INSIGHTS DE CIBERSEGURANÇA PARA SETORES NO BRASIL

EDIÇÃO

SETOR DA SAÚDE

heimdall
security research

SUMÁRIO

1. Quando o risco digital ameaça vidas

O setor da saúde tornou-se uma das principais fronteiras da cibersegurança no Brasil. A digitalização de prontuários, exames e sistemas clínicos, combinada ao aumento da interoperabilidade entre hospitais, operadoras e laboratórios, ampliou a superfície de ataque e elevou o risco de incidentes cibernéticos com impacto direto sobre vidas humanas.

De acordo com o **Health-ISAC Q2 2025**, o setor de saúde concentrou **5,8% dos ataques globais de ransomware**, e o **Brasil** apresentou um índice ainda maior: **6,7%**, evidenciando o crescente interesse de grupos de cibercriminosos por esse segmento.

Embora os números pareçam menores que os de setores como tecnologia e manufatura, o **impacto é desproporcional**. Um único ataque pode paralisar atendimentos, comprometer a confidencialidade de dados clínicos sensíveis e gerar prejuízos milionários e irreparáveis à reputação institucional.

O **Heimdall, equipe de Threat Intelligence da ISH,** identificou uma série de vulnerabilidades que vêm sendo exploradas com frequência no setor da saúde — desde **servidores PACS expostos e falhas em protocolos DICOM** até **ataques direcionados de ransomware como Akira, Rhysida e INC,** que utilizam táticas avançadas descritas no **MITRE ATT&CK Framework.**

Neste cenário, a cibersegurança precisa ser tratada como **um pilar estratégico de governança e resiliência,** e não apenas como função técnica de TI. Mais do que proteger dados, é necessário **proteger a continuidade operacional e a confiança dos pacientes.**

Ao longo deste e-book, você encontrará uma leitura analítica sobre **as principais tendências e ameaças mapeadas** pelo Heimdall, contextualizadas com dados globais e recomendações práticas da ISH para apoiar executivos, líderes de TI e gestores hospitalares na construção de uma postura de segurança mais madura e proativa.

2. O setor de saúde no alvo

Um alvo de alto valor e baixa resiliência

A digitalização do setor da saúde criou um ecossistema de inovação que conecta **desde dispositivos médicos até sistemas administrativos complexos**. Essa evolução, no entanto, também abriu portas para uma nova geração de riscos.

Hospitais, clínicas e laboratórios brasileiros estão entre os alvos mais frequentes de ataques de ransomware e exploração de vulnerabilidades — e não apenas pela sensibilidade dos dados, mas pela **impossibilidade de interromper operações críticas sem causar impacto direto em vidas humanas.**

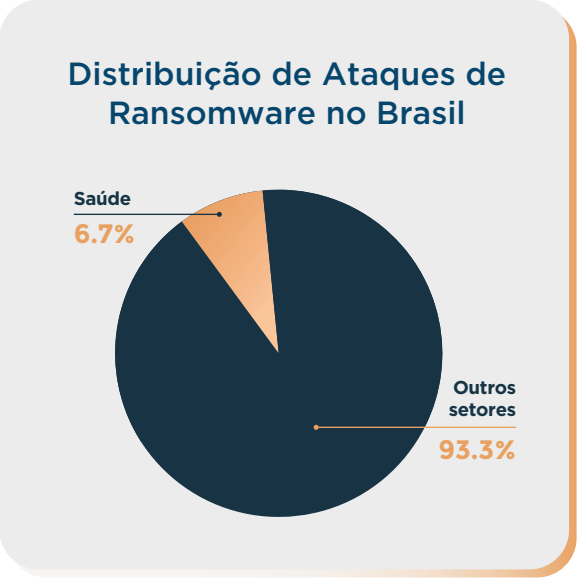


Figura 1 – Distribuição de Ataques de Ransomware no Brasil

Entre janeiro e junho de 2025, o **Heimdall Security Research** registrou **93 ataques de ransomware direcionados à saúde,** equivalentes a **5,8% do total global.** No Brasil, o índice chega a **6,7%**, posicionando o país **acima da média mundial** e entre os focos regionais mais relevantes da América Latina.

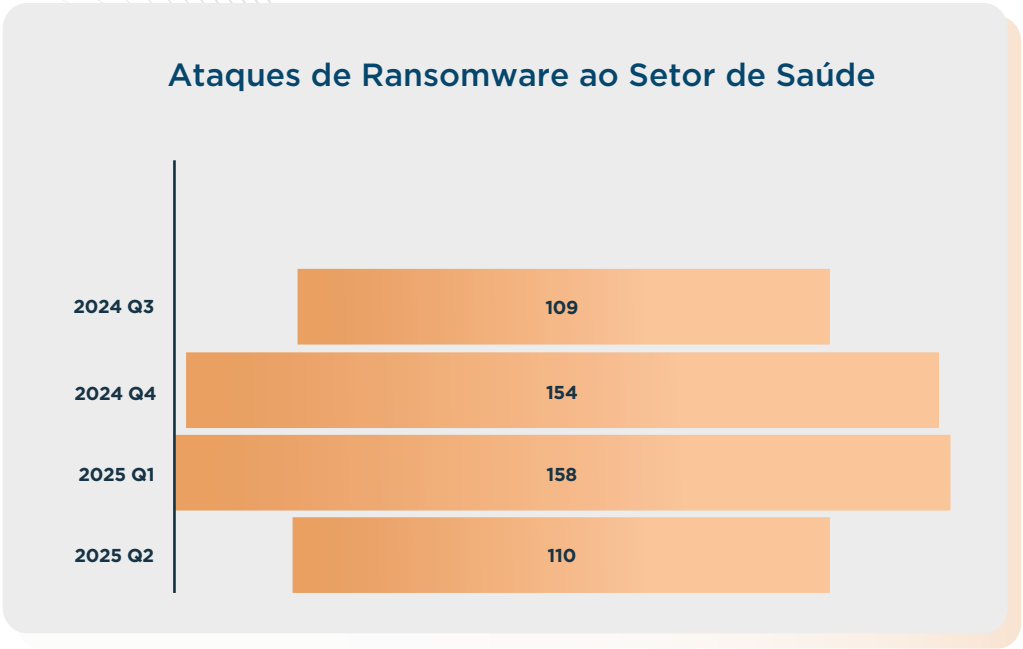


Figura 2 – Distribuição de ataques de ransomware no Brasil (Q1–Q2 2025)

Mesmo com uma leve oscilação no número total de incidentes, o relatório aponta **mudança na natureza dos ataques:** eles estão mais direcionados, com foco em **alvos críticos e interconectados** — sistemas hospitalares que centralizam diagnósticos, agendamentos e comunicação entre equipes médicas.

Por que o setor é tão vulnerável

A atratividade do setor de saúde para ofensores digitais vem de um conjunto de fatores técnicos, operacionais e humanos que tornam esse ecossistema um dos mais lucrativos e frágeis do mundo cibernético.

1. Alta dependência de sistemas críticos: hospitais operam 24x7 com dezenas de aplicações integradas, desde prontuários eletrônicos e laboratórios até sistemas de faturamento e regulação. Uma falha em um único ponto pode paralisar toda a operação.

2. Valor elevado dos dados médicos: no submundo digital, **credenciais e acessos hospitalares são vendidos entre US$ 1.200 e US$ 20.000**, dependendo do tamanho da rede e da sensibilidade dos dados. Esses pacotes geralmente incluem credenciais administrativas, IPs internos e registros de pacientes.

3. Infraestrutura legada e sistemas obsoletos: equipamentos médicos que não recebem atualizações, servidores PACS (Picture Archiving and Communication System) expostos e DNS vulneráveis (Dangling DNS) continuam sendo brechas críticas.

4. Interdependência entre áreas clínicas e TI: a falta de integração entre times técnicos e assistenciais dificulta respostas rápidas e coordenadas a incidentes. A segurança é muitas vezes vista como obstáculo, não como parte essencial da operação.

5. Engenharia social e ataques direcionados: criminosos utilizam doxxing e campanhas de phishing personalizadas, explorando perfis de profissionais de saúde e executivos para obter credenciais e aplicar golpes de extorsão.

As brechas mais exploradas

O relatório evidencia que a maior parte das violações observadas no setor deriva de vulnerabilidades conhecidas e negligenciadas, muitas vezes associadas à manutenção precária e à falta de segmentação entre redes clínicas e corporativas.

Entre os vetores mais comuns:

- **Dangling DNS:** redirecionamentos indevidos de tráfego, explorados para ataques de phishing e roubo de credenciais.

- **PACS/DICOM expostos:** acesso não autenticado a imagens e dados sensíveis de pacientes.

- **Dispositivos IoT sem proteção:** equipamentos hospitalares conectados sem criptografia, com firmware desatualizado e sem controle de acesso.

- **Phishing e credenciais comprometidas:** o vetor inicial mais frequente, responsável por abrir caminho para ataques de ransomware e movimentação lateral.

Essas brechas se mantêm não apenas por falhas tecnológicas, mas **pela ausência de governança robusta e de práticas integradas de gestão de risco**. Em muitos casos, políticas de atualização e controle de acesso ficam subordinadas a contratos de fornecedores, dificultando respostas rápidas.

O custo da exposição

A consequência dessa fragilidade é clara e mensurável. Em **agosto e setembro de 2024**, incidentes de ransomware em grandes hospitais brasileiros **paralisaram atendimentos por mais de 48 horas**, interromperam cirurgias e expuseram milhares de prontuários.

O dano financeiro é apenas parte da equação; o impacto reputacional e o risco à vida dos pacientes são **incalculáveis**. Além dos prejuízos diretos, essas violações ampliam custos com resposta a incidentes, notificações regulatórias e ações judiciais, tornando a **saúde um dos setores com maior custo médio por violação de dados,** segundo estimativas globais.

A saúde está no epicentro das ameaças cibernéticas. Não há neutralidade possível. Instituições que não priorizam segurança tornam-se parte da estatística. A única estratégia viável é a antecipação: **visibilidade total dos ativos, controle rigoroso de acessos, segmentação de redes e integração entre defesa e operação clínica.**

3. Panorama de ameaças e tendências

O panorama atual revela que o setor da saúde segue no centro das operações cibercriminosas, especialmente com foco em **ransomware, vazamento de dados médicos e exploração de dispositivos conectados.** As estatísticas do Heimdall CTI mostram uma atuação coordenada de grupos conhecidos internacionalmente, com alto grau de especialização e técnicas que combinam **invasão, persistência e extorsão múltipla.**

Ransomware: a principal ameaça à saúde digital

No segundo trimestre de 2025, o **ransomware continuou sendo o vetor mais ativo** de ataques contra o setor. Entre os grupos mais atuantes, destacam-se **Akira, Rhysida, INC Ransom e Arcusmedia,** todos com histórico de atuação no Brasil.

Essas quadrilhas exploram **falhas conhecidas em sistemas legados e configurações inseguras** de infraestrutura hospitalar, aproveitando-se da dependência crítica de continuidade operacional.

O modus operandi permanece focado na **dupla ou tripla extorsão**, combinando criptografia, exfiltração de dados e ameaça de divulgação pública; um modelo que transforma cada incidente em crise operacional, reputacional e jurídica.

De acordo com a análise, **grupos como:**

Akira e Rhysida concentram esforços em **ataques direcionados a hospitais e clínicas de grande porte.**

Enquanto INC e Arcusmedia mantêm estratégias mais pulverizadas, visando tanto entidades públicas quanto privadas.

Esses ataques não apenas interrompem serviços essenciais, mas também **exibem o valor estratégico do setor da saúde como alvo:** a impossibilidade de suspender atendimentos críticos aumenta a pressão para o pagamento de resgates e acelera a tomada de decisão por parte das vítimas.

IoT e dispositivos médicos: a nova superfície de ataque

A digitalização dos hospitais expôs um novo vetor crítico: **os dispositivos médicos conectados (IoT)**. Bombas de infusão, monitores, respiradores e servidores PACS (Picture Archiving and Communication System) — todos elementos essenciais ao atendimento médico — **têm sido conectados diretamente à internet**, muitas vezes sem autenticação, criptografia ou segmentação adequada.

O relatório aponta falhas recorrentes, como:

- **Interfaces web sem autenticação** ou com credenciais padrão ativas;
- **Protocolos obsoletos** (HTTP, VNC, Telnet) ainda em uso;
- **Integrações vulneráveis** com sistemas HIS e RIS;
- **Portas críticas expostas**, como 104, 5800, 5900 e 3389;
- **Configurações incorretas** em servidores de imagem e prontuários eletrônicos.

Ferramentas como o **Shodan** facilitam a localização desses dispositivos, permitindo que qualquer atacante identifique equipamentos médicos expostos com termos simples como “PACS” ou “DICOM”.

Essa negligência técnica cria **um elo direto entre vulnerabilidade operacional e risco à vida humana**, uma vez que o comprometimento de equipamentos clínicos pode afetar diagnósticos e procedimentos em tempo real.

Exposição de servidores PACS e DICOM no Brasil

A pesquisa identificou **centenas de servidores PACS acessíveis publicamente**, contendo imagens e dados sensíveis de pacientes.

São Paulo lidera o ranking nacional de exposição, seguida por cidades como Araçatuba, Brasília, Campinas e São José do Rio Preto, todas com forte presença hospitalar.

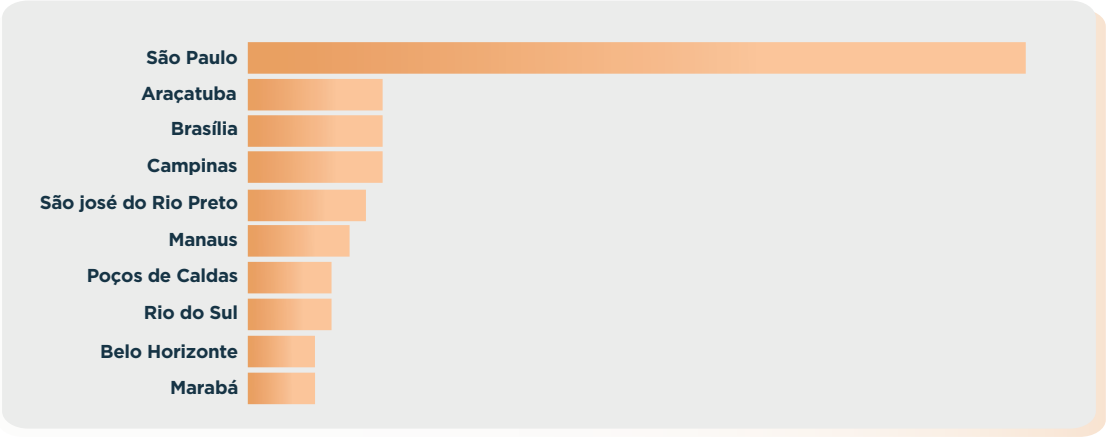


Figura 3 – Top 3 cidades brasileiras com servidores PACS expostos online

Esses sistemas, ao armazenarem exames e laudos, tornam-se **alvos ideais para roubo de dados e chantagem**, ampliando o mercado negro de informações médicas.

A falta de segmentação de rede e de autenticação forte ainda permite que atacantes **se movimentem lateralmente entre sistemas clínicos e administrativos**, explorando brechas em infraestrutura híbrida (local e em nuvem).

Impacto ampliado e implicações estratégicas

A cibersegurança na saúde ultrapassou o limite do tecnológico e se tornou **questão de resiliência institucional e segurança pública.** Hospitais e clínicas estão expostos a **interrupções operacionais, perda de dados sensíveis e danos reputacionais.**

Combinado à pressão de regulamentações como a **LGPD** e à escassez de equipes especializadas, o cenário exige que a **cibersegurança seja tratada como pilar estratégico**, sustentada por inteligência de ameaças, monitoramento contínuo e resposta integrada a incidentes.

4. Como os atacantes operam: ciclo, táticas e vetores explorados

Os grupos **Akira, Rhysida** e **INC** estão entre os mais ativos no Brasil, conduzindo ataques de **ransomware com dupla extorsão,** combinação entre criptografia de dados e ameaça de vazamento público.

Esses ataques exploram um cenário conhecido: **sistemas legados, equipamentos médicos conectados, redes expostas e falhas de atualização.** O resultado é uma superfície de ataque extensa e difícil de proteger.

Ciclo do ataque

O processo geralmente segue cinco etapas principais:

1 Acesso inicial

Exploração de vulnerabilidades conhecidas, phishing e credenciais comprometidas em portais públicos (VPN, Citrix, NetScaler).

2 Execução e persistência

Uso de scripts PowerShell e ferramentas legítimas (Living off the Land) para evitar detecção.

3 Movimentação lateral

Exploração de RDP, SMB e ferramentas administrativas para alcançar servidores críticos.

4 Exfiltração

Extração silenciosa de dados clínicos e administrativos antes da criptografia.

5 Impacto e extorsão

Criptografia em larga escala e pressão por pagamento, com risco adicional de exposição pública dos dados.

Táticas mais usadas (MITRE ATT&CK)

FASE	TÉCNICA PREDOMINANTE	FREQUÊNCIA OBSERVADA	IMPACTO DIRETO
Initial Access	Exploração de CVEs (Citrix/NetScaler) e phishing	27,9%	Invasão de sistemas expostos
Execution	PowerShell e macros automatizadas	25,4%	Instalação de ransomware
Credential Access	Dumping de senhas e hashes	13,9%	Controle administrativo completo
Persistence	Ferramentas de acesso remoto	11,8%	Manutenção de acesso mesmo após limpeza
Exfiltration	Upload para nuvem e túneis criptografados	7,3%	Vazamento de dados sensíveis

Essas técnicas permitem **ataques rápidos, silenciosos e de alto impacto,** explorando o intervalo entre o comprometimento e a detecção.

Padrões críticos observados

• **Reaproveitamento de CVEs conhecidas:** vulnerabilidades antigas continuam exploradas por falhas de patching em ambientes críticos.

• **Uso de ferramentas legítimas:** softwares como AnyDesk, Ngrok e WinSCP ajudam a disfarçar o tráfego malicioso.

• **Ataques a dispositivos IoT e PACS:** sistemas de imagem e monitoramento com autenticação fraca ampliam a superfície de ataque.

• **Exploração humana:** pressão, urgência e engenharia social aceleram decisões inseguras.

Os ataques ao setor de saúde não são apenas técnicos, **são operacionais e humanos.** Os invasores conhecem as vulnerabilidades de sistemas críticos e exploram a **falta de tempo, de integração e de governança** das equipes.

Proteger hospitais e operadoras exige **visibilidade, automação e resposta coordenada** — três pilares que precisam estar conectados desde a borda até o dado sensível do paciente.

5. Impactos reais: cibersegurança como questão de continuidade e confiança

A cibersegurança na saúde é um **fator determinante para a continuidade dos serviços e a proteção da vida humana**. Os dados analisados mostram que cada incidente no setor representa uma interrupção direta em atividades críticas e uma ameaça real à integridade dos pacientes e da operação.

Entre janeiro e junho de 2025, o **Brasil registrou 11.426 violações de segurança, sendo 97 incidentes confirmados com impacto direto**. Embora o número total pareça pequeno diante de outros segmentos, o **nível de severidade** é o que chama atenção: sistemas paralisados, prontuários expostos e serviços interrompidos por dias.

Esses eventos mostram que o impacto dos crimes digitais na saúde **é desproporcional ao volume de ataques** e seus efeitos se multiplicam em escala humana e financeira.

O preço da pausa: custos operacionais invisíveis

Ataques de **ransomware** e intrusões em sistemas clínicos essenciais têm provocado **interrupções que variam de 72 horas a mais de 10 dias**, afetando diretamente o atendimento médico. Cada minuto de indisponibilidade representa diagnósticos atrasados, cirurgias canceladas e pacientes sem acesso a cuidados críticos.

Além disso, as instituições precisam lidar com o **reagendamento de procedimentos**, o desgaste de imagem e o estresse das equipes clínicas que operam sob contingência.

O resultado é um cenário de vulnerabilidade operacional que reforça a necessidade de **planos de resposta estruturados e testes regulares de continuidade.**

A conta que não aparece no balanço: prejuízo financeiro e moral

Os custos de uma violação no setor de saúde são os mais altos entre todos os segmentos da economia. Em **2024**, o **custo médio global por incidente chegou a US$ 9,23 milhões**, mais que o dobro da média geral.

No Brasil, observamos que as instituições afetadas enfrentaram:

Esses custos diretos são agravados por perdas intangíveis, como **interrupção de faturamento, evasão de pacientes** e a necessidade de **reconstruir a confiança** de investidores e conselhos.

A **confiança** é o ativo mais valioso na saúde e também o mais frágil diante de um incidente de cibersegurança. Segundo o **Gartner (2025), 81% dos consumidores deixariam de contratar ou utilizar serviços de uma empresa após uma falha grave de segurança.**

Para hospitais e clínicas, esse dado é alarmante. Um ataque que expõe **dados de pacientes, históricos médicos e diagnósticos** afeta diretamente a credibilidade e pode gerar **danos irreversíveis à reputação institucional.**

Além da dimensão pública, há o dilema ético: **cada prontuário vazado representa uma violação à privacidade individual e uma ameaça à dignidade humana.**

Da interrupção à tragédia: o limite da resiliência hospitalar

O impacto humano é o ponto mais crítico. Em **2020**, o **Hospital Universitário de Düsseldorf (Alemanha)** foi vítima de ransomware que **interrompeu o acesso a sistemas clínicos**, levando à morte indireta de uma paciente que precisou ser transferida.

No **Brasil**, episódios registrados entre **agosto e setembro de 2024** em grandes redes hospitalares também paralisaram operações e expuseram milhares de prontuários.

Esses casos reforçam uma mensagem central: **a cibersegurança hospitalar não é uma pauta de TI, é uma pauta de saúde pública**. Garantir resiliência digital é proteger a vida, a confiança e a sustentabilidade das instituições de saúde.

6. Da prevenção à resiliência: o caminho para a maturidade cibernética na saúde

A cibersegurança no setor da saúde não se limita mais à prevenção de incidentes — ela se tornou um fator crítico de **continuidade de negócios, confiança pública e governança institucional.**

A pergunta já não é "como evitar o ataque", mas "como garantir que o hospital continue funcionando quando ele ocorrer".

A nova lógica da proteção

Em um ambiente onde a disponibilidade salva vidas, **resiliência** é a métrica mais importante. A maturidade cibernética de uma instituição de saúde depende de três dimensões complementares:

Visibilidade completa do ambiente digital

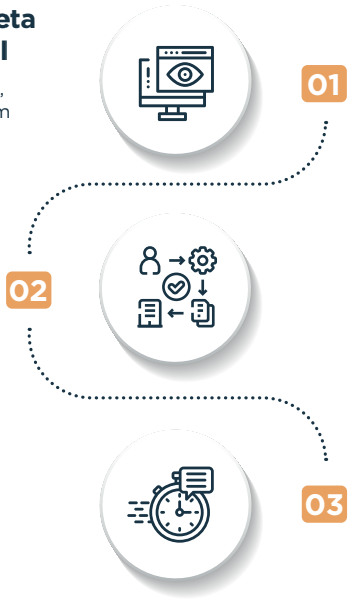
saber o que está conectado, onde estão os dados e quem tem acesso.

Integração entre times e processos

segurança, infraestrutura, TI clínica e compliance operando de forma coordenada.

Capacidade de resposta rápida e documentada

processos testados para detectar, conter e restaurar operações críticas.



Essa abordagem transforma a cibersegurança de um gasto reativo em um **ativo estratégico**, capaz de proteger pacientes, reputação e receita.

Maturidade em evolução: do controle ao contexto

Hospitais e operadoras que evoluíram em maturidade cibernética adotam uma visão contextual da segurança: não se trata apenas de monitorar ameaças, mas de entender **quais ativos sustentam a missão clínica e quais riscos realmente paralisam a operação.**

Modelos como o **Zero Trust** e o **Defense in Depth** são eficazes quando aplicados de forma inteligente, priorizando:

• **Identidade como perímetro:** autenticação forte, gestão de privilégios e rastreabilidade de acessos.

• **Segmentação inteligente:** separação de redes administrativas, clínicas e de pesquisa.

• **Telemetria unificada:** integração entre EDR, NDR e SIEM para reduzir tempo de resposta.

• **Automação com supervisão humana:** uso de IA e SOAR para correlacionar alertas e acelerar triagem.

Da reação à antecipação

Dados do **Heimdall** mostram que 63% dos ataques ao setor de saúde foram detectados **após o início da exfiltração**, indicando que o monitoramento ainda é majoritariamente reativo.

A transição para um modelo proativo exige:

• **Threat Intelligence aplicada ao negócio:** correlacionar indicadores técnicos com impacto clínico e financeiro.

• **Simulações periódicas de crise (tabletop tests):** avaliar tempo de resposta e capacidade de decisão executiva.

• **Planos de continuidade integrados à segurança:** definir prioridades de restauração baseadas na criticidade do serviço — UTI, sistemas de diagnóstico e agendamentos.

O papel da liderança executiva

A resiliência digital é uma decisão de liderança. Enquanto a área técnica executa, é o board quem define se a organização está preparada para operar sob ataque. Empresas maduras integram **cibersegurança à governança corporativa**, com indicadores de risco reportados junto a métricas financeiras e operacionais.

A adoção de frameworks como **NIST CSF 2.0** e **ISO 27001:2022** tem permitido que líderes priorizem investimentos baseados em risco real e não em percepções ou pressões momentâneas.

7. Da ameaça à oportunidade de evolução

O setor da saúde vive um momento decisivo. A conectividade, que impulsiona eficiência e inovação, também expôs o sistema a riscos que ultrapassam o campo digital. **Atingem vidas, reputações e a confiança pública.**

Hospitais, operadoras e laboratórios que tratam a segurança como parte da estratégia — e não como uma área isolada de TI — alcançam níveis superiores de **continuidade e previsibilidade.**

A maturidade cibernética não se constrói com ferramentas isoladas, mas com **contexto, visibilidade e coordenação.** É preciso entender o ambiente clínico, as dependências críticas e os impactos de cada decisão, conectando tecnologia, pessoas e processos sob uma mesma visão: **proteger para continuar operando.**

O papel da ISH nesse cenário

Combinando **inteligência de ameaças (Heimdall), operações avançadas de segurança (SOC e MSS) e consultoria estratégica**, a ISH apoia o setor da saúde a evoluir de um modelo reativo para um modelo resiliente.

A atuação integrada da ISH envolve:

- **Monitoramento contínuo de vulnerabilidades em ambientes ICS/OT e clínicos.**
- **Avaliação de maturidade e priorização de riscos com base em impacto real.**
- **Implementação de estruturas de Zero Trust e segmentação segura.**
- **Resposta rápida e coordenada a incidentes, com equipes especializadas 24/7.**

Essa combinação de **tecnologia, metodologia e experiência** permite que instituições hospitalares mantenham a confiança dos pacientes e a estabilidade de suas operações, mesmo sob pressão de ameaças emergentes.

Próximo passo: fortalecendo a resiliência do seu ambiente

A **ISH** coloca sua experiência técnica e estratégica à disposição das organizações que desejam **transformar dados em inteligência e risco em vantagem competitiva.**

heimdall
security research

Fale com nossos especialistas

E descubra como aplicar os insights deste relatório no contexto do seu hospital, laboratório ou operadora.

Agende uma avaliação de maturidade e veja onde estão as lacunas que comprometem sua continuidade digital.