PRÉMIOS DE SEGURANÇA
SECURITY MAGAZINE | REVISTA DOS PROFISSIONAIS DE SEGURANÇA

Serviços Partilhados do Ministério da Saúde – SPMS - Equipa

A Serviços Partilhados do Ministério da Saúde, E.P.E. (SPMS) integra na sua estratégia de segurança da informação a colaboração com um parceiro que presta serviços dedicados de operações de segurança (Security Operations Centre - SOC). Esta prestação de serviços reforça e complementa as capacidades internas da equipa de resposta a incidentes de cibersegurança da SPMS (CSIRT-SPMS), com atividades de monitorização e deteção proativa em regime 24/7, análise e resposta a eventos e incidentes, entre outros. O SOC reforça, assim, a visibilidade sobre a comunidade e âmbito abrangido pela CSIRT-SPMS, permitindo identificar ameaças e riscos em tempo real e escalar rapidamente situações anómalas.

A CSIRT-SPMS, foi formalmente constituída a 17 de dezembro de 2019. No entanto, nos últimos anos, existiram várias reestruturações da mesma, nomeadamente em termos de governação, âmbito e comunidade abrangida e atividades realizadas. Estas alterações decorrem da necessidade de um alinhamento estratégico com a evolução do contexto nacional e europeu em matéria de cibersegurança e segurança da informação, bem como da adaptação às disposições legais e regulamentares aplicáveis, garantindo uma resposta mais eficaz, coordenada e adequada aos desafios emergentes neste domínio.

A CSIRT-SPMS insere-se na Unidade de Cibersegurança, que reporta hierarquicamente ao Conselho de Administração da SPMS.

A equipa interna da CSIRT-SPMS é composta, atualmente, por 10 colaboradores, incluindo funções de gestão, análise e resposta a incidentes, gestão de vulnerabilidades, engenharia e threat intelligence, garantindo e contribuindo para a capacidade operacional para as atividades de deteção, proteção e resposta a incidentes.

A equipa CSIRT-SPMS visa a proteção das infraestruturas centrais de TI que suportam os serviços aplicacionais internos da SPMS, bem como os serviços proporcionados a entidades externas, nomeadamente a entidades que executem atividades específicas da área da saúde. O CSIRT-SPMS contribui ainda para o reforço de cibersegurança das entidades ligadas à Rede de Informação da Saúde (RIS), englobando serviços limitados para o eSIS (Ecossistema Sistemas de Informação da Saúde) constituído por entidades do Ministério da Saúde e Serviço Nacional de Saúde (MS/SNS). Como funções principais desta equipa inclui-se a monitorização permanente, a deteção precoce de ameaças e a resposta estruturada a incidentes e vulnerabilidades. O CSIRT-SPMS realiza a triagem, a contenção, a erradicação e a recuperação, apoiado por análises técnicas e, quando necessário, forenses, que permitem identificar causas, vetores de ataque e definir recomendações eficazes para as equipas internas ou entidades do MS/SNS. A equipa promove igualmente a implementação de controlos e boas práticas de segurança transversais à SPMS e MS/SNS, com vista à contribuição para uma postura de segurança coerente e ativa num ecossistema tecnologicamente e processualmente heterogéneo.

A segurança da informação e a cibersegurança na SPMS assume um papel essencial e estratégico interno e no MS/SNS, decorrente da missão que desempenha no setor da saúde e na prestação de serviços críticos e essenciais nacionais. A crescente sofisticação das ameaças de cibersegurança, conjugada com a responsabilidade de ser uma entidade prestadora de serviços centralizados num setor essencial como é a saúde, exige uma abordagem proativa, diversificada e estruturada, onde a aplicação de medidas proativas e

preventivas são essenciais para manter a resiliência digital da organização e do ecossistema. Assim, a segurança na SPMS é abordada de forma holística e considerada como um elemento essencial para garantir a fiabilidade, a confiança, salvaguarda de dados sensíveis e a continuidade dos serviços digitais na saúde, assegurando um SNS mais seguro, resiliente e preparado para os desafios do presente e futuro.

A SPMS é um pilar tecnológico fundamental para o MS/SNS, pelo que garantir a disponibilidade, integridade e confidencialidade da informação, sistemas, redes e infraestruturas não é apenas uma necessidade operacional, mas um compromisso inegociável para com todo serviço público, profissionais da área da saúde e o cidadão. Em particular, a SPMS desempenha um papel fundamental no modelo de governação da política de cibersegurança no ecossistema da saúde em Portugal, resultando numa responsabilidade acrescida para promover uma cultura e práticas de gestão de risco no ecossistema de saúde. A SPMS assume um compromisso contínuo com a cibersegurança, refletido na melhoria contínua das suas políticas e práticas, garantindo o cumprimento da regulação em vigor e alinhada com as melhores práticas internacionais e de referência. Esta estratégia tem em vista garantir um ambiente tecnológico resiliente, protegido contra ameaças emergentes e preparado para sustentar a inovação e a excelência na prestação de serviços de saúde. Por sua vez, a CSIRT-SPMS desempenha um papel fundamental em toda esta estratégia, assegurando uma monitorização contínua de ameaças e riscos no contexto SPMS e MS/SNS e uma capacidade de reação ágil e eficaz para antecipação e minimização de impactos e efeitos adversos decorrentes de incidentes ou vulnerabilidades de cibersegurança.

O reconhecimento internacional da maturidade da SPMS foi consolidado com a integração do CSIRT-SPMS na rede FIRST (Forum of Incident Response and Security Teams, rede global de equipas de resposta a incidentes) e na TF-CSIRT (Task Force on Computer Security Incident Response Teams, comunidade europeia que promove a colaboração, confiança e partilha de boas práticas entre CSIRTs), que validam práticas técnicas e organizacionais alinhadas com os padrões mais exigentes na resposta a incidentes e na cooperação transfronteiriça.

A cibersegurança no setor da saúde é, por si só, um desafio pois contempla os desafios da cibersegurança num setor crítico e essencial como a saúde, onde está em causa a saúde e vida das pessoas. A SPMS enfrenta desafios significativos decorrentes da sua própria responsabilidade enquanto prestadora de serviços centralizados para o setor da Saúde.

A necessidade de garantir a continuidade e a disponibilidade de sistemas críticos que suportam o funcionamento de unidades de saúde, a proteção de dados sensíveis de milhões de cidadãos, não descurando da inovação e disponibilização de novos serviços alinhados com as necessidades da sociedade moderna, exige uma abordagem rigorosa e proativa. Além disso, a complexidade do ecossistema do MS/SNS, composto por centenas de entidades com diferentes níveis de maturidade, infraestruturas e estratégias distintas e cujos serviços, muitas vezes críticos de saúde são suportados por plataformas tecnológicas, dificultam a atualização e a uniformização de controlos de segurança. Aliado a isto, cada vez, mais a prestação de cuidados contempla aplicações, tecnologias emergentes e dispositivos médicos usados diretamente pelos cidadãos, aumentando a superfície de ataque, conjugado com o elevado valor dos dados de saúde em mercados da darkweb.

A SPMS promove várias atividades de sensibilização e formação de cibersegurança, com enfoque em vários domínios e dimensões, desde as práticas de ciber-higiene que os colaboradores têm de conhecer e aplicar

no seu dia-a-dia, às práticas de desenvolvimento seguro que devem ser aplicadas pelas equipas de desenvolvimento. A SPMS proporciona inúmeras ações formativas e sessões de sensibilização abrangendo diferentes públicos através de formações presenciais ou online, digital learnings e workshops específicos. Muitas destas formações ou ações estão disponíveis para os mais de 180 mil profissionais da área da saúde. Além das formações, a SPMS dissemina regularmente conteúdos informativos nos canais internos (Newsletters, Intranet) e públicos (redes sociais, websites) englobando não só os profissionais de saúde, mas também a capacitação dos cidadãos.

A SPMS promove ainda exercícios de phishing e dinamiza e participa em exercícios de cibersegurança como Capture The Flags e exercícios table top com vista a testar os seus procedimentos. A estratégia de formação e capacitação é baseada numa abordagem de capacitação contínua dos utilizadores, garantindo que todos compreendem as suas responsabilidades no cumprimento das políticas e normas de cibersegurança e os impactos que poderão advir de comportamentos inadequados.

A SPMS rege a sua atividade de acordo com os seguintes valores: Legalidade, Não discriminação, Igualdade de tratamento e imparcialidade, Proporcionalidade, Coerência, Boa-fé e transparência, Comunicação e partilha de informação, a Excelência profissional, bem como a Cordialidade e solidariedade. A equipa CSIRT-SPMS orienta igualmente a sua atuação por estes princípios, assegurando que todas as suas atividades se encontram alinhadas com os mesmos, reforçando-os através de uma cultura assente no rigor, na colaboração, na responsabilidade e no espírito de serviço público. O rigor traduz-se na adoção de práticas e metodologias alinhadas com referenciais nacionais e internacionais, promovendo a melhoria contínua, a qualidade e a consistência da resposta. A colaboração assenta no reconhecimento de que a cibersegurança só é eficaz quando existe articulação, confiança e partilha entre as várias partes interessadas, incluindo equipas internas da SPMS, entidades do MS/SNS e parceiros externos. Por sua vez, a responsabilidade e o espírito de serviço público refletem a consciência de que cada incidente prevenido ou mitigado pode ter impacto direto na prestação de cuidados de saúde e, consequentemente, na vida das pessoas. O lema, como não podia deixar de ser, é contribuir diariamente para uma segurança digital com impacto real na vida das pessoas.

A CSIRT-SPMS utiliza um conjunto integrado de tecnologias avançadas para prevenir, detetar e responder a incidentes de segurança. Entre estas, destacam-se soluções de monitorização contínua e correlação de eventos (SIEM - Security Information and Event Management), que permitem a identificação atempada de comportamentos anómalos e potenciais ameaças. Adicionalmente, são utilizadas plataformas de threat intelligence para contextualização de riscos emergentes, bem como ferramentas de gestão de vulnerabilidades, que permitem identificar vulnerabilidades, contribuindo para a antecipação de riscos e para a redução da superfície de ataque No domínio da proteção perimetral, são utilizadas tecnologias de segurança de rede, incluindo firewalls, sistemas de deteção e prevenção de intrusões (IDS/IPS) e soluções de segurança de DNS, que permitem bloquear comunicações maliciosas, prevenir acessos indevidos e mitigar ataques como phishing ou command and control. A equipa recorre ainda a plataformas de gestão de incidentes, que asseguram o registo, tratamento, priorização e acompanhamento estruturado de todos os eventos de segurança, bem como a plataformas de gestão de conhecimento, que promovem a partilha de informação, lições aprendidas e procedimentos normalizados. São igualmente utilizadas soluções de automação e orquestração, que permitem acelerar processos de triagem, contenção e resposta a incidentes, aumentando a eficiência operacional e reduzindo o tempo de resposta. Estas tecnologias são

suportadas por uma abordagem contínua de melhoria, baseada na análise de incidentes e na adaptação a novas ameaças, contribuindo para o reforço da resiliência e da segurança dos sistemas de informação no setor da saúde.

A equipa CSIRT-SPMS distingue-se pelo impacto direto da sua atuação na continuidade e segurança da prestação de cuidados de saúde.

A natureza crítica do setor da saúde confere à equipa um elevado sentido de responsabilidade, onde cada ação de prevenção, deteção ou resposta a incidentes pode ter implicações reais na saúde e vida dos cidadãos. Destaca-se igualmente pela sua credibilidade e reconhecimento a nível nacional e internacional, sendo membro reconhecido de comunidades de referência como a Rede Nacional de CSIRT (estrutura de cooperação entre equipas nacionais de resposta a incidentes), a FIRST (Forum of Incident Response and Security Teams, rede global de equipas de resposta a incidentes) e a TF-CSIRT (Task Force on Computer Security Incident Response Teams, comunidade europeia que promove a colaboração, confiança e partilha de boas práticas entre CSIRTs). Esta participação ativa permite o acesso a informação privilegiada sobre ameaças, a partilha de boas práticas e o reforço da capacidade de resposta a incidentes, alinhando a equipa com os mais elevados padrões internacionais. A equipa assegura ainda uma articulação estreita com as entidades do Ministério da Saúde, do SNS e com parceiros externos, potenciando atividades de proteção proativa da Rede de Informação da Saúde (RIS) e uma resposta coordenada e eficaz. Paralelamente, participa regularmente em exercícios nacionais e internacionais, reforçando a sua preparação e contribuindo para uma cultura de melhoria contínua. Adicionalmente, a CSIRT-SPMS assume um papel ativo na promoção da maturidade em cibersegurança no setor da saúde, apoiando as organizações na adoção de boas práticas e fomentando a antecipação de ameaças num contexto cada vez mais complexo e interligado. Por fim, destaca-se pela combinação entre rigor técnico, capacidade de adaptação e espírito de missão, posicionando-se como um pilar essencial na proteção da segurança digital do setor da saúde em Portugal.

O trabalho da CSIRT-SPMS tem contribuído de forma decisiva para o aumento da maturidade de segurança da SPMS e MS/SNS, estruturando e robustecendo capacidades e mecanismos que hoje permitem à SPMS e SNS operar com maior resiliência.

A evolução começa pela consolidação de capacidades de monitorização contínua, deteção e resposta a incidentes, que permite passar de um modelo reativo para uma postura preventiva e orientada ao risco. A implementação de tecnologias de deteção proativa de vulnerabilidades, incidentes e 'threat intelligence', aliadas ao desenvolvimento de procedimentos estruturados, criou uma base operacional robusta que sustenta decisões e ações rápidas e consistentes.

A equipa tem tido também um papel fundamental na uniformização de boas práticas em todo o ecossistema do MS/SNS, contribuindo para a adoção transversal de medidas estruturantes de hardening, gestão de acessos, segmentação de redes, desenvolvimento seguro, reforço dos controlos técnicos, entre outros. Esta capacidade de normalização é particularmente relevante num setor com grande heterogeneidade e maturidade tecnológica, permitindo elevar o nível de segurança.

Paralelamente, a equipa CSIRT-SPMS impulsionou uma cultura de segurança mais consciente e responsável, através de campanhas de sensibilização e apoio direto às unidades de saúde e cidadãos. O aumento da literacia em segurança entre profissionais clínicos, técnicos e cidadãos contribui para reduzir incidentes evitáveis e fortalecer o papel do fator humano como primeira linha de defesa.

No domínio estratégico, a equipa reforçou a implementação de metodologias alinhadas com referenciais internacionais apoiando auditorias, análises de risco e certificações como a do Selo de Maturidade Digital de Cibersegurança - nível Ouro que permitiram à SPMS identificar lacunas e priorizar atividades. Finalmente, a resposta coordenada a incidentes, a participação ativa em grupos de trabalho nacionais e europeus e o desenvolvimento de recomendações setoriais reforçaram a posição da SPMS enquanto referência na cibersegurança em saúde. Em conjunto, estes contributos consolidaram uma maturidade significativamente superior, assente numa abordagem integrada, resiliente e orientada à proteção contínua dos serviços essenciais da SPMS e do SNS.

Em 2025, a equipa CSIRT-SPMS consolidou a sua maturidade e posicionamento no ecossistema de cibersegurança, alcançando marcos relevantes ao nível da cooperação internacional, capacitação operacional e resiliência do setor da saúde. Destaca-se a integração em comunidades internacionais de referência, nomeadamente a adesão à FIRST, após um processo de avaliação técnica e organizacional. A CSIRT-SPMS integrou e evoluiu no modelo de maturidade da TF-CSIRT, alcançando o nível Accredited, um selo de confiança que atesta boas práticas e capacidade de resposta a incidentes.

A equipa contribuiu para a Certificação do Selo de Maturidade Digital de Cibersegurança nível Ouro da SPMS, promovendo a adoção de práticas e controlos de segurança e uma abordagem estruturada à gestão do risco. No domínio operacional, destaca-se a participação nos exercícios internacionais “Ciber Perseu 2025” e “Boss of the SOC” reforçando competências práticas de deteção e resposta a incidentes. Foram desenvolvidas ações de mitigação de ameaças, com identificação proativa de vulnerabilidades e remoção de sites maliciosos ou fraudulentos associados ao SNS, contribuindo para a proteção dos utilizadores e da confiança nos serviços digitais.

A CSIRT-SPMS teve um papel ativo na sensibilização para riscos de cibersegurança, com destaque para campanhas de alerta e prevenção de smishing dirigidas a utentes e profissionais do SNS, promovendo comportamentos seguros e redução da exposição a fraudes. Paralelamente, a equipa reforçou as suas capacidades de prevenção, deteção e resposta a incidentes na SPMS e no MS/SNS, contribuindo para a proteção das infraestruturas digitais e para a continuidade de serviços críticos de saúde. Estes resultados refletem o compromisso da equipa com a excelência, a melhoria contínua e a antecipação de ameaças, posicionando a CSIRT-SPMS como um pilar na proteção do ecossistema digital da saúde em Portugal.