VULNERABILIDADE E EXFILTRAÇÃO: UMA ANÁLISE SISTÊMICA DA ROTA DE DADOS BRUTOS ATÉ A DARK WEB NO BRASIL
VULNERABILITY AND EXFILTRATION: A SYSTEMIC ANALYSIS OF THE RAW DATA ROUTE TO THE DARK WEB IN BRAZIL

Amauri Emanuel Rodrigues[1]
Enzo Luan da Silva Vieira[2]
Evelyn de Oliveira Antunes[3]
Reginaldo Gabriel Picconi[4]
Silvia Roberta de Jesus Garcia[5]

Resumo: O avanço da transformação digital no Brasil ampliou a produção e armazenamento de dados como ativos estratégicos, mas também intensificou vazamentos de dados devido às vulnerabilidades tecnológicas, falhas de configuração e dependência de infraestruturas estrangeiras, conforme evidenciado por relatórios da Kaspersky, CGI.br e IBM Security. O estudo analisa sistematicamente a rota do vazamento da coleta ilegal via *phishing* e *malware*, passando pela exfiltração silenciosa, distribuição em fóruns restritos e comercialização na *Dark Web,* até o uso final em fraudes e novos ataques cibernéticos —, destacando um ecossistema cibercriminoso organizado que trata dados como *commodities* econômicas. Por meio de análise de casos governamentais, estatísticas recentes e modelos conceituais, este estudo identificou pontos críticos de vulnerabilidade e propôs estratégias integradas de prevenção, governança e conformidade com a LGPD para mitigar riscos e romper esse ciclo contínuo de exploração.
Palavras-chave: cibersegurança; malware; phishing; vazamento de dados.

ABSTRACT: The advancement of digital transformation in Brazil has expanded the production and storage of data as strategic assets, but it has also intensified data breaches due to technological vulnerabilities, configuration failures, and dependence on foreign infrastructures, as evidenced by reports from Kaspersky, CGI.br, and IBM Security. This study systematically analyzes the trajectory of data leakage—from illegal collection through phishing and malware, followed by silent exfiltration, distribution in restricted forums, and commercialization on the Dark Web, to its final use in fraud and further cyberattacks—highlighting an organized cybercriminal ecosystem that treats data as economic commodities. Through the analysis of governmental cases, recent statistics, and conceptual models, this study identified critical points of vulnerability and proposed integrated strategies for prevention, governance, and compliance with the LGPD in order to mitigate risks and disrupt this continuous cycle of exploitation.
Keywords: cybersecurity; malware; phishing; data leak.

Análise e Desenvolvimento de Sistemas - Fatec Itapetininga - E-mail: amauri.rodrigues@fatec.sp.gov.br[1]
Análise e Desenvolvimento de Sistemas - Fatec Itapetininga - E-mail: enzo.vieira@fatec.sp.gov.br[2]
Análise e Desenvolvimento de Sistemas - Fatec Itapetininga - E-mail: evelyn.antunes@fatec.sp.gov.br[3]
Análise e Desenvolvimento de Sistemas - Fatec Itapetininga - E-mail: reginaldo.picconi@fatec.sp.gov.br[4]
Prof.ª Orientadora Mestre - Fatec Itapetininga - E-mail: silvia.garcia01@fatec.sp.gov.br[5]

1 INTRODUÇÃO

O avanço da transformação digital no Brasil tem ampliado significativamente a produção, o armazenamento e o processamento de dados, consolidando-os como ativos estratégicos para organizações públicas e privadas. Esse cenário, no entanto, tem sido acompanhado pelo aumento expressivo de incidentes de segurança da informação, especialmente vazamentos de dados. A crescente digitalização, aliada à expansão da conectividade, amplia a superfície de ataque e torna sistemas e infraestruturas mais suscetíveis à exploração por agentes maliciosos, evidenciando a relevância do tema no contexto contemporâneo (Assolini, 2022).

Nesse contexto, as vulnerabilidades presentes na arquitetura tecnológica e na gestão da informação desempenham papel central na ocorrência desses incidentes. Falhas de configuração, ausência de políticas robustas de segurança e a baixa maturidade em práticas de proteção de dados contribuem para a exposição indevida de informações sensíveis. Além disso, a dependência de infraestruturas tecnológicas e soluções estrangeiras pode intensificar riscos estruturais, dificultando o controle e a proteção eficaz dos dados no ambiente digital brasileiro (CGI.br, 2024).

A partir dessas fragilidades, observa-se a consolidação de um ecossistema cibercriminoso altamente organizado, no qual dados vazados são tratados como ativos econômicos. Nesse cenário, a exfiltração de dados representa uma etapa crítica, sendo responsável pela transferência das informações comprometidas para ambientes externos aos sistemas invadidos. Posteriormente, esses dados são distribuídos e comercializados em espaços digitais anônimos, como a *Dark Web*, onde são utilizados para diversas práticas ilícitas, incluindo fraudes, roubo de identidade e novos ataques cibernéticos (IBM Security, 2024).

Diante desse cenário, o presente estudo tem como objetivo principal analisar a rota do vazamento de dados, buscando compreender de forma sistemática o fluxo percorrido pelas informações desde sua coleta ilegal até sua efetiva comercialização em ambientes da *Dark Web*. Para isso, investigam-se as etapas que compõem esse processo, incluindo a obtenção indevida dos dados, sua exfiltração de sistemas comprometidos, a distribuição inicial em fóruns restritos, a negociação em *marketplaces* clandestinos e, por fim, sua utilização em práticas ilícitas, como fraudes e novos ataques cibernéticos. Ao estruturar essa cadeia de eventos, pretende-se evidenciar os principais pontos de vulnerabilidade ao longo do percurso dos dados,

contribuindo para a ampliação do entendimento sobre o fenômeno e subsidiando estratégias mais eficazes de prevenção e mitigação.

2 METODOLOGIA

A presente pesquisa caracteriza-se como um estudo de natureza aplicada, com abordagem qualitativa e objetivo exploratório-descritivo, tendo em vista a intenção de compreender, interpretar e sistematizar o fenômeno do vazamento de dados no contexto da transformação digital e da segurança da informação no Brasil. Segundo Gil (2010), pesquisas exploratórias têm como finalidade proporcionar maior familiaridade com o problema investigado, enquanto estudos descritivos buscam observar, registrar e analisar características de determinado fenômeno, sem necessariamente manipulá-lo. Nesse sentido, a investigação foi orientada para a identificação das etapas que compõem a rota do vazamento de dados, desde sua coleta indevida até sua circulação e exploração em ambientes digitais clandestinos.

Do ponto de vista dos procedimentos técnicos, o estudo foi desenvolvido por meio de pesquisa bibliográfica e documental. A pesquisa bibliográfica fundamentou-se na análise de artigos científicos, livros, relatórios técnicos e publicações institucionais relacionados à segurança da informação, exfiltração de dados, cibercrime, Dark Web, governança digital e proteção de dados pessoais.

Complementarmente, a pesquisa documental foi empregada na análise de relatórios de mercado, documentos institucionais e estatísticas recentes produzidas por organizações especializadas, tais como o CGI.br(2024), IBM Security(2024) Kaspersky(2016) e órgãos públicos brasileiros, por se tratarem de fontes relevantes para a compreensão atualizada da problemática estudada.

A coleta de dados foi conduzida a partir de um levantamento sistemático da literatura e de evidências secundárias, com seleção de materiais publicados prioritariamente entre 2020 e 2025, em razão da rápida evolução dos cenários tecnológicos e das ameaças cibernéticas. Foram consultadas bases acadêmicas e fontes institucionais reconhecidas, incluindo Google Scholar, Scopus, SciELO, Web of Science, além de relatórios especializados de segurança cibernética.

Para a organização e interpretação dos dados, adotou-se a análise de conteúdo temática, conforme proposta por Bardin (2016), permitindo classificar e agrupar os achados em categorias analíticas compatíveis com o objetivo do estudo. A

partir desse procedimento, o fenômeno foi estruturado em cinco eixos principais: (i) coleta indevida de dados, (ii) exfiltração de informações, (iii) distribuição inicial em ambientes restritos, (iv) comercialização em fóruns e marketplaces clandestinos e (v) utilização final em fraudes, extorsões e novos ataques cibernéticos. Essa categorização possibilitou visualizar a rota do vazamento de dados como um fluxo contínuo e organizado, favorecendo a identificação dos principais pontos de vulnerabilidade técnica, processual e organizacional.

3 REFERENCIAL TEÓRICO

3.1 VAZAMENTOS DE DADOS E EXPOSIÇÃO DE INFORMAÇÕES NO BRASIL

Vazamentos de dados podem ser compreendidos como incidentes de segurança em que informações pessoais ou sensíveis são acessadas, divulgadas ou transferidas a terceiros sem autorização do titular, gerando impactos sociais, econômicos e jurídicos relevantes (Galvão, 2024).

De acordo com Webber (2024), a Lei Geral de Proteção de Dados (LGPD) estabelece que organizações responsáveis pelo tratamento de dados devem garantir a segurança das informações, sendo responsabilizadas quando falhas de proteção resultam em vazamentos ou danos aos titulares dos dados

Segundo Oliveira (2024), no contexto brasileiro, a discussão sobre vazamentos de dados ganhou maior relevância com a implementação da LGPD, que passou a estabelecer diretrizes para o tratamento de dados pessoais e para a responsabilização das instituições em casos de exposição indevida dessas informações.

A crescente digitalização de serviços públicos e privados ampliou a quantidade de dados armazenados por instituições, tornando mais frequentes os incidentes de segurança e os vazamentos de dados pessoais sensíveis em diferentes setores da administração pública e da iniciativa privada (Silva; Nazareno; Pinheiro, 2024).

3.2 VULNERABILIDADES DA ARQUITETURA DE SISTEMAS E INFRAESTRUTURA TECNOLÓGICA

A arquitetura de sistemas de informação envolve a organização e a integração de componentes de hardware, software e redes, de modo que falhas em sua

configuração ou na articulação entre esses elementos podem resultar em vulnerabilidades capazes de facilitar ataques cibernéticos e o acesso não autorizado a dados sensíveis, conforme apontam Laudon e Laudon (2021).

Nessa mesma perspectiva, Stallings (2018a) destaca que sistemas computacionais mal projetados ou sustentados por políticas inadequadas de segurança tendem a apresentar fragilidades exploráveis por agentes maliciosos, especialmente quando não são adotadas práticas adequadas de atualização de software, controle de acesso e manutenção preventiva.

Além disso, a crescente dependência de infraestruturas digitais e redes interconectadas ampliou de forma significativa a superfície de ataque das organizações, tornando indispensável a implementação de arquiteturas seguras e de mecanismos de proteção voltados à mitigação de riscos relacionados a invasões e vazamentos de dados, como observam Goodrich e Tamassia (2015).

Nesse cenário, a proteção da informação em ambientes corporativos depende diretamente da adoção de controles técnicos e estruturais que fortaleçam a segurança dos sistemas, incluindo recursos como autenticação, criptografia e monitoramento contínuo da infraestrutura tecnológica, conforme ressaltam Whitman e Mattord (2018).

3.3 MERCADO DE DADOS E ATIVIDADES CRIMINOSAS NA *Dark Web*

Os vazamentos de dados podem ser compreendidos como incidentes de segurança nos quais informações pessoais ou sensíveis são acessadas, divulgadas ou transferidas a terceiros sem a devida autorização do titular, gerando impactos significativos de ordem social, econômica e jurídica, conforme define Galvão (2024).

Nessa perspectiva, a Lei Geral de Proteção de Dados (LGPD) estabelece que as organizações responsáveis pelo tratamento dessas informações devem adotar medidas adequadas para assegurar sua proteção, podendo ser responsabilizadas sempre que falhas de segurança resultarem em exposição indevida ou danos aos titulares, como destaca Webber (2024).

No contexto brasileiro, a discussão acerca dos vazamentos de dados tornou-se ainda mais relevante com a implementação da LGPD, que passou a estabelecer diretrizes específicas para o tratamento de dados pessoais e para a responsabilização institucional em situações de comprometimento dessas informações, conforme observa Oliveira (2024).

Paralelamente, a intensificação da digitalização de serviços públicos e privados ampliou de maneira expressiva o volume de dados armazenados por diferentes instituições, tornando mais recorrentes os incidentes de segurança e os vazamentos de dados pessoais sensíveis em diversos setores da administração pública e da iniciativa privada, como apontam Silva, Nazareno e Pinheiro (2024).

3.4 SEGURANÇA DA INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A segurança da informação envolve a implementação de políticas, tecnologias e práticas destinadas a proteger dados contra acessos não autorizados, garantindo a confidencialidade, integridade e disponibilidade das informações nas organizações (Stallings, 2018a).

A Lei Geral de Proteção de Dados(LGPD) estabelece diretrizes para o tratamento de dados pessoais no Brasil, impondo às organizações a responsabilidade de adotar medidas técnicas e administrativas capazes de proteger essas informações contra acessos indevidos ou incidentes de segurança (Doneda, 2020).

A LGPD representa um avanço no cenário jurídico brasileiro ao estabelecer princípios e regras para o tratamento de dados pessoais, reforçando a importância da segurança da informação e da privacidade dos usuários no ambiente digital (Bioni, 2019).

A implementação de mecanismos de segurança da informação é essencial para a conformidade com a LGPD, pois a legislação exige que empresas e instituições adotem práticas adequadas de proteção de dados para evitar vazamentos e garantir os direitos dos titulares das informações (Pinheiro, 2021).

4 ANÁLISE DE DADOS

Nesta seção, apresentam-se análises sobre vazamento e a exploração ilegal de dados, com foco na compreensão do fluxo da informação desde sua obtenção até sua comercialização na *Dark Web*. Busca-se demonstrar, de forma objetiva, as etapas desse processo, incluindo coleta, exfiltração, distribuição e venda dos dados. A análise permite situar a pesquisa no contexto atual, identificando vulnerabilidades, convergências e lacunas relevantes.

4.1 ANÁLISE DAS ETAPAS DA ROTA DO VAZAMENTO DE DADOS

O vazamento de dados constitui uma das principais ameaças à segurança da informação no contexto da transformação digital, especialmente em razão da crescente dependência de sistemas informatizados por organizações públicas e privadas. Esse tipo de incidente pode ocasionar prejuízos financeiros, danos à reputação institucional, comprometimento da privacidade dos titulares dos dados e impactos operacionais relevantes. Nesse sentido, compreender as etapas do vazamento de dados torna-se fundamental para a identificação de vulnerabilidades, a mitigação de riscos e o fortalecimento das medidas de prevenção, detecção e resposta a incidentes de segurança (Kim; Solomon, 2016).

A análise da rota do vazamento de dados permite compreender o fluxo percorrido pelas informações desde sua obtenção indevida até sua utilização final em práticas ilícitas. Em termos gerais, esse processo pode ser entendido como uma cadeia estruturada de eventos, na qual os dados são coletados de forma ilegal, extraídos dos sistemas comprometidos, compartilhados em ambientes restritos, comercializados em mercados clandestinos e posteriormente utilizados em fraudes ou em novos ataques cibernéticos. Dessa forma, o vazamento de dados não deve ser interpretado como um evento isolado, mas como parte de um processo organizado e contínuo, característico do ecossistema do cibercrime contemporâneo (Holt; Bossler, 2014a).

A primeira etapa dessa rota corresponde à coleta ilegal de dados, momento em que agentes maliciosos obtêm acesso não autorizado a informações sensíveis por meio de diferentes técnicas de ataque. Entre os métodos mais recorrentes, destacam-se o *phishing*, a engenharia social, a exploração de vulnerabilidades em sistemas, a utilização de *malwares e spywares*, bem como o comprometimento de credenciais de acesso. Nessa fase, o objetivo principal é a obtenção de informações valiosas, como dados pessoais, credenciais de autenticação, informações financeiras, registros corporativos e documentos estratégicos. A efetividade dessa etapa está diretamente relacionada ao nível de maturidade dos controles de segurança adotados pela organização e ao grau de conscientização dos usuários quanto às boas práticas de segurança digital (Stallings, 2018a).

Após a obtenção indevida das informações, ocorre a etapa de exfiltração dos dados, que consiste na transferência não autorizada do conteúdo coletado para ambientes externos controlados pelos agentes maliciosos. Essa fase representa a materialização do vazamento propriamente dito, uma vez que os dados deixam o ambiente comprometido e passam a circular fora do domínio da organização afetada. Em muitos casos, a exfiltração é realizada de forma silenciosa, utilizando mecanismos de evasão, como criptografia, fragmentação dos arquivos, automação da transferência e canais ocultos de comunicação, com o objetivo de reduzir a probabilidade de detecção pelos sistemas de monitoramento e resposta (Stallings, 2018a).

Na sequência, os dados exfiltrados costumam ser submetidos a uma etapa de distribuição inicial em fóruns privados ou comunidades restritas, frequentemente acessíveis apenas a membros autorizados do meio cibercriminoso. Esses ambientes funcionam como espaços de validação e triagem, nos quais as informações são analisadas quanto à sua autenticidade, relevância, atualidade e potencial de exploração. Em muitos casos, amostras dos dados comprometidos são compartilhadas para comprovar sua legitimidade e despertar o interesse de possíveis compradores. Tal prática contribui para a construção de confiança entre os participantes dessas redes ilícitas e prepara o material para sua posterior monetização (Holt; Bossler, 2014a).

Posteriormente, os dados são direcionados para a etapa de comercialização em *marketplaces* da chamada *Dark Web*, ambiente amplamente utilizado para a negociação de ativos ilícitos em razão do emprego de tecnologias de anonimização e criptografia. Nesses mercados clandestinos, as informações podem ser ofertadas de diversas formas, incluindo bases completas, credenciais individuais, acessos específicos a sistemas comprometidos e pacotes segmentados conforme o tipo de dado. O valor atribuído a essas informações varia de acordo com fatores como sensibilidade, volume, atualidade, exclusividade e potencial de uso fraudulento, sendo dados financeiros, credenciais de acesso e registros corporativos estratégicos geralmente mais valorizados (Holt; Bossler, 2014b).

Na etapa final da rota, os dados adquiridos passam a ser utilizados para a realização de fraudes ou para a execução de novos ataques cibernéticos. Entre os principais usos observados, destacam-se o roubo de identidade, as fraudes financeiras, os acessos indevidos a contas e sistemas, a aplicação de golpes de engenharia social e a condução de campanhas de *phishing* mais direcionadas e

sofisticadas. Além disso, as informações vazadas podem ser reutilizadas em ataques futuros, o que contribui para a manutenção de um ciclo contínuo de exploração criminosa. Esse cenário demonstra que o vazamento de dados alimenta uma cadeia de valor do cibercrime, na qual as informações comprometidas são continuamente reaproveitadas para fins econômicos e operacionais (Kim; Solomon, 2016). A Figura 1 apresenta o modelo conceitual que destaca a rota de vazamento de dados.

Figura 1 – Modelo conceitual da rota de vazamento de dados

Fonte: Adaptado de Stallings (2018a), Holt e Bossler (2014b) e Kim e Solomon (2016)

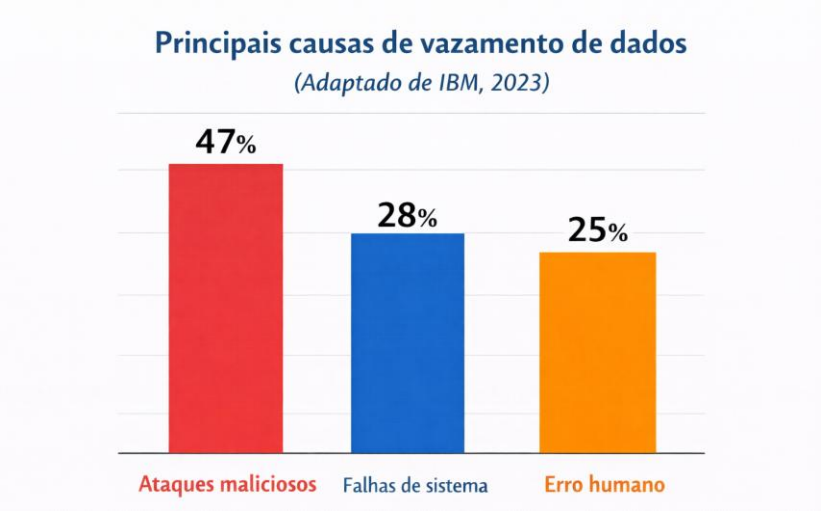
Dessa forma, a análise das etapas do vazamento de dados evidencia que os incidentes de segurança da informação seguem uma lógica operacional estruturada, composta por fases interdependentes que vão desde a obtenção indevida das informações até sua exploração final. A compreensão desse fluxo é essencial para o desenvolvimento de estratégias mais eficazes de prevenção e resposta, permitindo que organizações identifiquem pontos críticos de vulnerabilidade e fortaleçam seus mecanismos de proteção. Além disso, a representação desse processo por meio de modelos conceituais ou diagramas de fluxo pode contribuir significativamente para a visualização das relações entre as etapas, facilitando a sistematização do conhecimento e a elaboração de políticas de segurança mais consistentes (Stallings, 2018b).

4.2 VAZAMENTO DE DADOS NO CENÁRIO GOVERNAMENTAL.

O vazamento de dados no setor governamental brasileiro tem apresentado crescimento significativo nos últimos anos, evidenciando fragilidades estruturais na segurança da informação. Dados do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov, 2025) indicam que o governo federal registrou quase 58 mil incidentes cibernéticos, sendo mais de 9 mil relacionados a vazamentos de dados. Além disso, observa-se um crescimento expressivo desses incidentes, com aumento superior a 20 vezes desde 2020, período que coincide com a implementação da LGPD no Brasil. Esses dados evidenciam que, apesar dos avanços legais, a maturidade em segurança da informação ainda apresenta lacunas no setor público.

Do ponto de vista técnico, estudos baseados em relatórios da IBM (2023) apontam que os vazamentos de dados são predominantemente causados por ataques maliciosos (47%), seguidos por falhas de sistema (28%) e erro humano (25%). Como visto no Gráfico 1.

Gráfico 1 - Vazamento de dados

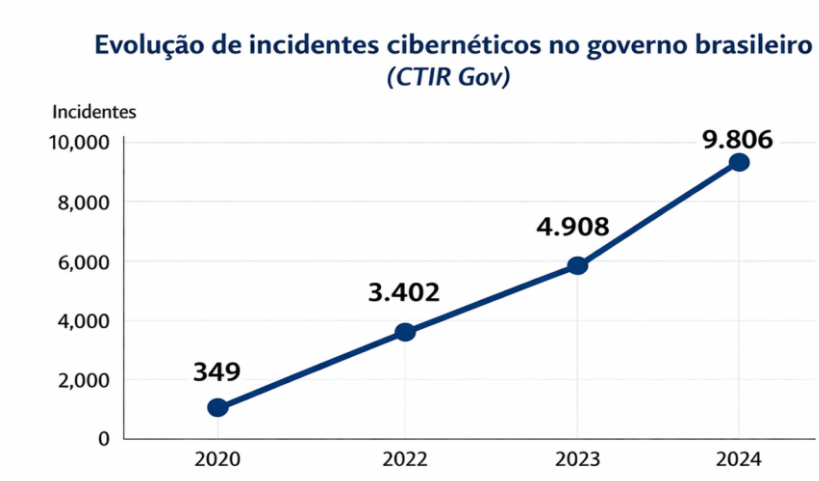


Fonte: Adaptado de IBM (2023).

Esses resultados indicam que as vulnerabilidades não estão apenas na infraestrutura tecnológica, mas também na gestão da informação e no fator humano. No contexto governamental, isso se torna ainda mais crítico devido à complexidade e à escala dos sistemas utilizados, que integram múltiplas bases de dados e serviços digitais.

Outro ponto relevante refere-se à magnitude dos vazamentos no Brasil. Um dos casos mais emblemáticos segundo CTIR Gov (2025) ocorreu em 2021, quando foram expostos dados de mais de 223 milhões de brasileiros, incluindo informações como CPF, nome e telefone como observado na Figura 2. Esse episódio evidenciou não apenas falhas na proteção de dados, mas também a existência de um ecossistema cibercriminoso capaz de explorar e comercializar essas informações em larga escala.

Gráfico 2 - Evolução de Incidentes Cibernéticos no Governo Brasileiro



Fonte: Adaptado de CTIR Gov (2025).

Complementarmente, estudos indicam que cerca de 43% dos dados vazados globalmente possuem origem no Brasil, demonstrando a relevância do país no cenário internacional de cibersegurança. Adicionalmente, observa-se que o crescimento dos ataques também está relacionado à ampliação da digitalização dos serviços públicos. Entre 2022 e 2025, os registros de invasões a sistemas governamentais aumentaram quase 190%, com milhares de ocorrências envolvendo exposição indevida de dados. Esse cenário reforça a ideia de que a expansão da infraestrutura digital, quando não acompanhada de investimentos equivalentes em segurança, tende a ampliar significativamente os riscos de vazamento.

5 RESULTADOS E DISCUSSÃO

O vazamento de dados no contexto brasileiro apresenta crescimento significativo, consolidando-se como uma das principais ameaças à segurança da informação. Esse processo ocorre de forma estruturada, conforme sintetizado na Tabela 1, iniciando-se pela coleta ilegal de dados sensíveis, seguida pela exfiltração de grandes volumes de informação, o que amplia os impactos operacionais e financeiros. Na sequência, há a validação e distribuição em ambientes restritos, a comercialização em mercados clandestinos e, por fim, o uso dessas informações em fraudes e novos ataques, caracterizando um ciclo contínuo de exploração.

Tabela 1: Análise atual da rota do vazamento de dados (2024–2025)

Etapa da rota	Descrição analítica	Dados atuais / estatísticas	Implicações
Coleta ilegal	Obtenção inicial por exploração técnica ou humana	94% dos ataques cibernéticos em 2024 envolveram roubo de dados	Demonstra que o foco do cibercrime é a captura de dados sensíveis
Exfiltração	Transferência dos dados para fora do sistema comprometido	Média de 592 GB de dados exfiltrados por ataque	Alto volume aumenta impacto financeiro e operacional
Validação e distribuição inicial	Compartilhamento em fóruns restritos para verificação	44,59% das atividades na *Dark Web* envolvem divulgação de vazamentos	Fóruns funcionam como “triagem” antes da venda
Comercialização	Venda em *marketplaces* clandestinos	41,15% dos conteúdos da *Dark Web* estão relacionados à venda de dados	Indica forte estrutura de mercado ilegal

Valor econômico dos dados	Precificação conforme volume e sensibilidade	Caso real: 2,9 bilhões de registros vendidos por US$ 3,5 milhões	Dados pessoais possuem alto valor comercial
Uso final	Aplicação em fraudes e novos ataques	Mais de 1 milhão de credenciais e milhares de cartões foram expostos em 2024	Ampliação do impacto e retroalimentação do ciclo
Impacto financeiro	Consequências econômicas dos vazamentos	Custo médio de US$ 5,21 milhões por incidente	Pressiona organizações a investir em segurança

Fonte: Adaptado de CTIR Gov (2025).

Com base na análise dos dados apresentados, observa-se que o vazamento de dados no contexto brasileiro, especialmente no setor governamental, apresenta crescimento significativo nos últimos anos, consolidando-se como uma das principais ameaças à segurança da informação (Brasil, 2025). Esse fenômeno ocorre de forma estruturada, conforme sintetizado na Tabela 1, evidenciando um processo contínuo que envolve coleta ilegal, exfiltração, distribuição, comercialização e uso indevido das informações.

A análise do Gráfico 2 indica uma tendência de crescimento contínuo dos incidentes, especialmente após 2020, associada à expansão da digitalização e ao aumento da superfície de ataque. Embora existam avanços regulatórios, como a LGPD, observa-se que as práticas de segurança ainda não evoluem na mesma proporção, uma vez que muitas organizações ainda enfrentam dificuldades na implementação efetiva de políticas de proteção de dados, monitoramento de riscos e mecanismos preventivos de segurança digital (Stallings, 2018b).

No que se refere às causas, os dados do Gráfico 1 mostram a predominância de ataques maliciosos (47%), seguidos por falhas de sistema (28%) e erros humanos (25%) (IBM, 2023). Esse cenário evidencia que o cibercrime atua de forma estratégica, priorizando dados de alto valor, ao mesmo tempo em que revela fragilidades internas relacionadas à gestão da segurança e à capacitação dos usuários. Além disso, casos de grande magnitude reforçam a gravidade dos vazamentos e sua exploração em larga escala. O aumento das invasões, impulsionado pela expansão dos serviços digitais, demonstra que a transformação digital amplia os riscos quando não acompanhada por investimentos adequados em segurança (Brasil, 2025). Nesse contexto, os impactos financeiros e operacionais evidenciam a necessidade de fortalecimento das práticas de governança, monitoramento e resposta a incidentes.

Dessa forma, os resultados confirmam que o vazamento de dados é um processo estruturado, influenciado por fatores técnicos, humanos e organizacionais. Por fim, apesar dos avanços normativos, ainda há lacunas na maturidade da segurança da informação no Brasil, o que reforça a necessidade de uma abordagem integrada para mitigação dos riscos.

6 CONSIDERAÇÕES FINAIS

A análise desenvolvida neste estudo permite afirmar que o avanço da transformação digital no Brasil, embora indispensável para a modernização institucional, tem sido acompanhado por um crescimento proporcional — e preocupante — dos vazamentos de dados. Esse cenário evidencia uma contradição estrutural: ao mesmo tempo em que os dados se consolidam como ativos estratégicos, sua proteção não evolui na mesma intensidade. A ampliação da superfície de ataque, impulsionada pela conectividade e pela digitalização acelerada, expõe fragilidades que são exploradas de forma sistemática por agentes cibercriminosos.

Nesse sentido, torna-se evidente que os vazamentos de dados não decorrem exclusivamente de falhas tecnológicas, mas de um conjunto articulado de vulnerabilidades que envolvem arquitetura de sistemas, gestão da informação e comportamento humano. A predominância de ataques maliciosos, aliada à expressiva participação de erros humanos e falhas técnicas, reforça que a segurança da informação ainda é tratada de forma fragmentada em muitas organizações. Além disso, embora a LGPD represente um avanço normativo relevante, sua efetividade é limitada quando não acompanhada por práticas concretas de governança e cultura organizacional voltadas à proteção de dados.

Outro aspecto central identificado é a consolidação de um ecossistema cibercriminoso estruturado, no qual os dados vazados são inseridos em uma lógica de mercado. A compreensão da rota do vazamento — desde a coleta ilegal até a comercialização e uso indevido — evidencia que esses incidentes não são eventos isolados, mas parte de uma cadeia contínua de exploração econômica. Essa dinâmica reforça a gravidade do problema, pois amplia o impacto dos vazamentos e contribui para a retroalimentação do cibercrime, tornando os dados comprometidos insumos para novas violações.

Diante disso, sustenta-se que a mitigação desse problema exige uma mudança de abordagem: não basta investir apenas em tecnologias de proteção, sendo necessário integrar políticas de governança, monitoramento contínuo e capacitação dos usuários. A segurança da informação deve ser compreendida como um elemento estratégico e transversal, capaz de acompanhar o ritmo da transformação digital. Assim, conclui-se que o fortalecimento de práticas preventivas e a adoção de estratégias integradas são condições essenciais para reduzir vulnerabilidades e limitar os impactos dos vazamentos de dados no contexto brasileiro.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA LUPA**. Sem proteção, dados vazados alimentam indústria de golpes no país.** 2025. Disponível em: <https://www.agencialupa.org/jornalismo/2025/05/26/sem-protecao-dados-vazados-alimentam-industria-de-golpes-no-pais/>. Acesso em: 27 mar. 2026.

ASSOLINI, Fábio**. Brasil é o maior alvo de ataques na América Latina.** Kaspersky, 16 nov. 2022. Disponível em: <https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2022/20311/>. Acesso em: 27 mar. 2026.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)**. Relatório de incidentes cibernéticos no governo federal.** Brasília, 2025**.**

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br)**. Nota pública sobre o atual debate regulatório em torno da segurança cibernética no Brasil.** São Paulo: CGI.br, 2024. Disponível em: <https://www.cgi.br/esclarecimento/nota-publica-sobre-o-atual-debate-regulatorio-em-torno-da-seguranca-cibernetica-no-brasil/>. Acesso em: 27 mar. 2026.

DIÁRIO DO GRANDE ABC**. Reclamações de uso ou vazamentos de dados crescem em 175%.** 2026. Disponível em: <https://www.dgabc.com.br/Noticia/4286492>. Acesso em: 27 mar. 2026.

EUAX**. Vazamento de dados: guia completo para proteger sua empresa em 2025.** 2024. Disponível em: <https://www.euax.com.br/2024/01/vazamento-de-dados/>. Acesso em: 27 mar. 2026.

GALVÃO, Heideivirlandia Leite et al. **Incidentes de segurança: regulação e prática de vazamento de dados pessoais frente à LGPD.** ID on Line: Revista de Psicologia, v. 18, n. 72, p. 179-197, 2024. Disponível em: <https://idonline.emnuvens.com.br/id/article/view/4042>. Acesso em: 13 maio 2026.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre: Bookman, 2015**.**

HARDWARE.COM.BR. **Vazamentos de dados: Brasil registra aumento de contas violadas.** 2025. Disponível em: <https://www.hardware.com.br/noticias/vazamento-dados-brasil/>. Acesso em: 27 mar. 2026.

HOLT, Thomas J.; BOSSLER, Adam**. An assessment of the current state of cybercrime scholarship.** Deviant Behavior, [s.l.], v. 35, n. 1, p. 20-40, 2014.

HOLT, Thomas J.; BOSSLER, Adam**. Cybercrime in progress: theory and prevention of technology-enabled offenses.** New York: Routledge, 2014.

IBM SECURITY**. Cost of a Data Breach Report 2023.** Armonk: IBM Corporation, 2023.

IBM SECURITY. **Resumo de 2024: principais histórias de violações de dados e tendências de segurança.** IBM Brasil, 18 dez. 2024. Disponível em: <https://www.ibm.com/br-pt/think/insights/2024-roundup-top-data-breach-stories-and-industry-trends>. Acesso em: 27 mar. 2026.

KASPERSKY**. Brasil é o maior alvo de ataques na América Latina.** São Paulo: Kaspersky, 2022. Disponível em: <https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2022/20311/>. Acesso em: 27 mar. 2026.

KIM, David; SOLOMON, Michael G**. Fundamentals of information systems security.** 3. ed. Burlington: Jones & Bartlett Learning**,** 2016.

LAUDON, Kenneth C.; LAUDON, Jane P**. Sistemas de informação gerenciais.** 14. ed. São Paulo: Pearson Education do Brasil, 2021.

NAHAPETYAN, Aleksandr et al. **Characterizing phishing pages by JavaScript capabilities.** arXiv preprint arXiv:2509.13186, 2025. Disponível em: <https://arxiv.org/abs/2509.13186>. Acesso em: 27 mar. 2026.

OLIVEIRA, R**. A implementação da LGPD e a responsabilidade civil das instituições.** Brasília: Revista de Direito Digital, 2024.

OWASP FOUNDATION**. OWASP Top 10: 2024.** 2024. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 11 mar. 2026.

PDCA TI. **Maturidade Digital no Brasil 2025: panorama de segurança e vazamento de dados.** 2025. Disponível em: <https://www.pdcati.com.br/dados-ti-brasil/>. Acesso em: 27 mar. 2026.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva, 2021.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de**. Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico.** 2. ed. Novo Hamburgo: Feevale, 2013.

ROSE, Scott et al. **Zero Trust Architecture.** Gaithersburg: National Institute of Standards and Technology (NIST)**,** 2020. (NIST Special Publication 800-207). Disponível em: <https://doi.org/10.6028/NIST.SP.800-207>. Acesso em: 11 mar. 2026.

SILVA, J.; NAZARENO, M.; PINHEIRO, R**. Digitalização e incidentes de segurança na administração pública**. Rio de Janeiro: Tecnologia & Sociedade, 2024.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 7. ed. São Paulo: Pearson Education do Brasil, 2018a.

STALLINGS, William. **Effective cybersecurity: a guide to using best practices and standards**. Boston: Pearson, 2018b.

WEBBER, L**. Segurança da informação e conformidade legal.** Porto Alegre: Editora Acadêmica, 2024.

WHITMAN, Michael E.; MATTORD, Herbert J**. Principles of Information Security.** 6. ed. Boston: Cengage Learning, 2018.