Cibersegurança e Ciberresiliência em Saúde: prevenção em primeiro lugar

Ana Sofia Novo Oliveira [1,2,3]

[1] Médica Assistente de Medicina Geral e Familiar, ULS Santo António
[2] Pós-graduada em Saúde Digital pelo ISAG
[3] Presidente da Direção AIMGF 2024/2025, Presidente da Assembleia Geral AIMGF 2026/2027

A digitalização dos sistemas de saúde representa uma das transformações mais profundas da medicina contemporânea. Em Portugal, o Serviço Nacional de Saúde (SNS) tem investido progressivamente na modernização das plataformas digitais, com avanços ao nível da partilha de informação clínica, no acesso dos cidadãos aos seus dados de saúde e à utilização de serviços de telemedicina. Contudo, esta evolução tecnológica traz consigo uma responsabilidade acrescida que, a julgar pelos acontecimentos recentes, não se encontra salvaguardada: a de garantir que os sistemas são seguros, resilientes e dignos da confiança que os utentes neles depositam.

Segundo o Centro Nacional de Cibersegurança (CNCS), Portugal registou em 2024 um total de 2.758 incidentes de cibersegurança, traduzindo um aumento de cerca de 36% face ao ano anterior, sendo esta uma realidade sucessivamente crescente desde 2019[1]. O setor da saúde constitui um dos alvos preferenciais, por ser considerada uma infraestrutura crítica a partir da qual qualquer incidente poderá resultar em consequências severas. A vulnerabilidade a estes ataques prende-se com vários fatores, nomeadamente a desatualização dos sistemas informáticos, a utilização inadequada dos gestores de credenciais de acesso e ainda o conhecimento escasso relativo a matérias de cibersegurança por parte das organizações de saúde. A esta realidade não é alheio o contexto geopolítico internacional, em relação ao qual diariamente constatamos uma situação de instabilidade sem precedentes.

Os últimos ciberataques ocorridos em instituições de saúde são diversos e de gravidade crescente. Em 2022, o Hospital Garcia de Orta e o Hospital do Litoral Alentejano sofreram ataques que comprometeram os seus sistemas de forma significativa[2]. Em 2023, o ciberataque ao SESARAM afetou simultaneamente três hospitais e 47 centros de saúde da Região Autónoma da Madeira[3]. Mais recentemente, em maio de 2026, foi reportado um acesso indevido a dados pessoais de mais de 100.000 utentes do SNS através do Portal SNS24, num caso que envolveu a Polícia Judiciária e o Ministério Público para investigação deste crime informático, que partiu de um roubo de identidade e credenciais e cujas consequências ainda não são conhecidas mas que se presumem graves de acordo com o Bastonário da Ordem dos Médicos[4].

Esta não é, contudo, nenhuma novidade para a comunidade científica. Em 2014, um artigo publicado no *New England Journal of Medicine* alertava para o facto de 94% das instituições de saúde terem reportado terem sido vítimas de ciberataques, identificando quatro categorias principais de incidentes: perda de dados, roubo financeiro, ataques a dispositivos médicos e ataques à infraestrutura crítica[5]. Os dispositivos médicos, nomeadamente equipamentos de monitorização dos doentes ou sistemas de infusão de medicação, representam potenciais meios para um ataque com impacto direto na segurança clínica dos utentes. Por este motivo, a Assembleia Médica Mundial declarou formalmente que os ciberataques a sistemas de saúde e outras infraestruturas críticas constituem uma ameaça à saúde pública[6].

Para melhor compreendermos a dimensão deste tipo de problemas e as consequências de um ataque massivo a um sistema nacional de saúde, vale a pena olhar para o caso irlandês. Em maio de 2021, o *Health Service Executive* (HSE) — o equivalente irlandês do SNS — foi vítima de um ataque de *ransomware* por parte de um grupo criminoso, tendo este sido considerado o maior ataque alguma vez perpetrado contra um serviço de saúde nacional[7]. O ataque teve início oito semanas antes da sua ativação, quando um funcionário abriu, através da sua conta institucional, um ficheiro malicioso num *e-mail* de *phishing*[8]. Uma vez

dentro do sistema, os atacantes lentamente percorreram a rede, comprometendo 70.000 dispositivos e 52 hospitais, encriptando mais de 80% dos dados do HSE[9]. O impacto foi imediato e devastador: o número de consultas de certas especialidades caiu de forma abrupta, os profissionais foram forçados a regressar aos registos em papel, os laboratórios passaram a processar análises manualmente e os sistemas de imagiologia, obstetrícia e oncologia ficaram inoperacionais durante semanas[10]. A recuperação demorou mais de 4 meses, tendo acarretado um custo estimado superior a 500 milhões de euros (muito superior ao resgate de 16,5 milhões de euros exigido pelos atacantes, e que o HSE recusou pagar)[7]. Este caso exemplifica e reforça a necessidade urgente da criação de sistemas de defesa a ataques informáticos. Neste caso, a política de segurança do HSE datava de 2013, estando, como tal, desatualizada, não tendo sido capaz de bloquear a entrada do ficheiro malicioso no momento do ataque[8].

As consequências destes ataques ultrapassam largamente a escala habitualmente imaginada. Na dimensão dos direitos fundamentais, o impacto é particularmente grave: os dados de saúde são, por natureza, informação de caráter pessoal e sensível. O seu acesso não autorizado, a sua comercialização ou a sua utilização para fins desconhecidos pode afetar a vida das pessoas de formas que vão muito além do momento do ataque, por períodos de tempo prolongados. E, ao contrário do que acontece com outros dados, não é possível "alterar o historial clínico" para que este deixe de ser utilizado.

É neste sentido que se definem como cruciais os conceitos de **cibersegurança** e **ciberresiliência**, que devem constituir uma prioridade estratégica. A cibersegurança pode ser definida, de acordo com a norma ISO/IEC 27032, como a "preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço", traduzindo-se no conjunto de práticas, tecnologias e processos destinados a proteger sistemas, redes e dados contra ataques, danos ou acessos não autorizados[11]. A ciberresiliência, por sua vez, é um conceito complementar distinto: segundo o *National Institute of Standards and Technology* (NIST), trata-se da capacidade de uma organização antecipar, resistir, recuperar e adaptar-se perante condições adversas, ataques ou compromisso dos seus sistemas de informação[12]. Se a cibersegurança é o esforço de manter a ameaça afastada, a ciberresiliência é a capacidade de detetar e combater a ameaça, e ainda de recuperar quando se concretiza o ataque. No setor da saúde, esta distinção é fundamental: não basta proteger os sistemas; é necessário garantir que, perante um incidente, os cuidados aos doentes não ficam comprometidos.

Alcançar este nível de resiliência exige planos de segurança estruturados e previamente testados, equipas com formação específica, protocolos claros de comunicação — com as autoridades competentes, com os profissionais e com os próprios utentes afetados — e uma cultura organizacional na qual a cibersegurança não é vista como um custo adicional, mas sim como uma componente essencial da qualidade e da segurança dos cuidados. A sensibilidade dos dados de saúde torna essencial uma abordagem integrada e alinhada com as normas nacionais e europeias.

Neste contexto, é impossível ignorar o papel crescente da inteligência artificial (IA) e dos sistemas digitais na saúde, que prometem uma melhoria no diagnóstico, personalização terapêutica, deteção precoce de doenças, otimização de recursos, etc. No entanto, a sua implementação assenta sobre esta mesma infraestrutura digital vulnerável, utilizando os dados de saúde (descritos como sensíveis) para o seu processamento. A este respeito, o AI Act, em vigor na União Europeia desde 2024, estabelece obrigações concretas para sistemas de IA de alto risco na área da saúde, incluindo o estabelecimento de avaliações de risco e proteção reforçada[13]. Adotar estas tecnologias sem garantir a segurança da informação que as sustenta seria altamente ineficiente.

A solução não é, portanto, travar a inovação, mas sim garantir que ela é utilizada de forma responsável. Isso exige uma liderança organizacional comprometida, investimento adequado (incluindo a nível de recursos humanos e que não pode depender apenas da resolução de problemas informáticos do dia-a-dia de um profissional de saúde), formação contínua de todos os profissionais (reconhecendo o fator humano como crítico para a segurança da informação), e, por fim, regulamentação que acompanhe a velocidade da transformação tecnológica. A regulamentação existente a nível europeu estabelece um patamar mínimo de exigência em termos de obrigações[13,14]. Cumpri-las não é um exercício burocrático: é o mínimo ético exigível a quem tem a responsabilidade de guardar informação crítica de milhões de pessoas.

Enquanto médicos que conhecem bem os utentes, sabemos que a confiança é o alicerce de cada consulta, de cada diagnóstico partilhado, de cada decisão terapêutica tomada em conjunto. Essa confiança estende-se, inevitavelmente, ao sistema de informação que regista e transporta essa relação. Protegê-la é, também, por isso, um ato de cuidado.

REFERÊNCIAS BIBLIOGRÁFICAS:

1- Centro Nacional de Cibersegurança (CNCS). Relatório de Cibersegurança — Riscos & Conflitos, 6.ª edição. Portugal, setembro de 2025. Disponível em: https://www.cncs.gov.pt
2- WeLiveSecurity / ESET. Ataques cibernéticos atingem hospitais em Portugal [Hospital Garcia de Orta e Hospital do Litoral Alentejano]. Abril de 2022. Disponível em: https://www.welivesecurity.com/br/2022/04/27/ataques-ciberneticos-atingem-hospitais-em-portugal/
3- Sábado. Hospitais na mira dos hackers. Mais de 4 mil ataques à saúde nos últimos seis meses. Agosto de 2023. Disponível em: https://www.sabado.pt
4- CNN Portugal / Público. Acesso indevido a dados do SNS atingiu mais de 100.000 vítimas de todo o país. Maio de 2026. Disponível em: https://cnnportugal.iol.pt
5- Perakslis ED. Cybersecurity in Health Care. N Engl J Med. 2014;371(5):395–397. DOI: 10.1056/NEJMp1404358
6- Zelmer J. Cybersecurity in Health: A 21st-Century Imperative [Editorial]. Healthcare Policy. 2018;13(4):6–7. [Inclui referência à: World Medical Assembly. WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure. Taipei, 2016.]
7- Clark Hill PLC. The HSE Cyberattack: Lessons Learned. 2022. Disponível em: https://www.clarkhill.com/news-events/news/the-hse-cyberattack-lessons-learned/
8- Panaseer. What does the Irish health service ransomware attack tell us about security controls? 2022. Disponível em: https://panaseer.com
9- SharkStriker. Ransomware attack on HSE Ireland — Health Service Executive explained. 2025. Disponível em: https://sharkstriker.com
10- BBC News. Cyber-attack on Irish health service 'catastrophic'. Maio de 2021. Disponível em: https://www.bbc.com/news/world-europe-57184977
11- ISO/IEC 27032:2023. Information technology — Cybersecurity — Guidelines for Internet security. International Organization for Standardization. Disponível em: https://www.iso.org/standard/27032
12- National Institute of Standards and Technology (NIST). Cyber Resiliency Engineering Framework — NIST SP 800-160, Vol. 2 Rev. 1. 2021. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final
13- European Commission. AI Act — Regulation on Artificial Intelligence. Em vigor desde 2024. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
14- European Parliament. Diretiva NIS2 (2022/2555) relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União. 2022. Disponível em: https://eur-lex.europa.eu