FALHAS DE SEGURANÇA EM SISTEMAS GOVERNAMENTAIS:

Impactos e consequências para população brasileira.

Paulo Ricardo Dos Santos
Faculdade de Tecnologia de Assis
paulo.santos306@fatec.sp.gov.br

Dr. Fábio Eder Cardoso
Faculdade de Tecnologia de Assis
fabio.cardoso6@fatec.sp.gov.br

RESUMO

Este artigo examina a vulnerabilidade dos sistemas de informação governamentais, abrangendo sites, bancos de dados, servidores e demais componentes críticos. A incidência de falhas de segurança nesses sistemas tem se tornado cada vez mais frequente, expondo uma parcela significativa da população ao risco de vazamento de dados sensíveis. Embora muitas dessas falhas sejam evitáveis por meio de investimentos adequados em infraestrutura e qualificação profissional, observa-se uma aparente negligência por parte do governo na adoção de medidas eficazes para mitigar tais riscos. Diante desse cenário, este estudo busca conscientizar a população sobre a recorrência desses incidentes e suas consequências, além de incentivar a implementação de políticas públicas voltadas à proteção dos cidadãos Brasileiros.

Palavras-chave: Segurança da informação; Sistemas Governamentais; Vazamento de dados; Políticas Públicas; Cidadãos Brasileiros.

ABSTRACT

This article examines the vulnerability of government information systems, including websites, databases, servers, and other critical components. The increasing frequency of security breaches in these systems has exposed a significant portion of the population to the risk of sensitive data leaks. Although many of these failures could be prevented through proper investment in infrastructure and professional training, there appears to be a lack of effective measures by the government to mitigate such risks. In light of this scenario, this study aims to raise public awareness about the recurrence of these incidents and their consequences, as well as to encourage the implementation of public policies focused on protecting Brazilian citizens.

Keywords: Information Security; Government Systems; Data Breach; Public Policies; Brazilian Citizens.

1 INTRODUÇÃO

O Brasil encontra-se em um processo contínuo de digitalização dos serviços públicos oferecidos aos cidadãos. Atualmente, áreas essenciais como saúde, educação e segurança já podem ser acessadas por meio de dispositivos eletrônicos pessoais. Um exemplo notável dessa transformação é a plataforma gov.br, que centraliza diversos serviços públicos digitais em um único ambiente, permitindo que cada cidadão realize seu cadastro e usufrua de forma prática e integrada dos serviços disponibilizados.

Contudo, à medida que a transformação digital avança, observa-se também um crescimento significativo nos incidentes, em grande parte decorrentes da atuação de cibercriminosos e da fragilidade das estruturas de proteção da informação. A gravidade do problema se intensifica quando as falhas atingem sistemas governamentais. Fragilidades em bancos de dados, servidores e demais estruturas de armazenamento de informações revelam vulnerabilidades que abalam a confiança da sociedade na capacidade do Estado de garantir segurança digital.

Diante disso, torna-se fundamental evidenciar essas falhas, de modo que sejam debatidas e enfrentadas de maneira adequada. A proteção de dados e a segurança da informação, nesse contexto, representam elementos centrais da gestão pública, influenciando diretamente a confiabilidade, a continuidade e a credibilidade dos serviços digitais oferecidos à população.

O objetivo geral deste trabalho é analisar as falhas de segurança da informação em sistemas governamentais. Para atingir esse propósito, o estudo busca examinar o processo de digitalização dos serviços públicos, investigar a incidência e as causas das vulnerabilidades identificadas, avaliar os impactos dessas falhas sobre os cidadãos e discutir a recorrente negligência dos órgãos responsáveis pela gestão da segurança da informação. Também se faz necessário identificar quais os tipos de incidentes e vulnerabilidades mais recorrentes em tais sistemas.

A presente pesquisa justifica-se pela crescente necessidade de fortalecer a proteção dos dados pessoais e de preservar a confiança da população nos serviços digitais oferecidos pelo governo. Contribui ao indicar caminhos para o aprimoramento de medidas administrativas e de políticas públicas voltadas à consolidação de uma governança digital mais segura, eficiente e confiável.

2 DESENVOLVIMENTO

2.1 Breve História dos Sistemas da Informação no Brasil

O desenvolvimento da Tecnologia da Informação no Brasil teve início de forma mais expressiva a partir da década de 1960, com a chegada dos primeiros computadores. Inicialmente, eram utilizados principalmente por instituições financeiras privadas e por órgãos governamentais responsáveis pelo processamento de dados.

Em razão da crescente demanda por avanços no processamento de dados, posteriormente foi estabelecida a criação do Serviço Federal de Processamento de Dados (Serpro), o que proporcionou uma ampliação significativa no uso da Tecnologia da Informação pelo governo federal.

> O Serviço Federal de Processamento de Dados (Serpro) foi criado em 1964 como resposta à patente necessidade de modernização da gestão financeira e operacional do Estado brasileiro. Criado pela Lei n.° 4.516 de 1° de dezembro de 1964, a Serpro é uma empresa pública, vinculada ao ministério com objetivo de executar, com exclusividade, o processamento de dados e o tratamento de informações necessários aos órgãos do Ministério da Fazenda. (LIMA, 2014).

Atualmente, o Serpro permanece desempenhando um papel fundamental no desenvolvimento de soluções tecnológicas para o governo, com o objetivo de promover a transformação digital.

Entre as décadas de 1980 e 1990, ocorreu uma expansão da modernização e integração de ministérios e serviços públicos, resultando na criação de sistemas integrados. Ainda nesta década, o uso da internet no Brasil cresceu exponencialmente, impulsionado principalmente pelo meio acadêmico.

Em 1988, o Brasil fez seu primeiro contato com a internet por meio de uma conexão realizada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), em parceria com o Fermilab, centro de pesquisa dos Estados Unidos (VIEIRA, 2003). O uso da internet em serviços públicos ocorreu um pouco mais tarde a partir da ação do governo federal.

Entre as décadas de 2000 e 2010, houve um avanço na digitalização dos serviços públicos, impulsionado pela implementação do Governo Eletrônico (e-Gov) que consiste na utilização da tecnologia da informação para otimizar a

operação e acesso aos serviços governamentais. A Serpro participou ativamente do desenvolvimento de tais aplicações, sendo responsável pela segurança de tais sistemas até hoje.

2.2 Desafios na Implementação de Segurança da Informação

Com o avanço da tecnologia da informação, tornou-se fundamental evitar falhas de segurança nos sistemas. Para isso, iniciou-se a modelagem do conceito de segurança da informação, bem como um pensamento mais crítico sobre o tema.

Um dos desafios relacionados à implementação da Segurança da Informação no contexto brasileiro foi a ausência de interesse pelo tema, que apenas passou a ser discutido de forma significativa décadas após a introdução da internet no país. No trecho a seguir, temos uma perspectiva da possível causa de tal desinteresse sobre essa questão.

> Em teoria, qualquer questão pública pode ser posicionada em um espectro que varia de não politizada (o que significa que o Estado não lida com ela e que, de qualquer outra forma, não é considerada um assunto de debate e decisão pública), passando por politizada (quando a questão faz parte das políticas públicas, exigindo decisões governamentais, alocação de recursos ou, mais raramente, alguma outra forma de governança coletiva), até securitizada (quando a questão é apresentada como uma ameaça existencial, exigindo medidas de emergência e justificando ações fora dos limites normais do processo político). (BUZAN et al., 1998, p. 23-24)

Quando os problemas relacionados à segurança da informação começaram a se intensificar em âmbito global, a reação dos governos foi lenta. No caso do Brasil, a criação de legislações específicas para a internet ocorreu apenas anos mais tarde.

Esse atraso pode ser atribuído tanto à falta de familiaridade com o tema quanto à percepção limitada da sua relevância à época. Essa demora regulatória contribuiu para a vulnerabilidade atual do país diante das ameaças digitais.

2.3 Falhas de Segurança

As falhas de segurança da informação caracterizam-se como incidentes resultantes da exploração de vulnerabilidades em sistemas de informação. Quando ocorrem em ambientes governamentais, podem gerar consequências para todo o Brasil.

Segundo o jornal CNN Brasil (2024), durante um evento promovido pela Cyber Security Summit em 2024, foi revelado que o Brasil é o segundo país com mais ataques cibernéticos do mundo, totalizando aproximadamente 700 milhões de ataques em um ano. No entanto, os sistemas governamentais, também têm sido alvo em vazamentos significativos de informações.

O maior vazamento de dados da história do Brasil foi registrado em 2021, expondo informações de mais de 223 milhões de brasileiros, incluindo pessoas falecidas. O incidente foi revelado pela empresa de cibersegurança PSafe (LANDIM, 2025). A vulnerabilidade permitiu acessos indevidos a bases de dados governamentais, resultando no vazamento massivo de informações pessoais.

Além disso, conforme apontado pelo site TecMundo (PALMEIRA, 2024), os dados vazados continuam disponíveis na internet, uma vez que, após serem expostos, tornam-se praticamente impossíveis de remover por completo.

Segundo dados obtidos do Registro de Incidentes com Dados Pessoais entre abril de 2019 e junho de 2022 houve um possível vazamento de credencial no sistema CADSUS. Outras falhas ocorreram no SCPA e e-SUS Notifica (GOVERNO FEDERAL, 2025).

A falha envolvendo o CADSUS em 2019 permitia acesso a dados pessoais de diversos cidadãos, afetando negativamente mais de 2,4 milhões de usuários do SUS (PADRÃO, 2019). O governo negou o vazamento, mas a divergência entre relatos e declarações oficiais evidencia inconsistências quanto à transparência e às medidas de segurança adotadas.

Em 2022, um novo crime cibernético envolvendo dados governamentais foi registrado. Dessa vez, foram identificadas vendas ilegais de bases de dados administrativas extraídas de sistemas governamentais, especificamente do CADSUS e do e-SUS Notifica (GOVERNO FEDERAL, 2025).

Outra falha registrada no site de incidentes com dados pessoais foi o acesso indevido ao Sistema de Cadastro e Permissão de Acesso (SCPA). Essa vulnerabilidade permitia a consulta de dados utilizando apenas o número do CPF dos indivíduos (GOVERNO FEDERAL, 2025). As informações disponibilizadas eram extensas, evidenciando mais um cenário preocupante de fragilidade na segurança da informação em sistemas públicos.

Mas esses ataques não têm apenas o objetivo de expor dados da população. Em 2021, um ataque hacker desativou o serviço do Conecte SUS em plena pandemia, impossibilitando a emissão de carteiras de vacinação contra a Covid-19.

> O ataque gerou uma série de problemas. Em vários locais de vacinação, acabou provocando aumento nas filas e demora no atendimento. Em Goiânia, por exemplo, o registro da aplicação das doses estava sendo feita manualmente. Em Teresina, a prefeitura registrou a aplicação das doses em um site alternativo. Em Salvador, alguns passageiros foram impedidos de embarcar em ônibus intermunicipais porque, com aplicativo fora do ar, não conseguiram mostrar o comprovante de vacinação (G1 JORNAL NACIONAL, 2021).

2.4 Leis e Regulamentações da Segurança da Informação

Para enfrentar esse cenário preocupante, uma das primeiras iniciativas de destaque foi a promulgação da Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação. Essa lei estabelece diretrizes para garantir aos cidadãos o acesso a informações públicas no Brasil, promovendo a transparência governamental e a prestação de contas por parte do Estado (BRASIL, 2011).

Em 2014, foi criado o Marco Civil da Internet, com o objetivo de assegurar o exercício da cidadania, promover a diversidade e garantir a liberdade de expressão no ambiente digital (AGÊNCIA SENADO, 2024). A lei também exige o consentimento expresso para a coleta e uso dessas informações, promovendo a segurança digital (BRASIL, 2014). Apesar de representar um avanço, o Marco Civil não contemplava integralmente todos os aspectos de segurança da informação. Com o avanço tecnológico e o aumento das violações, tornou-se necessária a criação de medidas mais específicas.

Assim, surgiu a Lei Geral de Proteção de Dados (LGPD), estabelecendo diretrizes e princípios para a proteção dos usuários no ambiente digital. Essa lei busca padronizar a forma como empresas e órgãos públicos lidam com esses dados, prevenindo abusos e fortalecendo a privacidade dos usuários (BRASIL, 2018).

A LGPD trouxe mudanças significativas para os setores público e privado, impondo adequações nos processos de coleta, armazenamento e tratamento de dados. Embora sua aprovação tenha ocorrido em 2018, sua entrada em vigor só

se deu em setembro de 2020, após um longo processo de discussão iniciado na década de 2010.

Nesse contexto, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e regulamentar a aplicação da LGPD. A ANPD atua na definição de diretrizes e na supervisão de práticas relacionadas ao tratamento de dados, desempenhando papel central no fortalecimento da segurança da informação, inclusive em sistemas governamentais.

3 METODOLOGIA

O estudo adota uma abordagem qualitativa e quantitativa, baseada na análise de fontes diversas, como matérias jornalísticas, revistas especializadas, livros, artigos acadêmicos e documentos oficiais. Foram examinados dados sobre vazamentos de informações em sistemas governamentais, possibilitando identificar causas e efeitos, avaliando a recorrência desses incidentes em sistemas da informação governamentais.

4 ANÁLISE DE RESULTADOS E DISCUSSÃO

O Brasil é um dos principais alvos mundiais de ataques cibernéticos, essa reputação negativa tem causas pouco conhecidas. Tal cenário pode estar relacionado à percepção, por parte dos criminosos, de que os sistemas nacionais apresentam maior vulnerabilidade, entre outros fatores.

Segundo dados divulgados pela CTIR - órgão responsável por levantar dados estatísticos de incidentes e vulnerabilidades em plataformas governamentais – o Brasil possui quantidades elevadas desses problemas.

Tabela 1 - Dados de Vulnerabilidades e incidentes entre 2021 e 2024

Ano	Vulnerabilidades	Incidentes	Quantidade
2021	4.964	4.903	9.867
2022	5.128	3.402	8.530
2023	10.224	4.908	15.132
2024	5.115	9.806	14.921
Total	25.431	23.019	48.450

Fonte: BRASIL (2025).

Segundo os dados apresentados, o número de vulnerabilidades e incidentes variou de forma significativa entre 2021 e 2024. Entre 2021 e 2022, observou-se um crescimento de 3,30% nas vulnerabilidades, acompanhado por uma redução de 30,61% nos incidentes, resultando em uma queda total de 13,55% nos registros.

Já no período de 2022 para 2023, houve um crescimento expressivo, com aumento de 99,38% nas vulnerabilidades, 44,27% nos incidentes e uma elevação total de 77,40%.

Por fim, entre 2023 e 2024, verificou-se uma redução de 49,97% nas vulnerabilidades, enquanto os incidentes aumentaram em 99,80%, o que gerou uma oscilação que culminou em um decréscimo discreto de 1,39% no total.

Esses dados reforçam que os anos de 2023 e 2024 foram os de maior concentração de falhas de segurança da informação no contexto governamental, caracterizados por forte instabilidade e variação no comportamento das ocorrências.

Tabela 2 - Tipo de Vulnerabilidades e Incidentes entre 2021 e 2024

Tipo	Quantidade
Abuso de Sítio Web	8.267
Abuso no Serviço de E-mail (SMTP)	959
Página Falsa	1.277
Phishing	1.611
Ransonware	33
Scan	2.918
Software Vulnerável	3.746
Vazamento de Dados	8.741
Vulnerabilidade de Criptografia	12.557
Vulnerabilidade DRDoS	8.341
Total	48.450

Fonte: BRASIL (2025).

A elevada incidência de falhas em sistemas governamentais vai além da falta de investimento e do comprometimento do governo com a segurança da informação.

Entre as causas destacam-se o uso de sistemas legados sem atualização adequada, a ausência de políticas consistentes de configuração e segmentação

de redes, além de controles de acesso frágeis e práticas de criptografia insuficientes.

A vulnerabilidade de criptografia é a com mais casos envolvidos. No CADSUS, entre abril de 2019 e junho de 2022, credenciais comprometidas expuseram dados da população, exigindo bloqueio e substituição de acessos.

Essas fragilidades estruturais expõem dados sensíveis, comprometem a privacidade e enfraquecem a confiança da sociedade nos serviços digitais públicos. Entre os diversos riscos decorrentes dessas vulnerabilidades, o vazamento de dados se destaca como o principal fator que impacta diretamente a população.

Um exemplo emblemático ocorreu em 2021, quando a Receita Federal e o Serpro foram diretamente envolvidos em um dos maiores vazamentos já registrados, no qual aproximadamente 223 milhões de dados de brasileiros foram expostos online.

O Conecte SUS, por sua vez, sofreu um ataque que comprometeu o registro de vacinações contra a Covid-19, provocando filas, atrasos, falhas na emissão de comprovantes e a necessidade de registros manuais ou terceirização dos serviços em algumas cidades. Esse cenário demonstra como as falhas de segurança impactaram diretamente a vida da população.

No SCPA, entre novembro de 2021 e maio de 2022, outro caso de vazamento de dados estava em ocorrência, onde qualquer pessoa conseguia realizar consultas avançadas apenas inserindo um CPF. Relatórios recentes indicam que os dados desses vazamentos continuam circulando na internet.

Tabela 3 - Vazamentos de dados entre 2021 e 2024

Ano	Quantidade
2021	233
2022	127
2023	905
2024	7.476
Total	8.741

Fonte: BRASIL (2025).

Como pode ser observado na tabela acima, houve um salto percentual no número de ocorrências de vazamentos de dados da população. Em 2022, registrou-se um número relativamente baixo, com uma redução de 45,49% em relação a 2021. Contudo, esse cenário de queda revelou-se apenas momentâneo, pois nos anos seguintes verificou-se um crescimento expressivo nos casos registrados.

Entre 2022 e 2023, ocorreu um aumento de 612,60% no número de ocorrências, evidenciando uma tendência de agravamento. O ano de 2024, entretanto, apresentou o resultado mais crítico, com um crescimento de 726,50% em relação a 2023, consolidando-se como o período de maior incidência de vazamentos de dados.

Diante desses números, torna-se pertinente o questionamento acerca do real comprometimento do governo com a proteção das informações pessoais de seus cidadãos. Vazamentos de dados comprometem informações pessoais e sensíveis dos cidadãos, gerando impactos que vão desde fraudes e golpes até a perda de confiança nos serviços digitais públicos, sendo uma consequência negativa dos incidentes e falhas de segurança.

A análise dos dados demonstra que, longe de apontar para uma redução nos incidentes, o cenário evidenciou uma escalada significativa, o que fragiliza a confiança da população na gestão da segurança da informação em sistemas governamentais.

Por fim, observa-se que a inserção de legislações e normas voltadas à segurança da informação no Brasil ocorreu de forma lenta, corroborando a teoria de Buzan, segundo a qual apenas após um longo processo de politização um tema é tratado como questão de segurança. No país, esse movimento foi tardio, levando quase três décadas para a definição de uma legislação específica.

5 CONSIDERAÇÕES FINAIS

A pesquisa demonstrou que a segurança da informação nos sistemas governamentais brasileiros ainda apresenta falhas significativas, comprometendo a privacidade e a integridade dos dados da população. Casos

de vazamentos de informações tornaram-se recorrentes, revelando a frequência e a gravidade dos incidentes que afetam esses sistemas. Diversos tipos de vulnerabilidades e ataques ocorrem de forma massiva e, muitas vezes, sem o devido controle ou resposta eficaz por parte das instituições responsáveis.

Os objetivos propostos foram plenamente alcançados. O estudo possibilitou compreender o processo de digitalização dos serviços públicos e identificar as principais vulnerabilidades presentes nos sistemas governamentais. Também foi possível avaliar os impactos dessas falhas sobre os cidadãos e discutir a atuação dos órgãos responsáveis pela segurança da informação, evidenciando a necessidade de maior investimento, monitoramento e fiscalização nessa área. Além disso, foi possível identificar os tipos de vulnerabilidades e incidentes mais recorrentes nos sistemas públicos digitais.

Os incidentes e vulnerabilidades analisados evidenciam a postura negligente do governo diante da recorrência dessas falhas, que persistem ao longo do tempo. Os vazamentos de dados já afetaram milhões de brasileiros, muitos dos quais desconhecem que suas informações, que deveriam estar protegidas pelo Estado, circulam livremente na internet.

Os resultados obtidos reforçam a importância da implementação de políticas públicas mais rigorosas e de estratégias de governança digital que assegurem a proteção das informações e o fortalecimento da confiança da população nos serviços públicos digitais.

6 REFERÊNCIAS

AGÊNCIA SENADO. **Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA**. Senado Federal, Brasília, DF, 26 abr. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia#:~:text=O%20Marco%20Civil%20da%20Internet,liberdade%20de%20express%C3%A3o%20na%20internet. Acesso em: 29 mar. 2025.

BRASIL. **Centro de Tratamento de Incidentes de Rede do Governo – CTIR Gov.** Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. Brasília: GSI/PR, 2025. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 28 set. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 mar. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mar. 2025.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap. **Security:** The New Framework for Analysis. Boulder: Lynne Rienner, 1998.

CNN Brasil. **Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo**. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/. Acesso em: 11 mar. 2025.

G1 Jornal Nacional. **Ataque hacker ao site do Ministério da Saúde tira do ar o ConecteSUS**. Publicado em 10 de dezembro de 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml. Acesso em: 03 abr. 2025.

GOVERNO FEDERAL. **Ministério da Saúde. Registro de Incidentes com Dados Pessoais.** 2025. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais. Acesso em: 30 mar. 2025.

LANDIM, Mariana. **Tudo que você precisa saber sobre o vazamento de dados de 223 milhões de brasileiros.** JusBrasil, 2025. Disponível em: https://www.jusbrasil.com.br/artigos/tudo-que-voce-precisa-saber-sobre-o-vazamento-de-dados-de-223-milhoes-de-brasileiros/1163835014. Acesso em: 02 abr. 2025.

LIMA, Weldson Queiroz de. **Contribuições do SERPRO para a formação do Programa de Governo Eletrônico Brasileiro em uma perspectiva fazendária.** 2014. Disponível em: https://lume.ufrgs.br/handle/10183/127404. Acesso em: 13 mar. 2025.

MACHADO, Cezar de Souza. **Gerenciamento Da Segurança Da Informação Em Sistemas De Teletrabalho.** Orientador: Roberto Carlos dos Santos Pacheco. 2002. Dissertação (Mestrado Profissional em Engenharia da Produção) – Universidade Federal de Santa Catarina. Disponível: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/84431/188664.pdf?sequence=1&isAllowed=y. Acesso: 14 mar. 2025.

PADRÃO, Márcio. **Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet.** UOL , São Paulo, 11 de abril de 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm. Acesso em: 1 abr. 2025.

PALMEIRA, Carlos. **Dados de milhões de brasileiros vazados em 2021 continuam circulando, sugere site.** TecMundo, 2024. Disponível em: https://www.tecmundo.com.br/seguranca/276809-dados-milhoes-brasileiros-vazados-2021-continuam-circulando-sugere-site.htm. Acesso em: 02 abr. 2025.

VIEIRA, Eduardo. **Os bastidores da internet:** a história de quem criou os primeiros negócios digitais do Brasil. Barueri: Manole, 2003.