PRIVACIDADE DE DADOS NA SAÚDE PÚBLICA: ANÁLISE DA EFETIVIDADE NA PREVENÇÃO DE AMEAÇAS RELEVANTES

DATA PRIVACY IN PUBLIC HEALTH: ANALYSIS OF EFFECTIVENESS IN THE PREVENTION OF RELEVANT THREATS

Wellington Aquino dos Santos[1]
Carlos Henrique de Santana Soares[2]
Gustavo Barros Lins[3]

RESUMO

Esta pesquisa pretende compreender a importância da privacidade de dados e sua relevância no que se refere à saúde pública, avaliando a eficácia, resolução e prevenção desses dados nesses sistemas. O estudo busca fornecer informações valiosas para o desenvolvimento de políticas e estratégias de gerenciamento de dados de saúde pública mais eficazes e confiáveis. Revisando uma bagagem de literatura já existente, contendo estudos de caso, relatórios e regulamentos relevantes, para auxiliar a compreensão desse contexto atual a qual estamos inseridos. A implementação de soluções eficazes de segurança da informação em saúde pública é fundamental para prevenir ameaças cibernéticas e proteger a privacidade dos dados pessoais dos cidadãos, mantendo a transparência e a confiança nas políticas de saúde pública. O estudo também busca reconhecer os principais desafios enfrentados por essas soluções de segurança da informação neste ramo da saúde, que muitas vezes essas informações confidenciais podem ser manipuladas por profissionais não aptos.

Palavras-chave: Privacidade; dados; saúde.

ABSTRACT

This research intends to understand the importance of data privacy and its relevance with regard to public health, evaluating the manipulated by unqualified professionals. Reviewing existing literature, containing case studies, reports and relevant regulations, to help understand the current context in which we operate. The implementation of effective information security solutions in public health is essential to prevent cyber threats and protect the privacy of citizens' personal data, maintaining transparency and trust in public health policies. The study also seeks to provide valuable information for the development of more effective and reliable public health data management policies and strategies.effectiveness, resolution and prevention of these data in these systems. The study seeks to recognize the main challenges faced by these information security solutions in this field of health, that often this confidential information can be manipulated by unqualified professionals.

Keywords: Privacy; data; health.

1 Bacharelando em Sistemas da Informação pela UNIFACOL
2 Orientador e docente do curso de bacharelado em Sistemas de Informação da UNIFACOL

1 INTRODUÇÃO

A sociedade evoluiu muito nos últimos anos e junto com ela a tecnologia, a quantidade e o acesso à informação chegaram a patamares nunca vistos, o compartilhamento dessas informações gera cada vez mais preocupações quanto a sua segurança e a demanda de protegê-las de possíveis ameaças. Consequentemente a coleta e uso de dados nessa era digital encontra-se em nível exponencial. A crescente demanda por segurança da informação é um reflexo da sociedade digital em que vivemos. A avaliação de ataques cibernéticos desempenha um papel vital na classificação de comportamentos que representam uma ameaça à segurança cibernética de empresas, instituições e indivíduos. Como tal, a realização desta análise torna-se ainda mais importante à medida que aumenta o risco de ataques cibernéticos (Silvestre, 2021).

Conforme o passar dos anos foram desenvolvidas soluções afins de contornar isso, como regulamentações governamentais, tecnologias de criptografia, padrões de codificação e práticas de privacidade (Direito de um indivíduo controlar a coleta, uso e divulgação de suas informações pessoais). Essas medidas são essenciais para garantir a proteção dos dados dos usuários e permitir que as tecnologias digitais continuem a ser utilizadas com segurança.

Nesse sentido, esta pesquisa tem como objetivo geral entender a importância da privacidade de dados e sua relevância para a saúde pública e como objetivos específicos identificar os principais desafios enfrentados na segurança da informação na área da saúde, verificar as soluções de privacidade de dados mais comuns e avaliar a eficácia dessas soluções.

Para contribuir com a compreensão do atual estado do tema, será feito com estudos de caso, relatórios e regulamentações relevantes, oferecendo assim informações que podem ser valiosas, para elaborar estratégias no que se refere aos dados e gestão da saúde pública.

Segundo afirmam os especialistas, ao avaliar a eficácia das soluções em diferentes contextos e ameaças, é crucial levar em consideração elementos como facilidade de uso e escalabilidade. No caso das arquiteturas monolíticas, observa-se que, embora o desenvolvimento do software possa ser inicialmente simples, à medida que o sistema se expande, sua complexidade também se intensifica (Silvestre, 2021 apud Kalsk, 2019). Um serviço dedicado à transferência de dados, usando uma arquitetura baseada em micro serviços e suportando a anonimização dessas informações. Neste contexto, busca-se compreender

como elas podem ajudar e identificar as melhores práticas a fim de assegurar a intimidade dos dados.

A segurança dessas soluções tem sido bastante discutida, todavia as leis de privacidade evidenciam proteção legal aos usuários, as empresas tendem a não as cumprir em sua forma prevista, por falta de conhecimento no assunto muitas vezes, as tecnologias de criptografia por exemplo podem ser de desconhecimento ou difíceis de se utilizar no dia a dia, por consequência podem não oferecer a proteção esperada, ou simplesmente complexa a sua implementação.

Saber encontrar uma harmonia entre a proteção desses dados e a usabilidade é de suma importância para que as empresas garantam a sua segurança, sendo esse um dos desafios a serem enfrentados atualmente, a fim de assegurar a segurança das informações sem prejudicar a experiência do usuário, que espera uma interação fácil e agradável. Embora a sua experiência possa representar mais um desafio, é bastante fundamental para preservá-las e deixá-las de forma segura e eficiente. A análise de soluções utilizadas no dia a dia das empresas pode contribuir para o desenvolvimento de novas soluções mais robustas e eficientes e encorajar os setores que lidam com esses dados a implementar medidas para proteger as informações pessoais dos usuários. Diante disso, a pergunta central desta pesquisa é: Quais são as principais soluções de privacidade de dados pessoais na saúde pública e qual a efetividade dessas soluções na prevenção das mais relevantes ameaças cibernéticas?

2 REFERENCIAL TEÓRICO

2.1 Dados

A palavra "dado" é derivada da forma plural do latim "datum", que significa dádiva, oferenda ou algo reconhecido e usado como apoio de cálculo. Este termo representa a nossa conexão com a ampla gama de fenômenos em que estamos imersos. Os primeiros métodos de registro de dados podem ter sido pedaços de madeira para marcar a passagem dos dias, ou estacas cravadas no solo para marcar o surgir do sol no solstício de verão. Existem várias histórias destacando o nascimento da palavra. Mais tarde, a invenção do ábaco facilitou o cálculo dessas informações, e o crescimento da escrita ampliou extraordinariamente a habilidade do ser humano de registrar experiências e eventos do globo, resultando em um

aumento na porção de informações coletadas (Sayão e Sales 2020 apud Kelleher e Tierney,2018). Nos últimos 150 anos, a chegada dos sensores elétricos, a digitalização dos dados e a invenção dos computadores contribuíram para um aumento dramático no número de dados coletados e armazenados.

Livrar-se da palavra "dados" agora é um desafio, porém, como muitos outros conceitos usados para finalidades diferentes, a palavra "dados" têm significados diferentes dependendo muito do contexto em que são usados (SWANSON; RINEHART, 2016). Isso é especialmente evidente quando nos referimos a configurações específicas de pesquisa. A compreensão dos termos e conceitos relacionados a dados é fundamental para navegar pelo mundo da informação atual. Mesmo quando nos referimos ao ambiente específico da pesquisa. Conforme definição de (Da Silveira ,2022), dados pessoais englobam uma ampla gama de informações, como nome, data de nascimento, CPF, RG, carteira nacional de habilitação (CNH), carteira de trabalho, passaporte, título de eleitor, sexo, endereço, e-mail, telefone, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização, informações sobre saúde ou orientação sexual, além de dados genéticos ou biométricos, informações essas que necessitam de bastante privacidade.

Antes de abordarmos qualquer aspecto, é crucial reconhecer que a onipresença dos dados não é uma realidade limitada apenas aos tempos contemporâneos. Governos, empresas, a pesquisa científica e diversos outros setores da sociedade sempre fizeram uso de dados e informações para embasar suas decisões, direcionar suas iniciativas e fundamentar suas descobertas. Entretanto, nas últimas décadas, uma transformação sem precedentes tem mudado nossa sociedade, marcada por uma mudança na disponibilidade de informações: da escassez à ampla profusão de dados. Esse fenômeno acarreta profundas mudanças em nosso mundo, representando uma revolução que reconfigura nossa forma de viver, trabalhar, nos divertir e até mesmo gerar conhecimento científico (SAYÃO; SALES, 2019).

2.2 Privacidade

A privacidade é um conceito fundamental na sociedade, que sempre esteve presente nas preocupações relacionadas à liberdade e às garantias individuais. Como aponta (Sousa, 2017), os princípios do conceito de privacidade estão enraizados na cultura e nos valores sociais. Nesse sentido, a legislação e as diretrizes destinadas a proteger os direitos dos indivíduos, especialmente em relação à privacidade, têm como base a Declaração Universal dos Direitos Humanos. Aprovada pela Assembleia Geral das Nações Unidas (AGNU) em

1948, a declaração é um dos principais marcos da defesa dos direitos humanos no mundo. Para que a privacidade e a proteção de dados sejam asseguradas, as instituições devem dar prioridade a essas questões e garantir a confiança de seus pacientes, como destacado por (Sousa, 2017 apud Walker, 2017).

A Lei Geral de Proteção de Dados (LGPD) define privacidade de dados como o direito fundamental do titular de dados pessoais de ter controle sobre as informações que são coletadas, usadas, compartilhadas e armazenadas por terceiros. Isso inclui o direito de ser informado sobre o processamento de seus dados, o direito de acessá-los, corrigi-los, excluí-los ou limitar seu uso, e o direito de revogar o consentimento para o seu processamento, ela também define dados pessoais como informações relacionadas a uma pessoa física identificada ou identificável, direta ou indiretamente, por meio de um identificador, como nome, identificação, dados de localização, identificadores eletrônicos, ou por elementos específicos de sua identidade física, fisiológica, genética, mental, econômica, cultural ou social.

Segundo (Thibes, 2017) houve uma grande mudança no conceito de privacidade no contexto do capitalismo, reinterpretando a noção de vida privada e as fronteiras entre público e privado. Os autores argumentam que o declínio da privacidade, muitas vezes atribuído a novas tecnologias que trouxeram mais interações virtuais e exposição de vidas privadas, é o resultado de uma mudança histórica nos conceitos sociais. Isso também se refere ao conceito de Max Weber do "espírito do capitalismo", que apresenta a cultura capitalista como um modo de vida que vai além de um simples sistema econômico ou de produção, “a noção de uma esfera doméstica separada de outras esferas de existência é, portanto, o ponto de partida para a emergência da privacidade como um direito”.

Segundo (Bezerra e Waltz ,2014, p.159), nos últimos períodos a internet teve uma parte importante no âmbito público que teve alto impacto mundial. Os autores falam que as conexões estabelecidas entre os computadores nessa proporção têm acarretado mudanças nos contextos econômicos inseridos, assim como em partes políticas e socioculturais, havendo uma consequência na proteção dos direitos à privacidade e a intimidade, que se encontram em ameaça devido a vigilância e espionagem feita por grandes empresas e governos. Direitos esses que encapsulam não somente a o individual, como alcança também a questões familiares, correspondências e relações pessoais, e são definidos como aquilo que um indivíduo não pretende tornar público, mantendo-se reservados somente aos membros do seu círculo privado de convivência. A intimidade, por sua vez, é uma esfera que diz respeito exclusivamente ao indivíduo.

2.3 Saúde pública

O sistema público de saúde é resultado de décadas de luta lideradas pelo movimento da reforma sanitária. Sua criação foi instituída pela Constituição Federal de 1988 e posteriormente consolidada por meio das Leis 8.080 e 8.142. Esse sistema é chamado de Sistema Único de Saúde (SUS).

Dentre suas características, a mais fundamental é sua base constitucional, que estabelece a saúde como direito do cidadão e dever do Estado. A ênfase da Constituição na saúde reflete a relevância e prioridade do setor em relação a muitos outros. Ressalta-se que tanto a saúde pública quanto a privada são consideradas de relevância pública. Essa visão jurídica de relevância pública vai além da simples noção de que a saúde é uma mercadoria de mercado. Os serviços privados de saúde, apesar de sua relevância pública, são regulamentados, fiscalizados e controlados pelo SUS. Abrange tanto sistemas privados com fins lucrativos administrados por pessoas físicas ou jurídicas, como planos de saúde, seguradoras, cooperativas e órgãos autônomos, quanto sistemas privados sem fins lucrativos, como hospitais, clínicas, consultórios e laboratórios em vários países. (CARVALHO, 2013, p. 7-26).

2.4 Ameaças cibernéticas

A sociedade contemporânea depende cada vez mais de um espaço para comunicação, troca de dados e funcionamento de sistemas vitais, como por exemplo infraestruturas críticas e redes financeiras. No entanto, essa interdependência também expõe vulnerabilidades, tornando a cibersegurança uma preocupação constante. De acordo com a definição de (Gonzales e Portela, 2018, p. 217). O espaço cibernético desempenha um papel central em nossa era digital, representando o ambiente onde uma diversidade de informações, abrangendo desde dados confidenciais até informações públicas, esse é um cenário onde a interconexão prevalece, permitindo que informações de variados matizes circulem livremente.

Conforme mencionado por (SANTOS JUNIOR, 2020 apud PANDE, 2017) as Ameaças cibernéticas, por sua vez, representam as preocupações centrais da segurança cibernética e consistem em atividades ilícitas nas quais computadores ou dispositivos de computação, sejam independentes ou integrados a uma rede, são empregados como instrumentos e/ou alvos de condutas criminosas. Isso se manifesta na invasão e na exploração de dados sem a permissão do proprietário dessas informações.

No contexto global, a ocorrência de situações relacionadas a ciber ameaças está claramente inclinada a crescer. Esse aumento fica evidenciado pelo notável acúmulo de incidentes que vieram à tona durante a pandemia de COVID-19. Segundo observado por (LALLIE, 2020), em um intervalo relativamente curto entre o final de 2019 e 2020, foram registrados nada menos que 43 episódios de ataques que exploram uma variedade de vetores de ataque com o intuito de afetar as pessoas. Esse cenário reforça a urgência de medidas robustas de cibersegurança para salvaguardar as infraestruturas digitais e garantir a proteção dos indivíduos em meio a esse panorama desafiador.

3 METODOLOGIA

A coleta de dados teve início com revisões da literatura e análises de estudos e pesquisas relevantes já publicados sobre o tema. Essa fase proporcionou uma base teórica sólida e insights qualitativos sobre as ameaças à privacidade de dados na área de saúde e as soluções de segurança atualmente disponíveis. Em paralelo, foram analisadas as eficácias das soluções de segurança existentes no âmbito da privacidade de dados na área de saúde. Estes dados foram relacionados à performance das soluções, podendo incluir indicadores como a eficiência na detecção e prevenção de possíveis violações, a redução de incidentes de segurança e o tempo de resposta a potenciais ataques. Essas métricas foram fundamentais para a avaliação do impacto das soluções de segurança.

Foram utilizados como critérios de exclusão, a maior parte dos artigos publicados antes de 6 anos, para garantir a atualidade das fontes. Priorizaremos trabalhos de autores que tenham experiência na área e que demonstrem relevância para o nosso objetivo de pesquisa. Esses autores geralmente possuem uma bagagem de conhecimento substancial e têm maior probabilidade de contribuir de forma mais eficaz para nossa análise. Além disso, os artigos selecionados devem estar alinhados de forma coerente com nossos objetivos de pesquisa.

Posteriormente, os dados coletados serão submetidos a uma análise qualitativa e quantitativa. Além disso, esses dados serão utilizados para identificar tendências e padrões

relevantes. A etapa de discussão e conclusões será embasada na análise detalhada dos dados obtidos. Serão elaboradas discussões abrangentes sobre a eficácia das soluções de segurança na proteção da privacidade de dados na área de saúde, destacando as principais descobertas e implicações identificadas.

Por fim, nos resultados da pesquisa, essas recomendações visam orientar a melhoria das práticas de segurança de dados na área de saúde, com base na abordagem adotada, proporcionando uma avaliação holística das soluções de segurança, considerando os aspectos qualitativos e quantitativos relacionados à proteção da privacidade de dados na área de saúde.

4. A IMPORTÂNCIA DA PRIVACIDADE DE DADOS NA ÁREA DE SAÚDE

Na área da saúde todos os procedimentos sejam eles de curto ou longo prazo necessitam de informações, podemos citar por exemplo o registro clínico, que é extremamente útil no dia a dia dos enfermeiros, médicos, farmacêuticos e outros demais profissionais da saúde, sua compreensão é de bastante importância para otimizar o tempo e garantir a eficiência dos dados transcritos como destacado por (Barreto 2019).

A proteção da privacidade e da confidencialidade dos dados do paciente é uma parte essencial da relação entre a equipe médica e o paciente. Historicamente, os profissionais foram orientados pelos códigos de ética de suas profissões em todas as sociedades e culturas. Os pacientes permitem o acesso aos seus corpos para exames e tratamentos, mas esperam que os cuidadores os protejam de qualquer contato físico desnecessário ou constrangedor que possam expô-los.

Os profissionais obtêm informações confidenciais dos pacientes para entender seus problemas de saúde e essas informações são, de fato, confidenciais, o que significa que aqueles que as possuem têm a responsabilidade de protegê-las contra a divulgação a terceiros. (Do Nascimento-Silva-Junior, 2017).

De acordo com (Sousa, 2017 apud Rindfleisch, 1997) de forma mais ampla podemos citar informações como o histórico médico, diagnóstico, tratamentos, prescrições médicas, peso, altura e pressão arterial de um paciente, mas também podem conter informações mais sensíveis, como história reprodutiva, saúde mental, cuidados psiquiátricos, comportamento sexual e presença de doenças sexualmente transmissíveis. Dados esses que são de extrema importância para esses profissionais da saúde, são essenciais para garantir a qualidade e eficácia da prestação de cuidados com o paciente.

De acordo com a Organização Pan-Americana de Saúde (OPAS), a segurança é uma preocupação incluída nas organizações internacionais de saúde. Os Sistemas de Informações em Saúde (SIS) armazenam dados identificados sobre a saúde dos indivíduos e essas informações são consideradas sensíveis. Os dados médicos inserem-se na esfera mais íntima do indivíduo, podendo causar danos se utilizados fora da relação médico-paciente, o que pode levar a várias formas de discriminação, incriminação e violação de direitos fundamentais OPAS, citado por (Danyllo do Nascimento-Silva-Junior, 2017).

5. AMEAÇAS A PRIVACIDADE DE DADOS NA ÁREA DA SAÚDE

Segundo o (Ministério da Saúde, 2022),As medidas de segurança devem ser implementadas atendendo às especificadas Políticas de Segurança da Informação e Comunicações, que inclui procedimentos de segurança da tecnologia da informação.Com essas constantes mudanças na segurança da informação e trazem consigo evoluções, devem ser analisadas regularmente novas medidas para melhorá-la, nos dias atuais proteger os dados em todas as fases do seu ciclo de vida é primordial, desde a coleta até a destruição, com intuito de chegar nessa meta, uma variedade de sistemas, tecnologias e ferramentas são usadas para atender a esse ponto.

5.1 Vulnerabilidades na comunicação de dados de saúde

Grande parte dos utilizadores de sistemas não têm consigo o conhecimento de comunicação segura quando acessam informações de saúde pública, poucos sabem que nos navegadores existem camadas de seguranças e uma delas é o HTTPS (Hyper Text Transfer Protocol Secure), ou seja, o HTTP sobre SSL (Secure Sockets Layer)/TLS (Transport Layer Security). Na realidade, os próprios navegadores contribuem para esta percepção de segurança ao exibirem um ícone de cadeado verde ou fechado ao lado do endereço eletrônico, também conhecido como URL (Uniform Resource Locator). No entanto, de acordo com (Fiorenza, 2020 apud Bokslag, 2016), as investigações demonstram que, muitas vezes, o ambiente do HTTPS na disseminação de informações de saúde pública é, contrariamente ao que se imagina (ou ao senso comum), inseguro.

Acrescentando Fiorenza Existem muitos desafios e problemas de segurança que podem ocorrer em várias partes do ecossistema do HTTPS relacionadas com informações de saúde pública, incluindo deficiências na especificação ou na implementação dos protocolos de

segurança, configurações inadequadas dos certificados digitais nos servidores Web que hospedam conteúdo de saúde pública, erros na geração dos certificados digitais utilizados para autenticar sites de saúde pública, vulnerabilidades nas Infraestruturas de Chaves Públicas (ICPs) que sustentam a segurança online e outras vulnerabilidades. Sem a segurança adequada dados sensíveis como de pacientes, como Informações de Identificação Pessoal (PII), histórico de navegação, informações médicas, credenciais de login, entre outros podem ser capturados entre as requisições, colocando a privacidade deles em xeque, portanto, garantir a segurança das informações de saúde pública online é uma questão crítica que exige atenção contínua.

5.2 Ransoware

Ransomware é um tipo de software projetado para entrar em um sistema, travar o dispositivo e/ou criptografar seus dados, exigindo um pagamento em dinheiro para desbloquear as informações ou o dispositivo. Conforme mencionado por (Souza, 2017 apud Marvin, 2015) o primeiro ransomware foi criado por Joseph Popp em 1989, chamado de "AIDS". Este trojan enganava os usuários, alegando que a licença de um software havia expirado, criptografando os arquivos do disco rígido e pedindo o pagamento de 189 dólares à "PC Cyborg" para desbloquear o sistema.

Os ransomware mais modernos tendem a empregar os algoritmos de criptografia mais populares, nomeadamente AES (criptografia simétrica) e RSA (criptografia assimétrica). Embora ambos os tipos de algoritmos desempenhem basicamente a mesma função, cada algoritmo possui características diferentes que impactam diretamente a estratégia de investida e, consequentemente, a possibilidade da solução. Apesar da sua velocidade de encriptação, o algoritmo AES tem como maior vulnerabilidade o fato de sua chave ficar gravada nos arquivos criptografados. Na criptografia simétrica (AES), utiliza-se uma única chave para criptografar e descriptografar os dados, geralmente a chave irá ficar salva no computador infectado depois que for enviada a pessoa que realizou o ataque e o desempenho é pouco comprometido (Souza, 2017 apud Savage; Coogan Lau, 2015).

Houve um aumento significativo nos ataques usando Ryuk, visando principalmente organizações de saúde, sendo o setor de saúde dos EUA o alvo mais comum. Um exemplo interessante ocorreu em 27 de setembro de 2020, quando o Universal Health Services (UHS), um dos maiores prestadores de cuidados de saúde dos Estados Unidos, foi atacado. O incidente causou falhas nos sistemas de computadores e telefonia de diversas instalações do

UHS. Conforme relatado por (Zack Whittaker, 2020), uma pessoa com conhecimento do incidente observou que uma mensagem de Ryuk apareceu na tela de um computador instruindo os funcionários a desligarem seus computadores e não os ligar novamente, observando que isso levaria vários dias.

5.3 Phishing

Phishing é uma técnica virtual amplamente popular que visa enganar as pessoas para que adquiram informações confidenciais, como senhas e dados de cartões, diversas vezes combinando engenharia social e hacking (Martins, 2022). Os criminosos várias vezes remetem e-mails ou mensagens fraudulentas fingindo ser fontes confiáveis, como colegas de trabalho ou instituições bancárias, induzindo as vítimas a pensarem que estão recebendo comunicações legítimas. Como resultado, os criminosos podem disseminar impensadamente informações pessoais e obter acesso a sistemas reais para roubar a identidade virtual da vítima. De acordo com (Pereira, 2021 apud CheckPoint Research, 2020) O phishing foi proeminente durante a pandemia de 2020, incluindo páginas falsas relacionadas com a COVID-19, e-mails fraudulentos que alegavam ser da OMS e pedidos de doações a organizações como a OMS e as Nações Unidas.

Entre os vários tipos de ataques de phishing, o spear phishing tem como alvo alvos específicos usando os dados da vítima para aumentar a validade do ataque. O Vishing costuma usar comunicações de voz para se passar por gerentes de bancos ou agências governamentais, enquanto o smishing costuma usar mensagens de texto SMS para enganar as vítimas e usar situações como serviços de emergência para roubar informações pessoais. Esta tecnologia representa uma grande ameaça à segurança online. No Brasil, a resposta ao auxílio emergencial tornou-se um ímã para atividades maliciosas, conforme evidenciado pela IBM X-Force Incident Response and Intelligence Services, (Pereira, 2021 apud IRIS, 2020). Como consequência do estudo, foram expostos pelo menos 693 sites maliciosos criados internamente relacionados ao coronavírus e suprimentos de ajuda emergencial.

6. SOLUÇÕES PARA PRIVACIDADE DE DADOS NA AREA DE SAUDE

6.1 Estratégias para fortalecer a segurança na comunicação de dados de saúde

6.1.1 Navegadores e o uso de cifras

O handshake TLS é fundamental para estabelecer criptografia segura entre cliente e servidor com base nas diretrizes do NIST. A ferramenta testingsl.sh avalia a criptografia usada e mostra quais estão atualizadas para evitar erros que já podem ter sido solucionados como apontam (Fiorenza, 2020 apud McKay and Cooper 2019). No entanto, navegadores mais antigos, como o Internet Explorer 8, podem representar um risco porque acessam sites usando criptografia que não é recomendada. Uma solução eficaz é incentivar as atualizações do navegador e orientar os desenvolvedores a cumprirem as diretrizes de segurança do NIST. Isso garante conexões mais seguras e protege os dados do usuário, ao mesmo tempo sendo ela de muita importância para manter a integridade das comunicações online.

6.1.2 Utilização de PSF

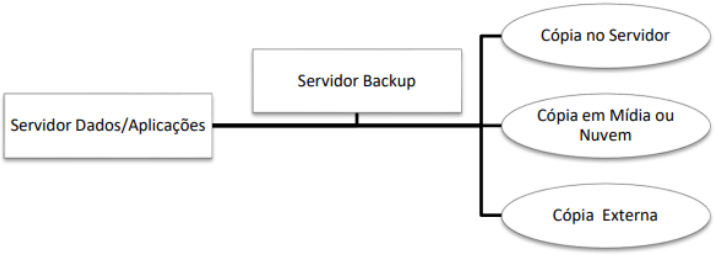
Perfect Forward Secrecy (PFS) descrito por (Fiorenza, 2020 apud Barbosa, 2018). Em 2019, desempenha um papel importante na segurança das comunicações dos dados. Esse recurso garante que mesmo que um invasor comprometa a chave privada da sessão atual, as informações trocadas em sessões anteriores permaneçam seguras. Ao contrário das conexões tradicionais, o PFS utiliza uma chave secreta diferente para cada nova seção entre cliente e servidor, o que melhora muito a segurança das comunicações.

6.2 Combates ao ransomware na área de saúde

6.2.1 Backups

Como afirma (Souza, 2017) a implementação de rotinas de backup é a base da política de segurança de uma empresa e serve como a última linha de defesa contra ataques de ransomware e sempre deve ser utilizada tanto para ataques de Ransomware e de outras origens. É importante identificar seus dados e servidores de aplicativos, avaliar seus requisitos ambientais e priorizar suas ações. Uma alternativa eficaz é usar um terminal de backup com um sistema operacional diferente, como Linux ou FreeBSD, para aumentar o nível de segurança. Porque estes sistemas não são vulneráveis a este tipo de ataque, pelo contrário possuem segurança um pouco mais robusta. Além disso, os backups devem ser acessíveis e restaurados, com atenção especial à seleção de mídia e, idealmente, pelo menos três backups disponíveis.

Backups Cotidianos



Fonte: Souza (2017)

A primeira cópia é armazenada no servidor de backup principal. A segunda é gravada em mídia externa ou serviço de armazenamento em nuvem. É importante ressaltar que é um erro grave deixar a mídia de gravação conectada ao terminal de destino. Isso ocorre porque se o seu dispositivo estiver infectado, sua mídia também ficará vulnerável. A terceira cópia é gravada em outra mídia que fica armazenada em local externo à outra mídia. Não adianta ter uma rotina de backup interna com datas e horários definidos se as cópias de backup não forem verificadas quanto à integridade dos arquivos. É igualmente importante resgatar alguns desses backups para testes reais, a fim de evitar surpresas, se necessário.

6.2.2 Firewall

Segundo (Landim e Martins, 2022 apud Cisco Systems, 2021) os firewalls desempenham um papel crucial na segurança da informação, monitorando o tráfego de rede e aplicando regras de segurança para permitir ou bloquear acessos. Na área da saúde, sua importância é ainda mais vital, protegendo dados sensíveis dos pacientes e garantindo que apenas acessos autorizados interajam com essas informações. Em um setor onde a privacidade e a integridade dos dados são críticas, os firewalls atuam como o primeiro e robusto escudo de defesa contra ameaças cibernéticas, como ransomware, que podem interromper serviços de saúde essenciais e colocar em risco a segurança dos pacientes. À medida que a tecnologia se

torna mais central na área da saúde, a presença e a manutenção adequadas dos firewalls são essenciais para garantir a proteção dos dados e, consequentemente, a qualidade do atendimento médico fornecido.

6.2.3 Antivírus

Os antivírus desempenham um papel importante na detecção e remoção de arquivos maliciosos do seu computador, incluindo vírus, spyware, ransomware e outros tipos de ameaças. Protegendo não apenas contra vírus, mas também agem como anti malware. Atualizar o software antivírus é essencial para a segurança do seu sistema. Muitos softwares antivírus já incluem dados sobre ransomware conhecidos, aumentando a proteção contra essas ameaças De acordo com (Landim e Martins, 2022 apud ATAIDES, 2018). Estas medidas ajudarão a reduzir significativamente o risco de comprometer a segurança, fixando mais uma camada de proteção nos estabelecimentos de saúde.

6.3 Mitigando ameaças de phishing

6.3.1 Conscientização do usuário

De acordo com (Matos, 2017 apud ALENCAR, 2013) a formação contínua e a sensibilização dos colaboradores desempenham um papel importante na melhoria da segurança da informação dentro de uma organização e fornecem uma solução que também beneficia a saúde pública. Este investimento fortalece os atuais pontos mais sensíveis da segurança da informação nas empresas. Além de proteger os dados internos, esta abordagem também contribui indiretamente para a segurança pública e para a sociedade, ao prevenir fugas e violações que possam afetar a confidencialidade de informações sensíveis, como dados de saúde, ao treinar funcionários como médicos e enfermeiros para evitar ataques de phishing, você pode usar recursos educacionais, como aplicativos móveis, que orientam os usuários a reconhecerem técnicas comuns de golpistas.

6.3.2 Senhas

É crucial modificar a senha e reforçar todas as medidas de recuperação de acesso da conta afetada para bloquear o atacante. No entanto, é ainda mais aconselhável que o usuário adote o hábito de regularmente alterar suas senhas, mesmo antes de suspeitar de qualquer tentativa de fraude. Criar uma senha forte é essencial. Isso inclui a criação de senhas exclusivas para cada conta que tenha um grau de importância, tendo a combinação de letras, números e símbolos sem usar informações pessoais ou termos comuns (GOOGLE, 2016). Além disso, é importante não os utilizar em diferentes serviços e ter cuidado ao utilizá-los.

6.3.3 Navegador

O Google Chrome é amplamente usado na internet, com cerca de 80% dos internautas brasileiros optando por ele em julho de 2016. Em termos de segurança, o Chrome alerta sobre sites suspeitos de phishing ou malware e mantém uma lista de sites de alto risco, além de analisar o conteúdo do site para emitir avisos (GOOGLE, 2016). Quando a detecção de phishing e malware está ativa, exibe mensagens informativas indicando suspeita de phishing.

6.3.4 Microsoft 365 Exchange online

As organizações que usam EOP Exchange Online ou Microsoft 365 com caixas de correio autônomas têm recursos antiphishing. Isso inclui inteligência com informações falsas, políticas antiphishing EOP e DMARC. Você pode gerenciar remetentes falsos e criar entradas manuais usando listas de permissão/bloqueio de inquilinos. Além disso, o EOP melhora as verificações de autenticação de e-mail, incluindo SPF, DKIM e DMARC, para identificar remetentes falsos e fortalecer a segurança (São Bernado Do Campo, 2023).

6.3.5 Antivírus (Avast)

Avast é um programa antivírus que detecta vírus e malware e protege sua rede doméstica de Internet. Análise arquivos desconhecidos em tempo real e identifique sites falsos. A Avast fornece aos usuários da Internet o Avast Online Security, uma proteção para o navegador Chrome, um plugin de reputação de sites gerenciado por uma comunidade de mais de 220 milhões de usuários. Ele coleta informações de sites de phishing e alerta os usuários quando eles visitam sites suspeitos (AVAST, 2016).

7. RESULTADOS

7.1 Navegadores e Uso de Cifras

7.1.1 Metodologia de Testes

Na pesquisa sobre a segurança das cifras em conexões TLS, dois principais métodos foram empregados. Primeiramente, o documento de referência do NIST foi utilizado como guia para determinar a segurança das cifras. Este documento serviu como um padrão de avaliação. Em segundo lugar, a ferramenta testssl.sh foi empregada para simular conexões em navegadores e coletar dados sobre as cifras utilizadas. Essa abordagem prática permitiu uma avaliação mais dinâmica e realista das práticas de segurança em conexões TLS.

7.1.2 Resultados Obtidos

Os resultados da pesquisa indicam que a atualização dos navegadores desempenha um papel crucial na segurança das comunicações online. Navegadores mais recentes tendem a se conectar a sites com cifras recomendadas, contribuindo para uma comunicação mais segura. Por outro lado, navegadores mais antigos, como o Internet Explorer 8, estão associados a cifras menos seguras. Além disso, foi observado que alguns navegadores mais recentes podem enfrentar dificuldades ao tentar se conectar a sites que não suportam certas cifras. Em resumo, a pesquisa destaca a importância da atualização de navegadores na segurança online e suas implicações nas escolhas de cifras em conexões TLS.

Eficácia Cifras (TLS)

Tabela 4. Navegadores atualizados e suas cifras

Navegador	Cifras recomendadas	Cifras não recomendadas	Sem conexão
Google Chrome 79	95,60%	4,39%	0,01%
Mozilla Firefox 71	93,32%	6,64%	0,04%
Internet Explorer 11	96,43%	3,57%	0%
Opera 66	95,61%	4,37%	0,02%
Safari 13	94,92%	5,06%	0,02%
Internet Explorer 8	0,90%	71,49%	27,61%

Fonte: Fiorenza (2020)

7.2 Utilização de PFS

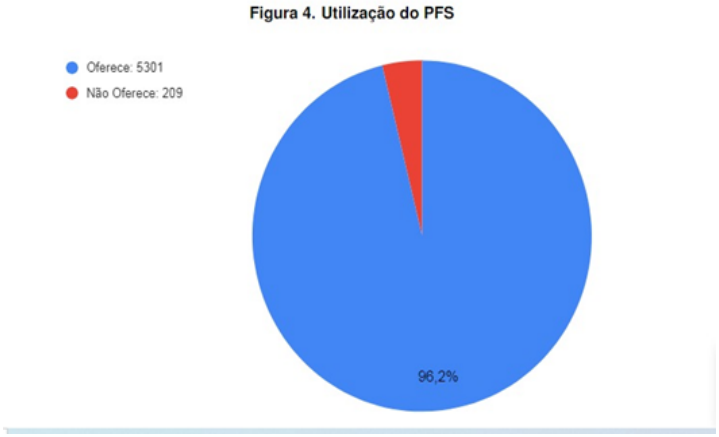
7.2.1 Metodologia de Teste

A metodologia utilizada envolve a geração de novas chaves em cada sessão. Esse processo, embora imponha uma carga computacional e de recursos adicionais, é realizado em troca do Perfect Forward Secrecy (PFS).

7.2.2 Resultados

De acordo com a análise realizada, os resultados indicam que 96,20% dos sites analisados utilizam algoritmos que suportam o sigilo de encaminhamento perfeito (PFS). Isso sugere uma adoção significativa dessa medida de segurança pelos sites avaliados. Além disso, o impacto no desempenho é potencialmente pequeno, o que sugere que a implementação do PFS não compromete substancialmente o desempenho das comunicações criptografadas.

Chaves PFS



Fonte: Fiorenza (2020)

7.3 Backup

7.3.1 Metodologia de Teste

A metodologia de teste inclui várias práticas para garantir a segurança e integridade dos dados. Primeiramente, destaca-se o armazenamento redundante em locais distintos, a conscientização sobre desconectar a mídia de gravação. Em nível de processamento, a metodologia envolve a verificação regular das cópias de segurança e a realização de testes

práticos. Esses testes práticos demonstram uma abordagem proativa para garantir a integridade dos dados.

7.3.2 Resultados da Análise

Os resultados dessa abordagem metodológica são descritos como uma combinação de práticas que refletem uma abordagem equilibrada. Essa combinação contribui para a eficácia operacional, assegurando que as informações estejam livres de corrupção quando necessário. Portanto, os resultados destacam que a implementação dessas práticas pode promover eficácia tanto na segurança quanto no processamento de dados.

7.4 Firewall

7.4.1 Metodologia de Pesquisa

Método de pesquisa utilizado envolve a execução do código do Wannacry em um ambiente de testes, firewall do Windows, mantido atualizado, desempenhando um papel crucial como uma barreira de defesa inicial contra ransomwares.

7.4.2 Resultados

A conclusão destaca que a integração dessas medidas cria uma barreira robusta contra ameaças cibernéticas e ressalta a necessidade de uma postura proativa na gestão da segurança digital, e destaca a importância de manter sempre atualizado o firewall.

Resultado Eficácia Firewall

Eficácia do Firewall do Windows

Aspecto	Avaliação
Prevenção contra Wannacry	Bem-sucedida
Monitoramento de Tráfego	Eficiente
Controle de Rede	Funcional
Atualizações	Regulares e automáticas

Fonte: Própria (2023)

7.5 Anti-Phishing

7.5.1 Metodologia dos Testes

Na primeira etapa do estudo, foram realizados acessos a sites maliciosos utilizando o navegador Chrome. Conduzindo testes específicos no programa antivírus Avast, explorando sua capacidade de detectar e bloquear potenciais ameaças. Os sites acessados foram previamente identificados como maliciosos, e durante essa etapa, foi observado atentamente os alertas e bloqueios gerados pelas ferramentas de segurança. Cada resultado foi devidamente registrado, destacando tanto os casos em que foram identificados alertas (resultados positivos) quanto aqueles em que não houve nenhum alerta (resultados negativos). Essa abordagem meticulosa permitiu uma avaliação abrangente da eficácia das ferramentas empregadas na detecção e prevenção de atividades maliciosas durante o acesso a sites suspeitos.

Na segunda etapa do estudo, o foco foi na abertura de e-mails de phishing, empregando uma abordagem abrangente. Utilizando o navegador Chrome, o programa antivírus Avast e diversas extensões anti-phishing (Netcraft, McAfee, Urlcheck e WOT) para avaliar a capacidade dessas ferramentas na detecção de ameaças. Durante esse processo, foram abertos e-mails que continham links ou arquivos maliciosos, monitorando atentamente os alertas e bloqueios gerados pelas ferramentas durante a abertura dos e-mails e a ativação dos links. Os resultados, sejam positivos ou negativos (com alertas e bloqueios) ou negativos (sem alertas e bloqueios), foram meticulosamente registrados. Essa metodologia permitiu uma avaliação minuciosa do desempenho das ferramentas em um cenário de abertura de e-mails fraudulentos.

7.5.2 Resultados

Na análise dos navegadores web, notou-se que tanto o Google Chrome quanto o Mozilla Firefox demonstraram um desempenho satisfatório na detecção de sites maliciosos. Contudo, observamos uma diferença na eficácia, onde o Chrome se destacou ao bloquear a maioria dos sites fraudulentos, enquanto o Firefox permitiu a passagem de alguns. A utilização de extensões anti-phishing nos navegadores contribuiu para a detecção, embora tenhamos observado variações em sua eficácia.

A avaliação dos programas antivírus (Avast, AVG e Avira) revelou um desempenho misto na detecção de sites maliciosos. O Avast obteve resultados mais positivos, bloqueando a maioria dos sites fraudulentos, enquanto o AVG e o Avira apresentaram um desempenho

menos eficaz. No contexto da conscientização do usuário na prevenção de phishing, destacamos a grande importância desse aspecto. Os usuários desempenham um papel crítico na identificação de e-mails e sites maliciosos. A educação sobre o reconhecimento e relato de e-mails suspeitos, a verificação da autenticidade dos sites e a compreensão do uso de extensões de segurança são elementos fundamentais. A formação contínua e a conscientização dos colaboradores emergem como peças-chave para a melhoria da segurança da informação.

Finalmente, a importância da segurança de senhas na prevenção de ataques de phishing. Foi observado que a criação de senhas fortes e exclusivas, combinando letras, números e símbolos, é essencial. A recomendação de alterar regularmente as senhas, mesmo na ausência de suspeita de fraude, é crucial. Alertamos sobre os riscos de reutilizar senhas em diferentes serviços e destaca a necessidade de conscientização sobre a importância de manter senhas seguras e adotar boas práticas de gerenciamento para reduzir o risco de phishing.

Eficacia Anti-Phishing

Teste	Resultado
Conscientização do Usuário	Conforme os testes, a conscientização do usuário é fundamental na prevenção de ataques de phishing. Embora as ferramentas tenham utilidade na segurança online, a responsabilidade de criar senhas fortes e exclusivas é do usuário.
Senhas	Os resultados dos testes destacam a importância de senhas fortes e exclusivas para cada conta. As ferramentas não conseguiram bloquear todas as tentativas de phishing, enfatizando a necessidade de senhas seguras e não reutilizadas.
Navegador	O navegador Chrome têm recursos para alertar sobre sites suspeitos de phishing ou malware. O Chrome teve um desempenho melhor na detecção de ameaças, destacando sua utilidade na proteção contra ataques de phishing.
Antivírus (Avast)	O programa antivírus Avast mostrou ser eficaz na detecção de vírus e malware, fornecendo proteção para a rede doméstica de Internet. A extensão Avast Online Security para o navegador Chrome ajuda a identificar sites suspeitos de phishing.

Fonte: Própria (2023)

7.6 Microsoft 365 Exchange Online

7.6.1 Metodología de Testes

Durante um período de 30 dias, realizamos análises para avaliar a eficiência da ferramenta de detecção de phishing do Microsoft 365 Exchange online.

7.6.2 Resultados

Nesse período, identificamos 216 casos de phishing, dos quais 4 foram classificados como falsos positivos após avaliação por seres humanos. Para medir a eficácia da ferramenta, calculamos a porcentagem de detecção correta, utilizando a fórmula:

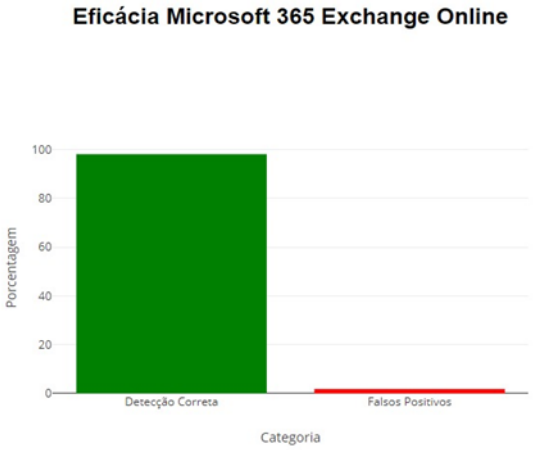
Eficiência na detecção de phishing real (PMR) = ((Total de phishing detectados) - (Falsos positivos)) / (Total de phishing detectados) * 100

Nesse contexto, a eficiência na detecção de phishing (PMR) é calculada da seguinte forma:

PMR = ((216 - 4) / 216) * 100 PMR = 98,14%

Sendo assim, a eficácia da ferramenta é de 98,14% na identificação de phishings reais, com apenas 1,85% de casos de falsos positivos.

Eficácia Microsoft 395 Exchange Online



São Bernado Do Campo (2023)

CONSIDERAÇÕES FINAIS

A pergunta central foi abordada de maneira abrangente. Para pesquisas futuras, tende-se como sugestões explorar estratégias de aprimoramento da eficácia dessas soluções, comparar práticas em diferentes setores, investigar avanços tecnológicos emergentes e conduzir estudos de caso em organizações de saúde. Essas pesquisas contribuirão para melhorar a segurança de dados em saúde e proteger a privacidade dos pacientes.

REFERENCIAIS

AVAST. **Antivírus**. Disponível em: https://www.avast.com/. Acesso em: 01/10/2023.

BARRETO, Joice de Jesus Santos et al. **REGISTROS DE ENFERMAGEM E OS DESAFIOS DE SUA EXECUÇÃO NA PRÁTICA ASSISTENCIAL**. Reme: Rev. Min. Enferm., Belo Horizonte, v. 23, e-1234, 2019. Disponível em http://www.revenf.bvs.br/scielo.php?script=sci_arttext&pid=S1415-27622019000100277&lng=pt&nrm=iso. acessos em 26 set. 2023. Epub 20-Dez-2019. http://dx.doi.org/10.5935/1415-2762.20190082.

BEZERRA, Arthur Coelho; WALTZ, Igor. **Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil**. Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura – Revista Eptic Online, v. 16, n. 2, p.161-175, maio/ago. 2014. Disponível em: http://ridi.ibict.br/handle/123456789/858. Acesso em: 27 set. 2023.

CARVALHO, Gilson**. A saúde pública no Brasil. Estudos avançados**, São Paulo, v. 27, p. 7-26, 2013. Disponível em https://doi.org/10.1590/S0103-40142013000200002. Acesso em abril de 2023.

COMPLEXO DE SAÚDE SÃO BERNARDO DO CAMPO. **Relatório técnico de informática.** São Bernardo do Campo, 28 de junho de 2023. Disponível em: https://fuabc.org.br/wp-content/uploads/2023/08/Relatorio-T.I.pdf Acesso em: 6 de outubro de 2023.

DA SILVEIRA, Kamilla Dória. **Segurança em Banco de Dados para Adequação a LGPD**. In: Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. SBC, 2022. p. 278-287. DOI: https://doi.org/10.5753/sbseg.2022.223953.

DO NASCIMENTO-SILVA-JUNIOR, Danyllo; LIMA-DE-ARAUJO, Janieiry; GURGEL-COSME-DO-NASCIMENTO, Ellany. **Privacidade e confidencialidade no contexto mundial de saúde: uma revisão integrativa.** Rev. Bioética y Derecho, Barcelona, n. 40, p. 195-214, 2017. Disponible en

http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200015&lng=es&nrm=iso. accedido en 06 oct. 2023. Epub 02-Nov-2020.

FIORENZA, Maurício M.; KREUTZ, Diego; ESCARRONE, Thiago; TEMP, Daniel. **Uma Análise da Utilização de HTTPS no Brasil**. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 38., 2020, Rio de Janeiro. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 966-979. ISSN 2177-9384. DOI: https://doi.org/10.5753/sbrc.2020.12338.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. **A Geopolítica do Espaço Cibernético Sul-americano: (In) conformação de Políticas de Segurança e Defesa Cibernética?** Disponível em: https://seer.ufrgs.br/austral/article/download/87994/50497. Acesso em: 01/10/2023.

GOOGLE. **Gerenciar alertas de phishing e malware.** Disponível em: https://support.google.com/chrome/answer/99020?hl=pt-BR&ref_topic=3421433. Acesso em: 01/10/2023.

LANDIM, Ranerson José Alves; MARTINS, Daves Marcio Silva. **Soluções de segurança da informação de baixo custo para pequenas empresas para prevenção de ataques de ransomware**. 2022. Disponível em: http://periodicos.jf.ifsudestemg.edu.br/revistabsi/article/view/576. Acesso em: Set/2023.

LALLIE, H. S. et al. Cyber security in the age of COVID-19: **A timeline and analysis of cyber-crime and cyber-attacks during the pandemic**. ScienceDIrect, Coventry, Reino Unido. Acesso em: 28 de junho. 2023.

MATOS, Odirley Pinheiro de. **Um estudo sobre ataques de phishing e suas medidas de contenção.** 2017. Disponível em: http://bdm.ufpa.br/jspui/handle/prefix/3001. Acesso em: Set/2023.

MINISTÉRIO DA SAÚDE. **Programa de Governança em Privacidade**. 2022. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/programa_governanca_privacidade.pdf. Acesso em: Out 2023.

ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE (OPAS), 1999. **Cyberspace Law and Ethics: A Health Sector Perspective.**

PEREIRA, Nicholas Bastos Nicholas de Lucas Bastos**. Ransomware e phishing durante a pandemia Covid-19 (Coronavírus).** 2021. Disponível em: https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/256. Acesso em: Set/2023.

SANTOS JUNIOR, João Benedito dos et al. **Novas ameaças e a cibersegurança: uma análise do sistema brasileiro de defesa cibernética frente ao caso da espionagem durante o governo Dilma Rousseff.** 27 de maio de 2020. Ministério da Defesa. https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/novasa_ameacasa_ea_aa_cibersegurancaa_umaa_analisea_doa_sistemaa_brasileiroa_dea_defesaa_cibernetica.pdf. Acesso em: agosto/2023.

SAYÃO, L. F.; SALES, L. F. **Afinal, o que é dado de pesquisa?** BIBLOS, [S. l.], v. 34, n. 2, 2020. DOI: 10.14295/biblos. v34i2.11875. Disponível em: https://periodicos.furg.br/biblos/article/view/11875. Acesso em: 26 set. 2023.

SAYÃO, Luis Fernando; SALES, Luana Farias. **O fim da teoria: o confronto entre a pesquisa orientada por dados e a pesquisa orientada por hipóteses.** Liinc em Revista, v. 15, n. 1, p. 16-26, maio 2019a. Disponível em: http://revista.ibict.br/liinc/article/view/4688/4135. Acesso em: 27 set 2023.

SILVESTRE, V.R.N. DOP-MS: **Serviço de Offloading de Dados usando uma Arquitetura de Microsserviços com Suporte a Anonimização de Dados.** Dissertação (Mestrado em Ciências da Computação) - Universidade Federal do Ceará, Fortaleza, 2021. http://www.repositorio.ufc.br/handle/riufc/68716. Acesso em: maio de 2023.

SOUSA, Mariana Leite**. OpenEHR como solução para o Regulamento Geral de Proteção de Dados na área da saúde.** Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjB46iSmIT_AhXYHLkGHbiNBPMQFnoECBIQAQ&url=https%3A%2F%2Fsigarra.up.pt%2Ffep%2Fen%2Fpub_geral.show_file%3Fpi_doc_id%3D104932&usg=AOvVaw3ZQcIQfunq3dNPRsIun__B. Acesso em: abril de 2023.

SOUZA, Raniery Rios Oliveira. **Sequestro de arquivos digitais: análise sobre as vulnerabilidades do ambiente e propostas de soluções em segurança.** 2017. Disponível em: https://www.unibalsas.edu.br/wp-content/uploads/2017/01/ARTIGO-RANIERY.pdf. Acesso em: abril de 2023.

SWANSON, Juleah; RINEHART, Amanda K. **Data in context: Using case studies to generate a common understanding of data in academic libraries.** The Journal of Academic Librarianship, v. 42, n. 1, p. 97-101, 2016. Disponível em: https://kb.osu.edu/bitstream/handle/1811/82202/1/SwansonJ_RinehartA_JAL_Data_in_Context_Preprint.pdf. Acesso em: 27 set. 2023.

THIBES, Mariana Zanata. **As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais.** Sociologias, Porto Alegre, v. 19, n. 46, p. 316-343, set./dez. 2017. Disponível em: http://dx.doi.org/10.1590/15174522-019004613. Acesso em: 27 set. 2023.

WHITTAKER, Z. **"Healthcare giant UHS hit by ransomware attack, sources say".** Disponível em: https://techcrunch.com/2020/09/28/universal-health-services-ransomware/. Acesso em: Out de 2020.