Conselho
da União Europeia

Bruxelas, 16 de janeiro de 2025
(OR. en)

5426/25

CYBER 21
SAN 15

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	15 de janeiro de 2025
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2025) 10 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Plano de Ação Europeu para a Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde

Envia-se em anexo, à atenção das delegações, o documento COM(2025) 10 final.

Anexo: COM(2025) 10 final

COMISSÃO
EUROPEIA

Bruxelas, 15.1.2025
COM(2025) 10 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Plano de Ação Europeu para a Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde

1. Introdução

O ambiente de segurança da UE está a mudar rapidamente, tendo-se registado uma escalada de ataques híbridos e ciberataques que visam desestabilizar a nossa sociedade, criar divisões e perturbações, mas também obter lucros decorrentes da cibercriminalidade. Por conseguinte, a Europa tem de reforçar urgentemente a sua preparação e resiliência para fazer face a esta nova realidade, em todos os setores e em consonância com uma abordagem «global da sociedade» e de «governação integrada», tal como solicitado no relatório de Sauli Niinistö, conselheiro especial da presidente da Comissão Europeia.

Sistemas de saúde seguros e resilientes são uma pedra angular do modelo social da UE. No entanto, os hospitais e os sistemas de saúde enfrentam ameaças crescentes, em especial de gangues que utilizam *software* de sequestro e que os visam com o intuito de obter ganhos financeiros, movidos pelo valor elevado dos dados dos doentes, incluindo registos de saúde eletrónicos. O setor da saúde tornou-se, de facto, a indústria mais atacada na UE nos últimos quatro anos, nomeadamente durante a pandemia de COVID-19, período em que o número de ciberataques de que foram alvo as infraestruturas de saúde aumentou progressivamente. Os ciberataques contra hospitais e prestadores de cuidados de saúde estão a causar danos diretos às pessoas, atrasando procedimentos médicos, causando congestionamentos nos serviços de urgência e podendo, em casos extremos, conduzir à perda de vidas.

Os riscos são ainda maiores uma vez que o setor passa por uma transformação digital vital. A saúde digital e a utilização e reutilização de dados de saúde podem permitir modelos de cuidados mais adequados às necessidades e preferências das pessoas e dos doentes, prevenindo o aparecimento de doenças ou permitindo um tratamento mais precoce. A integração de soluções e ferramentas digitais nos processos clínicos, bem como a utilização e reutilização de dados de saúde, podem servir de base a melhores decisões clínicas, contribuir para a automatização no setor da saúde e agilizar e melhorar a prestação de cuidados aos doentes. As ferramentas digitais, a utilização de dados e os dispositivos médicos — frequentemente ligados à Internet e alimentados por inteligência artificial (IA) — são também fundamentais para enfrentar desafios como a escassez de profissionais de saúde.

Simultaneamente, as ferramentas digitais também aumentam os potenciais alvos dos cibercriminosos. Além disso, alguns intervenientes estatais não hesitam em visar as instalações de cuidados de saúde, como o demonstra a guerra de agressão em curso da Rússia contra a Ucrânia. Tal torna o setor um potencial alvo de ciberataques no âmbito de uma campanha híbrida mais vasta. Os ciberataques não só comprometem a segurança dos doentes, como também minam a confiança do público nas infraestruturas de saúde e acarretam custos de recuperação significativos. Dispor de uma infraestrutura digital resiliente e segura é essencial não só para garantir a proteção contra ciberataques, mas também para apoiar a implementação e a plena implantação do Espaço Europeu de Dados de Saúde[1] (EEDS).

Por conseguinte, é tempo de aumentar e reforçar a cibersegurança e a resiliência dos hospitais e dos prestadores de cuidados de saúde da Europa, tal como salientado pela presidente Ursula von der Leyen nas suas Orientações políticas para a Comissão Europeia 2024-2029[2]. O presente plano de ação dá resposta à urgência da situação e às ameaças ímpares que o setor enfrenta. Não existe uma solução

[1] https://www.consilium.europa.eu/pt/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.
[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_pt.

«milagrosa» para os desafios no domínio da cibersegurança nos cuidados de saúde. Em vez disso, o plano de ação apela ao reforço da prevenção e da preparação e à adoção de uma abordagem mais coordenada da solidariedade, tirando simultaneamente partido dos conhecimentos especializados do setor europeu da cibersegurança. Como tal, o plano de ação reflete a abordagem da UE em matéria de segurança, que será desenvolvida e formalizada na próxima Estratégia Europeia de Segurança Interna, definindo uma resposta abrangente para enfrentar todas as ameaças à segurança interna e centrando-se na capacidade de antecipar ameaças, prevenir danos e proteger as pessoas, atuando a todos os níveis com uma abordagem «global da sociedade».

O setor da saúde inclui um vasto número de entidades e intervenientes, nomeadamente hospitais, clínicas, residências assistidas, centros de reabilitação e vários prestadores de cuidados de saúde, juntamente com a indústria farmacêutica, médica e biotecnológica, fabricantes de dispositivos médicos e instituições de investigação no domínio da saúde. O presente plano de ação centra-se predominantemente na cibersegurança dos hospitais e dos prestadores de cuidados de saúde, entendidos como uma pessoa singular ou coletiva — ou outra entidade — que preste legalmente cuidados de saúde no território de um Estado-Membro[3]. Os hospitais e os prestadores de cuidados de saúde são interdependentes de outras entidades de saúde e estão mais próximos das pessoas. Simultaneamente, as medidas destinadas a reforçar a cibersegurança dos hospitais e dos prestadores de cuidados de saúde devem também abordar os riscos que afetam o ecossistema e a cadeia de abastecimento em geral, decorrentes, por exemplo, de entidades que utilizam dados de saúde para fins de investigação e aprendizagem automática ou que produzem dispositivos médicos, em especial dispositivos médicos digitais que se ligam à Internet ou a outros dispositivos («Internet das coisas»).

Embora a segurança dos sistemas de saúde seja essencialmente uma competência nacional, a saúde é também um setor crítico nos termos da Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na UE (SRI 2)[4]. Os cibercriminosos e outros perpetradores operam além-fronteiras e os desafios no domínio da cibersegurança enfrentados pelas organizações de cuidados de saúde são também semelhantes em todos os Estados-Membros. A cooperação a nível europeu é importante para partilhar e expandir boas práticas nacionais e a nível da UE. Por conseguinte, o plano de ação propõe medidas e uma coordenação a nível da UE, apelando simultaneamente aos Estados-Membros para que tomem providências que permitam fazer a diferença nos cuidados de saúde e no ecossistema da saúde em geral.

Em primeiro lugar, o plano de ação centra-se no reforço das capacidades do setor para **prevenir** incidentes de cibersegurança, uma vez que é sempre melhor prevenir do que remediar. Em segundo lugar, o plano de ação especifica ações destinadas a melhorar a partilha de informações em matéria de cibersegurança e a capacidade de **detetar** ciberameaças, permitindo uma reação mais rápida. Em terceiro lugar, prevê medidas para **responder** melhor aos incidentes e **recuperar** dos mesmos. Por último, o

[3] Artigo 3.º, alínea g), da Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32011L0024.

[4] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

plano de ação prevê formas de **dissuadir** os perpetradores de ciberameaças de lançarem ataques contra os sistemas de saúde na Europa.

O plano de ação será executado em colaboração com os prestadores de cuidados de saúde e o ecossistema da saúde em geral, os Estados-Membros e a comunidade de cibersegurança. A adoção de uma abordagem colaborativa é fundamental para definir e aperfeiçoar as ações com maior impacto, de modo que todos os prestadores de cuidados de saúde críticos da Europa possam delas beneficiar. Por conseguinte, a presente comunicação será acompanhada do lançamento de uma consulta abrangente das partes interessadas, do setor e dos Estados-Membros. A cooperação internacional é importante para a cibersegurança devido à natureza sem fronteiras e interligada das ciberameaças. Os países do alargamento e da vizinhança e outros países parceiros estratégicos da UE também enfrentam ameaças de cibersegurança comparáveis. Tal pode, em última análise, pôr em risco a segurança de infraestruturas críticas na UE. Por conseguinte, será importante refletir os ensinamentos retirados da execução do plano de ação também na cooperação da UE com os países do alargamento e com outros países parceiros, tendo em conta os níveis de ameaça a que estão, respetivamente, expostos.

2. O desafio da cibersegurança dos hospitais e prestadores de cuidados de saúde

Ciberameaças ao setor da saúde

Os ciberataques estão a aumentar a nível mundial e no seio da UE, sendo o panorama de ameaças cada vez mais complexo e dinâmico. A evolução da inteligência artificial (IA) está a dotar os agentes criminosos e mal-intencionados de ferramentas poderosas que lhes permitem aumentar a precisão e o impacto das suas operações e, ao mesmo tempo, a reformular as possibilidades de ciberdefesa, possibilitando uma ação automatizada e em tempo real contra ataques.

O *software* de sequestro continua a constituir um desafio crítico no domínio da cibersegurança na UE e a nível mundial, tendo um relatório estimado um custo anual mundial superior a 250 mil milhões de EUR até 2031[5]. Quando os criminosos que utilizam *software* de sequestro atacam, não só encriptam os dados das vítimas para efeitos de resgate, como também divulgam, cada vez mais, informações sensíveis para exercer pressão adicional. As vulnerabilidades do *software* e do equipamento informático constituem outro desafio importante: de acordo com a Agência da União Europeia para a Cibersegurança (ENISA)[6], o setor dos cuidados de saúde foi o que declarou mais incidentes de segurança relacionados com essas vulnerabilidades[7]. Outras ameaças crescentes incluem ataques distribuídos de negação de serviço

[5] Cybersecurity Ventures (1 de junho de 2024): «Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031», disponível em https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[6] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação (Regulamento Cibersegurança), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.
[7] *ENISA Threat Landscape: Health Sector* (não traduzido para português), julho de 2023.

(DDoS), concebidos para sobrecarregar um sistema específico com um fluxo de tráfego, tornando-o inacessível aos utilizadores legítimos[8].

O setor da saúde enfrenta tendências semelhantes em matéria de ameaças de cibersegurança, com forte destaque para os ataques de *software* de sequestro. De acordo com a ENISA, o *software* de sequestro foi responsável por 54 % dos incidentes de cibersegurança analisados no setor da saúde no período de 2021-2023. Oitenta e três por cento dos ataques tiveram uma motivação financeira, impulsionada pelo elevado valor dos dados relativos aos cuidados de saúde, enquanto 10 % dos ataques tiveram uma motivação ideológica[9]. Do mesmo modo, um relatório de 2024 da Comissão concluiu que 71 % dos ataques com efeitos na prestação de cuidados aos doentes, como o diagnóstico e o tratamento tardios e o acesso dificultado aos serviços de urgência, foram perpetrados com recurso a *software* de sequestro[10]. Os ataques de *software* de sequestro podem ter um efeito particularmente perturbador na prestação de serviços de saúde, colocando em risco a segurança dos doentes. Além disso, os ataques de *software* de sequestro estão frequentemente associados a violações dos dados dos doentes[11], que muitas vezes incluem dados sensíveis relacionados com a saúde e violam o direito fundamental das pessoas à proteção dos dados pessoais.

Simultaneamente, com a crescente digitalização dos cuidados de saúde, a superfície de ataque está a aumentar. De acordo com o Relatório sobre o estado da Década Digital 2024, uma média de 79 % dos cidadãos da UE têm acesso em linha aos seus registos de saúde eletrónicos referentes a cuidados primários[12]. Os registos de saúde eletrónicos, os sistemas de informação clínica, os sistemas de fluxo de trabalho hospitalar, os sistemas informáticos para gerir o reembolso de tratamentos, os sistemas de imagiologia médica e os dispositivos médicos utilizados para fins de diagnóstico ou de monitorização dos doentes são exemplos de ferramentas digitais que podem desempenhar um papel importante no reforço da eficiência e do desempenho do setor da saúde, mas são também potenciais alvos de ataques à cibersegurança. Certas atividades de cuidados de saúde, como os cuidados intensivos e a imagiologia radiológica, ou domínios médicos como a oncologia e a cardiologia, que são altamente dependentes de dispositivos digitais, correm um risco especial de sofrer ciberataques. Além disso, problemas relacionados com a cadeia de abastecimento podem conduzir à aquisição de dispositivos que não disponham de um nível suficiente de cibersegurança, agravando os riscos gerais existentes.

---

[8] *ENISA Threat Landscape 2024* (não traduzido para português).

[9] *ENISA Threat Landscape: Health Sector* (não traduzido para português), julho de 2023. O relatório analisou os prestadores de cuidados de saúde, bem como outros tipos de organizações, incluindo organizações que realizam investigação relacionada com a saúde, entidades que fabricam determinados produtos relacionados com a saúde, autoridades de saúde, organizações de seguros de saúde, instalações de tratamento residencial e prestadores de serviços sociais. Disponível em https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Comissão Europeia: Centro Comum de Investigação, Reina, V. e Griesinger, C., *Cyber security in the health and medicine setor: a study on available evidence of patient health consequences from Cyber incidents in health setting* (não traduzido para português), Serviço das Publicações da União Europeia, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] De acordo com o relatório do estado das ameaças no setor da saúde elaborado pela ENISA (*ENISA Threat Landscape: Health Sector*), confirmou-se a violação ou o roubo de dados em 43 % dos incidentes que envolveram o recurso a *software* de sequestro analisados.

[12] Relatório sobre o estado da Década Digital 2024.

Por exemplo, durante a pandemia de COVID-19, um ataque de *software* de sequestro paralisou grande parte do sistema de saúde irlandês, conduzindo ao cancelamento de, pelo menos, alguns serviços em 31 dos 54 hospitais de agudos na manhã do incidente[13]. Os serviços de saúde tiveram de voltar a utilizar registos em papel, o que reduziu a eficiência das operações. O ataque teve origem numa mensagem de correio eletrónico com mistificação da interface que continha um anexo malicioso[14]. O incidente demonstrou o potencial de propagação dos ciberataques em diferentes sistemas e, consequentemente, a importância de proteger toda a superfície de ataque de uma organização de cuidados de saúde. Sublinhou igualmente a importância de assegurar uma cultura fundamental de ciber-higiene e cibersegurança em todas as organizações.

Maturidade em matéria de cibersegurança dos hospitais e prestadores de cuidados de saúde

O panorama dos cuidados de saúde na UE é muito diversificado, variando os hospitais e outros prestadores de cuidados de saúde consideravelmente em termos de propriedade, estrutura e dimensão entre os Estados-Membros. Em alguns casos, a governação dos cuidados de saúde pode basear-se numa abordagem centralizada a nível nacional, noutros a nível regional e local; os prestadores de cuidados de saúde podem ser públicos ou privados. Além disso, podem também existir diferenças no seio de um mesmo país, por exemplo, quando existem disparidades socioeconómicas e territoriais significativas entre regiões, o que complica a situação. Este panorama complexo dos cuidados de saúde pode ser posto à prova por importantes crises sanitárias, devido a doenças transmissíveis, como a pandemia de COVID-19, mas também por outros riscos para a saúde, por exemplo, relacionados com as alterações climáticas. Por último, existe uma variabilidade e uma fragmentação significativas no nível de digitalização e adoção de tecnologias pelos prestadores de cuidados de saúde. O facto de a indisponibilidade do serviço causada por um incidente de cibersegurança poder resultar em graves danos e prejuízos para os doentes, mesmo em instalações de cuidados de saúde de pequena escala, incluindo clínicas ou serviços de emergência médica que prestam um serviço essencial a um número relativamente baixo de utilizadores, exemplifica esta complexidade.

De acordo com o relatório de 2024 da ENISA sobre o estado da cibersegurança na União[15], a maturidade em matéria de cibersegurança do setor da saúde da UE é moderada e existem grandes diferenças no nível de maturidade em matéria de cibersegurança entre as entidades prestadoras de cuidados de saúde em toda a Europa. É possível observar deficiências em domínios fundamentais como a disponibilidade de recursos humanos suficientes, os conhecimentos das organizações sobre as respetivas cadeias de abastecimento de tecnologias da informação e comunicação (TIC) e a instalação de elementos de segurança atualizados nos produtos. O setor debate-se para garantir uma ciber-higiene básica e medidas fundamentais no domínio da segurança, como o demonstra o facto de quase todas as organizações de

[13] Irish Health Service Executive: «Conti cyber attack on the HSE: Independent Post Incident Review», 2021.
[14] Irish Health Service Executive: «Cyber-attack and HSE response». Disponível em https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA, *2024 Report on the State of Cybersecurity in the Union* (não traduzido para português), setembro de 2024. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

saúde inquiridas enfrentarem dificuldades aquando da realização de avaliações dos riscos de cibersegurança, tendo quase metade delas nunca realizado uma análise dos riscos[16].

Outro desafio significativo para a cibersegurança dos hospitais é a intersecção das tecnologias da informação (TI) com as tecnologias operacionais (TO), caso em que convergem diferentes prioridades de segurança no que diz respeito à confidencialidade, disponibilidade e fiabilidade e em que uma violação num domínio pode afetar o outro. O relatório de 2024 da ENISA sobre o estado da cibersegurança na União salienta ainda que o setor da saúde não está a ter um desempenho adequado para garantir a segurança dos produtos e processos de TIC que utiliza, devido à grande variedade de entidades, dispositivos e produtos de saúde.

Esta diversidade, aliada a níveis variáveis de sensibilização do pessoal e da gestão hospitalar para a cibersegurança, cria um desafio complexo quando se trata de garantir a cibersegurança dos sistemas de saúde. Por exemplo, de acordo com o Eurobarómetro de 2024 sobre competências de cibersegurança, apenas 25 % das empresas inquiridas nos setores da saúde, da educação e da assistência social tinham ministrado formação ou realizado ações de sensibilização para a cibersegurança nos 12 meses anteriores[17]. São necessárias medidas para promover uma cultura de sensibilização para a cibersegurança entre os profissionais de saúde da linha da frente. Por exemplo, as rotações de pessoal, a utilização de estações de trabalho partilhadas, a má gestão da autenticação e a utilização de suportes amovíveis são fontes adicionais de vulnerabilidades que afetam a cibersegurança dos prestadores de cuidados de saúde[18].

Em muitos casos, as TI e as TO são, pelo menos em parte, externalizadas. O Eurobarómetro de 2024 concluiu que a percentagem de empresas que externalizam, pelo menos, alguns aspetos da sua cibersegurança é mais elevada nos setores da saúde, da educação e da assistência social, com 57 % das empresas inquiridas a fazê-lo[19]. Do mesmo modo, verifica-se uma forte tendência de migração para a computação em nuvem, impulsionada pela necessidade de um armazenamento e uma gestão escaláveis de dados, de eficiência em termos de custos, de uma melhor colaboração e do apoio a tecnologias avançadas, como a IA e a Internet das coisas médicas. Em 2022, 58 % das organizações de saúde utilizaram uma plataforma digital de saúde baseada na nuvem[20]. No entanto, embora esta mudança possa trazer ganhos de eficiência significativos, também acarreta riscos que exigem a tomada de decisões informadas no que respeita à contratação e a uma configuração segura.

A questão do reforço das capacidades e do financiamento é fundamental para enfrentar todos estes desafios. O financiamento da cibersegurança no setor da saúde tem sido limitado e continua a constituir

---

[16] *ENISA Threat Landscape: Health Sector* (não traduzido para português), julho de 2023. Disponível em https://www.enisa.europa.eu/publications/health-threat-landscape.

[17] Eurobarómetro Flash n.º 547 sobre competências de cibersegurança (maio de 2024). Disponível em https://europa.eu/eurobarometer/surveys/detail/3176.

[18] PANACEA, *People-centric cybersecurity in healthcare*: *White Paper — Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres*, 2021.

[19] Eurobarómetro Flash n.º 547 sobre competências de cibersegurança (maio de 2024). Disponível em https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISA, *NIS Investments Report 2022* (não traduzido para português), novembro de 2022. Disponível em https://www.enisa.europa.eu/publications/nis-investments-2022.

um desafio universal em toda a UE[21]. Além disso, estes desafios de financiamento surgem no contexto do envelhecimento da população, que deverá criar pressões orçamentais generalizadas sobre os sistemas de saúde da Europa nas próximas décadas.

A utilização contínua de ferramentas obsoletas e sistemas legados, os recursos limitados para prevenir ou reagir a incidentes e as lacunas na maturidade em matéria de cibersegurança resultam frequentemente de défices de financiamento. Os hospitais enfrentam um desafio contínuo para equilibrar uma infraestrutura digital e segura atualizada com outros investimentos necessários para melhorar a prestação de cuidados aos doentes, como a contratação de médicos e outros profissionais de saúde, a aplicação de novos métodos de diagnóstico e tratamento e a aquisição de dispositivos. De acordo com a ENISA[22], o setor da saúde ocupa apenas o 7.º lugar entre os 12 setores estudados no que diz respeito à proporção das despesas com a segurança da informação em relação às despesas totais com TI. A sua mediana é de 8,3 %.

3. Centro Europeu de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde

O quadro de cibersegurança da UE proporciona um vasto leque de ferramentas que devem ser aproveitadas para melhorar a segurança e a resiliência dos hospitais e dos prestadores de cuidados de saúde. Para fazer face aos numerosos desafios acima referidos, é necessário desenvolver uma abordagem estratégica unificada a nível da UE que reúna os recursos, os conhecimentos especializados e as ferramentas necessários para combater eficazmente as ciberameaças. Uma visão global, bem como um melhor planeamento e coordenação, são essenciais para ajudar os prestadores de cuidados de saúde em toda a UE a reforçar as suas defesas. Para o efeito, a ENISA está em melhor posição para criar, na sua organização, um **Centro Europeu de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde**[23] específico, no âmbito do seu mandato[24], para salvaguardar e apoiar as infraestruturas críticas da UE.

O centro de apoio deve **desenvolver progressivamente um catálogo de serviços abrangente que responda às necessidades dos hospitais e dos prestadores de cuidados de saúde**, descrevendo o leque de serviços disponíveis em matéria de preparação, prevenção, deteção e resposta. Em colaboração com as autoridades dos Estados-Membros e com base nas experiências dos hospitais e dos prestadores de cuidados de saúde, o centro de apoio deve desenvolver um repositório de fácil acesso e utilização de todos os instrumentos disponíveis a nível europeu, nacional e regional. No exercício das suas atividades,

[21] A organização e prestação de serviços de saúde e de cuidados médicos são da competência nacional nos termos do artigo 168.º do Tratado sobre o Funcionamento da União Europeia, e o financiamento dos sistemas de saúde varia consoante os Estados-Membros.

[22] ENISA, *NIS Investments Report 2022* (não traduzido para português), novembro de 2022. Disponível em https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] No presente documento, a expressão «centro de apoio» é utilizada indiscriminadamente.

[24] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), JO L 151 de 7.6.2019, p. 15.

deve assegurar uma coordenação adequada com os Estados-Membros e apoiar a definição de prioridades e a realização das ações necessárias em tempo real.

Enquanto elemento essencial para o desenvolvimento do catálogo de serviços do centro de apoio, a Comissão proporá o lançamento de projetos-piloto em toda a UE para elaborar boas práticas em matéria de ciber-higiene e avaliação dos riscos de segurança, bem como para dar resposta à necessidade de monitorização contínua da cibersegurança, informações sobre ameaças e resposta a incidentes utilizando soluções de cibersegurança de ponta. Os resultados destes projetos-piloto, que serão financiados pelo Programa Europa Digital e executados pelo Centro Europeu de Competências em Cibersegurança (ECCC), servirão de base a outras ações a nível da UE, nomeadamente ao trabalho do centro de apoio.

Figura 1: Conceitos do catálogo de serviços do centro de apoio aos hospitais e prestadores de cuidados de saúde

3.1. Prevenção de incidentes de cibersegurança

Ações simples que alteram as probabilidades

Medidas básicas de cibersegurança, como a atualização dos sistemas, a gestão das cópias de segurança e a utilização da autenticação multifatores, podem, de acordo com uma estimativa, proteger as organizações de até 98 % dos ataques[25]. A adoção de muitas das medidas de ciber-higiene e de gestão dos riscos com maior impacto é relativamente simples, o que as torna soluções de primeiro recurso para melhorar a cibersegurança. Por conseguinte, um dos principais papéis do centro de apoio deve consistir na **elaboração de orientações claras e específicas que destaquem as práticas de cibersegurança mais críticas e ajudem os prestadores de cuidados de saúde a aplicá-las**. Este apoio tem de estender-se para além dos hospitais de grande dimensão e incluir aconselhamento personalizado para entidades de menor dimensão, como os consultórios locais de médicos de clínica geral e as clínicas especializadas, que muitas vezes não dispõem de recursos para equipas específicas de cibersegurança, mas continuam igualmente vulneráveis a ataques. Além disso, é necessário ter em conta a importância regional de entidades prestadoras de cuidados de saúde específicas para assegurar a prestação de cuidados aos doentes, por exemplo em zonas escassamente povoadas. Os institutos de investigação no domínio da saúde que tratam grandes quantidades de dados pessoais sensíveis também poderiam beneficiar da receção de orientações sobre medidas básicas de cibersegurança para reforçar a sua resiliência.

As organizações de cuidados de saúde estão igualmente sujeitas a uma série de obrigações relacionadas com a cibersegurança decorrentes da legislação da UE[26]. Embora as obrigações sejam cruciais para providenciar uma base de referência comum elevada para a cibersegurança e a segurança dos dados, é

[25] *Microsoft Digital Defense Report 2022*. Disponível em https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Como a Diretiva SRI 2; o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais (Regulamento de Ciber-Resiliência), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; o Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos (Regulamento Dispositivos Médicos), https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng; o Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico *in vitro* (Regulamento Dispositivos Médicos para Diagnóstico *in Vitro*), https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679; o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689; e a Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao Espaço Europeu de Dados de Saúde, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52022PC0197. As negociações foram concluídas com um acordo político na primavera de 2024 e, após a sua finalização, a publicação no Jornal Oficial está prevista para a primavera de 2025.

essencial garantir que o panorama regulamentar não crie desnecessariamente dificuldades e encargos. O facto de se dar uma grande ênfase ao cumprimento não deve prejudicar o objetivo de promover uma forte cultura de cibersegurança. Uma **ferramenta de levantamento da regulamentação de fácil acesso pode ajudar a minimizar os encargos administrativos das entidades sujeitas a múltiplos instrumentos regulamentares**. A par da elaboração de orientações e de conjuntos de ferramentas, o centro de apoio deve trabalhar em estreita colaboração com a Comissão e os Estados-Membros para desenvolver e divulgar essa ferramenta o mais rapidamente possível. Por conseguinte, o centro de apoio desempenharia um papel importante na simplificação da compreensão e da aplicação das regras em matéria de cibersegurança, por exemplo, fornecendo orientações sobre a aplicação[27] e, se necessário, promovendo normas pertinentes.

As futuras **carteiras europeias de identidade digital** são outra ferramenta destinada a facilitar a aplicação simples de boas práticas de ciber-higiene. É essencial reduzir a dependência de mecanismos de identificação fracos, como as palavras-passe, para atenuar os riscos de acesso não autorizado a dados de saúde. A transição para soluções de autenticação seguras baseadas numa identificação fiável é fundamental. A carteira de identidade digital da UE proporciona uma abordagem harmonizada à escala da UE da identificação eletrónica para os profissionais de saúde, proporcionando uma solução sólida e unificada a partir do final de 2026. Todos os sistemas de informação sobre saúde em linha que tenham de implementar uma autenticação forte do utente serão obrigados a aceitar a carteira para efeitos de identificação a partir do final de 2027[28].

Preparação e apoio específico

Os testes de preparação, que envolvem ações como os testes de penetração, são uma pedra angular de uma cibersegurança eficaz, tendo a Comissão já atribuído financiamento à ENISA para a realização de iniciativas-piloto de preparação, que revelaram que o setor da saúde se encontra entre os domínios mais procurados para testar e realizar novas avaliações com o intuito de identificar lacunas na maturidade em matéria de cibersegurança. Com a entrada em vigor do Regulamento de Cibersolidariedade, estes esforços expandir-se-ão significativamente, sob a liderança do ECCC. Para dar resposta a esta necessidade, a Comissão proporá, em consulta com o Grupo de Cooperação SRI, a Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe)[29] e a ENISA, que a saúde seja identificada como um setor elegível para receber apoio para a realização de **testes coordenados de preparação** ao abrigo do Regulamento de Cibersolidariedade. Além disso, o centro de apoio deve desenvolver um **quadro adaptado para as avaliações da maturidade em matéria de cibersegurança específicas para os cuidados de saúde**. Essas avaliações da maturidade forneceriam às entidades informações úteis sobre as suas vulnerabilidades, permitindo-lhes simultaneamente demonstrar aos doentes e às partes interessadas a sua preparação em termos de cibersegurança, reforçando a confiança nos seus serviços. A nível

[27] A elaboração de orientações sobre a interpretação do Regulamento Geral sobre a Proteção de Dados (RGPD) é da responsabilidade do Comité Europeu para a Proteção de Dados (CEPD). A elaboração de orientações pela ENISA deve respeitar plenamente as prerrogativas do CEPD.
[28] Artigo 5.º-F, n.os 1 e 2, do Regulamento (UE) n.º 910/2014.
[29] Rede Europeia de Organizações de Coordenação de Cibercrises.

agregado, o centro de apoio deve realizar uma **avaliação anual da maturidade em matéria de cibersegurança no setor da saúde**, que estabeleça uma panorâmica clara da cibersegurança no setor da saúde, tanto a nível nacional como a nível da UE.

O setor da saúde depende fortemente de contratantes externos para a prestação de serviços de cibersegurança[30], o que evidencia a necessidade de apoio específico para reforçar as defesas. Com base em iniciativas bem-sucedidas, como os vales de inovação da UE, os **Estados-Membros devem ponderar a adoção de medidas específicas, como os vales de cibersegurança para os micro, pequenos e médios hospitais e prestadores de cuidados de saúde**. Estes vales providenciariam assistência financeira para a aplicação de medidas específicas de cibersegurança. A priorização da atribuição de vales deve basear-se nos resultados dos testes de preparação e das avaliações da maturidade.

O conhecimento e o contexto locais são cruciais para a implantação eficaz dos vales ou de outros programas de apoio, assegurando a sua pertinência e acessibilidade. Fundos da UE, como o Fundo Europeu de Desenvolvimento Regional, já apoiam iniciativas no domínio da cibersegurança e da saúde digital, podendo, por conseguinte, servir de veículo para desenvolver sistemas de vales de cibersegurança específicos para os prestadores de cuidados de saúde. Para impulsionar este esforço, o centro de apoio colaboraria com os Estados-Membros e as autoridades responsáveis pelos programas regionais no sentido de apoiar o desenvolvimento desses sistemas de vales regionais, tirando partido dos ensinamentos retirados dos projetos nacionais existentes, bem como das ações financiadas ao abrigo do Programa Europa Digital, a fim de assegurar uma execução prática e com impacto.

Além disso, desde 2014, os programas Horizonte têm desempenhado um papel fundamental no financiamento de uma série de iniciativas de investigação centradas no reforço da resiliência das instituições de prestação de cuidados de saúde, como os hospitais, contra ciberameaças e na atenuação dos riscos associados à utilização indevida de tecnologias emergentes. Os resultados obtidos incluem um conjunto de ferramentas, quadros e sistemas especializados, como ferramentas de avaliação dos riscos, plataformas de partilha de dados que preservam a privacidade, soluções criptográficas, programas de formação que visam sensibilizar para a cibersegurança e sistemas de deteção de ameaças em tempo real. Nomeadamente, estas soluções foram rigorosamente validadas através de implementações-piloto em condições reais de ambientes de cuidados de saúde, garantindo a sua eficácia e aplicabilidade prática na proteção contra ciberameaças.

Garantia da segurança das cadeias de abastecimento de cuidados de saúde

Um desafio fundamental para as organizações de cuidados de saúde é a gestão de cadeias de abastecimento de TIC complexas, que envolvem uma série de produtos, como dispositivos médicos conectados, sistemas de registos de saúde eletrónicos e equipamento informático de escritório. Os hospitais e os prestadores de cuidados de saúde necessitam de sistemas e serviços de TIC fiáveis e seguros para as suas operações. Para ajudar a enfrentar os desafios de cibersegurança no setor da saúde,

[30] Ver o relatório de 2023 da ENISA sobre investimentos na SRI (*NIS Investments Report 2023*, não traduzido para português, novembro de 2023), que destaca a importância do apoio externo para a auditoria e a conformidade em matéria de cibersegurança. Disponível em https://www.enisa.europa.eu/publications/nis-investments-2023.

o Grupo de Cooperação SRI deve realizar uma **avaliação coordenada dos riscos de segurança, aferindo os riscos técnicos e estratégicos relacionados com as cadeias de abastecimento de dispositivos médicos e propondo medidas de atenuação**[31]. Se for caso disso, o Grupo de Cooperação SRI deve colaborar com o Grupo de Coordenação dos Dispositivos Médicos.

O Regulamento de Ciber-Resiliência é um novo quadro abrangente que estabelece requisitos de cibersegurança para o planeamento, a conceção, o desenvolvimento, bem como o tratamento, a atualização corretiva e a comunicação de vulnerabilidades ativamente exploradas relativamente a quase todos os produtos de *hardware* e *software*, em cada fase da cadeia de valor[32]. Os dispositivos médicos são um tipo de produto utilizado num dos domínios mais sensíveis da nossa sociedade. Os requisitos de cibersegurança para estes produtos decorrem do Regulamento Dispositivos Médicos preexistente e do Regulamento Dispositivos Médicos para Diagnóstico *in Vitro*[33]. A avaliação em curso desses regulamentos está a analisar o potencial para uma maior coerência e sinergias entre estes quadros, a fim de garantir a simplificação e uma cibersegurança de ponta.

Além disso, as conclusões da avaliação dos riscos devem ajudar as organizações de cuidados de saúde a rever as suas práticas de cibersegurança da cadeia de abastecimento, tal como exigido pela Diretiva SRI 2, e poderão servir de base para a elaboração de novas **diretrizes em matéria de contratação**[34]. Elaboradas pela ENISA através do seu centro de apoio, estas diretrizes devem refletir tendências recentes, como a migração para a nuvem do armazenamento de dados dos doentes, incluindo a necessidade de migração segura de dados de saúde eletrónicos para ambientes de computação em nuvem. Além disso, as novas diretrizes devem proporcionar às organizações ferramentas práticas que lhes permitam acompanhar as suas cadeias de abastecimento, incluindo os prestadores de serviços de segurança geridos, os relatórios de certificação ou as avaliações dos riscos por terceiros.

No que diz respeito à nuvem, são necessárias medidas adicionais para fazer face aos desafios ímpares da gestão de dados sensíveis no domínio dos cuidados de saúde, nomeadamente aos riscos acrescidos para a segurança, a privacidade e operacionais. A fim de reforçar as salvaguardas, os peritos recomendam a incorporação da «segurança por defeito e desde a conceção» nos serviços de computação em nuvem. Esta abordagem dá prioridade a uma infraestrutura segura, à gestão proativa das vulnerabilidades e a uma combinação de soluções de computação em nuvem governamentais e privadas. A monitorização contínua e as certificações específicas dos fornecedores, como as certificações dos prestadores de serviços de segurança e as auditorias de conformidade com as normas nacionais e internacionais, são também essenciais para garantir práticas de segurança sólidas.

---

[31] Nos termos do artigo 22.º da Diretiva SRI 2.

[32] Numa primeira fase, a partir de 1 de agosto de 2025, as grandes categorias de equipamentos de rádio, não abrangidas pelo âmbito de aplicação do Regulamento Dispositivos Médicos e do Regulamento Dispositivos Médicos para Diagnóstico *in Vitro*, terão de cumprir os requisitos essenciais da Diretiva Equipamento de Rádio relacionados com a cibersegurança quando forem colocadas no mercado único. Numa segunda fase, a partir de 11 de dezembro de 2027, o Regulamento de Ciber-Resiliência entrará em aplicação.

[33] Em dezembro de 2019, o Grupo de Coordenação dos Dispositivos Médicos emitiu orientações em matéria de cibersegurança dos dispositivos médicos, que apoiam os fabricantes no cumprimento dos requisitos do anexo I dos dois regulamentos: https://ec.europa.eu/docsroom/documents/41863.

[34] Com base nas diretrizes de 2020 da ENISA em matéria de contratação pública para a cibersegurança nos hospitais (*Procurement Guidelines for Cybersecurity in Hospitals*, não traduzidas para português, fevereiro de 2020). Disponível em https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

No caso de serviços como a infraestrutura como serviço, a plataforma como serviço e o *software* como serviço, a implementação da segurança incumbe frequentemente ao cliente. No entanto, muitas organizações de cuidados de saúde não dispõem dos recursos necessários para satisfazer estes requisitos de forma independente. Para resolver este problema, **os prestadores de serviços de computação em nuvem devem ser incentivados a aplicar medidas de segurança de base como característica padrão**. Estas medidas reduziriam o risco de configurações incorretas, manteriam uma proteção coerente em todos os ambientes geridos pelos clientes e proporcionariam uma maior garantia aos utilizadores. O estabelecimento de uma base de referência de segurança por defeito teria por objetivo conciliar proteção sólida e praticabilidade, garantindo a facilidade de utilização para um vasto leque de organizações de cuidados de saúde. Este esforço implicaria uma estreita colaboração entre os prestadores de serviços de computação em nuvem e o setor da saúde, tirando partido das melhores práticas do setor para criar soluções eficazes e escaláveis.

Formação e desenvolvimento de competências

Dispor de mão de obra com as competências necessárias é importante para o crescimento sustentável a longo prazo e a competitividade na Europa, bem como para a prestação de serviços de elevada qualidade, incluindo serviços de saúde. A escassez de profissionais de cibersegurança qualificados constitui um desafio significativo em toda a Europa, com um défice estimado de 299 000 profissionais para satisfazer as necessidades de mão de obra na UE[35]. De acordo com o Eurobarómetro de 2024 sobre competências de cibersegurança[36], 81 % das empresas consideram que as dificuldades na contratação de pessoal de cibersegurança constituem um dos principais fatores de risco de ciberataque. Nos setores da educação, da saúde e da assistência social, 66 % das funções de cibersegurança são desempenhadas por trabalhadores que transitam de cargos não relacionados com a cibersegurança, o que realça a necessidade urgente de requalificação e melhoria de competências.

Para fazer face a este desafio, o centro de apoio deve colaborar com o futuro consórcio para uma infraestrutura digital europeia (EDIC) no domínio das competências de cibersegurança previsto na Comunicação da Comissão sobre a Academia de Competências de Cibersegurança[37]. O trabalho deve facilitar os intercâmbios entre profissionais de cibersegurança no setor da saúde, como os responsáveis principais pela segurança da informação. Uma potencial ação seria a criação de uma **rede europeia de responsáveis principais pela segurança da informação no domínio da saúde**, começando por um grupo de peritos para partilhar e desenvolver boas práticas, estratégias de retenção de talentos e soluções para atrair profissionais de cibersegurança para o setor da saúde. Além disso, sob a égide da Academia de Competências de Cibersegurança, devem ser desenvolvidos recursos para reforçar a mão de obra no domínio da cibersegurança no setor da saúde, com o apoio do setor e do meio académico. Neste contexto,

[35] *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study* | Plataforma para as Competências e o Emprego na Área Digital.
[36] Eurobarómetro Flash n.º 547 sobre competências de cibersegurança.
[37] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Colmatar o défice de talentos no domínio da cibersegurança para reforçar a competitividade, o crescimento e a resiliência da UE ("Academia de Competências de Cibersegurança")», COM(2023) 207 final.

as partes interessadas do setor devem ser incentivadas a comprometer-se a apoiar o reforço da formação em cibersegurança.

O erro humano continua a ser um dos principais fatores que contribuem para os incidentes de cibersegurança nos cuidados de saúde, o que sublinha a necessidade crítica de formação abrangente do pessoal e de sensibilização para a cibersegurança. Dada a frequência com que os profissionais de saúde utilizam ferramentas digitais, é vital dotá-los de conhecimentos sobre práticas seguras. As ações de formação e campanhas de sensibilização específicas podem reduzir significativamente os riscos. Para o efeito, o centro de apoio deve trabalhar com os profissionais de saúde e prestadores de cuidados de saúde e cooperar com os prestadores de ensino e formação, o setor, o EDIC no domínio das competências de cibersegurança, bem como com as autoridades dos Estados-Membros, a fim de criar e divulgar **módulos e cursos de formação em linha extensos e de fácil acesso**.

A incorporação de módulos de competências digitais e de cibersegurança nos programas de ensino é crucial para criar uma base sólida em matéria de cibersegurança nos cuidados de saúde. Estes módulos devem abordar questões setoriais específicas, como a proteção dos dados dos doentes e as vulnerabilidades de segurança dos dispositivos médicos. O desenvolvimento destes recursos deve ter em conta ações anteriores, como o projeto BeWell, financiado ao abrigo do programa Erasmus+[38], e o projeto PANACEA, financiado ao abrigo do Horizonte 2020[39].

3.2. Capacidades europeias de deteção de ciberameaças contra o setor da saúde

A deteção eficaz de ciberameaças é essencial para uma resposta rápida a incidentes. Os perpetradores de ameaças podem utilizar técnicas para dificultar a deteção de intrusões, o que lhes permite aceder sem autorização a um sistema durante longos períodos[40]. Por conseguinte, melhores capacidades de deteção de ameaças podem ajudar a travar os ciberataques de imediato. Por exemplo, no ataque de *software* de sequestro contra o prestador de serviços de psicoterapia finlandês Vastaamo, durante o qual o perpetrador extorquiu dinheiro a doentes cujos registos confidenciais foram roubados, a intrusão inicial ocorreu em 2018, mas o prestador só teve conhecimento da mesma em 2020[41].

A partilha de informações e a colaboração eficientes são essenciais para melhorar a deteção de ameaças e o conhecimento da situação em toda a UE. As equipas de resposta a incidentes de segurança informática (CSIRT) desempenham um papel fundamental na receção de relatórios de incidentes, quase incidentes e potenciais ameaças, disponibilizando orientações sobre medidas de atenuação a nível nacional. No entanto, **os Estados-Membros são fortemente incentivados a partilhar também todas as notificações de ciberincidentes provenientes de hospitais e prestadores de cuidados de saúde com o centro de**

[38] *BeWell — Blueprint alliance for a future health workforce strategy on digital and green skills*. Disponível em https://bewell-project.eu/.
[39] *PANACEA — Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people.* Disponível em https://cordis.europa.eu/project/id/826293.
[40] *ENISA Health Threat Landscape 2023* (não traduzido para português).
[41] Decisão n.º 1150/161/2021 da Provedoria da proteção de dados finlandesa.

apoio da ENISA, a fim de permitir o conhecimento da situação na UE. Idealmente, esta partilha deve ser acompanhada de uma caracterização significativa das várias dimensões pertinentes dos incidentes, incluindo as vulnerabilidades profundas conhecidas, os efeitos nos serviços de saúde e os acontecimentos adversos para os doentes. Além disso, os fabricantes de dispositivos médicos e de dispositivos para diagnóstico *in vitro* são incentivados a comunicar voluntariamente, através da plataforma única de comunicação de informações a criar e gerir pela ENISA no âmbito do Regulamento de Ciber-Resiliência, as vulnerabilidades ativamente exploradas ou os ciberincidentes graves que tenham impacto na segurança desses dispositivos, bem como, eventualmente, outras vulnerabilidades, incidentes, quase incidentes ou ciberameaças que possam afetar o perfil de risco desses dispositivos.

Se as informações contidas nos relatórios deixarem de ser sensíveis, o centro de apoio poderá criar um catálogo europeu de vulnerabilidades exploradas conhecidas, patrocinado pela ENISA, para dispositivos médicos, sistemas de registos de saúde eletrónicos e fornecedores de equipamento e *software* de TIC no domínio da saúde. Para fazer face aos desafios significativos da deteção de ameaças, o centro de apoio deve introduzir **um serviço de subscrição de alerta rápido à escala da UE para o setor da saúde, que emita alertas em tempo quase real**. Este serviço basear-se-ia em dados tratados provenientes das CSIRT, dos fabricantes e das entidades de prestação de cuidados de saúde, de informações públicas (OSINT) e de outros intervenientes pertinentes, como as plataformas de cibersegurança, os centros de partilha e análise de informações e as autoridades policiais. O reforço da cooperação entre a ENISA e a Agência da União Europeia para a Cooperação Policial (Europol) — por exemplo, no que respeita aos padrões de cibercriminalidade contra o setor da saúde — aumentaria ainda mais o conhecimento da situação.

Os centros de partilha e análise de informações funcionam como recursos centrais para informações sobre ciberameaças, promovendo a partilha bidirecional de informações entre os setores público e privado e o reforço da confiança. O centro de apoio deve intensificar o apoio ao **centro europeu de partilha e análise de informações em matéria de saúde** através da disponibilização de ferramentas e do intercâmbio de informações, de relatórios setoriais de conhecimento da situação, bem como da promoção de uma comunidade de confiança para efeitos de colaboração tática e estratégica. Os Estados-Membros devem incentivar o desenvolvimento de centros nacionais de partilha e análise de informações de saúde[42]. Os centros de partilha e análise de informações devem também ser incentivados a reunir os prestadores de cuidados de saúde com os fabricantes, a fim de permitir um entendimento comum das ameaças de cibersegurança, nomeadamente na cadeia de abastecimento, e facilitar um diálogo sobre a conceção segura de produtos que tenha verdadeiramente em conta as realidades de implantação no terreno.

[42] Por exemplo, a Finlândia dispõe de um centro nacional de partilha e análise de informações para os setores da assistência social e dos cuidados de saúde. Ver Centro Nacional de Cibersegurança finlandês: «ISAC information sharing groups», disponível em https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

3.3.Resposta e recuperação rápidas

Dada a elevada sensibilidade dos dados de saúde dos doentes e os efeitos potencialmente devastadores dos ciberataques nos serviços de saúde, uma resposta rápida e eficaz aos incidentes de cibersegurança é crucial para salvaguardar a segurança dos doentes. Quando um hospital ou um prestador de cuidados de saúde enfrenta um ciberataque, o primeiro ponto de contacto é a CSIRT nacional competente[43]. A CSIRT é responsável pela prestação de apoio atempado, idealmente no prazo de 24 horas, para ajudar a gerir incidentes significativos. No entanto, se um incidente exceder a capacidade da CSIRT, deve ser disponibilizado apoio da UE para assegurar uma resposta rápida e eficaz.

A Reserva de Cibersegurança da UE, criada ao abrigo do Regulamento de Cibersolidariedade, disponibiliza serviços de resposta a incidentes através de prestadores de serviços de segurança geridos de confiança para ajudar a gerir incidentes de cibersegurança significativos ou em grande escala e os esforços iniciais de recuperação. Esta reserva destina-se a complementar os esforços das CSIRT dos Estados-Membros, permitindo-lhes solicitar apoio adicional em casos que envolvam setores críticos como o da saúde. Para reforçar este sistema, a **Comissão e a ENISA devem assegurar que a reserva inclua um serviço de resposta rápida especificamente para o setor da saúde.** Em complementaridade com outros quadros existentes, este serviço destacaria peritos para gerir, sem demora, incidentes de cibersegurança significativos ou em grande escala no setor da prestação de cuidados de saúde quando o apoio nacional fosse insuficiente.

Para melhorar a resposta e a recuperação, o centro de apoio, em colaboração com o Grupo de Cooperação SRI, a rede de CSIRT e, quando pertinente, a Europol, deve elaborar **manuais táticos de resposta a ciberincidentes adaptados ao setor da prestação de cuidados de saúde**. Estes manuais táticos orientariam tanto as CSIRT como as organizações de cuidados de saúde na resposta a ameaças de cibersegurança específicas, incluindo o *software* de sequestro. Dada a importância de uma cooperação eficaz entre as CSIRT e as autoridades policiais na resposta e na investigação de incidentes de cibersegurança de natureza criminosa, os manuais táticos devem, entre outros aspetos, fornecer orientações claras sobre a comunicação desses incidentes às autoridades policiais. Além disso, o centro de apoio poderia **facilitar uma ampla realização de exercícios nacionais de cibersegurança, com base em experiências de exercícios como o exercício «Cyber Europe 2022» da ENISA, para testar os manuais táticos e reforçar os protocolos de resposta a incidentes.**

Para fundamentar as políticas e avaliar a eficácia das medidas tomadas contra ataques de *software* de sequestro, é necessário recolher mais dados. Para o efeito, os Estados-Membros devem solicitar às entidades abrangidas pela Diretiva SRI 2, incluindo as organizações de cuidados de saúde, que comuniquem quaisquer pagamentos de resgate efetuados e os pagamentos de resgate que tencionam efetuar, juntamente com outras informações que forneçam aquando da comunicação de incidentes de cibersegurança significativos. Essa comunicação apoia a investigação eficaz de incidentes com recurso

[43] O artigo 23.º, n.º 1, da Diretiva SRI 2 estabelece a obrigação de as entidades essenciais e importantes notificarem a sua CSIRT, ou, se aplicável, a sua autoridade competente, dos incidentes significativos.

a *software* de sequestro, incluindo o rastreio de pagamentos em plataformas de câmbio de criptomoedas, a fim de identificar os destinatários.

A velocidade de recuperação é um fator crítico para manter a resiliência e a confiança do público, em especial nos cuidados de saúde, em que os períodos de indisponibilidade podem perturbar a prestação de cuidados aos doentes. Para uma recuperação eficaz de ataques de *software* de sequestro, os prestadores de cuidados de saúde têm de dispor de cópias de segurança seguras, atualizadas e isoladas que possam ser rapidamente restauradas. No âmbito do seu catálogo de serviços, o centro de apoio poderia disponibilizar **um serviço por subscrição de recuperação de ataques de *software* de sequestro, ajudando os hospitais e os prestadores de cuidados de saúde a preparar planos de recuperação com antecedência**. A ENISA e a Europol devem colaborar na identificação dos tipos mais comuns de *software* de sequestro que visam as organizações de cuidados de saúde e **alargar o repositório de ferramentas de decifragem** disponíveis no quadro do projeto «No More Ransom»[44]. Devem também elaborar e promover orientações acessíveis para ajudar os prestadores de cuidados de saúde a evitar o pagamento de resgates mediante a utilização de ferramentas de decifragem.

A **Iniciativa Internacional de Combate ao *Software* de Sequestro**[45] constitui uma instância valiosa para o intercâmbio de informações sobre incidentes específicos com recurso a *software* de sequestro, bem como para o desenvolvimento das capacidades dos países membros para reforçar os seus quadros de cibersegurança e as suas capacidades de investigação contra os perpetradores que utilizam este *software*. A Comissão, em colaboração com a alta representante, continuará a promover a cooperação no âmbito da Iniciativa de Combate ao *Software* de Sequestro, nomeadamente contra as ameaças de *software* de sequestro ao setor da saúde. Além disso, a Comissão procurará cooperar no âmbito do **Grupo de Trabalho para a Cibersegurança do G7**, a fim de reforçar a cibersegurança do setor da saúde. Em especial, o grupo de trabalho poderia ponderar a possibilidade de apoiar o setor da saúde contra ameaças como o *software* de sequestro, com base em reflexões como a Declaração Conjunta sobre ataques de *software* de sequestro contra as instalações de cuidados de saúde, de 8 de novembro de 2024, apresentada no contexto do Conselho de Segurança das Nações Unidas[46].

4. Ações nacionais

A capacidade do presente plano de ação para melhorar a cibersegurança no setor da saúde depende da participação ativa e do empenho dos Estados-Membros. Para executar com êxito o plano de ação, os Estados-Membros poderão designar **centros nacionais de apoio à cibersegurança especificamente para hospitais e prestadores de cuidados de saúde**. Estes centros funcionariam como os principais pontos de contacto para o setor da saúde a nível nacional, colaborando estreitamente com o centro de

[44] https://www.nomoreransom.org/pt/index.html.
[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

apoio da ENISA. Sempre que possível e pertinente, os Estados-Membros devem designar organismos existentes, como as CSIRT nacionais no domínio da saúde ou as autoridades competentes, como centros nacionais de apoio à cibersegurança.

Os Estados-Membros são igualmente incentivados a criar **planos de ação nacionais centrados na cibersegurança no setor da saúde**. Estes planos descreveriam os riscos específicos de cibersegurança enfrentados pelos sistemas de saúde e as medidas nacionais em curso para os enfrentar, garantindo simultaneamente uma utilização eficaz dos recursos e das práticas a nível europeu. O centro de apoio da ENISA pode prestar assistência na elaboração destes planos, tendo em conta os planos nacionais já existentes e coordenando esforços para assegurar que os recursos e as estratégias de cada Estado-Membro se complementem.

Outro aspeto fundamental para os Estados-Membros consiste em facilitar a partilha de recursos entre os prestadores de cuidados de saúde, o que poderia ser alcançado através da **contratação conjunta ou da agregação de recursos** a nível nacional, regional ou mesmo europeu. Esta abordagem reduziria os encargos financeiros que recaem sobre cada entidade, aumentando simultaneamente o seu poder de negociação com os prestadores de serviços de cibersegurança.

Por exemplo, o programa CaRE francês[47] introduziu uma série de medidas a nível nacional e regional para dar resposta aos desafios em matéria de recursos: um catálogo de ofertas cibernéticas apresenta uma panorâmica das soluções e dos pacotes cibernéticos disponibilizados aos hospitais através da agência nacional de cibersegurança, da agência de saúde digital, das agências regionais, das organizações nacionais adquirentes, bem como uma panorâmica das soluções comerciais. Este programa é complementado por financiamento adicional destinado às agências regionais para que possam disponibilizar recursos partilhados.

Os Estados-Membros devem também abordar os níveis insuficientes de investimento em cibersegurança no setor da saúde. A fim de assegurar um financiamento adequado, devem estabelecer **parâmetros de referência não vinculativos e monitorizar as metas de financiamento especificamente destinadas à cibersegurança**, garantindo simultaneamente que estes investimentos não prejudiquem a prestação de cuidados essenciais aos doentes. Estas metas de financiamento devem também visar a integração de considerações de segurança em todos os investimentos digitais no setor. Os Estados-Membros podem proceder ao intercâmbio de boas práticas e de aconselhamento sobre estas metas através de plataformas como a rede de saúde em linha[48].

5. Cooperação público-privada

[47] Agence du numérique en santé: *Cybersécurité acceleration et Résilience des Établissements* (CaRE). Disponível em https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] A rede de saúde em linha é uma rede voluntária de autoridades nacionais responsáveis pela saúde em linha designadas pelos Estados-Membros, tendo sido criada por força do artigo 14.º da Diretiva 2011/24/UE.

A cooperação público-privada e a consulta dos prestadores de cuidados de saúde, de outras entidades do setor da saúde, bem como dos intervenientes pertinentes do setor da cibersegurança, são essenciais para o êxito da execução do plano de ação. A fim de continuar a contribuir para o trabalho do centro de apoio, **a Comissão, com o apoio da ENISA, criará um conselho consultivo misto para a cibersegurança no domínio da saúde,** com representantes de alto nível de ambos os domínios — cuidados de saúde e cibersegurança —, que poderá prestar aconselhamento à Comissão e ao centro de apoio sobre ações com impacto e debater o desenvolvimento de parcerias público-privadas neste domínio. O conselho basear-se-á nos esforços envidados no âmbito das parcerias público-privadas, incluindo o centro europeu de partilha e análise de informações em matéria de saúde.

Além disso, a Comissão lançará **um apelo à ação**, dirigido às empresas de cibersegurança, às fundações, aos estabelecimentos de ensino e às partes interessadas do setor, para que **se comprometam a tomar medidas para dar resposta aos desafios enfrentados pelo setor**. Esses compromissos podem basear-se na experiência da Academia de Competências de Cibersegurança e incluir, por exemplo, no âmbito dessa academia, a ministração de cursos de formação e a disponibilização de materiais centrados no setor da saúde destinados aos profissionais de cibersegurança[49]. Outros compromissos poderão também incidir em atividades de sensibilização ou na prestação de serviços de segurança geridos a entidades particularmente vulneráveis, a título gratuito ou a custo reduzido, a fim de aumentar a sua preparação e resiliência em matéria de cibersegurança. Além disso, os compromissos poderão consistir na partilha de informações sobre ciberameaças com o centro de apoio da ENISA. O centro de apoio deve manter uma panorâmica dos compromissos assumidos no âmbito do apelo à ação, com o objetivo de assegurar a sua coerência e complementaridade.

6. Dissuasão dos perpetradores de ciberameaças

As políticas internas e externas da UE em matéria de cibersegurança devem apoiar o objetivo de dissuadir os perpetradores de ciberameaças de atacarem os sistemas de saúde europeus. Os ciberataques contra organizações de cuidados de saúde são um tipo particularmente inaceitável de ciberatividade maliciosa, dada a sua capacidade para ameaçar a segurança dos doentes e a vida humana. Por conseguinte, as capacidades de dissuasão da UE no domínio da cibersegurança e da aplicação da lei, na sua plenitude, devem ser utilizadas para comprometer o modelo de negócio global dos perpetradores de ameaças que visam o setor da saúde e privá-los de lucros fáceis. Tal incluirá a promoção de investigações transfronteiriças através de uma maior partilha de indicadores de comprometimento e de outros dados pertinentes, bem como uma maior ênfase nos alvos de elevado valor e nos principais facilitadores criminosos, como os serviços de alojamento blindado ou de mistura de criptomoedas.

O **conjunto de instrumentos de ciberdiplomacia** proporciona um quadro para prevenir, dissuadir e responder a ciberataques contra a UE, os Estados-Membros e os parceiros. A alta representante continuará a utilizar o atual quadro de cibersanções para dar resposta às ameaças que visam os sistemas de saúde.

A responsabilização dos criminosos pelos seus atos constitui um importante fator de dissuasão. Por conseguinte, os Estados-Membros devem assegurar que a aplicação da lei seja plenamente integrada nos

[49] Academia de Cibercompetências: Participe | Plataforma para as Competências e o Emprego na Área Digital.

seus planos de ação nacionais. Em especial, devem utilizar plenamente as disposições da Diretiva relativa a ataques contra os sistemas de informação[50] e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa para dissuadir ataques, levar os criminosos a tribunal e desmantelar as infraestruturas criminosas que facilitam os ataques[51]. A aplicação bem-sucedida destas ferramentas deve assegurar que as ações criminosas e maliciosas contra os cuidados de saúde sejam punidas.

7. Execução e acompanhamento do plano de ação

Ao longo do presente plano de ação, foram previstas várias tarefas para a criação de um centro de apoio na ENISA. Deste modo, garante-se uma execução holística e coerente do plano de ação, evitando simultaneamente a criação de novas entidades suscetível de conduzir a potenciais sobreposições e custos gerais. A Comissão tenciona assegurar a disponibilização de recursos adequados ao centro de apoio.

Assim que o centro de apoio estiver operacional, a ENISA, em consulta com a Comissão, deve fornecer regularmente atualizações sobre o trabalho do centro de apoio ao Conselho de Administração da ENISA, bem como às redes pertinentes dos Estados-Membros, em especial ao Grupo de Cooperação SRI, à rede de CSIRT, à rede de saúde em linha e, quando pertinente, ao Conselho do Espaço Europeu de Dados de Saúde. Além disso, a ENISA deve manter com o conselho consultivo público-privado para a cibersegurança no domínio da saúde um intercâmbio contínuo de informações sobre a execução das ações previstas pelo centro de apoio.

Os relatórios periódicos da ENISA, como o relatório sobre o estado da cibersegurança na União, que fornece uma avaliação agregada do nível de maturidade das capacidades e dos recursos em matéria de cibersegurança em toda a UE, nomeadamente no setor da saúde, devem servir de ocasião para publicar dados pertinentes, apoiando o acompanhamento do plano de ação. Além disso, o índice de cibersegurança da UE da ENISA[52] pode fornecer dados quantitativos e qualitativos, servindo de base factual para avaliar a criticalidade e a maturidade do setor da saúde.

8. Próximas etapas

A presente comunicação estabeleceu uma agenda ambiciosa para reforçar a cibersegurança do setor da saúde na UE. Com a proposta de desenvolvimento do Centro de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde no seio da ENISA, o plano de ação estabelece uma via para a criação de uma abordagem europeia coerente e partilhada do desafio da cibersegurança no setor.

---

[50] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.

[51] Convenção sobre o Cibercrime (Convenção de Budapeste, STCE n.º 185) e respetivos protocolos: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[52] ENISA, *EU Cybersecurity Index, Framework and Methodological Note* (não traduzido para português), 2024. Disponível em https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

A presente comunicação deve ser vista como o início de um processo destinado a melhorar a cibersegurança no setor da saúde. Por conseguinte, a adoção do plano de ação será acompanhada do lançamento de amplas consultas das partes interessadas e da prossecução dos intercâmbios com os Estados-Membros e as redes pertinentes para recolher informações. Com base nos resultados das consultas, a Comissão tenciona apresentar, no quarto trimestre de 2025, recomendações destinadas a aperfeiçoar ainda mais o plano de ação.

A Comissão insta os Estados-Membros e todas as partes interessadas a trabalharem em conjunto para concretizar a ambição do plano de ação.

ANEXO — Síntese das ações propostas

A Comissão:

Centro de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde da ENISA	
Garantir recursos adequados para o Centro de Apoio à Cibersegurança Trabalhar com o ECCC para lançar projetos-piloto com o intuito de desenvolver boas práticas em matéria de ciber-higiene e avaliação dos riscos de segurança, bem como para dar resposta à necessidade de monitorização contínua da cibersegurança, informações sobre ameaças e resposta a incidentes utilizando soluções de cibersegurança de ponta, tendo em vista o desenvolvimento do catálogo de serviços do Centro Europeu de Apoio à Cibersegurança	2025
Prevenção de incidentes de cibersegurança	
Em consulta com o Grupo de Cooperação SRI, a UE-CyCLONe e a ENISA, explorar a possibilidade de identificar a saúde como um setor elegível para receber apoio para a realização de testes coordenados de preparação ao abrigo do Regulamento de Cibersolidariedade	T1 2025
Resposta e recuperação rápidas	
Juntamente com a ENISA, garantir que a Reserva de Cibersegurança da UE inclua um serviço de resposta rápida especificamente para o setor da saúde	T4 2025
Cooperação público-privada	
Com o apoio da ENISA, criar um conselho consultivo misto para a cibersegurança no domínio da saúde	T1 2025
Lançar um apelo à ação, dirigido às empresas de cibersegurança, às fundações, aos estabelecimentos de ensino e às partes interessadas do setor, no sentido de se comprometerem a tomar medidas para dar resposta aos desafios enfrentados pelo setor da saúde	T2 2025
Dissuasão dos perpetradores de ciberameaças	
Em conjunto com a alta representante, explorar a utilização das medidas do conjunto de instrumentos de ciberdiplomacia para prevenir, desencorajar, dissuadir	2025

e responder a atividades maliciosas contra os sistemas de saúde	
Promover a cooperação internacional contra os perpetradores que utilizam *software* de sequestro, nomeadamente no âmbito da Iniciativa Internacional de Combate ao *Software* de Sequestro, em colaboração com a alta representante	2025-2026
Procurar cooperar no âmbito do Grupo de Trabalho para a Cibersegurança do G7, a fim de reforçar a cibersegurança do setor da saúde	2025-2026
Próximas etapas	
Lançar amplas consultas das partes interessadas	T1 2025
Adotar recomendações destinadas a aperfeiçoar ainda mais o plano de ação	T4 2025

ENISA:

Centro Europeu de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde	
Iniciar os trabalhos de criação de um Centro Europeu de Apoio à Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde	T2 2025
Desenvolver um catálogo abrangente de serviços a prestar pelo Centro de Apoio à Cibersegurança	A partir do T4 2025
Prevenção de incidentes de cibersegurança	
Emitir orientações que destaquem as práticas de cibersegurança mais críticas e ajudem os prestadores de cuidados de saúde a aplicá-las	T3 2025
Desenvolver, em estreita colaboração com a Comissão e os Estados-Membros, uma ferramenta de levantamento da regulamentação	T1 2025
Desenvolver um quadro para as avaliações da maturidade em matéria de cibersegurança específicas para os cuidados de saúde	T3 2025
Realizar uma avaliação anual da maturidade em matéria de cibersegurança no setor da saúde	2025-2026

Colaborar com os Estados-Membros e as autoridades responsáveis pelos programas regionais para criar programas-modelo de vales de cibersegurança	2025-2026
Elaborar novas diretrizes em matéria de contratação para cibersegurança dos hospitais e dos prestadores de cuidados de saúde	T3 2025
Criar uma rede europeia de responsáveis principais pela segurança da informação no domínio da saúde	T1 2026
Conceber e promover módulos e cursos de formação destinados a profissionais de saúde	T1 2026
Capacidades europeias de deteção de ciberameaças contra o setor da saúde	
Criar um catálogo europeu de vulnerabilidades exploradas conhecidas para dispositivos médicos, sistemas de registos de saúde eletrónicos e fornecedores de equipamento e *software* de TIC no domínio da saúde	T4 2025
Introduzir um serviço de subscrição de alerta rápido à escala da UE para o setor da saúde	A partir de 2026
Apoiar o centro europeu de partilha e análise de informações em matéria de saúde através da disponibilização de ferramentas e do intercâmbio de informações	2025-2026
Resposta e recuperação rápidas	
Juntamente com a Comissão, garantir que a Reserva de Cibersegurança da UE inclua um serviço de resposta rápida especificamente para o setor da saúde	T4 2025
Em colaboração com a rede de CSIRT, elaborar manuais táticos de resposta a ciberincidentes adaptados ao setor da prestação de cuidados de saúde	T3 2025
Facilitar a realização de exercícios nacionais de cibersegurança em grande escala para testar os manuais táticos e reforçar os protocolos de resposta a incidentes	A partir do T4 2025
Prestar um serviço por subscrição de recuperação de ataques de *software* de sequestro	A partir de 2026
Juntamente com a Europol, identificar os tipos mais comuns de *software* de sequestro que visam as	T4 2025

organizações de cuidados de saúde e alargar o repositório de ferramentas de decifragem no quadro do projeto «No More Ransom»	
Em conjunto com a Europol, elaborar orientações acessíveis para ajudar os prestadores de cuidados de saúde a evitar o pagamento de resgates	T3 2025
Ações nacionais	
Ajudar os Estados-Membros na elaboração de planos de ação nacionais	2025
Coordenar esforços para assegurar que os recursos e as estratégias de cada Estado-Membro se complementem	2025-2026
Execução e acompanhamento do plano de ação	
Em consulta com a Comissão, fornecer regularmente atualizações sobre o trabalho do Centro de Apoio à Cibersegurança às redes pertinentes dos Estados-Membros	2025-2026
Manter um intercâmbio contínuo de informações com o conselho consultivo para a cibersegurança no domínio da saúde	2025-2026

Estados-Membros:

Capacidades europeias de deteção de ciberameaças contra o setor da saúde	
Partilhar notificações de ciberincidentes provenientes de hospitais e prestadores de cuidados de saúde nos termos da Diretiva SRI 2 com o Centro Europeu de Apoio à Cibersegurança	A partir do T4 2025
Incentivar o desenvolvimento de centros nacionais de partilha e análise de informações de saúde	2025-2026
Prevenção de incidentes de cibersegurança	
No âmbito do Grupo de Cooperação SRI, realizar uma avaliação coordenada dos riscos de segurança, aferindo os riscos técnicos e estratégicos relacionados com as cadeias de abastecimento de dispositivos médicos	T4 2025

Resposta e recuperação rápidas	
Realizar exercícios nacionais de cibersegurança para testar os manuais táticos e reforçar os protocolos de resposta a incidentes	A partir de 2026
Ações nacionais	
Designar centros nacionais de apoio à cibersegurança dos hospitais e dos prestadores de cuidados de saúde	T2 2025
Criar planos de ação nacionais centrados na cibersegurança no setor da saúde	T4 2025
Facilitar a partilha de recursos entre os prestadores de cuidados de saúde	2025-2026
Estabelecer parâmetros de referência não vinculativos e monitorizar as metas de financiamento especificamente destinadas à cibersegurança	T4 2025
Solicitar às organizações de cuidados de saúde e a outras entidades abrangidas pela Diretiva SRI 2 que comuniquem as suas intenções de pagar resgates	T4 2025