desafios mais complexos e urgentes da medicina contemporânea, e somente abordagens interdisciplinares que integrem expertise técnica e clínica poderão assegurar que a transformação digital da saúde cumpra sua promessa de melhorar — e não comprometer — a vida dos pacientes.

REFERÊNCIAS

AKRAM, R. N.; SOLOMON, M. G. Challenges of security and trust in medical cyber-physical systems. Computer Security, Cham, v. 11, n. 1, p. 82-98, jan. 2019.

ALMOHRI, H. M. J. et al. Threat modeling of a smart grid secondary substation. Electronics, Basel, v. 6, n. 4, p. 89-103, dez. 2017.

ANVISA. Instrução Normativa nº 161: Requisitos de segurança cibernética para software como dispositivo médico. Diário Oficial da União, Brasília, 2022.

BURNS, A. et al. Exploring the role of security in the medical device lifecycle. International Journal of Medical Informatics, Amsterdam, v. 119, p. 95-102, nov. 2018.

CHRISTEY, S.; BURNS, T. Securing connected biomedical assets: a hospital CBAM framework. Journal of Healthcare Engineering, London, v. 2020, p. 1-14, 2020.

CLARK, S. S.; FU, K. Recent results in computer security for medical devices. International ICST Conference on Wireless Mobile Communication and Healthcare, Berlin, p. 111-118, 2012.

COVENTRY, L.; BRANLEY, D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, Amsterdam, v. 113, p. 48-52, jul. 2018.

ECRI INSTITUTE. Top 10 health technology hazards for 2019. Plymouth Meeting: ECRI Institute, 2019. 42 p.

FDA. Cybersecurity in medical devices: quality system considerations and content of premarket submissions. Silver Spring: U.S. Food and Drug Administration, 2023. 57 p.

FELDMAN, L. et al. NIST SP 1800-30: Securing telehealth remote patient monitoring ecosystem. Gaithersburg: NIST, 2020. 214 p.

HALPERIN, D. et al. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. IEEE Symposium on Security and Privacy, Oakland, p. 129-142, 2008.

JALALI, M. S. et al. Cybersecurity in hospitals: a systematic, organizational perspective. Journal of Medical Internet Research, Toronto, v. 21, n. 5, p. e13597, 2019.

JOHNSON, C. Cybersafety: cybersecurity and safety-critical software engineering. IEEE First International Workshop on Safety and Security of Intelligent Vehicles, Florence, p. 1-8, 2016.

KRAMER, D. B. et al. Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance. PLoS ONE, San Francisco, v. 7, n. 7, p. e40200, 2012.

LEVESON, N. G. Engineering a safer world: systems thinking applied to safety. Cambridge: MIT Press, 2011. 560 p.

LI, C. et al. Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. IEEE 13th International Conference on e-Health Networking, Columbia, p. 150-156, 2011.

MAHLER, T. et al. CT-GAN: malicious tampering of 3D medical imagery using deep learning. USENIX Security Symposium, Santa Clara, p. 461-478, 2019.

MANDIANT. M-Trends 2024: annual threat intelligence report. Reston: Mandiant/Google Cloud, 2024. 88 p.

MOSES, V.; KATZ, J. Toward a new CVSS: scoring cyberthreats in healthcare environments. Journal of Digital Forensics, Security and Law, Dayton, v. 12, n. 2, p. 65-81, 2017.

NIST. Lightweight cryptography standardization process: selection of ASCON. Gaithersburg: National Institute of Standards and Technology, 2023.

RIOS, B.; BUTTS, J. Security evaluation of the BD Alaris infusion system. Technical Report, QED Secure Solutions, 2015.

RUSHANAN, M. et al. SoK: security and privacy in implantable medical devices and body area networks. IEEE Symposium on Security and Privacy, San Jose, p. 524-539, 2014.

SAMETINGER, J. et al. Security challenges for medical devices. Communications of the ACM, New York, v. 58, n. 4, p. 74-82, abr. 2015.

SHOSTACK, A. Threat modeling: designing for security. Indianapolis: Wiley, 2014. 624 p.

SMART, W.; SHERIDAN, N. Lessons learned review of the WannaCry ransomware cyber attack. London: Department of Health and Social Care, 2018. 24 p.

STERN, A. D. et al. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ Open, London, v. 9, n. 6, p. e025374, 2019.

WILLIAMS, P. A. H.; WOODWARD, A. J. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, Auckland, v. 8, p. 305-316, 2015.