Revista Portuguesa de Diabetes. 2023; 18 (1): 34-38

Diabetes e Cibersegurança: O Elefante na Sala?

Diabetes and Cybersecurity: The Elephant in the Room?

H. Carmona Alexandrino, D. Ramalho, M. Almeida Ferreira, M. João Oliveira
Serviço de Endocrinologia, Centro Hospitalar Vila Nova de Gaia/Espinho, Vila Nova de Gaia, Portugal.

> INTRODUÇÃO

A Diabetes *Mellitus* (DM) é uma doença com uma incidência crescente no mundo, sendo a única das 4 principais doenças não comunicáveis cuja mortalidade precoce tem vindo a aumentar. [1] O uso de dispositivos médicos na Diabetes (DMD) como glucómetros, *smartpens* e os sistemas de monitorização contínua de glicose (MCM), têm assumido um papel cada vez mais relevante no tratamento atual da pessoa com DM, estando amplamente difundidos. Estes dispositivos ajudam a pessoa com DM a tomar melhores decisões no dia-a-dia, quanto à sua doença. Se, nos primórdios, estes DMD funcionavam de forma isolada e estanque, atualmente encontram-se cada vez mais conectados a outros dispositivos (*smartphones*, *smartwatches*) e também à *internet* e à *cloud*. Este nível de integração e centralização de dados tem vantagens e possibilitará, no futuro, a criação de um verdadeiro pâncreas artificial. No entanto também escondem uma verdade inconveniente, por possibilitarem o extravio, roubo ou adulteração de informação pessoal e médica de forma remota. A cibersegurança, num mundo cada vez mais digital, deverá também fazer parte dos pilares do tratamento da DM dado que, se esta não estiver assegurada, a pessoa com DM poderá correr sérios riscos.

CORRESPONDÊNCIA/*CORRESPONDENCE*

Henrique Carmona Alexandrino
R. Conceição Fernandes S/N,
4434-502 Vila Nova de Gaia
Portugal
E-mail: jhenriquealexandrino@gmail.com

> O QUE É A SEGURANÇA DIGITAL (CIBERSEGURANÇA)?

O termo **segurança** pode ser definido, de acordo com Serviços Partilhados do Ministério da Saúde, [2] como sendo o *"processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação"*, estando assente em três pilares fundamentais: confidencialidade, integridade e disponibilidade. A confidencialidade significa que a informação é somente acessível a pessoas devidamente autorizadas e por utilizadores legítimos; a integridade garante que a informação é verdadeira e que não pode ser alvo de modificação por terceiros; e a disponibilidade, que esta informação está acessível sempre que é necessário. Deste modo, a **cibersegurança** destina-se à prática de proteger as informações digitais, dispositivos, programas, computadores, redes e dados contra qualquer tipo de ameaça cibernética, de danos e intrusão ilícita. Promover a cibersegurança será também promover a saúde da pessoa com DM, visto que este poderá sair lesado, caso haja comprometimento dos seus dados pessoais e médicos.

> QUAL A RELEVÂNCIA DA CIBERSEGURANÇA NA ÁREA DA SAÚDE?

Quais poderão ser as motivações para o roubo de informação médica pessoal? A informação deve ser vista como um ativo, com valor para negócios ou atividades lícitas ou ilícitas e, como tal, deve ser protegida. Em particular, a informação médica pessoal é uma informação muito sensível, dado que é imutável e muito valiosa na economia paralela.
Desde a pandemia *Coronavirus disease* 2019 (COVID-19), tem havido um aumento relevante no volume de incidentes de cibersegurança (cibercrime) contra infraestru-

Recebido/Received: 28/12/2022; Aceite/Accepted: 30/04/2023.

turas de saúde um pouco por todo o mundo. [3] Portugal também não foi exceção e várias infraestruturas médicas, públicas e privadas, também foram visadas. Estes ataques tiveram um propósito disruptivo ou financeiro, sendo usados vários métodos, como por exemplo: 1) *ransomware*, que cifra informação fulcral para o funcionamento da entidade, tornando-o indisponível, associando-se um pedido um resgaste; 2) ataques DDoS (*denial of service*), que impossibilitam o acesso aos serviços digitais da entidade; 3) e ainda por ataques de *phishing*, dirigida a colaboradores ou utentes da entidade, com o fim de furtar dados sensíveis. Este tipo de ataques tem impacto relevante nos cuidados assistenciais aos doentes. Nalguns casos, houve atraso ou cancelamento de consultas e cirurgias por perda de acesso aos registos clínicos, assim como constrangimentos nos serviços clínicos, pela necessidade de voltar a utilizar registos em papel. Em Portugal, que os autores saibam, não houve nenhuma morte diretamente relacionada com o cibercrime. No entanto, na Europa, em particular na Alemanha, em 2020, já terá ocorrido pelo menos uma morte devido a um ataque informático (*ransomware*), o que resultou num atraso ao acesso de cuidados médicos, dado que a doente teve que ser transferida para outro hospital. [4] As redes hospitalares são um alvo apetecível, já que, para além de possuírem um manancial de informação sensível, frequentemente têm sistemas de informáticos desatualizados, recursos humanos sobrecarregados, mal-financiados e com múltiplos pontos de acesso passíveis de serem aproveitados. No futuro, a tendência será um aumento deste tipo de ataques, o que reflete um mundo cada vez mais digital e interligado. Hoje em dia já não se discute se os sistemas de saúde serão afetados, mas sim em que momento, durante quanto tempo e de que forma. Torna-se assim fulcral cada vez mais pensar na cibersegurança como um investimento nos cuidados de saúde, a oferecer a nível populacional. Sem um sistema de segurança informático robusto, estamos à mercê de qualquer cidadão ou grupo de indivíduos com objetivos maliciosos. No caso específico da pessoa com DM, hoje, têm à sua disposição, múltiplos dispositivos médicos de fácil acesso e utilização. Estes dispositivos permitem ligação à internet e aos *smartphones*, sendo até encorajados pelos próprios fabricantes dos dispositivos. Esta conetividade, que traz vantagens indubitáveis às pessoas com DM, aumenta concomitantemente o risco de haver um comprometimento dos seus dados pessoais.

> CIBERSEGURANÇA NA DIABETES *MELLITUS*

Há múltiplos dispositivos médicos disponíveis para a pessoa com DM, com diferentes níveis de acessibilidade, para medir, registar e controlar os seus níveis de glicemia. Em termos conceptuais, temos quatro tipos de dispositivos médicos disponíveis: glucómetros, MCG, dispositivos de Perfusão Subcutânea Contínua de Insulina (PSCI) e, ainda, sistemas fechados (*closed-loop*) ou pâncreas artificial.

Graças ao rápido desenvolvimento tecnológico, estes dispositivos são cada vez mais sofisticados e têm capacidade de colher informação, diariamente, hora-a-hora e até minuto-a-minuto, não só relativamente à glicemia da pessoa com DM, mas também a outros dados médicos, tais como: saturação de oxigénio, temperatura corporal, frequência e ritmo cardíacos e localização. Atualmente, muito deles têm hardware e software que permitem transmitir, à distância, esta informação, seja por *Bluetooth* ou via tecnologia *Wi-Fi*. Isto permite que estes dispositivos consigam comunicar entre si, diretamente com os *smartphones*, aos *wearables*, à *internet* e até aos sistemas de informação na *cloud*. Este tipo de interoperabilidade e capacidade de colheita de dados consegue criar gráficos úteis para análise, pela pessoa com DM e também pelos profissionais de saúde. Isto permite que sejam dadas sugestões de intervenção baseadas nos elementos recolhidos, como por exemplo: alerta de situações potencialmente danosas para a pessoa com DM (por exemplo, risco de hipoglicemia nos minutos subsequentes), sugestões da quantidade de insulina a administrar e, ainda, relatórios completos (com uma grande variedade de métricas relativas ao estado glicémico da pessoa com DM). No limite, será este tipo de interligação que permitirá, no futuro, a criação de um pâncreas artificial, cuja interação da pessoa com DM ao dispositivo seja mínima, permitindo que esta consiga viver como uma pessoa sem DM. A questão que se coloca é saber quais os potenciais riscos desta colheita intensiva, agregação de dados e a sua conectividade entre vários dispositivos. Todas as potencialidades descritas podem ser abusivamente direcionadas contra o utilizador.

> QUAIS SÃO OS RISCOS?

A primeira demonstração pública de *hacking* a um sistema PCSI foi feita em 2011, numa conferência em Las Vegas, por um investigador chamado Jay Radcliffe. [5] Este investigador conseguiu, remotamente, desconectar o sistema PCSI e esvaziar um cartucho inteiro de insulina. Na altura, foi necessário recorrer a equipamento e software específico, especialmente desenhados para o efeito, e ter conhecimento prévio do número de série do

sistema PCSI. [6] No ano seguinte, outro investigador, chamado Barnaby Jack, conseguiu esvaziar um cartucho de insulina, remotamente, através de uma ligação wireless e sem necessidade de saber o número de identificação. Em 2019, a Medtronic emitiu um comunicado de segurança a incentivar a troca de sistemas PCSI da série Minimed™ 508 e Minimed™Paradigm™, por modelos mais recentes, após terem sido detetadas falhas de segurança. [7]

Os sistemas MCG também têm vulnerabilidades e estas já foram testadas em ambiente experimental, em particular o sistema *FreeStyle Libre*. O investigador Apvrille mostrou que era possível modificar valores de glicemia, a data de expiração do sensor, inutilizá-lo ou até reativar um sensor já expirado. [8] O autor demonstrou, ainda, que a maior vulnerabilidade não seriam os sensores, mas sim os *smartphones*. Esta vulnerabilidade decorre, sobretudo, através da utilização de *apps* maliciosas (relacionadas ou não com a DM) ou de ataques dirigidos diretamente aos *smartphones*. Se é certo que o *smartphone* é considerado um objeto pessoal do indivíduo, a partir do momento em que tem conexão com dispositivos médicos, passa a estar integrado nesta rede e, como tal, suscetível a ataques e à atenção da parte de todos os intervenientes.

O Quadro I permite resumir alguns dos riscos teóricos que as pessoas com DM podem estar sujeitas, quando dispõem de sistemas de monitorização de glicose conectados à *internet* ou *smartphone* ou ainda de dispositivos de PSCI. No Quadro II sistematiza-se estes riscos segundo a metodologia STRIDE. [9] A metodologia STRIDE (*Spoofing*; *Tampering*; *Repudiation*; *Information disclosure*; *Denial of Service*; *Elevation of Privilege*) é um modelo que permite identificar potenciais vulnerabilidades, o que ajuda a conceptualizar o impacto possível a que as pessoas com DM podem estar sujeitas.

É importante notar que os riscos descritos resultam das vulnerabilidades já relatadas publicamente, pelo que poderão existir outros métodos ou vulnerabilidades não conhecidas ou exploradas ainda. Apesar de os glucómetros ou dispositivos de MCG apenas medirem glicemia e não administrarem insulina, a verdade é que as pessoas com DM tomam decisões com base nestes valores. Embora o cenário descrito acima possa parecer alarmista, é fundamental rever os factos. Por enquanto, e que se saiba, não ocorreu nenhum evento considerado grave, nomeadamente morte ou hospitalização, conhecida a nível global, relacionado com o aproveitamento das vulnerabilidades dos DMD. Por esse motivo, não devemos excluir a utilização das novas tecnologias que tanto benefício providenciam ao tratamento da pessoa com DM. Devemos sim estar vigilantes e promover, junto das entidades governamentais e dos fabricantes, a criação de estruturas (*frameworks*) robustas e eficazes que permitam mitigar estes riscos.

> FUTURO E POSSÍVEIS SOLUÇÕES

É utópico pensar que é possível construir qualquer dispositivo eletrónico completamente imune a ataques cibernéticos. É ainda mais complicado quando estes dispõem de múltiplas funções, em que algumas impliquem conectividade através da *internet*. Deve-se incentivar o fabrico de dispositivos que sejam difíceis de serem atacados e, caso o sejam, que o dano, eventualmente infligido, seja o menor possível.

As medidas para melhorar a cibersegurança devem ser tomadas a nível individual (junto da pessoa com DM), dos operadores económicos (fabricantes, importadores, distribuidores), dos reguladores e do governo.

Nos Estados Unidos da América, a *Food & Drug Administration* tem vindo, cada vez mais, a considerar o risco de um possível cibercrime no momento da aprovação dos dispositivos médicos. Desde 2016, que estabeleceu diretrizes e sugestões dirigidas aos fabricantes, em conjunto com outras entidades governamentais, de como devem desenhar e manter atualizados os dispositivos médicos nestas matérias. [10]

A União Europeia (EU) também tem tido esta preocupação e, em 2019, aprovou o seu regulamento de cibersegurança que introduziu um sistema de certificação à escala da EU e uma nova agência dedicada à cibersegurança, denominada ENISA. [11] A EU emitiu orientações europeias relativas à Cibersegurança de Dispositivos Médicos num documento – MDCG 2019-16. Este documento permite esclarecer os meios necessários à obtenção do cumprimento dos requisitos essenciais relativos à cibersegurança, previstos no Regulamento dos Dispositivos Médicos (RDM). Desde 26 de Maio de 2021 que entrou em vigor o RDM Europeu e passou a ser aplicável a grande maioria das orientações e regulamentos descritos, o que permitirá aproximar a legislação europeia, às normas e boas práticas internacionais. Estes documentos aplicam-se a todos os países da EU entre eles Portugal. A relevância destes documentos centra-se na obrigatoriedade da cibersegurança ser incluída, logo à partida, no desenho dos dispositivos médicos, estabelecendo requisitos mínimos a serem cumpridos, sempre de acordo com o estado de arte do setor. [12,13]

A nível individual, a pessoa com DM e os profissionais de saúde também devem tomar algumas medidas simples, que podem ser aplicadas em vários cenários. Devem ser

Quadro I - Riscos teóricos associados ao cibercrime, em pessoas com Diabetes *Mellitus*.

Tipo de ataque	Como?	Possível impacto
Inviabilizar um sensor MCG	Por tecnologia NFC (implica proximidade do sensor); Através de *app* maliciosa.	Risco médico relevante para a pessoa com DM. Necessário substituir o sensor ou utilizar alternativas (glucómetro). Se acoplado a um sistema PSCI, com impacto directo no funcionamento do sistema.
Modificar valor de glicose num glucómetro ou sensor MCG	Por tecnologia NFC (implica proximidade do sensor e modificação da memória); Através de *app* maliciosa.	Risco médico relevante para o doente. Podem ser tomadas decisões com base em valores errados.
Leitura à distância de um valor de glicose	Por tecnologia NFC (implica proximidade do sensor e modificação da memória); Através de *app* maliciosa.	Risco de invasão da privacidade
DdoS* no smartphone; *ramsomware	Através de *app* maliciosa.	Risco médico relevante para o doente. Requer utilização de outros métodos de monitorização de glicose. Se acoplado a um sistema PSCI, com impacto direto no funcionamento do sistema.
Alteração na administração de insulina	Remotamente. Através de *app* maliciosa.	Risco médico relevante para o doente. Possibilidade de suspender administração (risco de hiperglicémia) ou de maior dose que a desejada (hipoglicémia).

Adaptado de: Apvrille A. Goodspeed T. (2020) *Security analysis of a Connected Glucose Sensor for Diabetes*. https://passthesalt.ubicast.tv/protected/videos/v125f57aae-7bfmvm2r6cajw3qr9nws/attachments/pts2020_talk_15_pique_curiosity_not_diabetic_fingers_technical_report.pdf. **Abreviaturas:** MCG – Monitorização Contínua de Glicose; DM – Diabetes *Mellitus*; PSCI – dispositivos de Perfusão Subcutânea Contínua de Insulina; DDoS – *denial of service*; NFC – *Near Field Communication*.

Quadro II - Taxonomia dos riscos teóricos associados ao cibercrime, em pessoas com Diabetes *Mellitus*.

Propriedade passível ser afetada	Ameaça (STRIDE)	Definição	Possíveis exemplos e eventuais impactos de ataques dirigidos aos DMD
Autenticação	*Spoofing Identity* (falsificação de identidade)	Personificação de um utilizador legítimo/ autorizado	– Personificar o doente e reprogramar privilégios de acesso ou da terapêutica (pode servir de ponte para outras ameaças descritas abaixo).
Integridade	*Tampering with data* (adulteração de dados)	Adulterar dados ou código	– Adulterar valores de glicemia (impacto clínico relevante) – Adulterar as unidades de insulina administrada por sistemas PSCI (impacto clínico relevante) – Modificar a comunicação de dados entre os diferentes dispositivos (impacto clínico dependente da modificação em questão)
Não-repúdio	*Repudiation* (repúdio)	Alegar não ter realizado uma ação (repúdio)	– Apagar dos registos de pessoas que acederam aos dispositivos médicos (impede rastreamento de quem acedeu indevidamente)
Confidencialidade	*Information disclosure* (divulgação de informação)	Obtenção de informação de forma ilegítima	– Identificar uma pessoa que utiliza um sistema de PSCI ou sensor de MCG e qual o modelo (quebra de privacidade). – Aceder a informação médica como controlo metabólico, dose de insulina utilizada, horário das refeições (quebra de privacidade). – Localizar o doente através dos dispositivos (quebra de privacidade)
Disponibilidade	*Denial of service* (negação de serviço)	Degradar ou impedir o acesso e/ou o funcionamento do sistema	– Drenar a bateria dos dispositivos (impede utilização dos mesmos) – Impedir a comunicação de dados entre os diferentes dispositivos (impacto clínico relevante) – Sobrecarregar os dispositivos com dados, o que impede a sua utilização (impacto clínico relevante)
Autorização	*Elevation of privilege* (elevação de privilégios)	Elevar os privilégios dentro do sistema de forma ilegítima.	– Desligar os dispositivos remotamente (impacto clínico relevante) – Reprogramar a terapêutica do doente remotamente (impacto clínico relevante)

Adaptado de: Camara C, et al. *Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey. Journal of Biomedical Informatics. 2015; 55: 272-289. https://doi.org/10.1016/j.jbi.2015.04.007.* **Abreviaturas:** PSCI – dispositivos de Perfusão Subcutânea Contínua de Insulina; MCG – sistema de monitorização contínua de glicose; STRIDE – *Spoofing Identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege*; DMD – dispositivos médicos na Diabetes

promovidas sugestões úteis, tais como: 1) proteger os dispositivos com uma *password* única e de boa qualidade (por exemplo, evitar datas de nascimento, próprio nome); 2) necessidade de os dispositivos se encontrarem na proximidade do individuo; 3) conectar apenas com outros dispositivos ou *software* que os fabricantes ou os profissionais de saúde considerem seguros; 3) atualizar os dispositivos para a sua versão mais recente (inclui também o *smartphone*).

> CONCLUSÃO

As novas tecnologias na área da saúde têm revolucionado o tratamento de muitas doenças crónicas. Este avanço tem permitido uma verdadeira revolução no seu tratamento, com benefícios inolvidáveis para a pessoa com DM, em termos de comodidade e de possibilidades terapêuticas. No entanto, há custos e riscos associados nesta crescente onda de tecnologia para os utilizadores, caso haja disfunções fortuitas ou propositadas. As entidades governamentais e os fabricantes, nos últimos anos, têm-se preocupado com esta temática. Têm-se desenvolvido esforços na criação de legislação e *frameworks*, com ênfase na confidencialidade, integridade e disponibilidade da informação contida nestes dispositivos médicos. Infelizmente, estes esforços têm ficado aquém na capacidade de fornecer aos profissionais de saúde e às pessoas com DM, as ferramentas necessárias à avaliação e compreensão do risco cibernético, aquando da utilização destas novas tecnologias. A literacia na área de cibersegurança é fundamental para otimizarmos os ganhos em saúde. Caso os procedimentos de segurança não sejam criados e bem estabelecidos, corremos o risco de algumas novas tecnologias (por exemplo, pâncreas artificial) não serem atingíveis, pelo risco de colocarem a pessoa com DM em perigo e, deste modo, reduzir a confiança na sua utilização. A cibersegurança torna-se, assim, um pilar fundamental no futuro do tratamento da DM. <

BIBLIOGRAFIA

1. Loke, A. "Diabetes - Key Facts." World Health Organization, World Health Organization, Setembro 2022, https://www.who.int/news-room/fact-sheets/detail/diabetes. Acedido a 9 de Dezembro de 2022
2. Serviços Partilhados do Ministério da Saúde - "A Segurança da Informação", Novembro 2017 https://spms.min-saude.pt/wp-content/uploads/2017/11/eSIS_Seguranca_da_Informacao.pdf. Acedido a 9 de Dezembro de 2022
3. Shaw, Glenda Fauntleroy. "Phish Tank: Avoiding Cyberattacks in the Lab." Endocrine News, 27 Oct. 2022, https://endocrinenews.endocrine.org/phish-tank-avoiding-cyberattacks-in-the-lab/. Acedido a 9 de Dezembro de 2022
4. Wetsman N. "Woman dies during a ransomware attack on a German hospital. The Verge". Setembro 2020. https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity. Acedido a 9 de Dezembro de 2022
5. Kaplan, Dan, and Paul Wagenseil. "Black Hat: Insulin Pumps Can Be Hacked." SC Media, Junho 2021, https://www.scmagazine.com/news/network-security/black-hat-insulin-pumps-can-be-hacked. Acedido a 9 de Dezembro de 2022
6. Goodin D. "Insulin pump hack delivers fatal dosage over the air: sugar blues, James Bond style". Outubro 2011 https://www.theregister.com/2011/10/27/fatal_insulin_pump_attack/. Acedido em 9 Dezembro 2022
7. Medtronic "URGENT FIELD SAFETY NOTIFICATION, MiniMed™ 508 Insulin Pump and MiniMed™ Paradigm™ Series Insulin Pumps CybersecurityConcerns", Junho 2019. https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter. Acedido a 9 de Dezembro de 2022
8. Apvrille, A. andGoodspeed, T. (2020) "Securityanalysisof a Connected Glucose Sensor for Diabetes.", https://passthesalt.ubicast.tv/protected/videos/v125f57aae7bfmvm2r6cajw3qr-9nws/attachments/pts2020_talk_15_pique_curiosity_not_diabetic_fingers_technical_report.pdf. Acedido em 9 Dezembro 2022
9. Camara, Carmen, et al. "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey." Journal of Biomedical Informatics, vol. 55, 2015, pp. 272–289., https://doi.org/10.1016/j.jbi.2015.04.007
10. US Food and Drug Administration. "Postmarket management of cybersecurity in medical devices. Draftguidance". Janeiro 2016. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Acedido em 9 Dezembro 2022
11. Conselho Europeu - Conselho da União Europeia: "Cibersegurança: Como Combate a UE as Ciberameaças." Consilium, Novembro 2022, https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acedido em 9 Dezembro 2022
12. Circular Informativa N.º 042/CD/100.20.200 "Orientações Europeias relativas à Cibersegurança de Dispositivos Médicos" Infarmed. Fevereiro 2020.
13. Circular Informativa N.º 065/CD/550.20.001 "Aplicação do Regulamento dos Dispositivos Médicos (RDM)" Infarmed. Maio 2021