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

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

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

Marcelo de Melo Marcon[1]

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

PUBLICADO: 10/2026

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 tiene por objetivo proponer un modelo de observabilidad y respuesta aplicable a 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, con el desarrollo de un artefacto de tipo modelo a partir de una base documental compuesta por normas técnicas, publicaciones de agencias gubernamentales y literatura revisada por pares, incluidos estudios que asocian los ataques de ransomware con desenlaces clínicos adversos. 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 efectivamente comprimible; una arquitectura de telemetría en siete capas; la estratificación de la respuesta en cuatro niveles de autonomía; casos de uso de detección 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. Se concluye que, bajo restricción asistencial, la observabilidad determina qué respuestas existen, y no solo cuándo comienzan.

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

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. Os resultados compreendem a formulação da restrição assistencial como propriedade do ambiente; a

[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 artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

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

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.

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. 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 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.

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

INTRODUCCIÓN

Un hospital contemporáneo depende de sistemas de información en prácticamente todos sus procesos asistenciales: la historia clínica electrónica organiza la prescripción y el registro clínico, el sistema de imagen distribuye estudios, y bombas de infusión, monitores y ventiladores se comunican en red. La indisponibilidad de estos sistemas no produce un inconveniente administrativo: produce retraso diagnóstico, suspensión de procedimientos y desvío de ambulancias.

La evidencia empírica sobre esta cadena causal ha dejado de ser anecdótica. Una investigación con datos de reclamaciones del sistema público de salud estadounidense identificó un aumento del 34% al 38% en la mortalidad intrahospitalaria entre pacientes ya internados cuando se desencadena un ataque de ransomware, además de una caída del 17% al 24% en el volumen de atenciones durante la primera semana (Neprash et al., 2026). Un estudio cualitativo en cuatro organizaciones afectadas documentó la prolongación del tiempo de permanencia en urgencias, retrasos en estudios y transferencias adicionales (van Boven et al., 2024). El ataque cibernético a un hospital es, así, un evento de seguridad del paciente antes de ser un evento de seguridad de la información. El costo financiero acompaña al clínico: la salud permanece, por decimotercer año consecutivo, como el sector de mayor costo medio por violación de datos, con 6,64 millones de

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

dólares por incidente frente a una media global de 4,99 millones, y el tiempo medio para identificar y contener subió a 247 días (IBM, 2026).

La respuesta organizacional consolidada consiste en ampliar la pila de detección y respuesta. Esta arquitectura es adecuada y necesaria, pero conlleva un supuesto que el entorno hospitalario invalida: el de que, una vez identificado el incidente, la organización puede contenerlo. En un hospital, las acciones canónicas de contención tienen costo clínico. Aislar un endpoint puede ser aislar la estación que muestra el informe de imagen durante un procedimiento; revocar credenciales de forma masiva puede impedir el acceso a la historia clínica en una admisión de urgencia; poner un segmento en cuarentena puede silenciar la telemetría de los monitores en cuidados intensivos. Ninguna es inadmisible en términos absolutos; todas están condicionadas por lo que le ocurre al paciente en ese instante.

A partir de ello formulamos la proposición que orienta el trabajo: en organizaciones de salud, el tiempo medio de respuesta tiene un piso impuesto por la seguridad del paciente, mientras que el tiempo medio de detección no tiene un piso equivalente. Las dos variables, tratadas como simétricas por la literatura, no son igualmente comprimibles. En consecuencia, la observabilidad deja de ser instrumentación de apoyo a la detección y pasa a determinar qué respuestas están disponibles: cuanto antes y con más contexto se observa el evento, mayor es el conjunto de intervenciones clínicamente aceptables, porque la contención todavía puede ocurrir antes de que el activo entre en uso asistencial.

Definimos la siguiente pregunta: ¿cómo estructurar la observabilidad y la respuesta a incidentes en una organización de salud en la que las acciones convencionales de contención están clínicamente restringidas? El objetivo general es proponer un modelo que condicione la respuesta a la criticidad asistencial del activo afectado. Como objetivos específicos: (i) caracterizar la restricción asistencial como propiedad del entorno; (ii) demostrar la asimetría entre los tiempos de detección y de respuesta; (iii) proponer una arquitectura de telemetría con contexto clínico; (iv) estratificar la respuesta por nivel de autonomía gobernada; y (v) definir indicadores y mapear el modelo contra referenciales normativos. Se justifica porque la literatura de detección rara vez considera el costo de la contención como restricción del problema; porque las organizaciones de salud mantienen plataformas de orquestación en modo solo informativo por temor al impacto asistencial; y porque la continuidad asistencial es un bien jurídico distinto de la confidencialidad. El modelo se construyó a partir de literatura pública y experiencia profesional, sin identificación de la organización, por las razones de la subsección 2.3.

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

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

1 - MARCO TEÓRICO

1.1 Monitoreo, observabilidad y telemetría

Los tres términos se usan de modo intercambiable en la práctica, pero designan capacidades distintas. El monitoreo es la recolección de señales predefinidas para indicar estado y tendencia, y presupone saber de antemano qué preguntar. La observabilidad es la capacidad de inferir el estado interno de un sistema a partir de sus salidas medibles, incluso para preguntas no anticipadas en la instrumentación (Sridharan, 2018). La telemetría es el conjunto de datos que los componentes emiten. La distinción importa porque un ataque rara vez activa una alerta prevista: el monitoreo informa que un servidor está indisponible; la observabilidad permite preguntar, después, por qué quedó indisponible y qué otros activos presentaron el mismo patrón. La tríada que sustenta esta capacidad comprende métricas, adecuadas para alertas de nivel de servicio (Beyer et al., 2016); registros, base del análisis forense (Kent & Souppaya, 2006); y trazas, que relacionan causa y efecto entre componentes.

1.2 La pila de detección y el contexto de activos

Los sistemas de detección y prevención de intrusiones inspeccionan tráfico o actividad de host en busca de firmas y anomalías, y pueden operar en modo pasivo, solo alertando, o en línea, bloqueando (Scarfone & Mell, 2007). La distinción es decisiva en una red clínica, porque el bloqueo en línea introduce un punto de falla en el camino de datos de los equipos asistenciales. La plataforma de gestión de eventos e información de seguridad correlaciona eventos de orígenes heterogéneos, y es la capa donde la detección deja de ser local y pasa a ser sistémica; la detección y respuesta en endpoint ofrece visibilidad de proceso y contención en el propio host; la detección y respuesta en red aprende el comportamiento del tráfico sin depender de un agente instalado, atributo relevante para dispositivos clínicos que no admiten software adicional; y la orquestación encadena estas capacidades en flujos predefinidos. Las recomendaciones del NIST, reorganizadas en 2025 para alinearse con el Cybersecurity Framework 2.0, tratan la preparación, la detección, el análisis, la contención, la erradicación y la recuperación como actividades gobernadas y no como etapas puramente técnicas (Nelson et al., 2025). Es en esa dimensión donde interviene el presente trabajo.

La correlación de eventos sin contexto de activo produce alertas técnicamente correctas y operativamente inútiles. Saber que un host presentó una autenticación anómala es distinto de saber que ese host es el servidor de informes del quirófano, del cual dependen tres servicios clínicos. Ese contexto reside en el inventario de activos, que la ISO/IEC 27001:2022 trata como control organizacional (International Organization for Standardization [ISO], 2022). En el entorno hospitalario el inventario adquiere una dimensión adicional: además de la criticidad técnica, cada

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

activo carga una criticidad asistencial, que expresa la consecuencia clínica de su indisponibilidad. Son dos escalas, y la segunda es la que condiciona la respuesta.

1.3 Particularidades hospitalarias e indicadores de tiempo

Tres características diferencian la red hospitalaria de una corporativa. La primera es la presencia de dispositivos médicos conectados y de tecnología operativa que no admiten agente de seguridad y pueden comportarse de modo imprevisible bajo exploración activa — su seguridad depende de observación pasiva y de controles compensatorios. La segunda es la asimetría entre ventanas de mantenimiento y disponibilidad exigida: los servicios críticos operan de forma continua, y la ventana para aplicar una corrección es estrecha y frecuentemente cancelada por demanda clínica, acumulándose una deuda que no proviene de negligencia, sino de la prioridad asistencial. La tercera es la segmentación: el enfoque de zonas y conductos de la serie IEC 62443 agrupa activos por requisito de seguridad y media la comunicación mediante canales controlados (International Electrotechnical Commission [IEC], 2020), separando la zona clínica de la administrativa sin interrumpir flujos legítimos. Incide además la protección de datos: los registros de seguridad hospitalarios contienen identificadores de paciente, sujetando la telemetría a los principios de finalidad, necesidad y minimización de la LGPD brasileña (Lei n. 13.709, 2018).

El tiempo medio de detección mide el intervalo entre el compromiso y su identificación; el de respuesta, entre la identificación y la contención efectiva. Son los indicadores más difundidos en operaciones de seguridad, y la literatura de mercado suele tratarlos como objetivos simétricos de optimización. Según IBM (2026), las organizaciones que emplean automatización de modo extensivo contuvieron incidentes 65 días más rápido — hallazgo habitualmente leído como recomendación directa de automatizar. La sección de resultados examina por qué esa lectura exige matización en un entorno asistencial.

2 - METODOLOGÍA

2.1 Diseño de la investigación y etapas de construcción

La investigación es cualitativa en cuanto al enfoque, aplicada en cuanto a la naturaleza y documental en cuanto a los procedimientos. Adoptamos la Design Science Research, apropiada cuando el propósito no es describir un fenómeno, sino producir un artefacto que resuelva un problema organizacional identificado (Hevner et al., 2004). El producto es un modelo, entendido como representación que organiza constructos y relaciones para orientar decisiones en una situación concreta. El recorrido sigue las actividades de Peffers et al. (2007) — identificación del problema, definición de objetivos, diseño y desarrollo, demostración analítica — en cinco etapas: relevamiento y calificación de fuentes; caracterización de la restricción asistencial; derivación de la

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

asimetría entre los indicadores de tiempo; estructuración de la arquitectura de telemetría y de la estratificación de la respuesta; y definición de indicadores con el mapeo normativo.

2.2 Fuentes documentales y criterios de calificación

Establecimos una jerarquía de calificación en cuatro niveles. En el primero, normas técnicas y publicaciones de agencias gubernamentales. En el segundo, literatura académica revisada por pares, con prioridad para estudios que establezcan una relación empírica entre incidente cibernético y desenlace clínico. En el tercero, informes de telemetría e investigación sectorial de gran escala, admitidos cuando describen método muestral y período de recolección. En el cuarto, material de proveedores de soluciones, admitido para caracterización conceptual y nunca como base cuantitativa. Se descartaron los datos numéricos sin fuente primaria alcanzable.

2.3 Cuidados éticos y de seguridad de la información

Este trabajo no utiliza datos de pacientes, registros clínicos, datos de identificación de profesionales ni ninguna información personal, razón por la cual no se encuadra en los supuestos de sometimiento a un Comité de Ética en Investigación, y tampoco utiliza datos operativos de organización identificada. La omisión de la organización de origen no es una formalidad de anonimato, sino un requisito de seguridad: la descripción pública de la topología de red, de la cobertura de detección o de las limitaciones de respuesta de un hospital determinado es información de valor operativo para un adversario, y su divulgación aumentaría el riesgo de la propia organización que el trabajo pretende proteger. El modelo se presenta en el nivel de una arquitectura genérica, sin parámetros, proveedores, versiones ni umbrales que permitan inferencias sobre un entorno específico.

2.4 Limitaciones del estudio

Deben explicitarse tres limitaciones. El ciclo de la Design Science Research no fue completado: el artefacto fue diseñado y demostrado analíticamente, pero no sometido a evaluación empírica controlada, de modo que su utilidad es argumentada y no demostrada. La anonimización impide presentar la serie histórica de indicadores que sustentaría una comparación antes y después. Y la heterogeneidad del sector es relevante: los hospitales difieren en porte, perfil asistencial y madurez, y el modelo supone un entorno con servicios clínicos críticos informatizados y alguna capacidad de seguridad instalada.

2.5 Declaración del uso de inteligencia artificial

Los autores declaran el uso de un asistente de inteligencia artificial generativa en el relevamiento y cribado de fuentes, la organización analítica del material y la redacción del manuscrito. La definición del tema y del alcance, la formulación de la proposición central, las

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

decisiones sobre el diseño, los criterios de calificación de fuentes y la validación final son responsabilidad exclusiva de los autores. No se proporcionaron al sistema datos personales, sensibles, clínicos, confidenciales ni de identificación organizacional. Las salidas fueron revisadas comprobando cada referencia contra su fuente primaria y los datos cuantitativos contra los informes de origen. Los prompts, parámetros y registros metodológicamente relevantes están archivados por los autores y disponibles mediante solicitud, salvo información legalmente protegida. Al sistema le correspondió el cribado de fuentes, la derivación de la asimetría entre los indicadores de tiempo, la elaboración de las tablas y la producción del borrador; a los autores, además de la revisión y validación, la definición del tema a partir de la investigación de maestría en curso, la exclusión de un eje temático sin sustento en esa investigación, la anonimización integral del entorno operativo y la validación de la proposición central. Los autores asumen responsabilidad integral por la exactitud, integridad y contenido final del trabajo.

3 - RESULTADOS Y DISCUSIÓN

3.1 La restricción asistencial como propiedad del entorno

La primera contribución trata el costo clínico de la contención como propiedad estructural del entorno, y no como excepción negociada caso por caso.

Tabla 1

Acciones convencionales de contención, riesgo asistencial y alternativas admisibles

Acción convencional	Riesgo en activo de criticidad clínica	Alternativa admisible
Aislamiento de endpoint	Interrupción de una estación en uso asistencial, con pérdida de acceso a informe, prescripción o imagen durante un procedimiento.	Aislamiento selectivo con preservación de rutas hacia servicios clínicos esenciales, o monitoreo reforzado hasta la conclusión del procedimiento.
Revocación de credenciales	Impedimento de acceso a la historia clínica en admisión de urgencia o cambio de turno.	Revocación escalonada, iniciada por sesiones y accesos privilegiados, preservando una credencial de contingencia bajo auditoría.
Cuarentena de segmento	Silenciamiento de la telemetría de monitoreo de pacientes y de la comunicación de equipos asistenciales.	Restricción de conductos mediante lista de permitidos, manteniendo la comunicación prevista en el perfil del dispositivo.
Bloqueo de proceso	Interrupción del software que comanda un equipo en uso clínico.	Bloqueo restringido a activos fuera de uso asistencial, con activación condicionada al estado operativo.
Exploración activa	Comportamiento imprevisible de un dispositivo médico embebido ante un estímulo no previsto por el fabricante.	Descubrimiento pasivo por análisis de tráfico y correlación con base de vulnerabilidades por modelo y versión.
Apagado preventivo	Suspensión de procedimientos y desvío de pacientes.	Degradación controlada con contingencia clínica previamente ejercitada.

Nota. Elaborado por los autores con base en International Organization for Standardization (2022), National Institute of Standards and Technology (2024) y Nelson et al. (2025).

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

Dos observaciones se desprenden. Ninguna alternativa de la columna derecha es gratuita: todas exigen más información sobre el activo y su estado operativo. Aislar un endpoint requiere solo su dirección; aislarlo selectivamente requiere saber cuáles comunicaciones sustentan asistencia en curso. Y esa información no se obtiene durante el incidente: debe estar disponible antes, en el inventario y en la telemetría. La restricción asistencial se convierte en requisito de observabilidad.

3.2 La asimetría entre los tiempos de detección y de respuesta

El tiempo de respuesta comprende el intervalo entre la identificación del incidente y su contención. En un entorno corporativo está limitado por factores organizacionales — disponibilidad de personal, calidad de los procedimientos, grado de automatización — todos susceptibles de mejora mediante inversión. En un entorno asistencial se suma un limitante distinto: la ventana clínica. Si la contención exige que un procedimiento en curso termine, el tiempo de respuesta no puede reducirse por debajo de la duración de ese procedimiento, por madura que sea la operación de seguridad. Ese piso no es ineficiencia a corregir; es la expresión correcta de la prioridad del paciente. El tiempo de detección no tiene un limitante análogo: reducirlo depende de la cobertura de telemetría, de la calidad de la correlación y del contexto de activo — variables bajo control de la organización que no compiten con la asistencia. Un sensor pasivo adicional no interrumpe ninguna cirugía.

La consecuencia práctica invierte la intuición corriente. La lectura habitual del hallazgo de que la automatización reduce el tiempo de contención en 65 días (IBM, 2026) es que los hospitales deben automatizar la respuesta. La correcta bajo restricción asistencial es que deben automatizar solo donde la criticidad clínica lo permite, concentrando la inversión restante en la detección. Cada unidad de tiempo ahorrada en la detección se convierte en ventaja, porque desplaza la contención a un momento en que el conjunto de acciones admisibles todavía es amplio: detectar durante el reconocimiento permite bloquear en el perímetro; detectar tras el cifrado obliga a elegir entre daño clínico y daño informacional.

3.3 Arquitectura de telemetría propuesta

La tercera contribución estructura la cadena de telemetría en siete capas organizadas por punto de decisión: cada una responde a una elección que, si se resuelve mal, compromete las siguientes.

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

Tabla 2

Capas de la arquitectura de telemetría y sus puntos de decisión

Capa	Función	Decisión crítica y requisito clínico
Generación	Emisión de señales por hosts, aplicaciones, red y dispositivos clínicos.	Definir qué instrumentar sin exigir agente en activos que no lo admiten; privilegiar la emisión nativa y la observación de red.
Recolección	Captura mediante agentes, syslog, exportadores de flujo y espejado de tráfico.	Recolección pasiva como estándar en la zona clínica; espejado en lugar de inserción en línea en el camino de datos asistencial.
Transporte	Envío de los datos al punto de consolidación.	Canal cifrado e independiente de la red asistencial, para que la telemetría sobreviva a la degradación del segmento observado.
Normalización	Estandarización de campos y formatos.	Sincronización de tiempo confiable e identificador de activo consistente; sin ello la correlación es ilusoria.
Enriquecimiento	Agregación de contexto de inventario, criticidad y exposición.	Incorporar la criticidad asistencial como atributo distinto de la criticidad técnica.
Correlación	Detección sistémica mediante reglas y comportamiento.	Priorizar por impacto clínico potencial, no solo por severidad técnica.
Presentación	Paneles operativos y activación de la respuesta.	Exponer el estado operativo del activo al analista en el instante de la decisión de contención.

Nota. Elaborado por los autores con base en Kent y Souppaya (2006), Scarfone y Mell (2007), Sridharan (2018) e International Organization for Standardization (2022).

La capa de normalización merece destaque: la correlación entre orígenes distintos depende de un ordenamiento temporal confiable. Si los relojes divergen, la plataforma puede invertir la secuencia de causa y efecto y dejar de reconocer un encadenamiento que ocurrió. La sincronización de tiempo, tratada como detalle de infraestructura, es precondición de la detección sistémica.

3.4 Estratificación de la respuesta por autonomía gobernada

La cuarta contribución resuelve el impasse que lleva a las organizaciones de salud a adquirir plataformas de orquestación y mantenerlas inertes, y que deriva de tratar la automatización como decisión binaria.

Tabla 3

Niveles de autonomía de respuesta y criterios de asignación

Nivel	Comportamiento	Aplicación recomendada
N0 — Observación	Registro y alerta, sin acción sobre el activo.	Dispositivos clínicos en uso asistencial y sistemas de soporte vital, en cualquier hipótesis.
N1 — Acción reversible	Acciones que no interrumpen la función y pueden deshacerse sin efecto residual, como elevación de registro y captura de evidencia.	Cualquier activo, incluso de criticidad clínica máxima.
N2 — Acción bajo aprobación	Contención efectiva condicionada a autorización humana con plazo definido y escalamiento automático.	Activos de criticidad clínica alta fuera de uso asistencial en el momento de la decisión.
N3 — Acción automática	Contención inmediata sin intervención humana, con registro auditable y reversión predefinida.	Activos administrativos y de infraestructura sin dependencia asistencial directa.

Nota. Elaborado por los autores con base en Nelson et al. (2025) y National Institute of Standards and Technology (2024).

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

La asignación de nivel no es estática: depende del estado operativo del activo en el instante del evento. Una estación de quirófano opera en N0 durante un procedimiento y puede operar en N2 fuera de él. Esto exige que el estado asistencial sea una señal de telemetría, y no una información obtenida por teléfono durante el incidente — lo que refuerza el argumento de la subsección 3.1.

3.5 Casos de uso e indicadores propuestos

La quinta contribución reordena los casos de uso de detección por el impacto asistencial, y no por la frecuencia o la facilidad de implementación.

Tabla 4

Casos de uso de detección ordenados por impacto asistencial

Caso de uso	Señales correlacionadas	Consecuencia asistencial evitada
Precursores de ransomware	Comunicación repetitiva con destino externo, alteraciones en mecanismos de recuperación y elevación inusual de la actividad de escritura.	Indisponibilidad simultánea de historia clínica, imagen y laboratorio, con suspensión de procedimientos.
Compromiso de credencial privilegiada	Autenticación fuera del patrón de horario y origen, alteraciones en grupos privilegiados y fallas sucesivas en el segundo factor.	Acceso irrestricto a sistemas clínicos y capacidad de deshabilitar controles.
Desvío de comportamiento de dispositivo clínico	Comunicación con destino o protocolo fuera del perfil establecido para el modelo del dispositivo.	Interferencia en equipo asistencial y propagación desde un activo sin agente.
Movimiento lateral en zona clínica	Accesos anómalos entre estaciones de la misma zona y exploración interna de puertos.	Extensión del compromiso a servicios de soporte a la decisión clínica.
Exfiltración de datos de salud	Volumen de salida atípico, compresión inusual y destino no habitual, correlacionados con acceso a repositorio clínico.	Exposición de datos sensibles de paciente, con consecuencia regulatoria y de confianza.

Nota. Elaborado por los autores con base en MITRE Corporation (2024), Nelson et al. (2025) y van Boven et al. (2024).

El ordenamiento difiere del habitual: la exfiltración, tratada como riesgo principal en la mayoría de las matrices por su consecuencia regulatoria, aparece en último lugar — su consecuencia es patrimonial y reputacional, mientras que las cuatro primeras afectan la capacidad de prestar asistencia. Esa inversión expresa el tratamiento de la continuidad asistencial como propiedad de seguridad en sí.

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

Tabla 5

Indicadores operativos propuestos

Indicador	Definición operativa	Interpretación
Tiempo de detección segmentado por criticidad	Tiempo medio de detección calculado por separado para activos de criticidad asistencial alta y para los demás.	Revela si la cobertura de telemetría acompaña la importancia clínica.
Cobertura de telemetría por zona	Proporción de activos activos que emiten telemetría efectivamente ingerida, calculada por zona.	Mide la fracción de la superficie realmente observada; es el indicador limitante de los demás.
Latencia de la ventana admisible	Intervalo entre la detección y el primer instante en que la contención se vuelve clínicamente aceptable.	Cuantifica el piso de respuesta impuesto por la asistencia y separa la restricción clínica de la lentitud operativa.
Distribución de la respuesta por nivel de autonomía	Proporción de incidentes tratados en cada nivel de N0 a N3.	La concentración en N0 sugiere una plataforma de orquestación adquirida y no utilizada.
Precisión en activos clínicos	Razón entre alertas confirmadas y alertas emitidas, calculada solo para activos de criticidad asistencial alta.	El ruido en esa franja es especialmente dañino, pues induce desconfianza donde la contención es más delicada.

Nota. Elaborado por los autores.

El tercer indicador es el más útil en diálogo con la dirección clínica: separa dos causas frecuentemente confundidas de demora en la contención — la operación de seguridad fue lenta, o la ventana clínica no permitía actuar. Sin esa distinción, toda demora se atribuye al equipo técnico, y la discusión sobre el piso asistencial nunca ocurre.

3.6 Mapeo normativo y discusión

Tabla 6

Mapeo de los componentes del modelo contra referenciales normativos

Componente	ISO/IEC 27001:2022	NIST CSF 2.0	Continuidad
Contexto y criticidad de activos	5.9 Inventario de información y otros activos asociados	Identificar	ISO 22301 — análisis de impacto en el negocio
Arquitectura de telemetría	8.15 Registro de eventos; 8.16 Actividades de monitoreo	Detectar	—
Segmentación por zonas y conductos	8.20 Seguridad de redes; 8.22 Segregación de redes	Proteger	IEC 62443 — zonas y conductos
Respuesta estratificada	5.24 Planificación y preparación de la gestión de incidentes	Responder	ISO 22301 — procedimientos de respuesta
Contingencia clínica y degradación controlada	5.29 Seguridad durante la disrupción	Recuperar	ISO 22301 — estrategias de continuidad
Gobernanza de la autonomía de respuesta	5.2 Roles y responsabilidades	Gobernar	—

Nota. Elaborado por los autores con base en International Organization for Standardization (2022), National Institute of Standards and Technology (2024) e International Electrotechnical Commission (2020). Los identificadores de control deben comprobarse contra el texto íntegro de las normas antes de su uso en un proceso de auditoría.

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

El modelo dialoga críticamente con la literatura de detección, que concentra el esfuerzo en la exactitud de la clasificación, suponiendo que la acción subsiguiente es indiferente al contexto. El entorno hospitalario muestra que no lo es: dos alertas con la misma confianza estadística exigen conductas distintas si una recae sobre un servidor administrativo y la otra sobre la estación que muestra una imagen durante un procedimiento. La exactitud es necesaria e insuficiente.

Un segundo punto se refiere al estatuto de la disponibilidad: la tríada convencional atribuye igual peso a las tres propiedades, pero la inversión se concentra en las dos primeras. Los hallazgos que asocian el ransomware con el aumento de la mortalidad intrahospitalaria (Neprash et al., 2026) sugieren que, en salud, la disponibilidad es aquella cuya violación produce daño irreversible: la confidencialidad violada genera consecuencia grave y reparable; la asistencia interrumpida en condición tiempo-dependiente, no. Un tercer punto es la economía de la defensa: ninguna capa del modelo depende de detección avanzada, pues ampliar la cobertura, calificar el contexto de activo y estratificar la autonomía actúan sobre el conjunto de acciones disponibles, y no sobre la capacidad de distinguir al adversario.

Reconocemos, por último, una tensión no resuelta. El modelo exige que el estado operativo asistencial de cada activo sea una señal de telemetría disponible al analista en el instante de la decisión, y obtener esa señal implica integrar sistemas clínicos y de seguridad, ampliando la interconexión entre entornos que la segmentación recomienda separar. Hay conflicto entre la necesidad de contexto y el principio de segregación. La resolución práctica pasa por transmitir solo el estado — si el activo está o no en uso asistencial — sin contenido clínico, pero el diseño seguro de esa integración permanece abierto.

4 - CONSIDERACIONES FINALES

Este trabajo propuso un modelo de observabilidad y respuesta a incidentes para organizaciones de salud, construido mediante la Design Science Research, en el que la contención está condicionada por la criticidad asistencial del activo afectado.

Caracterizamos la restricción asistencial como propiedad estructural del entorno, mapeando seis acciones de contención contra el riesgo clínico correspondiente e identificando alternativas admisibles, todas dependientes de mayor información previa sobre el activo. Demostramos que el tiempo de respuesta tiene un piso impuesto por la ventana clínica, mientras que el de detección no lo tiene, lo que reorienta la prioridad de inversión. Propusimos una arquitectura de telemetría en siete capas, estratificamos la respuesta en cuatro niveles de autonomía y definimos cinco indicadores, con el mapeo normativo.

La contribución teórica consiste en incorporar el costo clínico de la contención como restricción del problema de detección y en demostrar la asimetría entre los indicadores temporales consagrados. La práctica reside en el modelo y en los indicadores, con destaque para la latencia de

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

la ventana admisible, que separa la demora operativa de la restricción asistencial. Las limitaciones se explicitaron en la metodología, con destaque para la ausencia de evaluación empírica controlada.

Como agenda futura sugerimos cuatro direcciones: la evaluación empírica del modelo en organizaciones de portes distintos, completando el ciclo de la Design Science Research; la investigación del diseño seguro de la integración entre sistemas clínicos y de seguridad para transmitir estado operativo sin contenido clínico; el estudio de la latencia de la ventana admisible como indicador, incluida su distribución por especialidad; y el análisis de las implicaciones regulatorias de la indisponibilidad asistencial en Brasil.

REFERENCIAS

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

Este artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.

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

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 artículo se publica en acceso abierto (Open Access) bajo licencia Creative Commons Attribution 4.0 Internacional (CC-BY), que permite uso, distribución y reproducción irrestrictos en cualquier medio, siempre que el autor original y la fuente sean acreditados.