INCIDENTES DE SEGURANÇA DE DADOS NO BRASIL: DESAFIOS, IMPACTOS E O PAPEL DA LGPD NA PROTEÇÃO DE INFORMAÇÕES PESSOAIS.

Richard Gabriel de Oliveira
Faculdade de Tecnologia do Estado de São Paulo (FATEC) - Assis
richard.oliveira18@fatec.sp.gov.br

João Lucas M.B.M. da Silva

Faculdade de Tecnologia do Estado de São Paulo (FATEC) - Assis
joao.silva740@fatec.sp.gov.br

Profº Me.Cleber Henrique de Oliveira
Faculdade de Tecnologia do Estado de São Paulo (FATEC) - Assis
cleber.oliveira16@fatec.sp.gov.br

RESUMO

O estudo examina incidentes de segurança no Brasil, destacando vulnerabilidades em pequenas e médias empresas, principais ataques cibernéticos e o papel da LGPD na proteção de dados, mitigação de riscos e impactos financeiros e reputacionais.

Palavras-chave: Segurança da informação. Incidentes de dados. LGPD. Proteção de dados pessoais. Governança digital.

ABSTRACT

The study examines security incidents in Brazil, highlighting vulnerabilities in small and medium enterprises, major cyberattacks, and the role of the LGPD in data protection, risk mitigation, and financial and reputational impacts.

Keywords: Information security. Data breaches. LGPD. Personal data protection. Digital governance.

1 INTRODUÇÃO

A transformação digital acelerou a integração de sistemas computacionais às atividades humanas, ampliando a coleta, o armazenamento e o compartilhamento de dados pessoais em diferentes setores da sociedade. Essa crescente digitalização, embora impulsione inovações e melhorias operacionais, também aumenta a exposição a incidentes de segurança da informação. Vazamentos, sequestros de dados e acessos não autorizados tornaram-se eventos recorrentes, afetando organizações públicas e privadas e colocando em risco direitos fundamentais dos indivíduos, como a privacidade e a autodeterminação informativa (Gonçalves, 2022).

O contexto brasileiro é particularmente desafiador. O país figura entre os que mais sofrem com vazamentos de dados em larga escala. De acordo com o relatório **Cost of a Data Breach 2024**, publicado pela IBM Security (International Business Machines Corporation), o custo médio de uma violação de dados no Brasil é de R$ 6,75 milhões, valor que aumenta significativamente em casos que envolvem dados sensíveis, como informações bancárias e de saúde (IBM SECURITY, 2024). Além do impacto financeiro, esses incidentes provocam sérios danos à reputação das empresas e comprometem a confiança dos consumidores, exigindo respostas legais e gerenciais rápidas e eficazes (Nassar, 2022).

Diante desse cenário, a promulgação da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – representou um marco regulatório no ordenamento jurídico brasileiro. Inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), a LGPD visa disciplinar o tratamento de dados pessoais e estabelecer padrões mínimos de segurança e transparência, especialmente no que tange à prevenção e ao tratamento de incidentes de segurança. A norma introduziu no país uma nova racionalidade jurídica baseada na responsabilização e na governança informacional, estabelecendo direitos claros aos titulares e deveres rigorosos aos agentes de tratamento (Doneda,2021).

Contudo, embora a LGPD represente um avanço normativo importante, sua efetividade na prática depende de uma série de fatores, incluindo a atuação proativa da Autoridade Nacional de Proteção de Dados (ANPD), a maturidade das organizações em segurança da informação e a consolidação de uma cultura de proteção de dados no país. A pesquisa TIC Empresas 2021, publicada pelo CETIC.br, revela que apenas 40% das empresas brasileiras afirmam adotar medidas preventivas formais contra vazamentos de dados, demonstrando a

fragilidade estrutural do ambiente corporativo nacional frente às exigências legais (CETIC.BR, 2022).

A relevância técnica e científica deste estudo reside na necessidade de compreender o alcance prático da legislação de proteção de dados em um país com elevados índices de exposição digital e baixo nível de cultura cibernética. Além disso, destaca-se o interesse social do tema, na medida em que a proteção de dados se relaciona diretamente com o exercício da cidadania e com a garantia de direitos fundamentais no ambiente digital (Fachin, 2021).

Diante disso, o presente trabalho tem como objetivo geral analisar os impactos dos incidentes de segurança de dados no Brasil, investigando os principais desafios enfrentados pelas organizações e o papel da LGPD na mitigação de riscos e na proteção de informações pessoais. Para alcançar esse objetivo, propõem-se, como metas específicas, conceituar segurança da informação e incidentes de dados, apresentar os principais fundamentos jurídicos da LGPD relacionados à segurança e discutir os efeitos concretos desses incidentes nas esferas empresarial, jurídica e social.

2 REVISÃO DE LITERATURA

2.1 Conceitos de Segurança da Informação e Incidentes de Dados

A segurança da informação deixou de ser um mero componente técnico para tornar-se uma dimensão estratégica no contexto organizacional e social contemporâneo. Trata-se do conjunto de processos, tecnologias e políticas voltadas à preservação da confidencialidade, integridade e disponibilidade das informações, princípios amplamente reconhecidos como essenciais para o funcionamento seguro de sistemas digitais. Em um ambiente cada vez mais orientado por dados, a proteção dessas informações constitui elemento central da confiança entre usuários, instituições e plataformas (Stallings, 2017).

Os incidentes de segurança configuram qualquer evento adverso, acidental ou intencional, que comprometa a proteção dos ativos informacionais de uma organização. Esses episódios englobam desde vazamentos de dados sensíveis até ataques estruturados, como ransomwares e invasões sistêmicas, podendo afetar tanto a continuidade das operações quanto a reputação corporativa (Almeida, 2021).

O cenário brasileiro tem revelado fragilidades significativas no enfrentamento desses riscos. Segundo o levantamento realizado pelo CETIC.br (2022), uma parcela expressiva das

empresas ainda não adota medidas preventivas formalizadas, como planos de resposta a incidentes ou auditorias regulares. Essa lacuna é mais acentuada entre organizações de pequeno e médio porte, que frequentemente carecem de estrutura técnica, orçamento e pessoal capacitado para garantir a proteção contínua das informações sob sua custódia.

Além dos danos operacionais, os incidentes acarretam repercussões reputacionais que afetam a confiança do público e a credibilidade da marca no mercado. Nassar (2022) observa que, diante de um vazamento de dados, a ausência de uma comunicação transparente e tempestiva pode intensificar o impacto negativo, levando a perdas financeiras e institucionais irreversíveis.

No Brasil, a ausência de uma cultura consolidada de segurança da informação expõe uma fragilidade estrutural que transcende os aspectos tecnológicos. Muitas organizações ainda enxergam a proteção de dados como um custo operacional, e não como uma diretriz estratégica vinculada à responsabilidade jurídica e à governança corporativa. Esse cenário evidencia a urgência de políticas institucionais que integrem a proteção de dados aos princípios de diligência, transparência e prestação de contas, fundamentos esses consagrados pela própria LGPD (Brasil, 2018).

A caracterização jurídica de um incidente de segurança nem sempre é evidente, exigindo uma análise técnica aliada à compreensão dos deveres normativos impostos aos controladores e operadores de dados. Quando ocorre o comprometimento da integridade, da confidencialidade ou da disponibilidade das informações, não se trata apenas de uma falha técnica, mas de um possível ilícito civil e regulatório, que enseja responsabilizações e pode gerar danos de natureza patrimonial e extrapatrimonial (Miragem, 2022).

2.2 Impactos dos Incidentes de Segurança: Desafios e Consequências

A Lei nº 13.709/2018, que institui a Lei Geral de Proteção de Dados (LGPD), insere-se em um movimento global de resposta aos abusos no uso de dados pessoais, especialmente após escândalos como o da Cambridge Analytica. A elaboração da lei foi motivada pela necessidade de proteger a privacidade dos cidadãos diante da manipulação de dados em larga escala. Antes da LGPD, o Brasil enfrentava um vácuo legislativo que deixava milhões de cidadãos vulneráveis. A mesma preencheu essa lacuna, criando um regime próprio e promovendo a constituição de uma cultura jurídica da informação, essencial para garantir o exercício da liberdade individual na era digital (Doneda, 2021).

Os incidentes de segurança de dados provocam impactos severos no ambiente empresarial, sobretudo em relação às perdas financeiras imediatas e aos efeitos a médio prazo sobre a capacidade competitiva. Além disso, afetam a reputação das organizações e geram consequências jurídicas, incluindo responsabilidade objetiva do controlador de dados, conforme previsto no artigo 42 da LGPD (Brasil, 2018).

Do ponto de vista dos indivíduos, a exposição indevida de dados compromete direitos fundamentais, podendo gerar prejuízos financeiros, sociais e emocionais. Fraudes como o roubo de identidade e o uso indevido de informações sensíveis têm se intensificado, demonstrando a necessidade de políticas de prevenção e resposta robustas (Serasa Experian, 2023; IBM SECURITY, 2024).

3 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa exploratória de abordagem qualitativa, baseada em análise documental. O objetivo é investigar os impactos dos incidentes de segurança de dados no Brasil, bem como compreender as principais ameaças cibernéticas enfrentadas por empresas, considerando o papel da Lei nº 13.709/2018 (LGPD) na mitigação desses riscos.

A coleta de dados será realizada por meio da seleção de relatórios, pesquisas e estudos técnicos disponíveis nos sites oficiais de instituições de referência, como o CETIC.br (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação), o Verizon DBIR (Verizon Data Breach Investigations Report) e fornecedores de inteligência em segurança digital, incluindo Microsoft Corporation, CrowdStrike, Inc. e Kaspersky Lab. Serão considerados documentos publicados no período de 2020 a 2024, visando identificar tendências recentes e relevantes para o cenário brasileiro e global.

Para a seleção das fontes, serão adotados critérios de relevância, abrangência e confiabilidade, priorizando documentos que abordem vulnerabilidades, tipos de ataques, políticas de mitigação e impactos sobre informações corporativas e pessoais.

A análise dos dados será conduzida por meio de categorização temática e comparação entre os conteúdos das diferentes fontes. As categorias previstas incluem tipos de ataque, motivação dos agentes de ameaça e estratégias de mitigação recomendadas. Espera-se,

assim, identificar padrões e diferenças nas abordagens adotadas por instituições nacionais e internacionais no monitoramento e prevenção de incidentes de segurança.

Por se tratar de pesquisa baseada exclusivamente em documentos públicos e relatórios técnicos, sem envolvimento de participantes humanos, não será necessária aprovação por Comitê de Ética em Pesquisa.

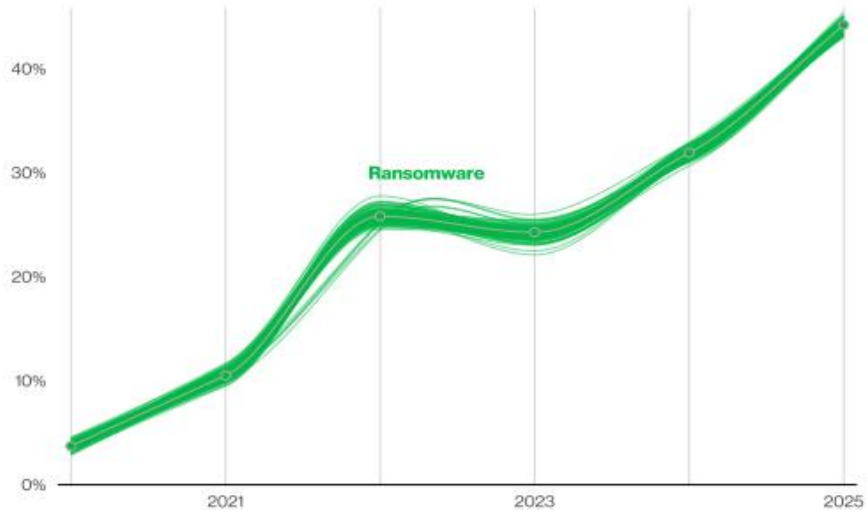
4 ANÁLISE DE RESULTADOS E DISCUSSÃO

A análise dos dados coletados permitiu identificar os principais tipos de ataques cibernéticos enfrentados por empresas no Brasil, considerando informações de fontes reconhecidas, como CETIC.br (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, Brasil), Verizon (Verizon Data Breach Investigations Report, EUA) e fornecedores de inteligência em segurança digital, como Microsoft Corporation (EUA) e CrowdStrike, Inc. (EUA).

Segundo o CETIC.br (TIC Empresas 2023), 31% das empresas brasileiras relataram ter sido afetadas por malware ou vírus, enquanto 26% informaram incidentes de phishing ou engenharia social, e outros 26% foram alvo de ataques de negação de serviço (Distributed Denial of Service ou DDoS). A exploração de vulnerabilidades, embora não detalhada em percentuais, também representa um risco significativo.

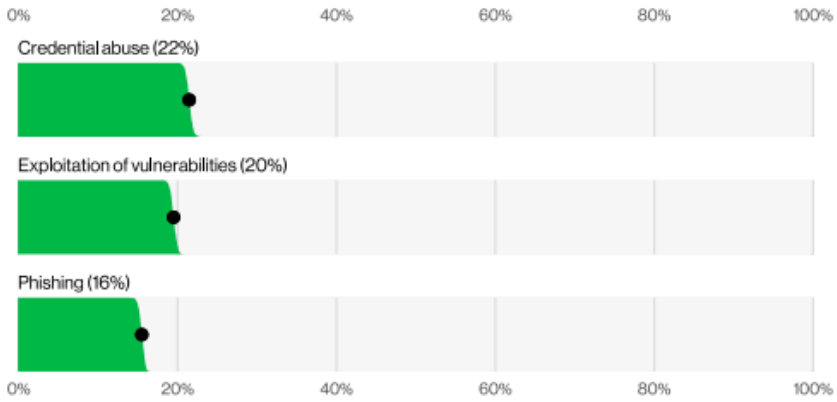
Esses dados indicam que muitas organizações enfrentam múltiplas formas de ameaças digitais, impactando tanto a continuidade operacional quanto a proteção de informações sensíveis. Verizon DBIR 2024/2025 aponta que com as explorações de vulnerabilidades teve um aumento significativo aos anos anteriores, apontando os incidentes mais ocorridos como o ransomware 39% das violações e crescendo ao longo dos anos.

Figura 1: Crescimentos de incidentes ao longo dos anos



Fonte: https://www.verizon.com/business/resources/reports/dbir

Figura 2: Incidentes Mais Ocorridos Como O Ransomware



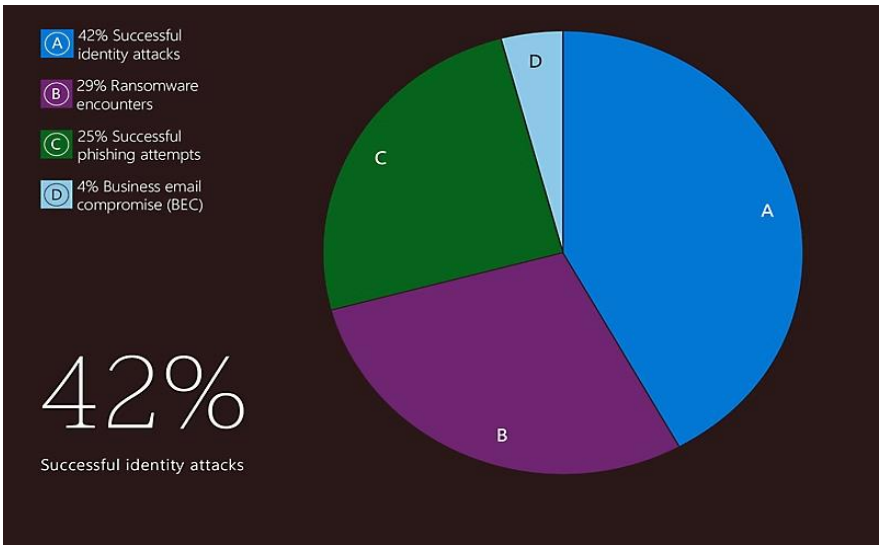
Fonte: https://www.verizon.com/business/resources/reports/dbir

Esses números evidenciam a diversidade de vetores de ataque em escala global, reforçando a necessidade de controles rigorosos de autenticação, monitoramento contínuo e políticas de segurança estruturadas.

Além disso, os dados fornecidos por empresas especializadas em inteligência de segurança digital Microsoft e CrowdStrike. Especialista do Microsoft defender enviam notificações aos seus clientes para saberem as informações específicas sobre o escopo,

método de entrada e instruções para remediação, e identificaram que essas foram as principais ameaças de 2023

Figura 3: Distribuição das quatro principais notificações de progressão de ataque



Fonte: https://www.microsoft.com/pt-br/security/security-insider/microsoft-digital-defense-report-2023-state-of-cybercrime

Que 42% Ataques de identidade bem-sucedidos, 29% Encontros com ransomware, 25% Tentativas de phishing direcionado bem-sucedidas e 4% Comprometimento de e-mail comercial (BEC).

A CrowdStrike relata que a maioria dos incidentes começa com o acesso inicial, e ataques baseados em identidade, que não recorrem mais a os malwares tradicionais, e sim a métodos mais rápidos e furtivos, como vishing, engenharia social, serviços de corretores de acesso e abuso de relacionamentos de confiança. Usando a ascensão dos corretores de acesso: especialistas que obtêm acesso a organizações e o vendem a outros atores de ameaça, incluindo operadores de ransomware. Essa atividade disparou em 2024, com acessos anunciados aumentando quase 50% em relação a 2023. O abuso por conta validas foi responsável a 35% dos incidentes conectados a nuvem, a identidade não é o único alvo eles exploram vulnerabilidades para ter acesso inicial, em 2024 52% das vulnerabilidades vistas estão relacionadas ao acesso inicial.

O impacto desses incidentes vai além da esfera operacional, alcançando dimensões econômicas, reputacionais e jurídicas. Pequenas e médias empresas, por exemplo, apresentam vulnerabilidades acentuadas devido à limitação de recursos tecnológicos e humanos. A microsoft aponta que muitas das empresas que são alvos dos incidentes, são empresas de pequeno e médio porte pois não há tanta segurança como uma empresa de grande porte, e que a maioria dos incidentes são de empresas educacionais.

O CrowdStrike destaca que a cibersegurança continua evoluindo constantemente apresentando desafios significativos para todas as empresas em ambos setores e regiões. E que é crítico a compreensão das ameaças atuais em todos os aspectos da segurança, pois os causadores de incidentes estão sempre inovando e se adaptando a novos ataques.

Pesquisa do CETIC.br (2022) indica que 58% dessas empresas destinam menos de 2% do orçamento de TI para medidas de proteção de dados. A migração acelerada de processos para plataformas digitais, sem planejamento adequado de segurança, aumenta a exposição a ataques e amplia o potencial de perdas financeiras, como fraudes bancárias e roubo de identidade, fenômenos que ocorrem com frequência no país. Relatórios da Serasa Experian (2023) apontam que uma tentativa de fraude ocorre a cada oito segundos no Brasil, muitas vezes a partir de informações obtidas em vazamentos de dados.

Além das consequências econômicas, os incidentes de segurança afetam a confiança de clientes, parceiros e titulares de dados, comprometendo a reputação corporativa. A exposição inadequada de informações pessoais também gera responsabilidades jurídicas, uma vez que a LGPD estabelece responsabilidade objetiva para os agentes de tratamento de dados, mas a efetivação de reparações enfrenta barreiras práticas e processuais, dificultando a compensação das vítimas (Doneda, 2021).

A pesquisa TIC Empresas (2022) revelou que apenas 27% das organizações promovem capacitação em proteção de dados. A falta de conscientização transforma falhas humanas em vetores de ataque, evidenciando que a efetividade da LGPD depende não apenas da existência de normas, mas do enraizamento de práticas de segurança nas rotinas institucionais.

Em síntese, os dados analisados indicam que, tanto no Brasil quanto internacionalmente, malware, ransomware, phishing e exploração de vulnerabilidades permanecem como as ameaças mais críticas.

A combinação de impactos econômicos, reputacionais e jurídicos reforça a necessidade da adoção de práticas de segurança avançadas, da conscientização contínua de usuários e da implementação de políticas internas consistentes, alinhadas à LGPD e demais normas de proteção digital. Tais medidas são essenciais não apenas para mitigar riscos de vazamentos e incidentes de segurança, mas também para proteger dados pessoais e corporativos, reduzir prejuízos financeiros e preservar a confiança de titulares e parceiros, garantindo o cumprimento das obrigações legais.

5 CONSIDERAÇÕES FINAIS

A partir da análise dos dados coletados, foi possível concluir que os incidentes de segurança de dados no Brasil representam desafios significativos para as organizações, com impactos que vão além da esfera operacional, atingindo dimensões econômicas, jurídicas e reputacionais. As informações do CETIC.br, Verizon DBIR e fornecedores de inteligência em segurança digital, como Microsoft e CrowdStrike, evidenciam que malware, ransomware, phishing e exploração de vulnerabilidades são as ameaças mais recorrentes e sofisticadas enfrentadas tanto nacional quanto internacionalmente.

As pequenas e médias empresas se destacam como o segmento mais vulnerável, devido à limitação de recursos tecnológicos e humanos, à baixa destinação de orçamento para segurança da informação e à ausência de políticas formais de resposta a incidentes. A falta de capacitação contínua dos colaboradores e a subnotificação de incidentes reforçam a necessidade de fortalecer a cultura organizacional de segurança, garantindo que as normas da LGPD se traduzam em práticas efetivas no dia a dia das instituições.

O estudo também evidencia que a proteção de dados pessoais não é apenas uma obrigação legal, mas um elemento estratégico para preservar a confiança de clientes, parceiros e titulares de dados, evitando prejuízos financeiros e danos à reputação. A adoção de políticas internas consistentes, combinada com monitoramento contínuo, conscientização de usuários e controles técnicos avançados, mostra-se essencial para mitigar riscos e responder de forma eficiente a incidentes cibernéticos.

Em síntese, os resultados reforçam a importância de integrar a LGPD às práticas organizacionais, promovendo uma abordagem proativa e estruturada de segurança digital. Apenas por meio de medidas preventivas, educação contínua e governança eficaz será

possível reduzir a exposição a ataques, proteger informações sensíveis e assegurar a conformidade legal, contribuindo para um ambiente digital mais seguro e confiável no Brasil.

6 REFERÊNCIAS

ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2005.

ALMEIDA, Laís Barbosa. O uso de tecnologias de segurança da informação no setor público brasileiro. *Revista Direito & TI*, v. 4, n. 2, p. 12-35, 2021.

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. Regulamenta a estrutura da ANPD. *Diário Oficial da União*, Brasília, DF, 27 ago. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

CETIC.BR. *Pesquisa TIC Empresas 2022*. São Paulo: CGI.br, 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Gen Forense, 2021.

FACHIN, Luiz Edson. A cidadania digital como direito fundamental. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 15, n. 2, p. 31-48, 2021.

IBM SECURITY. *Cost of a Data Breach Report 2024*. Armonk: IBM Corporation, 2024. Disponível em: https://www.ibm.com/reports/data-breach Acesso em: 15 abr. 2025.

MAGRANI, Eduardo. A proteção de dados pessoais no Brasil: desafios e perspectivas. *Revista Brasileira de Políticas Públicas*, v. 11, n. 1, p. 115-130, 2021.

MIRAGEM, Bruno. A tutela da privacidade e a responsabilidade civil na LGPD. *Revista de Direito do Consumidor*, v. 130, p. 79-98, 2022.

NASSAR, Pedro. Reputação institucional e vazamentos de dados: desafios para o setor empresarial. *Revista de Governança e Regulação*, v. 9, n. 3, p. 45-63, 2022.

SAMPiERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. *Metodologia de pesquisa*. 5. ed. Porto Alegre: Penso, 2013.

SERASA EXPERIAN. *Mapa da Fraude 2023*. São Paulo: Serasa Experian, 2023. Disponível em: https://www.serasaexperian.com.br. Acesso em: 10 abr. 2025.

STALLINGS, William. *Segurança em redes de computadores*. 6. ed. São Paulo: Pearson, 2017.

TIC EMPRESAS. *Pesquisa sobre o uso das tecnologias da informação e da comunicação nas empresas brasileiras: 2022*. São Paulo: NIC.br, 2022.

ZANATTA, Rafael. LGPD e regulação responsiva: caminhos para o fortalecimento da ANPD. *Revista Direito e Tecnologia*, v. 6, n. 1, p. 73-91, 2021.

VERIZON. Data Breach Investigations Report (DBIR) 2023. Nova York: Verizon Enterprise 2023.

MICROSOFT. Digital Defense Report 2023. Redmond: Microsoft, 2023.

CROWDSTRIKE. Global Threat Report 2023. Sunnyvale: CrowdStrike, 2023.