Research, Society and Development, v. 14, n. 5, e7414547190, 2025
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v14i5.47190

Integração da Cibersegurança na Medicina Veterinária: Protegendo Dados e Sistemas de Saúde Animal

Integrating Cybersecurity into Veterinary Medicine: Protecting Animal Health Data and Systems

Integración de la ciberseguridad en la medicina veterinaria: Protección de los datos y sistemas de sanidad animal

Recebido: 11/10/2024 | Revisado: 03/05/2025 | Aceitado: 18/05/2025 | Publicado: 22/05/2025

Angela Mazzeo
ORCID: https://orcid.org/0000-0001-8483-5002
Universidade de São Paulo, Brasil
Faculdade Ibptech, Brasil
E-mail: angela.mazzeo@ibptech.edu.br
Enrico Jardim Clemente Santos
ORCID: https://orcid.org/0000-0003-0869-3342
Instituto de Pesquisas Energéticas e Nucleares, Brasil
Celltrotec, Brasil
E-mail: enrico@celltrotec.com.br

Resumo
A cibersegurança é um campo emergente na convergência das ciências da vida e do mundo digital. Neste estudo temos por objetivo analisar a importância da segurança cibernética para clínicas, consultórios, laboratórios e hospitais veterinários apresentando os perigos, consequências e metodologias de defesa contra os ataques cibernéticos. Durante a prática da medicina veterinária o armazenamento de uma quantidade significativa de dados de alto valor agregado torna os consultórios, clínicas, laboratórios e hospitais veterinários alvos significativos dos cibercriminosos. Atualmente, as instituições veterinárias vêm sendo vítimas de ataques cibernéticos, principalmente por meio de e-mails suspeitos (*phishing*), mensagens de texto (*smishing*) e chamadas de voz (*vishing*). Portanto, é de fundamental importância a implementação de medidas de segurança que possam proteger as instituições veterinárias dos ataques dos cibercriminosos.
Palavras-chave: Segurança cibernética; Medicina Veterinária; Crime cibernético; Ataque cibernético.

Abstract
Cyberbiosecurity is an emerging field at the convergence of life sciences and the digital world. The aim of this study is to analyze the importance of cyber security for veterinary clinics, practices, laboratories and hospitals by presenting the dangers, consequences and methodologies for defending against cyber attacks. During the practice of veterinary medicine, the storage of a significant amount of high-value data makes veterinary practices, clinics, laboratories and hospitals significant targets for cybercriminals. Currently, veterinary institutions have been victims of cyber attacks mainly through suspicious emails (phishing), text messages (smishing) and voice calls (vishing). Therefore, it is of fundamental importance to implement security measures that can protect veterinary institutions from attacks by cybercriminals.
Keywords: Cybersecurity; Veterinary Medicine; Cybercrime; Cyber attack.

Resumen
La ciberseguridad es un campo emergente en la convergencia de las ciencias de la vida y el mundo digital. El objetivo de este estudio es analizar la importancia de la ciberseguridad para las clínicas, consultas, laboratorios y hospitales veterinarios, presentando los peligros, consecuencias y metodologías para defenderse de los ciberataques. Durante la práctica de la medicina veterinaria, el almacenamiento de una cantidad significativa de datos de alto valor convierte a las consultas, clínicas, laboratorios y hospitales veterinarios en objetivos importantes para los ciberdelincuentes. Actualmente, las instituciones veterinarias han sido víctimas de ciberataques principalmente a través de correos electrónicos sospechosos (*phishing*), mensajes de texto (*smishing*) y llamadas de voz (*vishing*). Por tanto, es de fundamental importancia implementar medidas de seguridad que puedan proteger a las instituciones veterinarias de los ataques de los ciberdelincuentes.
Palabras clave: Ciberseguridad; Medicina Veterinaria; Cibercrimen; Ciberataque.

1. Introdução

O mercado médico veterinário, principalmente o relacionado aos animais de estimação, tem se beneficiando com os avanços tecnológicos que vêm ocorrendo nos últimos anos, os quais têm como foco a prevenção e bem-estar animal. Dentre estes temos o desenvolvimento de técnicas cirúrgicas minimamente invasivas, o que propicia uma recuperação mais rápida e menos traumática do paciente, otimização da estrutura do sistema de internação veterinária e a telemedicina.

A telemedicina vem se tornado cada vez mais popular na medicina veterinária, possibilitando ao médico veterinário realizar consultas virtuais, diagnósticos remotos, prescrição de receitas de forma 100% digitais e reabilitação assistida. Por meio da telemedicina veterinária também conhecida como televet, os tutores dos animais de estimação tem a possibilidade de se comunicar com o veterinário do conforto de sua própria casa, expandindo assim o alcance da prática veterinária (Cushing, 2022). Esta nova abordagem, que foi regulamentada por meio da resolução CFMV 1.465, de 27 de junho de 2022, tende a ampliar o alcance da atuação dos médicos veterinários, melhorando o acesso aos cuidados da saúde animal. Porém, com a implementação da telemedicina, novas questões e riscos precisam ser avaliados, particularmente os relacionados à segurança da informação de forma a garantir a prestação de um serviço seguro e eficaz (Cubo, 2021; Jedličková, 2024).

O uso de Big Data é de fundamental importância na medicina veterinária uma vez que permite ao médico veterinário coletar e analisar diversos dados de forma rápida, fácil e efetiva, uma vez que cada paciente possui perfil próprio. Por meio do Big Data o médico veterinário pode visualizar os registros de resultados laboratoriais, histórico do paciente, imagens, documentos, diagnósticos, medicamentos e até mesmo suas informações de seguro. Este sistema propicia ao médico veterinário identificar e diagnosticar, precocemente, padrões e tendências de uma determinada doença, propiciando uma maior precisão e velocidade no tratamento. Além disso, é possível que o médico veterinário compartilhe, com os tutores, as informações relativas ao tratamento, possibilitando que estes acompanhem a evolução do quadro clínico e laboratorial do paciente (Paynter, 2021).

Um dos grandes problemas que a humanidade vem enfrentando está relacionado a cibersegurança. Esta pode ser definida como um conjunto de conceitos de segurança, ferramentas, políticas, guias, abordagens de gestão de risco, melhores práticas, tecnologias que podem ser utilizadas para proteger o ciberespaço, organizações e utilizadores deste mecanismo, evitando desta maneira, invasão de vírus para diversas atividades ilícitas (Oliveira, 2021).

Uma vez que a segurança da informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um determinado ativo, neste estudo temos por objetivo analisar a importância da segurança cibernética para clínicas, consultórios, laboratórios e hospitais veterinários apresentando os perigos, consequências e metodologias de defesa contra os ataques cibernéticos.

2. Metodologia

A metodologia científica é importante para que os artigos tenham reprodutilidade nos resultados e, que tenham aceitação pela comunidade acadêmica e científica (Pereira et al., 2018). O presente estudo teve como base, a pesquisa bibliográfica (Snyder, 2019; Sousa, Oliveira & Alves, 2021; Mattos, 2015) de cunho exploratório, descritivo e de natureza qualitativa e do tipo revisão de literatura narrativa (Rother, 2007; Cavalcante & Oliveira, 2020; Mendes, 2022; Casarin et al., 2020) junto às bases de dados do Google Academico, *Scientific Electronic Library Online* (Scielo), *Literatura Latino-Americanda do Carive em Ciencia da Saúde* (LILACS) e *Medical Litature Analysis and Retrieval System Online* (MEDLINE). Para a busca, foi realizado o recorte temporal de publicações entre os anos de 2017 à 2024, utilizando as seguintes palavras-chaves: segurança cibernética; medicina veterinária; crime cibernético; ataque cibernético.

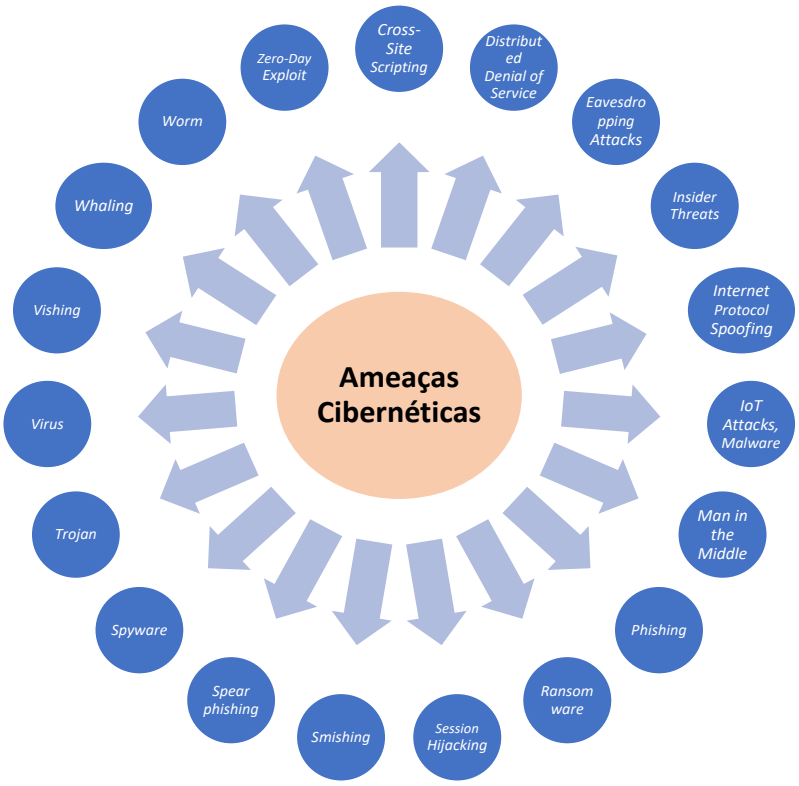
3. Resultados e Discussão

Nas últimas décadas os computadores e a internet, que conecta bilhões de pessoas ao redor do mundo, tornaram-se aspectos cruciais da sociedade moderna, transformado a maneira como vivemos, nos comunicamos e acessamos informações. Antes da "era da internet" a comunicação era realizada por meio de carta ou telefone fixo, as pesquisas eram realizadas em bibliotecas físicas, as transações comerciais eram realizadas pessoalmente em lojas físicas e a socialização era presencial. Com o advento da internet a sociedade teve seu dia a dia modificado de forma significativa como, por exemplo, a forma como nos comunicamos. Hoje em dia as redes sociais e aplicativos de mensagens propiciam uma comunicação instantânea e global, eliminando barreiras como distância e tempo. O consumo da informação e o entretenimento são realizados de forma online por meio da leitura de notícias, *podcasts*, vídeos e *streaming*, permitindo que as pessoas possam aprender sobre qualquer assunto, aprimorando suas habilidades e conhecimentos. A internet também propiciou o desenvolvimento do comércio eletrônico, permitindo que os consumidores adquiram produtos de todos os lugares, possibilitando mais opções, além de criar a oportunidades de negócios para empreendedores. Apesar dos diversos benefícios obtidos a internet também trouxe consigo desafios significativos para a sociedade moderna como questões relacionadas a confiabilidade e a disseminação de falsas notícias (Drăghici, 2023).

À medida que avançamos na era digital, desafios significativos vêm surgindo, sendo a segurança cibernética um dos principais problemas enfrentados pela sociedade moderna. Ameaças de ataques de *hackers*, roubo de dados pessoais, *softwares* maliciosos intencionalmente projetado visando causar danos a computadores ou redes (*malware*) e crimes cibernéticos têm se tornando cada vez mais frequentes tornando a privacidade online uma preocupação real, visto que nossas informações pessoais e dados financeiros podem ser coletados, armazenados e utilizados por terceiros sem nosso consentimento (Li, 2021).

No transcorrer dos últimos anos ataques cibernéticos têm sido realizados por meio de diferentes mecanismos dentre os quais temos o *Cross-Site Scripting, Distributed Denial of Service (DDoS), Eavesdropping Attacks, Insider Threats, Internet Protocol (IP) Spoofing, IoT Attacks, Malware, Man in the Middle (MitM), Phishing, Ransomware, Session Hijacking, Smishing, Spear phishing, Spyware, Trojan (Cavalo de Tróia), Virus, Vishing, Whaling, Worm* e *Zero-Day Exploit*. Tal fato faz com que o estabelecimento de um mecanismo de proteção seja de fundamental importância (Figura 1).

Figura 1 – Ameaças cibernéticas as quais clínicas, consultórios, laboratórios e hospitais veterinários estão suscetíveis.



Fonte: Autoria própria.

Com o surgimento do Chat GPT em 2022 surgiu a possibilidade de que potenciais criminosos possam, com apenas algumas perguntas feitas pelo *chatbot*, automatizar ataques as redes através de códigos lançados pela ferramenta. Como o Chat GPT tende a "aprender com o passado", para a criação e geração de conteúdo, ele pode ser facilmente utilizado por criminosos para: 1 - Elaboração de *phishing* objetivando gerar e-mails convincentes que parecem legítimos e solicitam informações pessoais, como senhas, números de cartão de crédito e outras informações confidenciais; 2 – Utilizar modelos de linguagem para gerar código malicioso ou scripts que possam infectar sistemas e redes, danificar, tentar adivinhar senhas ou roubar dados (*Malware*); 3 – Utilizar a tecnologia de *deep learning*, para criar conteúdo de mídia falso (áudio e/ou vídeo) que pode ser utilizado para enganar as pessoas e disseminar informações inverídicas e 4 - Criar perfis de mídia social falsos ou conversas falsas que visam enganar as pessoas e levá-las a revelar informações confidenciais (Al-Hawawr, 2023).

Consultórios, clínicas, laboratórios e hospitais veterinários vêm sofrendo ataques de cibercriminosos, pois estes consideram que as empresas veterinárias são negligentes quanto as medidas de segurança adotadas, o que pode resultar em grandes prejuízos financeiros. Estes se devem a provável perda de receita enquanto estiverem inativos, assim como possivelmente serem vistos como instituições não confiáveis, uma vez que não protegeram as informações de seus clientes (El Idrissi, 2021).

As informações coletadas e armazenadas pelas instituições veterinárias, como nomes, datas de nascimento, endereço de clientes, informações de cartão de crédito, detalhes das contas bancárias, informações de contas de e-mail e dados dos animais de estimação (os nomes destes podem a ser utilizados como senhas ou perguntas secretas de segurança), tendem a serem valiosas quando apreendidas pelo *hacker*, uma vez que podem ser utilizados para extorquir dinheiro das instituições veterinárias.

Os cibercriminosos vêm utilizando métodos para forçar os donos das instituições veterinárias a pagá-los, independente de ter ou não o sistema de *backup* de dados. Tomando como exemplo um ataque de *ransomware*, os cibercriminosos

inicialmente obtem acesso a rede da instituição veterinária e baixam todos os dados dos clientes, antes de implantar o *ransomware* para bloquear os computadores. Caso a empresa veterinária se recuse a pagar o resgate, em função de ter o *backup* dos dados, os cibercriminosos tendem a ameaçar venderem os dados dos clientes no mercado negro ou torna-los públicos (Maurya, 2018). Portanto, sendo você dono de um consultório, clínica, laboratório ou hospital veterinário, deve estar preparado.

O uso indevido ou roubo de informações de clientes pode ser desastroso para consultórios menores que podem não ter recursos financeiros para combater uma possível ação judicial, além de poder comprometer a capacidade da clínica de operar legalmente. Em 14 de agosto de 2018 foi promulgada a Lei nº 13.709/2018 denominada Lei Geral de Proteção de Dados (LGDP) que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, de pessoa física ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Com base nesta Lei as instituições veterinárias que tiveram seus dados roubados podem ser processadas (Fernandes, 2022).

No que se refere a saúde dos pacientes atendidos, pelas instituições veterinárias, os impactos diretos e indiretos de um ataque cibernético devem ser levados em consideração. Como impacto direto temos o cancelamento de consultas e operações, assim como o possível fechamento de Prontos-Socorros e internações. Já os impactos indiretos incluem a piora da saúde do paciente, devido a tratamentos atrasados, diagnósticos perdidos e consultas e procedimentos cancelados (Mayor, 2023).

Certificar-se acerca da segurança dos dados da instituição veterinária é de fundamental importância, o que faz com que diferentes metodologias de proteção sejam implementadas dentre as quais temos: 1 – *Backups* de dados em um servidor separado e não conectado à internet, de forma a propiciar a restauração do sistema de forma segura e eficaz, caso seja necessário; 2 – *Firewall* de segurança robusto e confiável; 3 – Ter um plano de emergência implementado, caso ocorra a violação de dados ou queda de energia configurando planos de segurança e desligamento e 4 – Implementação de auditorias regulares e verificações *antimalware* para garantir que a instituição veterinária esteja atualizada acerca dos protocolos de segurança cibernética mais recentes e que seus computadores estejam seguros e livres de vírus (Figura 2).

Figura 2 – Metodologias que podem ser implementadas pelas clínicas, consultórios, laboratórios e hospitais veterinários visando estabelecer um sistema de segurança eficaz quanto a ataques cibernéticos.

Fonte: Autoria própria.

Com o surgimento da engenharia social, que pode ser definida como uma técnica de manipulação psicológica que visa obter acesso a informações privadas, os profissionais de cibersegurança concordam unanimemente que o elo mais fraco no

sistema é o usuário (Bullée, 2020). Tal fato é consistente com os dados que mostram que a maioria dos ataques cibernéticos são desencadeados por meio da negligência exercida pelo indivíduo (Almutairi, 2022).

Por meio da engenharia social os *hackers* levam um destinatário desavisado a realizar uma ação de forma a expor dados confidenciais, dar acesso a sistemas restritos e/ou espalhar infecções por *malware*. Esta abordagem frequentemente se dá por meio de um e-mail, *links* maliciosos ou *malware* que tende a ser acessado pelo destinatário desavisado. Outra abordagem realizada com frequência, por parte dos *hackers*, é o ataque de *phishing*. Neste o *hacker* produz comunicações fraudulentas que podem ser interpretadas como legítimas pela vítima por alegarem vir de fontes confiáveis sendo o *deepfake* a sua forma mais recente. O *deepfake* envolve a criação de vídeos, imagens ou áudios falsos, por meio de inteligência artificial, visando obter dados confidenciais ou pagamentos (Almutairi, 2022).

Visando evitar possíveis ataques cibernéticos, que tenham como base a engenharia social, é de fundamental importância investir na equipe incutindo neles uma abordagem que priorize a segurança cibernética. Por exemplo, você deve implementar políticas que visem impedir ataques as senhas, educando sua equipe sobre os vários métodos pelos quais elas podem ser comprometidas (por exemplo, phishing) e estabelecer práticas prescritas de segurança cibernética que devem ser respeitadas por todos. Sendo assim, algumas diretrizes que devem ser adotadas pelas instituições veterinárias são: 1 - Não responder e-mails que peçam informações pessoais ou financeiras; 2 - Evitar pop-ups, e-mails e links desconhecidos; 3 - Nunca divulgar informações confidenciais ou mesmo aparentemente não confidenciais sobre você ou sua empresa, seja por telefone ou on-line, a menos que você possa primeiro verificar a identidade da pessoa que solicita, assim como a necessidade dessa ter acesso a mesma; 4 - Manter atualizados os dispositivos de segurança do seu computados como antivírus, *spyware*, *antimalware* e navegadores, executando verificações em seu sistema periodicamente; 5 - Utilizar navegadores que possuam filtro de *phishing*; 6 - Atualizar seus softwares com os patches de segurança mais recentes, executando os mais estáveis e recentes sistemas operacionais; 7 - Desabilitar o compartilhamento de arquivos e impressão remota; 8 - Utilizar senhas fortes (sem reutilizá-las); 9 - Sempre verifique os documentos, por meio de anti-virus, antes de abri-los em seu computador; 10 - Manter um *firewall* na rede visando protegê-la contra acesso não autorizado; 11 – Manter *backup* de todos os dados fora da rede, onde não podem ser comprometidos por meio de um ataque de *ransomware* e 12 - Em caso de dúvida, desconecte o computador da internet e converse com seu gerente sobre os próximos passos. Portanto, é importante ressaltar que a proteção e atualização dos sistemas devem ser uma política na prática veterinária de forma a evitar ataques que explorem as possíveis vulnerabilidades do sistema de segurança (Almutairi, 2022).

Atualmente é de fundamental importância que a equipe presente na clínica, consultório, laboratório ou hospital veterinário tenha uma mudança de mentalidade de forma a estar ciberconsciente, ou seja, compreenda que mesmo com os melhores sistemas de cibersegurança em vigor, eles ainda podem ser alvos de um ataque cibernético. Por esta razão é de fundamental importância que as instituições veterinárias implementem a cultura da "confiança zero", por meio da qual os profissionais passem a ver um e-mail ou ligação via *web* com confiança zero (Kang, 2023).

As violações de dados causadas por pessoas internas a instituição veterinária vêm crescendo de forma significativa no últimos anos, tanto em termos de frequência como de impacto. Entretando, poucas medidas vêm sendo implementadas visando garanir que o consultório, clínica, laboratório ou hospital veterinário não sejam vítimas de ataques cibernéticos originados de dentro da instituição. Em vez disso, elas confiam cegamente em seus funcionários. Estes, com acesso legítimo aos dados, podem usar seu acesso para prejudicar - seja intencionalmente ou não - a insituição veterinária, causando danos semelhantes aos sofridos por meio ataques realizados por cibercriminosos. Para evitar violações de dados, por parte de pessoas internas, as instituições veterinária devem implementar uma estratégia que envolve limitar o acesso à sua rede de sistemas, dispositivos, aplicativos e dados. Nesta estratégia as instituições veterinárias devem ser capazes de limitar e negar acesso imediato a qualquer usuário ou dispositivos que não esteja autorizado (Mazzarolo, 2020).

Os laptops, smartphones e outros dispositivos portáteis abriram um mundo de oportunidades que auxiliam nas práticas veterinárias em todo o mundo. Porem, esses dispositivos também se tornaram alvos para os cibercriminosos lançarem ataques cibernéticos, uma vez que são fáceis de perder e mais vulneráveis a roubo, facilitando o acesso dos cibercriminosos a contas e conteúdo que pertencem ao médico veterinário. Esses dispositivos moveis também são inseguros pois muitos não possuem senhas fortes de autenticação, o que facilita o acesso aos dados por parte do cibercriminoso. Alem disso, uma vez que os dispositivos portateis, que estejam comprometidos, tenham acesso a rede da instituição veterinária, seja pelos funcionários ou clíentes, eles podem colocar toda rede em perigo, levando pessoas não autorizadas a terem acessos a dados críticos da instituição veterinária (Dawson, 2016; Mishra, 2023).

4. Considerações Finais

O recente aumento de ataques cibernéticos contra consultórios, clínicas, laboratórios e hospitais veterinários é uma indicação clara de que os cibercriminosos vêm valor nos dados ali presentes. É de suma relevância que as instituições veterinárias entendam que não se trata da possíbilidade de sofrerem um ataque cibernético, mas sim quando eles ocorrerão. Portanto, é preciso estar preparado para o pior cenário, sendo de fundamental importância a implementação de medidas de segurança cibernética que podem proteger as instituições veterinária de tais ataques.

Referências

Al-Hawawreh, M., Aljuhani, A. & Jararweh, Y. (2023). ChatGPT For Cybersecurity: Practical Applications, Challenges, and Future Directions. 26, 3421–3436

Almutairi, B.S. and Alghamdi, A. (2022) The Role of Social Engi neering in Cybersecurity and Its Impact. Journal of Information Security, 13, 363-379.

Bullée, JW., Junger, M. (2020). Social Engineering. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_38

Casarin, S. T. et al. (2020). Tipos de revisão de literatura: considerações das editoras do Journal of Nursing and Health/Types of literature review: considerations of the editors of the Journal of Nursing and Health. Journal of Nursing and Health,10(5). DOI: https://doi.org/10.15210/jonah.v10i5.19924. https://periodicos.ufpel.edu.br/index.php/enfermagem/article/view/19924.

Cubo, E., Arnaiz-Rodriguez, A., Arnaiz-González, Á., Díez-Pastor, J. F., Spindler, M., Cardozo, A., Garcia-Bustillo, A., Mari, Z., & Bloem, B. R. (2021). Videoconferencing Software Options for Telemedicine: A Review for Movement Disorder Neurologists. *Frontiers in neurology*, *12*, 745917.

Cushing M. (2022). What Is Telemedicine, Telehealth, and Teletriage. *The Veterinary clinics of North America. Small animal practice*, *52*(5), 1069–1080.

Dawson, M., Wright, J., & Omar, M. (2016). Mobile Devices: The Case for Cyber Security Hardened Systems. In I. Management Association (Ed.), *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications* (pp. 1103-1123). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-4666-8751-6.ch047

Drăghici, D (2023). The Internet, lifestyle and Society. European Proceedings of Educational Sciences. Edu World 2022 p.160-167

Paynter, A. N., Dunbar, M. D., Creevy, K. E., & Ruple, A. (2021). Veterinary Big Data: When Data Goes to the Dogs. *Animals: an open access journal from MDPI*, *11*(7), 1872.

El Idrissi, A. H., Larfaoui, F., Dhingra, M., Johnson, A., Pinto, J., & Sumption, K. (2021). Digital technologies and implications for Veterinary Services. Digital technologies and implications for Veterinary Services. *Revue scientifique et technique (International Office of Epizootics)*, *40*(2), 455–468. https://doi.org/10.20506/rst.40.2.3237

Fernandes, M. E., & Nuzzi, A. P. E. (2022). Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. Research, Society and Development, 11(12), e310111234247.

Jedličková A. (2024). Ethical dimensions in telemedicine - balancing technology, responsible care, and patient protection. Etické aspekty v telemedicíně – balancování mezi výhodami technologií, odpovědnou péčí a ochranou pacienta. *Casopis lekaru ceskych*, *163*(3), 106–114.

Li Y & Liu Q (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports 7, p.8176–8186.

Maurya, A.K., Kumar, N., Agrawal, A. & Khan, R. A. (2018). Ransomware: Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering*, 6(1), 80-85.

Oliveira, V. F. M. Q. de. (2021). Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. Dissertação (Metrado) Mestrado em Gestão de Informação, especialização em Gestão dos Sistemas e Tecnologias de Informação. http://hdl.handle.net/10362/117660

Kang, H.; Liu, G.; Wang, Q.; Meng, L. & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. Entropy. 25, 1595

Kauthamy, K., Ashrafi, N. & Kuilboer, J-P. (2017). Mobile Devices and Cyber Security An Exploratory Study on User's Response to Cyber Security Challenges. In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017), pages 306-311

Mattos, P. C. (2015). Tipos de revisão de literatura. Unesp, 1-9. https://www.fca.unesp.br/Home/Biblioteca/tipos-de-evisao-de-literatura.pdf.

Mishra, S., & Soni, D. (2023). DSmishSMS-A System to Detect Smishing SMS. *Neural computing & applications*, *35*(7), 4975–4992. https://doi.org/10.1007/s00521-021-06305-y

Mazzarolo, G & Jurcut, A. D. (2020). Insider threats in Cyber Security: The enemy within the gates. European Cybersecurity Journal. 6(1), 57-63.

Mendes, C. (2022). O que é uma revisão narrativa de literatura: exemplos e considerações da metodologia. https://www.youtube.com/watch?v=YlBWSVsxvRM

Pereira, A. S. et al. (2018). Metodologia da pesquisa científica. [free ebook]. Editora da UFSM.

Rother, E. T. (2007). Revisão sistemática x revisão narrativa. Acta paul. enferm. 20 (2). https://doi.org/10.1590/S0103-21002007000200001.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

Sousa, A. S.; Oliveira, G. S.; Alves, L. H (2021). A pesquisa bibliográfica: princípios e fundamentos. Cadernos da Fucamp, 20(43). https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336.