REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

OBSERVABILIDADE COMO PRÉ-CONDIÇÃO DA DETECÇÃO EM AMBIENTE HOSPITALAR: UM MODELO DE TELEMETRIA E RESPOSTA SOB RESTRIÇÃO ASSISTENCIAL

OBSERVABILITY AS A PRECONDITION FOR DETECTION IN HOSPITAL ENVIRONMENTS: A TELEMETRY AND RESPONSE MODEL UNDER CLINICAL CONSTRAINTS

LA OBSERVABILIDAD COMO PRECONDICIÓN DE LA DETECCIÓN EN ENTORNOS HOSPITALARIOS: UN MODELO DE TELEMETRÍA Y RESPUESTA BAJO RESTRICCIÓN ASISTENCIAL

Marcelo de Melo Marcon[1]

e2138
https://doi.org/10.67553/sol21.v.2i1.38

PUBLICADO: 10/2026

RESUMO

A literatura sobre detecção de intrusões pressupõe que a organização possa conter um incidente assim que o identifica. Em ambiente hospitalar, esse pressuposto não se sustenta: isolar um endpoint, revogar uma credencial ou segmentar uma rede pode interromper assistência em curso e produzir dano ao paciente. Este artigo tem por objetivo propor um modelo de observabilidade e resposta aplicável a organizações de saúde, no qual a contenção é condicionada pela criticidade clínica do ativo afetado. Adota-se a Design Science Research como estratégia, com desenvolvimento de artefato do tipo modelo a partir de base documental composta por normas técnicas, publicações de agências governamentais e literatura revisada por pares, incluindo estudos que associam ataques de ransomware a desfechos clínicos adversos. Os resultados compreendem a formulação da restrição assistencial como propriedade do ambiente; a demonstração de que o tempo médio de resposta possui piso imposto pela segurança do paciente, de modo que o tempo médio de detecção é a única variável efetivamente compressível; uma arquitetura de telemetria em sete camadas; a estratificação da resposta em quatro níveis de autonomia; casos de uso de detecção priorizados por impacto clínico; cinco indicadores operacionais; e o mapeamento contra a ISO/IEC 27001:2022, o NIST Cybersecurity Framework 2.0 e a ISO 22301. Conclui-se que, sob restrição assistencial, a observabilidade determina quais respostas existem, e não apenas quando elas começam.

PALAVRAS-CHAVE: Observabilidade. Detecção de intrusões. Segurança hospitalar. Continuidade assistencial. Resposta a incidentes.

ABSTRACT

Intrusion detection literature assumes that an organization can contain an incident as soon as it identifies one. In hospital settings this assumption does not hold: isolating an endpoint, revoking a credential or segmenting a network may interrupt ongoing care and harm patients. This article proposes an observability and response model for healthcare organizations in which containment is conditioned by the clinical criticality of the affected asset. Design Science Research is adopted as the strategy, developing a model-type artifact from a documentary base of technical standards, government agency publications and peer-reviewed literature, including studies linking ransomware attacks to adverse clinical outcomes. The results comprise the formulation of clinical constraint as a property of the environment; the demonstration that mean time to respond has a floor imposed by

[1] Doutor Honoris Causa em Ciências Exatas pela World Christian University (WCU), Mestre em Direção Estratégica em Tecnologias da Informação pela Universidad Europea del Atlántico, pós-graduado em MBIS – Segurança da Informação e em Engenharia de Redes e Sistemas de Telecomunicações. Possui mais de 20 anos de experiência profissional em Tecnologia da Informação e Comunicação (TIC), com atuação em ambientes críticos nos setores de saúde, governo e telecomunicações. Sua experiência abrange Segurança da Informação, Cibersegurança, Proteção de Dados, Gestão de Riscos, Datacenters, Virtualização, Linux, Redes, Governança, Continuidade de Negócios e Melhoria de Processos. É instrutor da Escola Superior de Guerra – ADESG/Campinas, membro do Comitê Avançado e Altos Estudos de Tecnologia e Inovação da Digital Law Academy, Diretor do Comitê de Segurança da APDADOS e Imortal da Academia Brasileira de Ciências, Artes, História e Literatura (ABRASCI).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

patient safety, so that mean time to detect is the only genuinely compressible variable; a seven-layer telemetry architecture; response stratified into four levels of autonomy; detection use cases prioritized by clinical impact; five operational indicators; and a mapping against ISO/IEC 27001:2022, the NIST Cybersecurity Framework 2.0 and ISO 22301. The article concludes that under clinical constraint, observability determines which responses exist, not merely when they begin.

KEYWORDS: *Observability. Intrusion detection. Hospital security. Care continuity. Incident response.*

RESUMEN
La literatura sobre detección de intrusiones supone que la organización puede contener un incidente tan pronto como lo identifica. En el entorno hospitalario ese supuesto no se sostiene: aislar un endpoint, revocar una credencial o segmentar una red puede interrumpir la asistencia en curso y causar daño al paciente. Este artículo propone un modelo de observabilidad y respuesta para organizaciones de salud en el que la contención está condicionada por la criticidad clínica del activo afectado. Se adopta la Design Science Research como estrategia, desarrollando un artefacto de tipo modelo a partir de una base documental de normas técnicas, publicaciones de agencias gubernamentales y literatura revisada por pares. Los resultados comprenden la formulación de la restricción asistencial como propiedad del entorno; la demostración de que el tiempo medio de respuesta tiene un piso impuesto por la seguridad del paciente, de modo que el tiempo medio de detección es la única variable comprimible; una arquitectura de telemetría en siete capas; la estratificación de la respuesta en cuatro niveles de autonomía; casos de uso priorizados por impacto clínico; cinco indicadores operativos; y el mapeo contra la ISO/IEC 27001:2022, el NIST Cybersecurity Framework 2.0 y la ISO 22301.

PALABRAS CLAVE: *Observabilidad. Detección de intrusiones. Seguridad hospitalaria. Continuidad asistencial. Respuesta a incidentes.*

INTRODUÇÃO

Um hospital contemporâneo depende de sistemas de informação em praticamente todos os seus processos assistenciais: o prontuário eletrônico organiza a prescrição e o registro clínico, o sistema de imagem distribui exames, e bombas de infusão, monitores e ventiladores comunicam-se em rede. A indisponibilidade desses sistemas não produz inconveniência administrativa: produz atraso diagnóstico, suspensão de procedimentos e desvio de ambulâncias.

A evidência empírica sobre essa cadeia causal deixou de ser anedótica. Pesquisa com dados de sinistros do sistema público de saúde norte-americano identificou elevação de 34% a 38% na mortalidade intra-hospitalar entre pacientes já internados quando um ataque de ransomware é deflagrado, além de queda de 17% a 24% no volume de atendimentos na primeira semana (Neprash et al., 2026). Estudo qualitativo em quatro organizações atingidas documentou prolongamento do tempo de permanência em emergência, atraso em exames e transferências adicionais (van Boven et al., 2024). O ataque cibernético a um hospital é, assim, evento de segurança do paciente antes de ser evento de segurança da informação. O custo financeiro acompanha o clínico: a saúde permanece, pelo décimo terceiro ano consecutivo, como o setor de maior custo médio por violação,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

com 6,64 milhões de dólares por incidente contra média global de 4,99 milhões, e o tempo médio para identificar e conter subiu para 247 dias (IBM, 2026).

A resposta organizacional consolidada consiste em ampliar a pilha de detecção e resposta. Essa arquitetura é adequada e necessária, mas carrega um pressuposto que o ambiente hospitalar invalida: o de que, uma vez identificado o incidente, a organização pode contê-lo. Em um hospital, as ações canônicas de contenção têm custo clínico. Isolar um endpoint pode ser isolar a estação que exibe o laudo de imagem durante um procedimento; revogar credenciais em massa pode impedir o acesso ao prontuário na admissão de emergência; colocar um segmento em quarentena pode silenciar a telemetria de monitores em terapia intensiva. Nenhuma é inadmissível em termos absolutos; todas são condicionadas por aquilo que acontece com o paciente naquele instante.

Formulamos, a partir daí, a proposição que orienta o trabalho: em organizações de saúde, o tempo médio de resposta possui piso imposto pela segurança do paciente, ao passo que o tempo médio de detecção não possui piso equivalente. As duas variáveis, tratadas como simétricas pela literatura, não são igualmente compressíveis. Como consequência, a observabilidade deixa de ser instrumentação de apoio à detecção e passa a determinar quais respostas estão disponíveis: quanto mais cedo e com mais contexto o evento é observado, maior o conjunto de intervenções clinicamente aceitáveis, porque a contenção ainda pode ocorrer antes de o ativo entrar em uso assistencial.

Definimos a seguinte questão de pesquisa: como estruturar observabilidade e resposta a incidentes em uma organização de saúde na qual as ações convencionais de contenção são clinicamente restritas? O objetivo geral é propor um modelo que condicione a resposta à criticidade assistencial do ativo afetado. Como objetivos específicos: (i) caracterizar a restrição assistencial como propriedade do ambiente; (ii) demonstrar a assimetria entre os tempos de detecção e de resposta; (iii) propor uma arquitetura de telemetria com contexto clínico; (iv) estratificar a resposta por nível de autonomia governada; e (v) definir indicadores e mapear o modelo contra referenciais normativos. A pesquisa se justifica porque a literatura de detecção raramente considera o custo da contenção como restrição do problema; porque organizações de saúde mantêm plataformas de orquestração em modo apenas informativo por receio de impacto assistencial; e porque a continuidade da assistência é bem jurídico distinto da confidencialidade. O modelo foi construído a partir de literatura pública e de experiência profissional, sem identificação da organização, pelas razões da subseção 2.3.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

1 - REFERENCIAL TEÓRICO

1.1 Monitoramento, observabilidade e telemetria

Os três termos são usados de modo intercambiável na prática, mas designam capacidades distintas. Monitoramento é a coleta de sinais predefinidos para indicar estado e tendência, e pressupõe que se saiba de antemão o que perguntar. Observabilidade é a capacidade de inferir o estado interno de um sistema a partir de suas saídas mensuráveis, inclusive para perguntas não antecipadas na instrumentação (Sridharan, 2018). Telemetria é o conjunto de dados que os componentes emitem. A distinção importa porque um ataque raramente aciona um alerta previsto: o monitoramento informa que um servidor está indisponível; a observabilidade permite perguntar, depois, por que ficou indisponível e quais outros ativos apresentaram o mesmo padrão. A tríade que sustenta essa capacidade compreende métricas, adequadas a alertas de nível de serviço (Beyer et al., 2016); registros, base da análise forense (Kent & Souppaya, 2006); e rastros, que relacionam causa e efeito entre componentes.

1.2 A pilha de detecção e o contexto de ativos

Os sistemas de detecção e prevenção de intrusões inspecionam tráfego ou atividade de host em busca de assinaturas e anomalias, e podem operar em modo passivo, apenas alertando, ou em linha, bloqueando (Scarfone & Mell, 2007). A distinção é decisiva em rede clínica, porque o bloqueio em linha introduz um ponto de falha no caminho de dados de equipamentos assistenciais. A plataforma de gestão de eventos e informações de segurança correlaciona eventos de origens heterogêneas, sendo a camada onde a detecção deixa de ser local e passa a ser sistêmica; a detecção e resposta em endpoint oferece visibilidade de processo e contenção no próprio host; a detecção e resposta em rede aprende o comportamento de tráfego sem depender de agente instalado, atributo relevante para dispositivos clínicos que não admitem software adicional; e a orquestração encadeia essas capacidades em fluxos predefinidos. As recomendações do NIST, reorganizadas em 2025 para alinhar-se ao Cybersecurity Framework 2.0, tratam preparação, detecção, análise, contenção, erradicação e recuperação como atividades governadas, e não como etapas puramente técnicas (Nelson et al., 2025). É nessa dimensão que este trabalho intervém.

A correlação de eventos sem contexto de ativo produz alertas tecnicamente corretos e operacionalmente inúteis. Saber que um host apresentou autenticação anômala é diferente de saber que esse host é o servidor de laudos do centro cirúrgico, do qual dependem três serviços clínicos. Esse contexto reside no inventário de ativos, que a ISO/IEC 27001:2022 trata como controle organizacional (International Organization for Standardization [ISO], 2022). Em ambiente hospitalar o inventário adquire dimensão adicional: além da criticidade técnica, cada ativo carrega uma

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

criticidade assistencial, que expressa a consequência clínica de sua indisponibilidade. São duas escalas, e a segunda é a que condiciona a resposta.

1.3 Particularidades do ambiente hospitalar e indicadores de tempo

Três características diferenciam a rede hospitalar de uma rede corporativa. A primeira é a presença de dispositivos médicos conectados e de tecnologia operacional que não admitem agente de segurança e podem apresentar comportamento imprevisível sob varredura ativa — de modo que sua segurança depende de observação passiva e de controles compensatórios. A segunda é a assimetria entre janelas de manutenção e disponibilidade exigida: serviços críticos operam continuamente, e a janela para aplicar correção é estreita e frequentemente cancelada por demanda clínica, acumulando-se uma dívida que não decorre de negligência, mas da prioridade assistencial. A terceira é a segmentação: a abordagem de zonas e conduítes, da série IEC 62443, agrupa ativos por requisito de segurança e media a comunicação por canais controlados (International Electrotechnical Commission [IEC], 2020), separando a zona clínica da administrativa sem interromper fluxos legítimos. Incide ainda o regime de proteção de dados: registros de segurança hospitalares contêm identificadores de paciente, sujeitando a telemetria aos princípios de finalidade, necessidade e minimização da LGPD (Lei n. 13.709, 2018).

O tempo médio de detecção mede o intervalo entre o comprometimento e sua identificação; o de resposta, entre a identificação e a contenção efetiva. São os indicadores mais difundidos em operações de segurança, e a literatura de mercado costuma tratá-los como alvos simétricos de otimização. Segundo a IBM (2026), organizações que empregam automação de modo extensivo contiveram incidentes 65 dias mais rapidamente — achado habitualmente lido como recomendação direta de automação. A seção de resultados examina por que essa leitura exige qualificação em ambiente assistencial.

2 - METODOLOGIA

2.1 Delineamento e etapas de construção

A pesquisa é qualitativa quanto à abordagem, aplicada quanto à natureza e documental quanto aos procedimentos. Adotamos a Design Science Research como estratégia, apropriada quando o propósito não é descrever um fenômeno, mas produzir um artefato que resolva um problema organizacional identificado (Hevner et al., 2004). O produto é um modelo, entendido como representação que organiza construtos e relações de modo a orientar decisão em situação concreta. O percurso segue as atividades de Peffers et al. (2007), das quais foram conduzidas a identificação do problema, a definição dos objetivos, o projeto e desenvolvimento e a demonstração analítica, em cinco etapas: levantamento e qualificação das fontes; caracterização da restrição assistencial;

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

derivação da assimetria entre os indicadores de tempo; estruturação da arquitetura de telemetria e da estratificação da resposta; e definição de indicadores com o mapeamento normativo.

2.2 Fontes documentais e critérios de qualificação

Estabelecemos hierarquia de qualificação em quatro níveis. No primeiro, normas técnicas e publicações de agências governamentais. No segundo, literatura acadêmica revisada por pares, com prioridade para estudos que estabeleçam relação empírica entre incidente cibernético e desfecho clínico. No terceiro, relatórios de telemetria e pesquisa setorial de larga escala, admitidos quando descrevem método amostral e período de coleta. No quarto, material de fornecedores de solução, admitido para caracterização conceitual e nunca como base quantitativa. Foram descartados dados numéricos sem fonte primária alcançável.

2.3 Cuidados éticos e de segurança da informação

Este trabalho não utiliza dados de pacientes, registros clínicos, dados de identificação de profissionais ou qualquer informação pessoal, razão pela qual não se enquadra nas hipóteses de submissão a Comitê de Ética em Pesquisa, e tampouco utiliza dados operacionais de organização identificada. A omissão da organização de origem não é formalidade de anonimato, mas requisito de segurança: a descrição pública da topologia de rede, da cobertura de detecção ou das limitações de resposta de um hospital determinado é informação de valor operacional para um adversário, e sua divulgação aumentaria o risco da própria organização que o trabalho pretende proteger. O modelo é apresentado em nível de arquitetura genérica, sem parâmetros, fornecedores, versões ou limiares que permitam inferência sobre um ambiente específico.

2.4 Limitações do estudo

Três limitações devem ser explicitadas. O ciclo da Design Science Research não foi completado: o artefato foi projetado e demonstrado analiticamente, mas não submetido a avaliação empírica controlada, de modo que sua utilidade é argumentada e não demonstrada. A anonimização impede apresentar a série histórica de indicadores que sustentaria comparação antes e depois. E a heterogeneidade do setor é relevante: hospitais diferem em porte, perfil assistencial e maturidade, e o modelo assume ambiente com serviços clínicos críticos informatizados e alguma capacidade de segurança instalada.

2.5 Declaração do uso de inteligência artificial

Os autores declaram o uso de assistente de inteligência artificial generativa no levantamento e triagem de fontes documentais, na organização analítica do material e na redação do manuscrito. A definição do tema e do recorte, a formulação da proposição central, as decisões sobre o delineamento, os critérios de qualificação de fontes e a validação final são de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

responsabilidade exclusiva dos autores. Não foram fornecidos ao sistema dados pessoais, sensíveis, clínicos, confidenciais ou de identificação organizacional. As saídas foram revisadas mediante conferência de cada referência contra a fonte primária e checagem dos dados quantitativos contra os relatórios de origem. Os prompts, parâmetros e registros metodologicamente relevantes encontram-se arquivados pelos autores e disponíveis mediante solicitação, ressalvadas informações legalmente protegidas. Coube ao sistema a triagem de fontes, a derivação da assimetria entre os indicadores de tempo, a elaboração das tabelas e a produção do texto em rascunho; coube aos autores, além da revisão e validação, a definição do tema a partir da pesquisa de mestrado em andamento, a exclusão de um eixo temático sem sustentação na pesquisa prévia, a anonimização integral do ambiente operacional e a validação da proposição central. Os autores assumem responsabilidade integral pela exatidão, integridade e conteúdo final do trabalho.

3 - RESULTADOS E DISCUSSÃO

3.1 A restrição assistencial como propriedade do ambiente

A primeira contribuição trata o custo clínico da contenção como propriedade estrutural do ambiente, e não como exceção negociada caso a caso.

Tabela 1

Ações convencionais de contenção, risco assistencial e alternativas admissíveis

Ação convencional	Risco em ativo de criticidade clínica	Alternativa admissível
Isolamento de endpoint	Interrupção de estação em uso assistencial, com perda de acesso a laudo, prescrição ou imagem durante procedimento.	Isolamento seletivo com preservação de rotas para serviços clínicos essenciais, ou monitoração reforçada até a conclusão do procedimento.
Revogação de credenciais	Impedimento de acesso ao prontuário em admissão de emergência ou troca de plantão.	Revogação escalonada, iniciada por sessões e acessos privilegiados, com preservação de credencial de contingência sob auditoria.
Quarentena de segmento	Silenciamento de telemetria de monitoração de pacientes e de comunicação de equipamentos assistenciais.	Restrição de conduítes por lista de permissões, mantendo comunicação prevista no perfil do dispositivo.
Bloqueio de processo	Interrupção de software que comanda equipamento em uso clínico.	Bloqueio restrito a ativos fora de uso assistencial, com acionamento condicionado ao estado operacional.
Varredura ativa	Comportamento imprevisível de dispositivo médico embarcado sob estímulo não previsto pelo fabricante.	Descoberta passiva por análise de tráfego e correlação com base de vulnerabilidades por modelo e versão.
Desligamento preventivo	Suspensão de procedimentos e desvio de pacientes.	Degradação controlada com contingência clínica previamente exercitada.

Nota. Elaborado pelos autores com base em International Organization for Standardization (2022), National Institute of Standards and Technology (2024) e Nelson et al. (2025).

Duas observações decorrem do mapeamento. Nenhuma alternativa da coluna à direita é gratuita: todas exigem mais informação sobre o ativo e seu estado operacional. Isolar um endpoint requer apenas seu endereço; isolá-lo seletivamente requer saber quais comunicações sustentam

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

assistência em curso. E essa informação não é obtida no momento do incidente: precisa estar disponível antes, no inventário e na telemetria. A restrição assistencial converte-se em requisito de observabilidade.

3.2 A assimetria entre os tempos de detecção e de resposta

O tempo de resposta compreende o intervalo entre a identificação do incidente e sua contenção. Em ambiente corporativo, é limitado por fatores organizacionais — disponibilidade de equipe, qualidade dos procedimentos, grau de automação — todos passíveis de melhoria por investimento. Em ambiente assistencial soma-se um limitante distinto: a janela clínica. Se a contenção exige que um procedimento em curso termine, o tempo de resposta não pode ser reduzido abaixo da duração desse procedimento, por mais madura que seja a operação de segurança. Esse piso não é ineficiência a corrigir; é a expressão correta da prioridade do paciente. O tempo de detecção não possui limitante análogo: reduzi-lo depende de cobertura de telemetria, qualidade de correlação e contexto de ativo — variáveis sob controle da organização que não competem com a assistência. Um sensor passivo adicional não interrompe cirurgia alguma.

A consequência prática inverte a intuição corrente. A leitura habitual do achado de que a automação reduz o tempo de contenção em 65 dias (IBM, 2026) é que hospitais devem automatizar resposta. A leitura correta sob restrição assistencial é que devem automatizar apenas onde a criticidade clínica permite, concentrando o investimento remanescente em detecção. Cada unidade de tempo economizada na detecção converte-se integralmente em vantagem, porque desloca a contenção para um momento em que o conjunto de ações admissíveis ainda é amplo: detectar durante o reconhecimento permite bloquear no perímetro; detectar após a criptografia obriga a escolher entre dano clínico e dano informacional.

3.3 Arquitetura de telemetria proposta

A terceira contribuição estrutura a cadeia de telemetria em sete camadas organizadas pelo ponto de decisão: cada uma responde por uma escolha que, se mal resolvida, compromete as seguintes.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Tabela 2

Camadas da arquitetura de telemetria e seus pontos de decisão

Camada	Função	Decisão crítica e requisito clínico
Geração	Emissão de sinais por hosts, aplicações, rede e dispositivos clínicos.	Definir o que instrumentar sem exigir agente em ativo que não o admite; privilegiar emissão nativa e observação de rede.
Coleta	Captura por agentes, syslog, exportadores de fluxo e espelhamento de tráfego.	Coleta passiva como padrão na zona clínica; espelhamento em vez de inserção em linha no caminho de dados assistencial.
Transporte	Envio dos dados ao ponto de consolidação.	Canal cifrado e independente da rede assistencial, para que a telemetria sobreviva à degradação do segmento observado.
Normalização	Padronização de campos e formatos.	Sincronização de tempo confiável e identificador de ativo consistente; sem isso a correlação é ilusória.
Enriquecimento	Agregação de contexto de inventário, criticidade e exposição.	Incorporar a criticidade assistencial como atributo distinto da criticidade técnica.
Correlação	Detecção sistêmica por regras e comportamento.	Priorizar por impacto clínico potencial, não apenas por severidade técnica.
Apresentação	Painéis operacionais e acionamento de resposta.	Expor o estado operacional do ativo ao analista no instante da decisão de contenção.

Nota. Elaborado pelos autores com base em Kent e Souppaya (2006), Scarfone e Mell (2007), Sridharan (2018) e International Organization for Standardization (2022).

A camada de normalização merece destaque: a correlação entre origens distintas depende de ordenação temporal confiável. Se relógios divergem, a plataforma pode inverter a sequência de causa e efeito e deixar de reconhecer um encadeamento que ocorreu. A sincronização de tempo, tratada como detalhe de infraestrutura, é pré-condição da detecção sistêmica.

3.4 Estratificação da resposta por autonomia governada

A quarta contribuição resolve o impasse que leva organizações de saúde a adquirir plataformas de orquestração e mantê-las inertes, e que decorre de tratar a automação como decisão binária.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

Tabela 3

Níveis de autonomia de resposta e critérios de atribuição

Nível	Comportamento	Aplicação recomendada
N0 — Observação	Registro e alerta, sem ação sobre o ativo.	Dispositivos clínicos em uso assistencial e sistemas de suporte à vida, em qualquer hipótese.
N1 — Ação reversível	Ações que não interrompem função e podem ser desfeitas sem efeito residual, como elevação de registro e captura de evidência.	Qualquer ativo, inclusive de criticidade clínica máxima.
N2 — Ação sob aprovação	Contenção efetiva condicionada a autorização humana com prazo definido e escalonamento automático.	Ativos de criticidade clínica alta fora de uso assistencial no momento da decisão.
N3 — Ação automática	Contenção imediata sem intervenção humana, com registro auditável e reversão predefinida.	Ativos administrativos e de infraestrutura sem dependência assistencial direta.

Nota. Elaborado pelos autores com base em Nelson et al. (2025) e National Institute of Standards and Technology (2024).

A atribuição de nível não é estática: depende do estado operacional do ativo no instante do evento. Uma estação de centro cirúrgico opera em N0 durante procedimento e pode operar em N2 fora dele. Isso exige que o estado assistencial seja sinal de telemetria, e não informação obtida por telefonema durante o incidente — o que reforça o argumento da subseção 3.1.

3.5 Casos de uso e indicadores propostos

A quinta contribuição reordena os casos de uso de detecção pelo impacto assistencial, e não pela frequência ou facilidade de implementação.

Tabela 4

Casos de uso de detecção ordenados por impacto assistencial

Caso de uso	Sinais correlacionados	Consequência assistencial evitada
Precursores de ransomware	Comunicação repetitiva com destino externo, alterações em mecanismos de recuperação e elevação incomum de atividade de escrita.	Indisponibilidade simultânea de prontuário, imagem e laboratório, com suspensão de procedimentos.
Comprometimento de credencial privilegiada	Autenticação fora de padrão de horário e origem, alterações em grupos privilegiados e falhas sucessivas em segundo fator.	Acesso irrestrito a sistemas clínicos e capacidade de desabilitar controles.
Desvio de comportamento de dispositivo clínico	Comunicação com destino ou protocolo fora do perfil estabelecido para o modelo do dispositivo.	Interferência em equipamento assistencial e propagação a partir de ativo sem agente.
Movimentação lateral em zona clínica	Acessos anômalos entre estações da mesma zona e varredura interna de portas.	Extensão do comprometimento a serviços de suporte à decisão clínica.
Exfiltração de dados de saúde	Volume de saída atípico, compressão incomum e destino não habitual, correlacionados a acesso a repositório clínico.	Exposição de dados sensíveis de paciente, com consequência regulatória e de confiança.

Nota. Elaborado pelos autores com base em MITRE Corporation (2024), Nelson et al. (2025) e van Boven et al. (2024).

A ordenação difere da usual em um ponto: a exfiltração, tratada como risco principal na maioria das matrizes por sua consequência regulatória, aparece por último — sua consequência é patrimonial e reputacional, ao passo que as quatro primeiras afetam a capacidade de prestar

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

assistência. Essa inversão expressa o tratamento da continuidade assistencial como propriedade de segurança em si.

Tabela 5

Indicadores operacionais propostos

Indicador	Definição operacional	Interpretação
Tempo de detecção segmentado por criticidade	Tempo médio de detecção calculado separadamente para ativos de criticidade assistencial alta e demais ativos.	Revela se a cobertura de telemetria acompanha a importância clínica.
Cobertura de telemetria por zona	Proporção de ativos ativos que emitem telemetria efetivamente ingerida, calculada por zona.	Mede a fração da superfície realmente observada; é o indicador limitante dos demais.
Latência da janela admissível	Intervalo entre a detecção e o primeiro instante em que a contenção se torna clinicamente aceitável.	Quantifica o piso de resposta imposto pela assistência e separa restrição clínica de lentidão operacional.
Distribuição de resposta por nível de autonomia	Proporção de incidentes tratados em cada nível de N0 a N3.	Concentração em N0 sugere plataforma de orquestração adquirida e não utilizada.
Precisão em ativos clínicos	Razão entre alertas confirmados e alertas emitidos, calculada apenas para ativos de criticidade assistencial alta.	Ruído nessa faixa é especialmente danoso, pois induz desconfiança onde a contenção é mais delicada.

Nota. Elaborado pelos autores.

O terceiro indicador é o mais útil em diálogo com a direção clínica: separa duas causas frequentemente confundidas de demora na contenção — a operação de segurança foi lenta, ou a janela clínica não permitia agir. Sem essa distinção, toda demora é atribuída à equipe técnica, e a discussão sobre o piso assistencial nunca acontece.

3.6 Mapeamento normativo e discussão

Tabela 6

Mapeamento dos componentes do modelo contra referenciais normativos

Componente	ISO/IEC 27001:2022	NIST CSF 2.0	Continuidade
Contexto e criticidade de ativos	5.9 Inventário de informações e outros ativos associados	Identificar	ISO 22301 — análise de impacto no negócio
Arquitetura de telemetria	8.15 Registro de eventos; 8.16 Atividades de monitoramento	Detectar	—
Segmentação por zonas e conduítes	8.20 Segurança de redes; 8.22 Segregação de redes	Proteger	IEC 62443 — zonas e conduítes
Resposta estratificada	5.24 Planejamento e preparação da gestão de incidentes	Responder	ISO 22301 — procedimentos de resposta
Contingência clínica e degradação controlada	5.29 Segurança durante disrupção	Recuperar	ISO 22301 — estratégias de continuidade
Governança da autonomia de resposta	5.2 Papéis e responsabilidades	Governar	—

Nota. Elaborado pelos autores com base em International Organization for Standardization (2022), National Institute of Standards and Technology (2024) e International Electrotechnical Commission (2020). Os identificadores de controle devem ser conferidos contra o texto integral das normas antes de uso em processo de auditoria.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

O modelo dialoga criticamente com a literatura de detecção, que concentra esforço na acurácia da classificação, supondo que a ação subsequente é indiferente ao contexto. O ambiente hospitalar mostra que não é: dois alertas com a mesma confiança estatística exigem condutas distintas se um recai sobre servidor administrativo e o outro sobre a estação que exibe imagem durante procedimento. A acurácia é necessária e insuficiente.

Um segundo ponto refere-se ao estatuto da disponibilidade: a tríade convencional atribui igual peso às três propriedades, mas o investimento concentra-se nas duas primeiras. Os achados que associam ransomware a elevação da mortalidade intra-hospitalar (Neprash et al., 2026) sugerem que, em saúde, a disponibilidade é aquela cuja violação produz dano irreversível: confidencialidade violada gera consequência grave e reparável; assistência interrompida em condição tempo-dependente, não. Um terceiro ponto é a economia da defesa: nenhuma camada do modelo depende de detecção avançada, pois ampliar cobertura de telemetria, qualificar contexto de ativo e estratificar autonomia atuam sobre o conjunto de ações disponíveis, e não sobre a capacidade de distinguir o adversário.

Reconhecemos, por fim, uma tensão não resolvida. O modelo exige que o estado operacional assistencial de cada ativo seja sinal de telemetria disponível ao analista no instante da decisão, e obter esse sinal implica integrar sistemas clínicos e de segurança, ampliando a interconexão entre ambientes que a segmentação recomenda separar. Há conflito entre a necessidade de contexto e o princípio da segregação. A resolução prática passa por trafegar apenas o estado — se o ativo está ou não em uso assistencial — sem conteúdo clínico, mas o desenho seguro dessa integração permanece aberto.

4 - CONSIDERAÇÕES

Este trabalho propôs um modelo de observabilidade e resposta a incidentes para organizações de saúde, construído pela Design Science Research, no qual a contenção é condicionada pela criticidade assistencial do ativo afetado.

Caracterizamos a restrição assistencial como propriedade estrutural do ambiente, mapeando seis ações de contenção contra o risco clínico correspondente e identificando alternativas admissíveis, todas dependentes de mais informação prévia sobre o ativo. Demonstramos que o tempo de resposta possui piso imposto pela janela clínica, enquanto o de detecção não possui limitante análogo, o que reorienta a prioridade de investimento. Propusemos arquitetura de telemetria em sete camadas, estratificamos a resposta em quatro níveis de autonomia e definimos cinco indicadores, com o mapeamento normativo.

A contribuição teórica consiste em incorporar o custo clínico da contenção como restrição do problema de detecção e em demonstrar a assimetria entre os indicadores temporais consagrados. A prática reside no modelo e nos indicadores, com destaque para a latência da janela

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

admissível, que separa demora operacional de restrição assistencial. As limitações foram explicitadas na metodologia, com destaque para a ausência de avaliação empírica controlada.

Como agenda futura, sugerimos quatro direções: a avaliação empírica do modelo em organizações de portes distintos, completando o ciclo da Design Science Research; a investigação do desenho seguro da integração entre sistemas clínicos e de segurança para trafegar estado operacional sem conteúdo clínico; o estudo da latência da janela admissível como indicador, incluindo sua distribuição por especialidade; e a análise das implicações regulatórias da indisponibilidade assistencial no Brasil.

REFERÊNCIAS

Beyer, B., Jones, C., Petoff, J., & Murphy, N. R. (2016). *Site reliability engineering: How Google runs production systems*. O'Reilly Media.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

IBM. (2026). *Cost of a data breach report 2026*. IBM Security.

International Electrotechnical Commission. (2020). *IEC 62443-3-2: Security for industrial automation and control systems — Security risk assessment for system design*.

International Organization for Standardization. (2019). *ISO 22301:2019 — Security and resilience: Business continuity management systems: Requirements*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems: Requirements*.

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST SP 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

Lei n. 13.709, de 14 de agosto de 2018. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

MITRE Corporation. (2024). *ATT&CK for enterprise*. https://attack.mitre.org

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Neprash, H., McGlave, C., & Nikpay, S. (2026). Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *American Economic Journal: Economic Policy, 18*(1), 256–281. https://doi.org/10.1257/pol.20240594

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Sridharan, C. (2018). *Distributed systems observability: A guide to building robust systems*. O'Reilly Media.

van Boven, L. S., Kusters, R. W. J., Tin, D., van Osch, F. H. M., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking acute care: A qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of Emergency Medicine, 83*(1), 46–56. https://doi.org/10.1016/j.annemergmed.2023.04.025

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.