JANEIRO FEVEREIRO MARÇO 2022
Edição Trimestral
Nº 28

GESTÃO HOSPITALAR

DISTRIBUIÇÃO GRATUITA

APAH ASSOCIAÇÃO PORTUGUESA DE ADMINISTRADORES HOSPITALARES

TESTEMUNHO:
4 DÉCADAS DE ASSOCIATIVISMO

CIBERSEGURANÇA:
REFLEXÕES SOBRE O SISTEMA NACIONAL DE SAÚDE

CAMINHO DOS HOSPITAIS:
UM ROTEIRO PARA A INCLUSÃO E PROXIMIDADE

40 ANOS APAH

Cerimónia de distinção novos Sócios de Mérito APAH

OLHAR A HISTÓRIA, CONSTRUIR O FUTURO

CIBERSEGURANÇA: REFLEXÕES SOBRE O SISTEMA NACIONAL DE SAÚDE

António Carlos Coelho
CEO C3+ Consulting

João Figueiredo
GLINTT Diretor Mercado Healthcare

Ricardo Luz
Partner da Gestluz Consultores

Sérgio Rocha
Tenente-Coronel Exército Português

A transformação digital em marcha tem alavancado o desempenho das organizações, através da utilização das tecnologias, e repercutindo-se particularmente na concorrência e na criação de valor em todos os setores. Para além dos efeitos no desempenho, esta transformação gera também condições favoráveis ao surgimento de novas ameaças e riscos, contra os quais deverão ser implementadas medidas de mitigação adequadas. A cibersegurança adquire um papel de destaque neste âmbito, uma vez que procura garantir a estabilidade das infraestruturas críticas de informação, através da proteção dos sistemas de computadores e redes, e contra roubos de informação, danos no *hardware* e *software*, e disrupção dos serviços que suportam.

Para resistirem aos crescentes ataques e à exploração de novas vulnerabilidades, as organizações procuram desenvolver e manter estruturas cada vez mais resilientes, capazes de identificar, prevenir, detetar, responder e recuperar ou minimizar os danos.

O **Sistema Nacional de Saúde**, que abrange todos os sistemas de informação na saúde e respetivas infraestruturas, públicas, privadas e sociais, coabita com este processo de transformação digital e, à semelhança de muitos outros sistemas, está exposto aos novos riscos e ameaças.

Para além das mudanças ao nível digital impulsionadas pela tecnologia, a situação pandémica causou instabilidade financeira e incerteza de mercado para a maioria dos setores da indústria, facto que poderá aprofundar desigualdades e gerar ruturas. Se por um lado, alguns países estão a aumentar proactivamente a sua cooperação global, estabelecendo processos de transformação e transição digital de forma integrada e holística, através das respetivas estratégias de Defesa e Segurança Nacional, e avaliando continuamente as infraestruturas críticas, outros estão ou poderão ficar irremediavelmente para trás neste jogo global. As crescentes tensões sociais seguramente terão fortes implicações nas áreas da saúde, pelo que pretendemos neste trabalho alertar os decisores e órgãos de gestão do Estado Português sobre desenvolvimentos potenciais, com impacto estratégico significativo nas infraestruturas críticas da saúde, enquanto ainda é possível agir de forma preventiva ou até mesmo evitá-los.

Infraestruturas críticas em Portugal - o caso do Sistema Nacional de Saúde

Considera-se "Infraestrutura Crítica" a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico e social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções" (MDN, 2011).

As infraestruturas estabelecem interdependências que, de acordo com Rinaldi *et al.* (2001, p.14), consistem em relações bidirecionais entre duas infraestruturas através das quais o estado de cada uma influencia ou está correlacionado com o estado da outra. Estas interdependências podem ser físicas, cibernéticas, geográficas e lógicas (o estado de cada infraestrutura depende de um mecanismo que não é uma ligação física, cibernética ou geográfica).

A ameaça do terrorismo e criminalidade internacional e o crescente número de desastres naturais constituem um desafio crescente para a proteção das infraestruturas críticas de um país. Se pensarmos nas telecomunicações, em que um ataque cibernético pode colocar em causa todo o sistema, percebemos o quanto o funcionamento da sociedade atual, do ponto de vista da sua segurança e bem-estar económico e social, depende de um equilibrado funcionamento dos setores estratégicos de fornecimento de bens e serviços vitais.

O **Conceito Estratégico de Defesa Nacional (CEDN)** identifica um conjunto alargado de ameaças e riscos à segurança nacional, salientando-se o terrorismo, a criminalidade transnacional organizada, a cibercriminalidade e as pandemias e outros riscos sanitários. Particularmente no que concerne à cibercriminalidade, considera que os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna (RCM n.º 19, 2013, pp.1984-1985).

Face a um cenário desta natureza, o **CEDN** identifica como prioridade, para o reforço da capacidade de resposta nacional, garantir a proteção das infraestruturas críticas de informação, através da criação de um **Sistema de Proteção da Infraestrutura de Informação Nacional** e da definição uma **Estratégia Nacional de Cibersegurança**. (RCM n.º 19, 2013, p.1990).

Apesar do setor da Saúde não ser considerado, *per si,* uma infraestrutura crítica, é seguramente um dos setores com maior impacto num ataque a qualquer das infraestruturas consideradas: energia, telecomunicações, abastecimento de água ou gás, sistemas de pressão negativa (infeção viral), etc.

Plano de Ação para a Transição Digital

A Transformação Digital é um processo no qual as entidades fazem uso da tecnologia para melhorar o seu desempenho, aumentar o alcance e garantir melhores resultados. Consiste numa mudança estrutural nas organizações, dando um papel central à tecnologia. Tão importante como implementar tecnologias disruptivas e inovadoras, é garantir a capacitação das equipas que vão usar as tecnologias (Santos, 2019).

O **Plano de Ação para a Transição Digital** constitui-se como um documento estratégico de apoio à implementação de medidas que visam a transição digital do Estado, das empresas e do Cidadão em geral. Assenta em três pilares de atuação:

- Capacitação e inclusão digital das pessoas;
- Transformação digital do tecido empresarial e digitalização do Estado;
- Implementação de catalisadores da transição digital ▸

> O SISTEMA NACIONAL DE SAÚDE TEM ACOLHIDO TRANSFORMAÇÕES DIGITAIS E TECNOLOGIAS EMERGENTES, COMO A TELEMEDICINA, INTELIGÊNCIA ARTIFICIAL, BIG DATA, CLOUD E INTERNET OF THINGS (IOT), EVOLUINDO DE UMA CULTURA "ANALÓGICA" PARA UMA CULTURA "DIGITAL"

(RCM n.º 30, 2020, pp.6-9).
De acordo com Martins (2017), são identificadas seis etapas na transformação digital (TD) das organizações:
1. Inexistência e recurso a processos tradicionais;
2. TD presente e ativa;
3. TD formalizada;
4. Transformação estratégica (grupos de indivíduos começam a organizar-se para prestar cuidados, de formas diferentes, usando teleconsultas ou publicando dados no Portal do **Serviço Nacional de Saúde (SNS)** em vez de relatórios anuais);
5. Convergência de esforços (uma equipa dedicada à **TD** é constituída para guiar a estratégia e operações no novo paradigma);
6. Inovadora e adaptativa (a **TD** torna-se um hábito na reorganização dos processos de negócio. É criado um ecossistema de informação e valor e surgem alterações à medida que novos papéis e novos equilíbrios emergem).
No caso particular do **SNS**, Martins refere que esta transformação estará entre a 4ª e a 5ª etapa, identificando como condições necessárias: motivação e apoio social e político; *E-skills* dos profissionais de saúde e literacia digital dos cidadãos; competências dos quadros técnicos no Estado e nas empresas; fortalecimento da ação dos agentes da **TD**; infraestruturas robustas, redes rápidas e *hardware* apropriado; pilares digitais e experiência; princípio móvel-à-partida; pensamento *All2All*; cibersegurança como serviço; telesaúde como princípio e não como suplemento.
Esta transformação passa também pela cadeia de valor da saúde, dada a necessidade de integrar outras dimensões, para além da prestação de cuidados de saúde, permitindo a partilha de informação entre os vários operadores dos sistemas de saúde.

Em suma, a cadeia de valor da saúde está a mudar, evoluindo para uma lógica de *digital network*, uma vez que as tecnologias permitem a interação entre todos os pontos de rede, com transmissão permanente de dados, através de sistemas interligados que aprendem, adaptam-se e têm capacidade preditiva (Nabeto, 2020, p.86).

"Man-in-the-middle", *ransomware* e outros ataques à Rede Informática de Saúde (RIS)

O **Sistema Nacional de Saúde** tem acolhido transformações digitais e tecnologias emergentes, como a telemedicina, Inteligência Artificial, *Big Data*, *cloud* e *Internet of Things* (IoT), evoluindo de uma cultura "analógica" para uma cultura "digital". A pandemia veio reforçar e acelerar enormemente esta tendência.
Uma boa notícia sem dúvida, em especial para os utentes do **SNS**, mas também uma fonte de preocupação acrescida, dado que à medida que a transição digital se materializa aumentam as possibilidades de ciberataques, tanto mais graves quanto maior o seu impacto sobre um sistema cada vez mais digitalizado e interligado.
A maior parte das ameaças, decorrentes da velocidade com que se verificam as transformações digitais em curso, relacionam-se com a utilização do espaço cibernético para ações ilícitas destinadas à obtenção de vantagens indevidas por meio da exploração de brechas de segurança em dispositivos e *softwares*. A contínua expansão do acesso à *Internet*, a maior digitalização da economia e o vertiginoso crescimento da "IoT" aumentam os pontos vulneráveis e tornam mais complexas as ameaças à defesa e segurança cibernéticas.
Os ambientes médicos, apesar das informações sensíveis estarem em transição para o *Internet of Medical Things* (IoMT[1]), padecem de baixos níveis de cibersegurança. Devido às grandes quantidades de informação pessoal que armazenam e transferem, as organizações de saúde já se tornaram um alvo preferencial dos cibercriminosos. O baixo nível de segurança nos hospitais facilita o acesso a um enorme volume de informações sensíveis, o que permite a obtenção de elevados proveitos financeiros por parte dos atacantes.
Durante, por exemplo, um ataque *man-in-the-middle*[2], a comunicação é intercetada pelo atacante e retransmitida de uma forma discricionária. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação. Como os participantes legítimos da comunicação não se apercebem que os dados estão a ser adulterados tomam-nos como válidos, fornecendo informações e executando instruções por ordem do atacante.
Ou, como aconteceu em agosto de 2018, quando um grupo privado hospitalar em Portugal foi afetado por *SamSam ransomware* "…surgiram dificuldades no acesso ao sistema informático, motivadas pelo aparecimento de um vírus, prontamente detetado e controlado… estamos em estreita articulação com todas as autoridades competentes, nomeadamente com o **Centro Nacional de CiberSegurança (CNCS)**, estando igualmente a trabalhar com os nossos parceiros na resolução da situação". O processo em causa afetou toda a infraestrutura, incluindo os processos de *backup*, pelo que o impacto ainda hoje se encontra por avaliar na sua real dimensão.
Neste segundo caso, há indicação de que o grupo de *hackers* responsável por este *malware* fatura atualmente cerca de 300 mil dólares por mês (o pedido de resgaste neste caso chegou aos 10 milhões de euros) e que o continua a desenvolver no sentido de lhe adicionar novas funcionalidades.
É hoje claro, infelizmente não para todas as entidades responsáveis pela segurança da informação no **SNS**, a necessidade de antecipar temporalmente a elaboração de Planos de Recuperação de Desastres e de Continuidade do Negócio para a área da saúde em Portugal. É igualmente crítico prever e implementar uma (nova) estrutura de Segurança, bem como um sólido Programa de Segurança da Informação da Saúde.

Política de Cibersegurança para a saúde

Sanar todas as vulnerabilidades de um sistema de informação da dimensão atual e do que se prevê que venha a ser a do **SNS** em Portugal é muito difícil, senão mesmo impraticável.
No entanto, e apesar das suas vulnerabilidades, o **SNS** português demonstrou em plena pandemia a sua resiliência e elasticidade. Perante uma situação de catástrofe eminente, respondeu melhor que alguns sistemas mais capacitados, como o italiano e o espanhol. Porém, tal não se deveu a um plano de ação definido por nenhuma entidade central, mas devido às redes informais que, pela própria natureza das insuficiências do **SNS**, acabaram por surgir de forma quase espontânea. Em especial a Rede Hospital do Norte que, capaz de reagir e antecipar a sobrelotação, mostrou-se mais elástica, muito porque os seus Diretores Hospitalares mantêm relações de proximidade profissional e pessoal entre si, o que lhes permitiu trabalhar em rede na gestão e distribuição dos doentes pelos hospitais, em funções dos recursos disponíveis na região.
Se até há pouco o foco era quase em exclusivo dirigido à sustentabilidade do **SNS**, a pandemia demonstrou a sua resiliência. Mas a questão é como conseguirá o **SNS** migrar estas conexões informais para uma rede segura?
Desde logo, é necessária uma ampla revisão e integração da legislação de combate de crimes cibernéticos. Mas, para que seja seguro, há que implementar o acrónimo CIA (*confidentiality, integrity, availability*), protegendo e salvaguardando os dados. Tal envolve uma teia de processos, desde a complexidade de *passwords*, robustez do sistema, *backups*, graus de utilizadores, atualizações de *hardware*/*software*, antivírus, etc. E, seguindo um bom protocolo de cibersegurança, é possível minimizar a possibilidade de os dados dos utentes serem roubados, destruídos ou manipulados.
A complexidade do ambiente de segurança da informação torna necessários processos de gestão e integração que permitam uma visão global do ciclo de ameaça. O aumento de ativos conectados implica a necessidade de uma visão integrada de segurança que permita não apenas a proteção do sistema de informação, mas de todos os ativos conectados.
Com o aumento exponencial de ataques informáticos, as organizações têm de recrutar colaboradores com perfis de Segurança Informática e *Ethical Hacking*, dotando os departamentos de Tecnologias de Informação dos co- ▸

ENTIDADES PARCEIRAS INTERNACIONAIS

World Health Organization
International Hospital Federation
IFIC International Foundation for Integrated Care
EUROPEAN ASSOCIATION OF HOSPITAL MANAGERS
EHMA European Health Management Association
FBH FEDERAÇÃO BRASILEIRA DE HOSPITAIS
Ad bonum hospitalium Congregati FEDERAÇÃO BRASILEIRA DE ADMINISTRADORES HOSPITALARES
cbexs
sedisa sociedad española de directivos de la salud
Interreg España - Portugal INNHOSPITAL INNHOSPITAL

PORTUGAL TEM UMA DIMENSÃO ADEQUADA, E UMA POPULAÇÃO DIGITALMENTE CAPACITADA, PARA PILOTAR UMA EXPERIÊNCIA DE INOVAÇÃO E TRANSFORMAÇÃO DIGITAL NO SETOR DA SAÚDE E PARA ATRAIR INVESTIMENTO E CAPITAL INTELECTUAL PARA ENFRENTAR UMA DAS MAIORES INOVAÇÕES DO SÉCULO XXI

nhecimentos e ciberferramentas que permitam analisar e corrigir vulnerabilidades nos SI.

Como referido, é assim crítico implementar um **Programa de Segurança da Informação da Saúde** que inclua:

• Gestão de Serviços Externos, com desenho e execução de um Sistema de Gestão de Segurança da Informação e um Plano de Testes de Segurança, promovendo paralelamente a melhoria contínua em alinhamento com os requisitos normativos e de documentação relativos à Segurança da Informação;

• Apoio e integração na implementação de um *Security Operations Center*, com foco a apoiar e proteger proactivamente a saúde contra as mais avançadas ciberameaças, como *malware*, *ransomware*, fugas de informação, abusos de marca, e fraudes informáticas com impacto financeiro;

• Articulação direta com o **CNCS** na perspetiva de cumprir os requisitos do protocolo celebrado, formação e estreitar o modelo de relacionamento e cooperação entre ambas as entidades;

• Integrar as estruturas de Segurança, Risco e *Compliance*, *Marketing* Digital e DPO no projeto no sentido de garantir modelos de governação bem-sucedidos.

Segundo o Manual "Boas Práticas de Resiliência de Infraestruturas Críticas - Setor Privado e Empresarial do Estado" da ANEPC[3], há que levar em conta e dar resposta às quatro dimensões de catástrofe:

• Prevenção e Mitigação: definir estratégia com base nos riscos, criando um cadastro e um protocolo de segurança; estabelecer o princípio do acesso privilegiado, verificando os fluxos de acesso; e auditar o sistema;

• Preparação: formar colaboradores, (in)formar utentes, comprar dispositivos IoT com segurança comprovada, compartilhar informações e rever sistematicamente a abordagem;

• Alerta: instalar *software* e *firmware* mais recente e atualizá-lo continuamente;

• Resposta e Recuperação: além de melhorar a deteção de forma a evitar a intrusão, é fundamental tratar as violações rápida e eficazmente, para limitar os danos.

Concluindo, podemos dizer que Portugal tem uma dimensão adequada, e uma população digitalmente capacitada, para pilotar uma experiência de inovação e transformação digital no setor da saúde e para atrair investimento e capital intelectual para enfrentar uma das maiores inovações - oportunidade e ameaça - do século XXI. Mas para que tal aconteça é crítico que quem tem responsabilidades no **SNS**, nas suas várias componentes e sectores - público, privado e social - perceba a importância e urgência em atuar de imediato, trabalhando em equipa, envolvendo todos os atores e tendo claro que o que interessa, no fim do dia, é única e simplesmente garantir às pessoas o acesso aos melhores cuidados de saúde possíveis, em qualidade e segurança.

Até porque, um dia, face à emergência climática em que vivemos, chegará a Pandemia 2.0!

E depois, estaremos preparados, ou esperamos um *shutdown* das infraestruturas críticas da Saúde?

A confiança é conquistada quando as ações se juntam às palavras! ●

1. Coleção de dispositivos e aplicativos médicos que se conectam a sistemas de TI de saúde por meio de redes de computadores *online*. Dispositivos médicos equipados com *Wi-Fi* permitem a comunicação máquina a máquina, que é a base da IoMT. Os dispositivos IoMT são vinculados a plataformas em nuvem, como Amazon Web Services, nas quais os dados capturados podem ser armazenados e analisados.

2. Homem no meio, em referência ao atacante que intercepta dados (por exemplo, entre um cidadão e o seu banco) e possivelmente os altera sem que as vítimas se apercebam.

3. Manual "Boas Práticas de Resiliência de Infraestruturas Críticas - Setor Privado e Empresarial do Estado", foi publicado em 13/10/2017, e elaborado no âmbito da Plataforma Nacional para a Redução do Risco de Catástrofes, coordenada pela A.N. Emergência e Proteção Civil.

• Anon 2013. RCM nº 19. (em linha) Diário da República Eletrónico. Disponível em: https://dre.pt/pesquisa/-/search/259967/details/maximized (Acedido 9 Fev. 2021).

• Anon 2020. RCM nº 30. (em linha) Diário da República Eletrónico. Disponível em: https://dre.pt/web/guest/home/-/dre/132133788/details/maximized (Acedido 11 Fev. 2021).

• Martins, H., 2017. (em linha) SNS digital e as condições da transformação digital na saúde. Disponível em: http://spms.min-saude.pt/wp-content/uploads/2017/01/Exame-Inform%C3%A1tica-transforma%C3%A7%C3%A3o-Digital.pdf (Acedido 9 Fev. 2021).

• MDN, 2011. Decreto-Lei 62/2011, 2011-05-09. (em linha) Diário da República Eletrónico. Disponível em: https://dre.pt/pesquisa/-/search/286758/details/maximized (Acedido 14 Fev. 2021).

• Nabeto, A., 2020. A Transformação Digital no Sector da Saúde. Instituto Superior de Gestão.

• Rinaldi, M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, Understanding and Analyzing. In: Critical Infrastructure Interdependencies," IEEE Control Systems magazine. pp.11-25.

• Santos, M., 2019. IT Insight - Transformação digital na área da saúde. (em linha) IT Insight. Disponível em: https://www.itinsight.pt/news/opiniao/transformacao-digital-na-area-da-saude (Acedido 12 Fev. 2021).