SEVEN publicações acadêmicas
EM PARCERIA COM: IEMS UNIASSELVI

Cibersegurança e proteção contra vazamento de dados

Evandro Frederico Ramos
Instituição: Fatec Adamantina
E-mail: evandro.ramos01@fatec.sp.gov.br

Eliane Vendramini de Oliveira
Professora Doutora
E-mail: eliane.oliveira5@fatec.sp.gov.br

RESUMO
O presente artigo traz um estudo sobre a importância da cibersegurança nos dias de hoje, apontando as principais ameaças virtuais como vírus malware, phishing ransomware bem como estratégias para proteger dados, implementadas no mundo técnico e legal. Aborda-se, também, as leis LGPD e a GDPR, além da aplicação de boas práticas de segurança, criptografia, autenticação multifatorial e políticas organizacionais. O estudo ressalta, que além das tecnologias, a conscientização e educação digital são chaves para diminuir riscos e assegurar a integridade das informações. Finalizando, conclui-se que a cibersegurança é uma prioridade estratégica para as organizações e em todos os setores da sociedade, sendo vital para um ambiente digital mais seguro, ético e resiliente.

Palavras-chave: Cibersegurança. Proteção de Dados. Ransomware. LGPD. Boas Práticas de Segurança.

1 INTRODUÇÃO

A revolução digital, mudou a maneira como as pessoas, empresas e governos trabalham, fazendo dos dados algo importante e valioso. Segundo Stallings (2017) e Beal (2021), é crescente a necessidade de integração entre a tecnologia, leis e comportamento humano para um ambiente mais seguro e confiável. Portanto, a cibersegurança aparece como elemento crucial, cuidando dos sistemas, redes e dados contra vários perigos cibernéticos que não param de aparecer. Com cada vez mais pessoas conectadas, com a inteligência artificial avançando em diversas áreas, os riscos digitais ficaram mais complexos, necessitando de estratégias de defesa e proteção dos dados.

A segurança da informação vai além da parte técnica que as organizações empregam para garantir que seus dados estejam protegidos, ela se apresenta nas leis e na educação. Ataques como vírus, *phishing e ransomware*, muitas vezes motivados por dinheiro ou política, afetam todos, de pessoa física a grandes organizações, colocando em risco a economia e a segurança do país. Por isso, leis como a Lei Geral de Proteção de Dados (LGPD) e o General Data Protection Regulation (GDPR) surgiram para organizar a maneira como os dados são usados e proteger os direitos das pessoas na internet.

Este trabalho tem como objetivo geral analisar as práticas e estratégias de cibersegurança voltadas à prevenção de vazamento de dados nas organizações. Como objetivos específicos, busca-se: apresentação das principais ameaças digitais enfrentadas atualmente; descrever as tecnologias e boas práticas utilizadas

na proteção de sistemas de informações; examinar legislações e normas vigentes, como a LGPD; e a discussão sobre a importância da conscientização e treinamento dos usuários como parte da segurança da informação, reduzido os impactos com segurança de dados.

A metodologia adotada é de caráter qualitativo, com base em uma pesquisa exploratória e bibliográfica. Foram analisadas publicações acadêmicas, artigos técnicos, relatórios institucionais e legislações específicas, com o intuito de compor um panorama atual e relevante sobre o tema. A abordagem permite compreender os aspectos técnicos e humanos envolvidos na segurança da informação, bem como suas implicações sociais e econômicas.

Portanto, almeja-se com este trabalho, auxiliar no entendimento das problemáticas em segurança cibernética e medidas viáveis a serem implementadas para atenuar ameaças e riscos dentro do ambiente corporativo, intensificando a obrigação mútua entre tecnologia, regulamentação e conduta das pessoas.

2 CIBERSEGURANÇA

Segundo Stallings (2017) A cibersegurança é um campo essencial na era digital sendo responsável pela proteção dos sistemas, redes e dados contra ameaças cibernéticas. Com o aumento da demanda de tecnologias da informação, a segurança digital tornou-se primordial para organizações e indivíduos.

Portanto, define-se cibersegurança como o conjunto de práticas e políticas voltadas à defesa de sistemas de computador e redes, visando garantir a proteção, confiabilidade, integridade e disponibilidade das informações (ISO/IEC, 2013). Segundo Pereira (2023), a cibersegurança não envolve, somente, a proteção contra ataques externos, mas também a implementação de políticas, assegurando que os dados e sistemas não sejam comprometidos por falhas internas.

Com o advento e crescimento da internet a cibersegurança tornou-se imprescindível para proteção dos dados sensíveis, infraestruturas críticas e a privacidade dos cidadãos. Ataques cibernéticos podem ter impactos nocivos para os indivíduos e sociedade, podendo afetar desde de dados pessoais até sistemas financeiros e governamentais, e colocando em risco a segurança nacional e a economia global. (Cisco, 2022).

Com a evolução das ameaças cibernéticas, aliada ao uso da Inteligência Artificial (IA), torna-se cada vez mais desafiadora a detecção e a defesa contra esses ataques (ISO/IEC, 2013). A cibersegurança, não se restringe somente a questões tecnológicas, mas também envolve educação e conscientização, tanto para profissionais da área quanto para toda sociedade.

Deste modo, a cibersegurança é essencial, garantindo a proteção de sistemas, redes e dados contra ameaças cada vez mais avançadas. Devido ao avanço da tecnologia e o aumento da conectividade, cresce também a vulnerabilidade a ataques cibernéticos comprometendo os dados dos cidadãos. Torna-se necessário, a conscientização e a educação em segurança digital sendo fundamentais para retenção dos riscos

e fortalecer a resiliência frente aos desafios do ambiente digital. Com isso é vital o investimento em estratégias eficazes de cibersegurança é essencial para garantir um futuro digital seguro e confiável.

3 PRINCIPAIS AMEAÇAS

Devido ao avanço da tecnologia, é cada vez mais desafiador proteger os dados dos ataques cibernéticos. Dentre os ataques à segurança da informação, os mais comuns são: vírus, golpes *on-line, phishing*, e o sequestro de dados por *ransomware*. Ameaças que representam perigos tanto para indivíduos quanto para organizações.

Hospitais, redes elétricas, sistemas de abastecimento de água e serviços financeiros são os principais alvos de criminosos, pois causam danos em larga escala. Entretanto, esses ataques podem comprometer serviços essenciais, colocando em risco a segurança pública e gerando impactos econômicos severos.

3.1 VÍRUS E *MALWARES*

Os vírus e *malwares* (*softwares* maliciosos) estão entre as principais ameaças à segurança digital. Historicamente, os vírus surgiram como programas capazes de infectar computadores com a capacidade de se autorreplicar, diferente do *malware* que abrange uma ampla gama de códigos maliciosos, como *worms, trojans e spywares* (Moraes & Lima, 2022). Os avanços tecnológicos propiciaram ataques cada vez mais sofisticados dificultando a sua detecção (ABES, 2023).

De acordo NIST ,(2021) destacam-se os *malwares* , desenvolvidos para fins específicos, como roubo de dados confidenciais (*spyware*). Com isso seu impacto afeta desde usuários individuais até os de grandes corporações, resultando não apenas em prejuízos financeiros, mas também em danos reputacionais de longo prazo (Santos et al., 2021).

3.2 *PHISHING*

O *phishing* é caracterizado pelo envio de mensagens fraudulentas que tem por objetivo enganar os usuários para obtenção dos dados, como senhas e informações financeiras (KASPERSKY, 2024). Os golpes se utilizam de comunicações legítimas, recorrendo a técnicas de engenharia social para indução ao erro. O *phishing,* segundo especialistas se baseia na confiança e a desatenção humana, acarretando prejuízos financeiros e exposição indevida das informações. (EL PAÍS, 2024).

Com o avanço tecnológico o *phishing*, tem adotado ataques cada vez mais sofisticados, usando a IA para customização de mensagens (AS, 2024). Uso de *e-mails*, redes sociais, SMS (*smishing)* e até chamadas telefônicas *(vishing)* são empregados para aplicar golpes. A pandemia acelerou este processo, devido ao aumento do comércio *on-line* e do trabalho remoto, resultando desafios para a cibersegurança (EL PAÍS, 2024).

Especialistas recomendam o uso de técnicas como a adoção de ferramentas: filtros anti-*phishing*, autenticação multifator e certificados de segurança são essenciais. É primordial, a educação digital ensinada aos usuários ajudando a identificar os sinais de fraude, como URLs suspeitas e pedidos suspeitos. Treinamentos constantes reduzem consideravelmente a vulnerabilidade das organizações. (KASPERSKY, 2024)

Com isso, o *phishing* representa uma ameaça continua para o cenário da cibersegurança, exigindo uma ação continua entre inovação tecnológica e capacitação das pessoas. Sendo fundamental para mitigar seus impactos, garantindo um ambiente digital mais seguro.

3.3 SEQUESTRO DE DADOS (*RANSOMWARE*)

O sequestro de dados (*ransomware*), é uma ameaça cibernética que tem ganhado repercussão devido ao seu potencial destrutivo. Segundo Ribeiro (2020), o *ransomware* na internet que criptografa os arquivos do usuário solicitando o resgate por meio de pagamento, tem afetado as organizações públicas e privadas, além dos cidadãos que também são prejudicados.

O *ransomware* se infecta no sistema por meio de vetores como *e-mails* falsos, *downloads* maliciosos ou em *softwares* desatualizados. De acordo com Santos (2022), quando o *malware* se infiltra no sistema, ele criptografa os dados enviando uma mensagem ao usuário, requerendo pagamento dos dados roubados, utilizando as criptomoedas, para fornecer a chave de desencriptação. Desta forma, as vítimas ficam em uma posição delicada, pois não a garantia de que após o pagamento os dados serão liberados.

Em conformidade com Ferreira (2023), diversos setores têm enfrentado interrupções operacionais e perdas financeiras significativas devido ao *ransomware*. Baixos investimentos em cibersegurança e a falta de conscientização de práticas seguras contribuem para a vulnerabilidade das organizações.

Neste caso a adoção de medidas são primordiais para a redução das ameaças *ransomware*. Santos (2022) recomenda a utilização e manutenção de *backups* atualizados sendo armazenados fora da rede principal como uso da nuvem. Implementação de políticas de segurança robustas, a atualização periódica dos sistemas e *softwares*, aliado a realização de treinamentos aos colaboradores sobre o perigo de possíveis ameaças.

4 PROTEÇÃO DE DADOS E REGULAÇÕES

Na era digital a proteção dos dados tornou-se primordial para a segurança cibernética, o que possibilitou à implementação de legislações específicas ao redor do mundo. (EUROPEAN PARLIAMENT AND COUNCIL, 2016; BRASIL, 2018). No Brasil, a (LGPD) estabelece orientação para a coleta, armazenamento, tratamento e compartilhamento dos dados (BRASIL 2018).

Na União Europeia o GDPR estabelece normas e diretrizes rigorosos para a proteção dos dados, propiciando maior segurança nas informações pessoais tanto de empresas, e dos cidadãos europeus independentemente da sua localização (EUROPEAN PARLIAMENT AND COUNCIL, 2016).

4.1 LGPD E GDPR

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados ou LGPD, passou a vigorar em setembro de 2020, com o intuito de assegurar a privacidade e segurança dos dados dos cidadãos brasileiros. Entre os principais pontos estabelecidos estão a definição do que são dados pessoais e dados sensíveis, o consentimento do titular para explicito uso de suas informações, além de assegurar o direito de acesso e exclusão das informações caso necessário.

As empresas, pela lei, têm obrigatoriedade de adotar medidas de segurança com fiscalização da ANPD (Autoridade Nacional de Proteção de dados), o descumprimento das normas e diretrizes, podem resultar a empresa penalidades que podem chegar a 2% do faturamento da empresa, sendo limitadas ao valor de R$ 50 milhões por infração (BRASIL, 2018).

Criada em 2016, e implementada também em 2018 de forma semelhante a LGPD, o General Data Protection Regulation, em português Regulamento Geral sobre a Proteção de Dados ou GDPR tem por objetivo estabelecer diretrizes rigorosas para coleta e processamento dos dados dos cidadãos europeus independente da sua localização da empresa.

Suas principais medidas são: exigências rigorosas para a coleta e uso dos dados, direito ao esquecimento mediante pedido, transparência no tratamento das informações e regras sobre a portabilidade dos dados. Além disso o GDPR, estipula penalidades severas, onde o valor da multa pode atingir 20 milhões de euros ou 4% do faturamento global da empresa, além de responsabilizar as organizações para adoção de medidas de segurança e vazamento dos dados. (EUROPEAN PARLIAMENT AND COUNCIL, 2016).

4.2 OUTRAS NORMAS E REGULAMENTAÇÕES

O Brasil conta com outras regulamentações primordiais para a proteção e segurança de digital. O Marco Civil da Internet (Lei nº 12.965/2014), tem por objetivo, definir os direitos e obrigações no uso da internet, garantindo a liberdade de expressão e a privacidade do cidadão (BRASIL, 2014).

A Política Nacional de Cibersegurança (PNCiber), implantada pelo Decreto nº 11.856/2023, determina estratégias de fornecimento a segurança digital no país (BRASIL, 2023).Por outro lado, a Estratégia Nacional de Segurança Cibernética (E-Ciber), em 2020, determina a prevenção de incidentes cibernéticos, através da promoção de ações integradas de defesa (BRASIL, 2020). Portanto estas normas, juntas, fortalecem a segurança e proteção dos dados gerando um arcabouço legal para a cibersegurança no Brasil.

5 BOAS PRÁTICAS

5.1 TÉCNICAS E TECNOLOGIAS DE SEGURANÇA

Garantir a segurança das informações tornou-se imprescindível para garantir a proteção dos sistemas de dados contra ameaças cada vez mais elaboradas. Diversas técnicas vêm sendo aplicadas com o objetivo de mitigar as falhas e fortalecer as infraestruturas digitais. Uma das práticas adotadas é a segmentação de redes que executa papel primordial na limitação do acesso não autorizado as zonas prejudicadas garantindo que apenas usuários e dispositivos autorizados possam interagir a rede (Easttom, 2020).

A implementação de *firewalls* é uma estratégia essencial na proteção dos sistemas. Esses equipamentos funcionam como uma linha de defesa, ao filtrar e impedir a passagem de tráfego prejudicial, evitando ataques tanto de fora quanto de dentro da rede. Uma configuração apropriada dos *firewalls* garante um controle eficaz sobre as conexões que entram e saem, tornando mais difícil a exploração de falhas de segurança. O uso conjunto com sistemas de detecção e prevenção de intrusões (IDS/IPS) fortalece a segurança, possibilitando uma reação mais ágil a eventos de invasão.

Além dessas defesas, a execução regular de testes de penetração (*pentests*) é fundamental para detectar vulnerabilidades antes que criminosos possam aproveitá-las. Essa abordagem envolve reproduzir ataques autênticos para identificar fraquezas nos sistemas e remediar possíveis pontos de falha. A avaliação constante da segurança possibilita a antecipação de ameaças e a criação de planos de mitigação eficazes.

Um aspecto crucial é a autenticação multifatorial (MFA), que introduz níveis adicionais de segurança além das senhas tradicionais. Esse sistema integra diversas formas de verificação, incluindo senhas, *tokens* e dados biométricos, assegurando que somente usuários autorizados possam acessar os sistemas. Conforme mencionado por Stallings (2017), a MFA diminui consideravelmente a probabilidade de violação de credenciais, pois mesmo que um dos fatores seja comprometido, o acesso não será liberado sem a confirmação dos demais recursos de segurança.

Com isso, a atualização constante de programas e *softwares* é primordial para reduzir vulnerabilidades identificadas. Os criadores e fornecedores de tecnologia regularmente disponibilizam correções de segurança para resolver falhas detectadas. A falta dessas atualizações pode tornar os sistemas vulneráveis a ataques que exploram brechas conhecidas. Segundo Peltier (2016), manter os sistemas em dia diminui os riscos de ataques por *malware* e outras ameaças digitais, proporcionando um ambiente online mais protegido.

5.2 CRIPTOGRAFIA E MFA: PROTEÇÃO DE DADOS EM TRÂNSITO E REPOUSO.

Para assegurar que as informações permaneçam confidenciais e intactas, a criptografia desempenha um papel importante, seja durante a movimentação dos dados, seja quando estão guardados. Quando os dados trafegam por redes, públicas ou privadas, a criptografia assegura que apenas pessoas autorizadas

consigam entender o conteúdo, protegendo-os de interceptações. Estando os dados parados, como em discos, servidores ou na nuvem, a criptografia age como um escudo contra invasões, caso o sistema seja atacado fisicamente ou virtualmente. Stallings (2017) enfatiza a criptografia como base da segurança informacional.

A autenticação multifatorial (MFA) atua junto com a criptografia, fortalecendo o acesso. O MFA demanda que o usuário comprove quem é por meio de dois ou mais elementos diferentes: uma senha (algo que sabe), um *token* ou celular (algo que possui) e biometria (algo que é). Isso torna mais difícil ataques como o *phishing*, onde apenas a senha é roubada o que explica que usar vários métodos de autenticação diminui muito os riscos de invasão.

Ao unir criptografia e MFA, cria-se uma forte proteção. Um exemplo é usar criptografia de ponta a ponta em aplicativos de mensagens, junto com a obrigatoriedade do MFA para entrar. Assim, mesmo que os dados sejam pegos no caminho ou os aparelhos se percam, as informações ficam seguras. Beal (2021) salienta que essa combinação é perfeita para empresas e governos, onde proteger dados é essencial.

No entanto, colocar essas tecnologias em prática exige preparo e treinamento. É importante selecionar algoritmos de criptografia modernos (como AES e RSA) e garantir que o MFA não complique a vida do usuário. Além disso, é preciso criar regras internas para garantir que essas tecnologias sejam usadas corretamente e de forma consistente.

5.3 FERRAMENTAS

As empresas empregam uma gama de tecnologias para assegurar a proteção dos seus dados. A escolha depende das necessidades específicas e do nível de proteção almejado, incluindo antivírus, *firewalls*, sistemas IDS/IPS, *backups*, criptografia, entre outros. Estes instrumentos trabalham em conjunto, abrangendo diversas frentes de possíveis ataques.

O *firewall*, amplamente utilizado, funciona como um muro entre redes seguras e inseguras, supervisionando o fluxo de dados. Antivírus e antimalwares são cruciais para achar e eliminar *softwares* maliciosos. Para uma proteção antecipada, IDS e IPS vigiam o tráfego, avisando ou bloqueando invasões em tempo real (Tanenbaum & Wetherall, 2013).

Os SIEMs (Security Information and Event Management) também se destacam, reunindo e avaliando dados de segurança de origens variadas, facilitando a identificação de atividades suspeitas. *Backups* automáticos são cruciais para a recuperação em eventos como *ransomware*, garantindo a operação contínua da empresa. Beal (2021) concordam que o uso combinado dessas ferramentas aumenta a eficácia da segurança.

Porém, nenhuma ferramenta funciona sozinha. É essencial integrá-las numa estratégia completa, com configurações corretas e atualizações frequentes. Além disso, é fundamental treinar a equipe para entender os alertas e agir prontamente em caso de incidentes.

5.4 POLÍTICAS DE SEGURANÇA

As normas de proteção de dados são orientações oficiais que as companhias criam a fim de defender seus bens informativos. Elas estipulam leis, ações esperadas e deveres dos usuários e gestores no que se refere à proteção digital. Em linha com a NBR ISO/IEC 27002 (ABNT, 2013), tais normas são cruciais para a criação de um cenário seguro e forte.

Essas orientações incluem desde o controle de entrada em sistemas até o uso cabível de aparelhos, passando por normas de palavras-chave, divisão de dados e reação a imprevistos, conforme as normas de proteção tem de espelhar os intentos e o jeito da companhia, sendo límpida, direta e alcançável a todos os parceiros.

A criação de normas eficazes envolve a união de vários setores da firma e precisa ser aprovada pela alta gestão. Após definidas, as normas precisam ser bastante divulgadas e seguidas de formações. É primordial que os empregados entendam o motivo das leis e como usá-las no dia a dia. Segundo Oliveira (2020), o lado humano é crucial para o êxito ou não de toda norma de proteção.

A análise constante das normas também se faz precisa, já que o ambiente de perigos está sempre a mudar. Atualizações em tecnologias, trocas nos processos de negócios e novas regras podem pedir adaptações. Desse modo, normas severas, mas flexíveis, são uma necessidade atual.

6 METODOLOGIA

A metodologia utiliza no trabalho segue uma abordagem qualitativa, fundamentada em estudo exploratório e revisão bibliográfica. Foram examinados materiais como artigos acadêmicos, publicações técnicas, documentos institucionais e normas legais pertinentes, visando construir uma visão abrangente e atualizada do assunto. Essa perspectiva possibilita a análise tanto dos elementos técnicos quanto dos fatores humanos relacionados à segurança da informação, além de suas consequências sociais e econômicas.

7 CONSIDERAÇÕES FINAIS

Diante do panorama digital atual, a cibersegurança emerge como fundamental para proteger informações pessoais e de instituições. Ataques virtuais, cada vez mais sofisticados, impulsionados pela IA, demandam ações rápidas, eficientes, e que durem no tempo. Ameaças como *malware, phishing, e ransomware*, continuam a avançar, como se viu no trabalho, colocando em xeque não só dados importantes, mas também a estabilidade de serviços vitais e a fé na tecnologia.

Considerando as leis, LGPD e GDPR, a regulamentação mostra-se um apoio forte para a privacidade e para reforçar a responsabilidade digital. Mas não basta ter leis - é preciso que sejam bem aplicadas pelas empresas, junto com a conscientização constante de todos os usuários de tecnologia, para a importância de boas práticas e tecnologias como criptografia, autenticação de duas etapas e sistemas anti-invasão.

Essas ferramentas, aliadas a políticas internas bem estruturadas e a uma cultura organizacional voltada à segurança, constituem a base para a construção de um ambiente digital resiliente. No entanto, tais medidas só são efetivas quando acompanhadas de treinamentos contínuos e ações de educação digital, uma vez que o fator humano permanece como o elo mais vulnerável nas cadeias de segurança da informação.

Dessa maneira, conclui-se que cibersegurança não é um gasto a ser descartado, mas sim uma prioridade importante, em todos os níveis: pessoal, empresarial e governamental. Acredita-se que o futuro da segurança digital reside na colaboração entre tecnologia nova, leis que sejam bem aplicadas e, principalmente, a formação de uma sociedade que saiba o que deve e o que não deve fazer no mundo digital. Para se ter um ambiente seguro, é preciso dar valor à informação como algo valioso no mundo tecnológico de hoje.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DA EMPRESAS DE SOFTWARE. Relatório de Ameaças Cibernéticas 2023. São Paulo: Associação Brasileira das Empresas de Software, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. NBR ISO/IEC 27002: Código de Prática para Controles de Segurança da Informação. Rio de Janeiro: ABNT, 2013.

AS. Alerta por uma nova forma de roubar o dinheiro de sua conta bancária. 2024. Disponível em: https://as.com/actualidad/sociedad/alerta-por-una-nueva-forma-de-robar-el-dinero-de-tu-tarjeta. Acesso em: 27 de março de 2025.

BEAL, Adriano. Segurança da Informação na Prática. São Paulo: Novatec, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br. Acesso em: 31 mar. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2014-2016/2014/lei/l12965.htm. Acesso em: 31 mar. 2025.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm. Acesso em: 31 mar. 2025.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 31 mar. 2025.

CISCO. Relatório de segurança cibernética 2022. 2022. Disponível em: <https://www.cisco.com.> Acesso em: 25 de março de 2025

EASTTOM, Chuck. Computer Security Fundamentals. 4. ed. Boston: Pearson IT Certification, 2020.

EL PAÍS. A sofisticação dos ciberataques aumenta o sequestro de dados e redes sociais. 2024. Disponível em: https://elpais.com/mexico/2024-09-08/la-sofisticacion-de-los-ciberataques-aumenta-el-secuestro-de-datos-y-redes-sociales-en-mexico.html. Acesso em: 27 de março de 2025.

EUROPEAN PARLIAMENT AND COUNCIL. Regulation (EU) 2016/679. General Data Protection Regulation (GDPR). Disponível em: https://gdpr.eu. Acesso em: 31 mar. 2025.

FERREIRA, Vitor Magalhães. Os impactos organizacionais causados pelos incidentes de ataques de ransomware nos tribunais brasileiros. 2023. Disponível em: https://www.bdm.unb.br/bitstream/10483/35745/1/2023_VitorMagalhaesFerreira_tcc.pdf. Acesso em: 27 de março de 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO, 2013

KASPERSKY. Inteligência artificial para o bem ou mal? Relatório da Kaspersky mostra que ataques de phishing aumentaram com o uso da IA. 2024. Disponível em: https://www.kaspersky.com.br. Acesso em: 27 de março de 2025..

MORAES, Fábio; LIMA, Ricardo. A evolução dos vírus e malwares: Desafios e avanços na segurança digital. Revista Brasileira de Segurança da Informação, v. 12, n. 3, p. 45-58, 2022.

NIST. Malware and its Impact on Data Protection and Security. National Institute of Standards and Technology, 2021. Disponível em: https://www.nist.gov. Acesso em: 25 mar. 2025.

OLIVEIRA, André. Gestão da segurança da informação. São Paulo: Érica, 2020.

PELTIER, Thomas R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton: Auerbach Publications, 2016.

PEREIRA, F. Fundamentos de cibersegurança. Revista de Informática e Tecnologia, v. 24, n. 2, p. 78-92, 2023.

RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739. Acesso em: 27 de março 2025.

STALLINGS, William. Criptografia e segurança de redes. 7. ed. São Paulo: Pearson, 2017.

SANTOS, Carlos; OLIVEIRA, João; PEREIRA, Ana. Impactos dos malwares nas corporações e nas finanças: Uma análise dos efeitos de segurança digital em grandes empresas. Revista Internacional de Cibersegurança, v. 9, n. 2, p. 110-126, 2021.

SANTOS, Levi Alves dos. Os ataques ransomware e a camada de proteção em sistemas governamentais. 2022. Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware. Acesso em: 27 de março 2025.

TANENBAUM, Andrew S.; WETHERALL, David J. Redes de computadores. 5. ed. São Paulo: Pearson, 2013