ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

CARLOS **VITOR** PALHÃO MACHADO, Ten Cel Av

Blockchain e a Proteção de Dados Pessoais no COMAER

Trabalho de conclusão de curso apresentado à Escola de Comando e Estado-Maior da Escola da Aeronáutica como requisito parcial para aprovação no Curso de Comando e Estado-Maior.
Linha de Pesquisa: Administração, Planejamento e Governança Institucional.
Orientador: Ten Cel Av Raillander Lage Bonifácio.

Rio de Janeiro
2025

RESUMO

O presente estudo teve como objetivo analisar de que maneira a implementação da tecnologia *blockchain* pode impactar os *gaps* no tratamento de dados pessoais identificados no Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), elaborado pelo COMAER. Para enfrentar os desafios relacionados à proteção de dados pessoais no contexto da *blockchain*, adotou-se como referencial teórico o modelo de *blockchain* permissionada do tipo consórcio, com arquitetura baseada na plataforma *Hyperledger Fabric*, conforme proposto por Gonçalves, Da Silva e Da Cunha (2024). A metodologia adotada seguiu uma abordagem qualitativa e quantitativa, com orientação indutiva. Inicialmente, foram identificados os *gaps* no tratamento de dados pessoais e as ações estratégicas geradas a partir da matriz TOWS (SWOT cruzada), considerando a implementação da tecnologia *blockchain* no contexto institucional do COMAER. Posteriormente, realizou-se uma análise de correlação entre essas estratégias e os *gaps* mapeados, classificando-se a aderência em quatro níveis: alta, média, baixa ou nula. Os resultados obtidos indicaram que a arquitetura da *blockchain* adotada nesta pesquisa apresentou potencial para impactar positivamente, com alta aderência, em 96,1% dos *gaps* relativos ao tratamento de dados pessoais identificados no PCA 16-14/2022. Concluiu-se que, a arquitetura da *blockchain* adotada nesta pesquisa apresentou potencial para impactar positivamente, com alta aderência, em 96,1% dos *gaps* relativos ao tratamento de dados pessoais identificados no PCA 16-14/2022.

Palavras-chave: *blockchain;* COMAER; LGPD; dados pessoais.

ABSTRACT

This study aimed to analyze how the implementation of blockchain technology could impact the gaps in the processing of personal data identified in the Compliance Plan with the General Data Protection Law (PCA 16-14/2022), developed by the Brazilian Air Force Command (COMAER). To address the challenges related to personal data protection within the blockchain context, the theoretical framework adopted was the consortium-based permissioned blockchain model, with an architecture built on the Hyperledger Fabric platform, as proposed by Gonçalves, Da Silva, and Da Cunha (2024). The methodology employed followed a qualitative and quantitative approach, with an inductive orientation. Initially, the gaps in the processing of personal data were identified, along with the strategic actions generated from the TOWS matrix (crossed SWOT), considering the implementation of blockchain technology within COMAER's institutional context. Subsequently, a correlation analysis was conducted between these strategies and the mapped gaps, with the level of adherence classified into four categories: high, medium, low, or none. The results indicated that the blockchain architecture adopted in this study demonstrated a high potential to positively impact 96.1% of the gaps related to the processing of personal data identified in PCA 16-14/2022. It was concluded that the proposed blockchain architecture presented a high level of adherence and a strong potential to mitigate the identified gaps in COMAER's data processing practices.
Keywords: *Blockchain; COMAER; LGPD; Personal Data*.

1 INTRODUÇÃO

A crise financeira mundial de 2008 evidenciou fragilidades no sistema bancário tradicional e motivou o surgimento do Bitcoin, moeda digital descentralizada proposta por Nakamoto (2008). Essa inovação se fundamentou na tecnologia *blockchain*, que viabilizou o registro público, transparente e imutável de transações financeiras, eliminando a necessidade de intermediários (Nakamoto, 2008).

Embora sua origem esteja diretamente vinculada ao universo das criptomoedas, a *blockchain* passou a ser debatida como vetor de inovação em diversas outras áreas. Ainda assim, sua imagem permanece, de forma recorrente, atrelada ao Bitcoin e a outros criptoativos. Essa associação, embora compreensível, limita entendimento sobre o real potencial da tecnologia, que vem sendo explorada em setores como saúde, logística, defesa, governança digital e segurança da informação (Tapscott e Tapscott, 2016).

Do ponto de vista técnico, a *blockchain* é definida como um banco de dados – ou livro-razão digital – que armazena informações em blocos encadeados por funções criptográficas (*hashes*), replicados entre diversos computadores interligados em rede, também chamados de nós (Nakamoto, 2008). Cada nó segue um protocolo de consenso, que estabelece as regras para validação de novos blocos, garantindo a integridade do sistema. Esse arranjo confere à *blockchain* propriedades essenciais como segurança, imutabilidade, rastreabilidade e transparência (Nakamoto, 2008).

Entre essas propriedades, destacam-se a imutabilidade e a descentralização. De acordo com Zafar (2025), a imutabilidade garante que os dados registrados não possam ser modificados sem o devido consenso, assegurando a integridade e a transparência da informação. Já para Swan (2015), a descentralização elimina a dependência de uma autoridade central, promovendo maior resiliência, segurança e democratização no controle informacional. Tais características tornam a *blockchain* uma solução estratégica para ambientes que exigem confiança, rastreabilidade e resistência à manipulação (Tapscott e Tapscott, 2016).

Esse potencial já vem sendo explorado por instituições de alta relevância, como a Agência de Projetos de Pesquisa Avançada de Defesa (DARPA) e a Organização do Tratado do Atlântico Norte (OTAN), que adotaram a *blockchain* em operações militares. De acordo com Ahmad *et al*. (2021, p. 1, tradução nossa), “as características distintas e os recursos extremamente benéficos do *blockchain* permitiram que DARPA e OTAN realizassem operações militares de maneira segura, transparente, econômica e auditável”.

No Brasil, a expansão da *blockchain* também tem ganhado impulso por meio da Estratégia de Governo Digital (EGD), instituída pelo Decreto nº 10.332/2020, com o objetivo de modernizar a administração pública e promover maior eficiência e transparência nos serviços prestados ao cidadão (Brasil, 2020). Um dos frutos dessa diretriz foi a criação da Rede Blockchain Brasil (RBB), resultado da parceria entre o Tribunal de Contas da União (TCU) e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), visando o desenvolvimento de soluções públicas mais seguras, eficientes e inovadoras (Exame, 2022). Outro exemplo é o da Agência Nacional de Aviação Civil (ANAC), que adotou a tecnologia *blockchain* como base do Diário de Bordo Digital (eDB), proporcionando maior segurança, rastreabilidade e integridade aos registros de bordo (Brasil, 2022).

Apesar desses avanços e dos reconhecidos benefícios da tecnologia, sua implementação impõe desafios significativos sob a perspectiva da conformidade legal. Como destacam Gonçalves, Da Silva e Da Cunha (2024), os mesmos atributos que tornam a *blockchain* promissora, como a imutabilidade e a descentralização, podem entrar em conflito com normas de proteção de dados pessoais. No Brasil, tais exigências estão consolidadas na Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada pelo nº 13.709/2018, que estabelece princípios, direitos e deveres quanto ao tratamento de dados, exigindo adaptações nas estruturas e nos processos das instituições públicas e privadas (Brasil, 2018).

No âmbito do Comando da Aeronáutica (COMAER), tais exigências legais deram origem ao Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), que identificou *gaps* (lacunas) nos processos internos relacionados ao tratamento de dados pessoais, estabelecendo diretrizes para sua correção e conformidade.

Diante desse cenário, e considerando as propriedades técnicas da *blockchain*, surgiu o seguinte problema de pesquisa: de que maneira a implementação da tecnologia *blockchain* pode impactar os *gaps* no tratamento de dados pessoais identificados no Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), elaborado pelo COMAER?

Nesse contexto, o objetivo geral da pesquisa foi analisar de que maneira a implementação da tecnologia *blockchain* pode impactar os *gaps* no tratamento de dados pessoais identificados no Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), elaborado pelo COMAER.

Para alcançar o objetivo geral do trabalho, foram definidos os seguintes objetivos específicos (OE):

OE1 – Identificar os *gaps* no tratamento de dados pessoais no COMAER;

OE2 – Identificar as ações estratégicas para a mitigação dos *gaps* identificados no tratamento de dados pessoais no COMAER; e

OE3 – Correlacionar as ações estratégicas com os *gaps* no tratamento de dados pessoais no COMAER.

A relevância deste trabalho para o COMAER consiste na proposição de uma solução tecnológica que pode ser aplicada tanto na mitigação dos *gaps* identificados no tratamento de dados pessoais quanto como alternativa estratégica a sistemas centralizados, os quais apresentam maior vulnerabilidade à ausência de controles de acesso e à fragilidade na segurança da informação. A arquitetura de *blockchain* analisada revela-se compatível com os requisitos institucionais de confiabilidade, transparência e auditabilidade, podendo atuar no aprimoramento da gestão e na governança organizacional. Além disso, a adoção de tecnologias seguras e resilientes, como a proposta neste trabalho, contribui para a integração e o fortalecimento da infraestrutura digital da Força Aérea Brasileira, promovendo e consolidando avanços no processo de modernização administrativa incentivadas pelo Governo Federal.

2 REFERENCIAL TEÓRICO

Os referenciais teóricos adotados foram organizados em três eixos, que serviram de base para a construção e fundamentação deste estudo. As principais proposições de cada eixo estão consolidadas no Quadro 1, ao final desta seção.

2.1 EIXO TEÓRICO - *GAPS* NO TRATAMENTO DE DADOS PESSOAIS

Neste primeiro eixo, foram considerados os fundamentos teóricos e a base legal que estruturam o Plano de Adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados (PCA 16-14/2022). Nesse documento, o COMAER identificou diversos *gaps* no tratamento de dados pessoais, com base em um inventário abrangente dos principais macroprocessos internos (Brasil, 2022). O diagnóstico resultante foi sistematizado em fichas de controle, que orientaram a proposição de ações corretivas destinadas a todos os Órgãos de Direção Geral, Setorial e de Assessoria Direta ao Comandante da Aeronáutica (ODGSA).

Essa perspectiva normativa, conforme destacam Suripeddi e Purandare (2021), exige que as organizações, na qualidade de controladoras e operadoras de dados, demonstrem conformidade com os requisitos legais, registrem o progresso da implementação e realizem avaliações de risco e impacto em toda a instituição. Tais exigências encontram respaldo nos

princípios previstos no artigo 6º da LGPD, especialmente os de segurança, prevenção, responsabilização e prestação de contas (incisos VII a IX), que determinam a adoção de medidas eficazes para evitar danos, proteger os dados pessoais e comprovar conformidade com a legislação (Brasil, 2018).

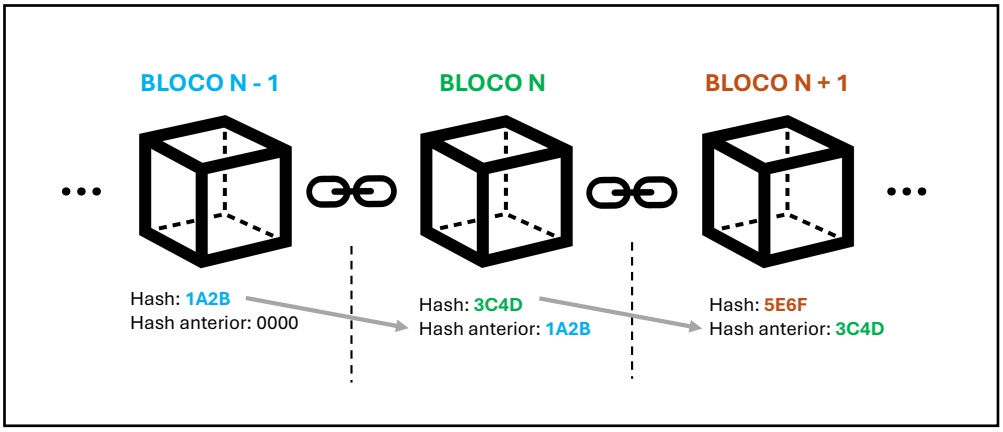
Complementando esse arcabouço normativo, o artigo 38 da LGPD determina a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), o qual deve conter a descrição das atividades de tratamento, a metodologia empregada, a análise de riscos e as respectivas salvaguardas adotadas. Tais exigências dialogam diretamente com o diagnóstico realizado pelo PCA 16-14/2022. Da mesma forma, os artigos 46 a 49 da LGPD reforçam a obrigatoriedade de adoção de medidas de segurança técnicas e administrativas, boas práticas de governança e procedimentos para a gestão de incidentes, elementos também contemplados nas classificações de risco e nas ações propostas no plano de adequação (Brasil, 2018).

Dessa forma, o PCA 16-14/2022 configura-se como um instrumento do COMAER alinhado à LGPD tanto do ponto de vista normativo quanto institucional, sendo, por isso, utilizado como fonte central para a coleta dos dados para este trabalho.

2.2 EIXO TEÓRICO - TECNOLOGIA *BLOCKCHAIN*

Este eixo apresenta os referenciais teóricos que embasam a escolha do tipo de *blockchain* adotado na pesquisa. Gonçalves, Da Silva e Da Cunha (2024, p. 1018, tradução nossa) argumentam que “a tecnologia *blockchain* tem sido cada vez mais adotada em instituições públicas devido à sua capacidade de garantir rastreabilidade, integridade e transparência na gestão de dados”. Essa expansão ocorre, sobretudo, em setores que demandam elevados padrões de segurança da informação, como saúde, finanças, logística e administração pública (Gonçalves; Da Silva; Da Cunha, 2024). Essa adoção se justifica pela capacidade da tecnologia em oferecer atributos como a imutabilidade, que impede a alteração dos dados registrados por meio de sua estrutura “*append-only*” (somente adição), combinada com o uso de funções criptográficas de encadeamento de blocos (*hashes*), conforme ilustrado na Figura 1 (Niranjanamurthy *et al*., 2018). Assim, a cada preenchimento de um bloco com informações e a criação de um novo, utiliza-se o *hash* do bloco anterior como base para gerar o *hash* do novo bloco, formando uma cadeia criptograficamente vinculada e segura (Nakamoto, 2008). Esse encadeamento se assemelha ao vínculo dos pais quando passam para o filho os seus sobrenomes, criando um vínculo nominal registrado em cartório.

Figura 1 - Encadeamento de blocos.



Fonte: O autor.

Quanto aos tipos de redes computacionais, Niranjanamurthy (2018), as classifica como:

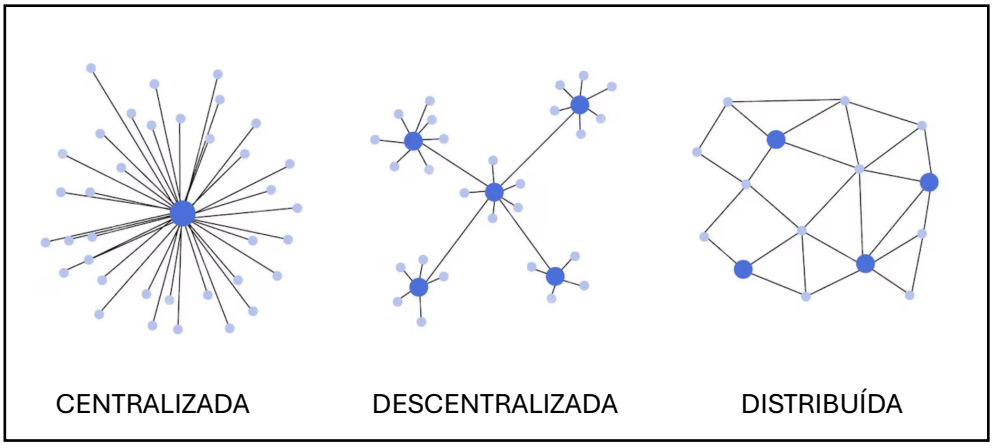
a) centralizadas - um único ponto ou nó controla todo o sistema, tornando-o vulnerável a falhas;

b) descentralizadas - distribuem funções entre vários nós, aumentando a resiliência; e

c) distribuídas - cada nó armazena e processa os dados integral ou parcialmente, promovendo robustez e auditabilidade.

A Figura 2 ilustra os tipos de redes e a disposição dos nós, representados pelos círculos maiores.

Figura 2 - Tipos de rede.



Fonte: Adaptada de Ethereum Classic (2022).

Em relação aos nós, Gonçalves, Da Silva e Da Cunha (2024), afirmam que são elementos essenciais da infraestrutura da *blockchain*, responsáveis por armazenar os dados, validar transações e adicionar novos blocos à cadeia. Em *blockchains* abertas (não permissionadas), qualquer usuário pode atuar como nó, ampliando a descentralização e a transparência. Já em redes fechadas (permissionadas), típicas de *blockchains* corporativas, apenas participantes autorizados desempenham essas funções, permitindo maior controle, governança e conformidade com normas institucionais (Gonçalves; Da Silva; Da Cunha, 2024).

Para assegurar que os blocos sejam adicionados de forma segura à cadeia, utilizam-se algoritmos de consenso – conjunto de regras que definem como as transações são validadas entre os participantes da rede. Em *blockchains* públicas, o *Proof of Work* (prova de trabalho), utilizado pelo Bitcoin, requer a resolução de cálculos matemáticos complexos, o que acarreta elevado consumo energético. O *Proof of Stake* (prova de participação), adotado pelo Ethereum 2.0, seleciona validadores com base na quantidade de ativos mantidos em custódia, o que pode levar à concentração de poder. Ambos são inadequados ao tratamento de dados pessoais, por sua natureza aberta e anonimizada (Gonçalves; Da Silva; Da Cunha, 2024).

Em contraste aos modelos públicos, a plataforma *Hyperledger Fabric*, adotada por Gonçalves, Da Silva e Da Cunha (2024), utiliza o protocolo de consenso *Raft*, baseado em eleição de líderes. Um dos nós assume temporariamente a liderança, coordenando a replicação de dados entre os demais, o que garante consistência, previsibilidade e tolerância a falhas (Gonçalves; Da Silva; Da Cunha, 2024).

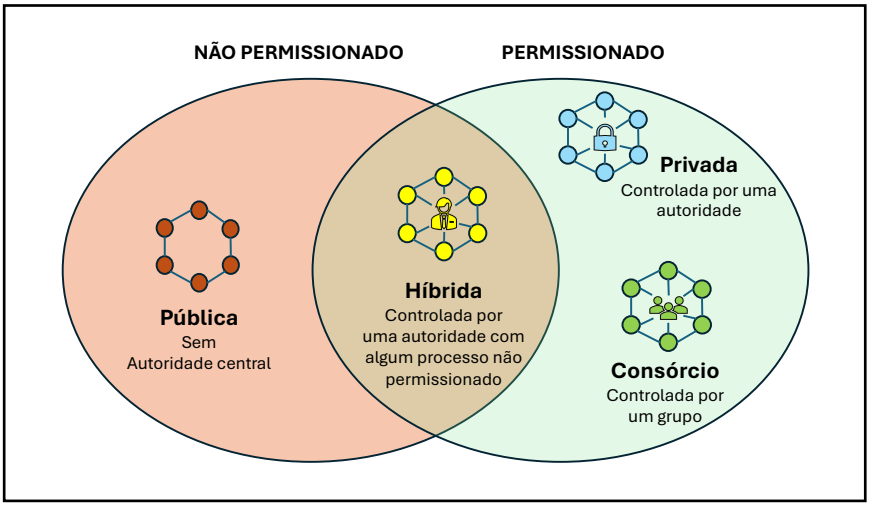
Quanto à classificação do controle de acesso e à governança, a *blockchain* se divide em dois grupos: permissionadas e não permissionadas (Bhutta *et al*., 2021). As não permissionadas permitem que qualquer indivíduo participe e valide transações na rede. As permissionadas, por outro lado, limitam essas funções a participantes previamente autorizados, garantindo maior controle e conformidade com normas regulatórias (Gonçalves; Da Silva; Da Cunha, 2024).

Dentro desse universo, Gonçalves, Da Silva e Da Cunha (2024) identificam quatro principais tipos de *blockchain*:

a) *blockchain* pública: aberta a todos os usuários, com validação descentralizada. Apesar da transparência, enfrenta desafios como escalabilidade, consumo energético e dificuldades em atender à privacidade, como por exemplo: Bitcoin, Ethereum e Litecoin;
b) *blockchain* privada: controlada por uma única entidade. Oferece desempenho, mas reduz a transparência externa, como por exemplo: Monax e MultiChain;
c) *blockchain* de consórcio: operada por várias organizações com governança compartilhada. Equilibra descentralização e controle, como por exemplo: *Hyperledger Fabric*, R3 Corda e B3i; e
d) *blockchain* híbrida: combina características públicas e privadas, permitindo que alguns dados sejam públicos e outros restritos, útil para prestação de contas por órgãos públicos.

Dessa maneira, a Figura 3 ilustra os dois tipos de controle de acesso e os quatro tipos de *blockchain*.

Figura 3 - Nível de controle de acesso e tipos de *blockchain.*



Fonte: Adaptada de Foley & Lardner LLP (2021).

Nesse sentido, Han e Park (2023, p. 2, tradução nossa), afirmam que "o tipo e a arquitetura da *blockchain* determinam a sua compatibilidade com as exigências regulatórias". Bhutta *et al*. (2021) reforçam que *blockchains* públicas não oferecem meios adequados para gerir o ciclo de vida dos dados, enquanto *blockchains* privadas sacrificam a confiança distribuída. As híbridas, apesar de flexíveis, enfrentam limitações quanto à governança. Assim, a *blockchain* permissionada do tipo consórcio, baseada na plataforma *Hyperledger Fabric*, é apresentada como alternativa de equilíbrio entre controle, auditabilidade e conformidade regulatória (Gonçalves; Da Silva; Da Cunha, 2024).

No contexto da proteção de dados pessoais, as propriedades técnicas da *blockchain* podem representar tanto soluções quanto desafios. A imutabilidade, por exemplo, pode entrar em conflito com o direito à anonimização e à eliminação de dados previsto na LGPD (Brasil, 2018). Para superar esses desafios, Gonçalves, Da Silva e Da Cunha (2024) propõem a utilização da plataforma *Hyperledger Fabric* e armazenamento *off-chain*, prática que possibilita excluir ou modificar dados fora da cadeia principal, o que apresenta conformidade com a legislação. Já a segurança é reforçada pelo uso de criptografia irreversível (*hashes*), que garante a confidencialidade dos dados mesmo em caso de acesso indevido. Dessa maneira, "é possível criar um sistema que supere os principais desafios de armazenar dados pessoais em uma *blockchain,* mantendo suas características desejáveis" (Gonçalves; Da Silva; Da Cunha, 2024, p. 1021, tradução nossa).

Corroborando com essa viabilidade de aplicação, Krey (2021) afirma que soluções como o armazenamento *off-chain* têm sido utilizadas para resolver conflitos resultantes da imutabilidade:

> A *blockchain* apenas armazenaria a informação necessária para acessar e descriptografar os dados registrados em banco de dados comum paralelo,

> possibilitando a retificação e apagamento de dados pessoais com maior facilidade, tornando a *blockchain* compatível com o próprio direito ao apagamento ou à eliminação de dados, positivado na LGPD brasileira no artigo 16 (Krey, 2021, p.50)

Dessa maneira, essas estratégias proporcionam a gestão do ciclo de vida dos dados, tornando o uso da *blockchain* viável em instituições públicas que demandam equilíbrio entre segurança informacional e conformidade legal (Gonçalves; Da Silva; Da Cunha, 2024; Krey, 2021). Assim, a escolha da *blockchain* permissionada do tipo consórcio, baseada na plataforma *Hyperledger Fabric*, alinha-se a esse cenário, conforme proposto e testado por Gonçalves, Da Silva e Da Cunha (2024), no artigo *Olympus: a GDPR Compliant Blockchain System* (Olympus: um Sistema de *Blockchain* em Conformidade com o GDPR)

2.3 EIXO TEÓRICO - MATRIZ SWOT E MATRIZ TOWS

Neste eixo, foram analisados os fundamentos teóricos relacionados à matriz SWOT e à matriz TOWS (ou matriz cruzada), com ênfase na geração de ações estratégicas que possibilitassem a mitigação dos *gaps* encontrados no tratamento de dados pessoais no COMAER.

A matriz SWOT, embora simples, é uma ferramenta poderosa para identificar os fatores internos (forças e fraquezas) e externos (oportunidades e ameaças) que afetam uma determinada organização (Gurel e Tat, 2017). Sua estrutura apresenta análise de elementos que, segundo Gurel e Tat (2017), são organizados em quatro categorias: forças (*strengths*) – características internas positivas que conferem vantagem à organização; fraquezas (*weaknesses*) – limitações ou deficiências internas que reduzem a eficácia ou competitividade; oportunidades (*opportunities*) – condições externas favoráveis que podem ser exploradas estrategicamente; e ameaças (*threats*) – fatores externos que podem comprometer o desempenho, a segurança ou a estabilidade da organização. Para Weihrich (1982) e Gurel e Tat (2017), a matriz deve ser construída com base em dados empíricos ou documentais para assegurar que as estratégias derivadas tenham validade prática e relevância analítica.

Por sua vez, a matriz TOWS ou SWOT cruzada é uma ferramenta que utiliza os elementos identificados na matriz SWOT, resultando em “estratégias, táticas e ações para a realização eficiente e eficaz dos objetivos organizacionais” (Weihrich, 1982, p. 54, tradução nossa). Segundo Weihrich (1982) a matriz TOWS apresenta quatro tipos de ações estratégicas:

a) ações estratégicas SO (*strengths* - *opportunities*): usam as forças internas para aproveitar oportunidades externas, resultando em ações estratégicas ofensivas;

b) ações estratégicas ST (*strengths* - *threats*): usam forças para minimizar ou neutralizar ameaças, resultando em ações estratégicas confrontativas;
c) ações estratégicas WO (*weaknesses* - *opportunities*): corrigem fraquezas aproveitando oportunidades, resultando em ações estratégicas de reforço; e
d) ações estratégicas WT (*weaknesses* - *threats*): visam minimizar fraquezas e evitar ameaças, resultando em ações estratégicas defensivas.

Dessa maneira, enquanto a análise SWOT organiza os elementos do ambiente interno e externo da organização, a matriz TOWS orienta a formulação de estratégias ao cruzar esses fatores, promovendo ações práticas a partir do diagnóstico situacional (Weihrich, 1982). Corroborando, Gurel e Tat (2017) destacam que "a força do modelo TOWS reside na sua capacidade de transformar o diagnóstico em planos de ação concretos, direcionando decisões e priorizando recursos com base na interação entre ambiente interno e externo" (Gurel e Tat, 2017, p. 100, tradução nossa). Assim, ao considerar os desafios institucionais mapeados, este trabalho adotou a aplicação combinada das matrizes SWOT e TOWS, conforme sugerido por Weihrich (1982), como instrumento estratégico para a formulação de ações voltadas à mitigação dos *gaps* no tratamento de dados pessoais.

2.4 SÍNTESE TEÓRICA DA PESQUISA

Com base nos referenciais teóricos adotados, o Quadro 1 foi estruturado com o objetivo de apresentar, de forma sistematizada, as principais proposições desenvolvidas ao longo dos três eixos teóricos abordados nesta pesquisa.

Quadro 1 - Estrutura teórica da pesquisa. (continua)

Eixo Teórico	**Proposição Teórica**
Gaps no Tratamento de Dados Pessoais	a) necessidade de medidas de segurança técnicas e administrativas, a adoção de boas práticas e a gestão de incidentes de segurança (Brasil, 2018).
Tecnologia *Blockchain*	a) "a tecnologia *blockchain* tem sido cada vez mais adotada em instituições públicas devido à sua capacidade de garantir rastreabilidade, integridade e transparência na gestão de dados" (Gonçalves; Da Silva; Da Cunha, 2024, p. 1018, tradução nossa); b) "o tipo e a arquitetura da *blockchain* determinam a sua compatibilidade com as exigências regulatórias". (Han e Park, 2023, p. 2, tradução nossa); c) "é possível criar um sistema que supere os principais desafios de armazenar dados pessoais em um *blockchain,* mantendo suas características desejáveis" (Gonçalves; Da Silva; Da Cunha, 2024, p. 1021);

(conclusão)

Eixo Teórico	Proposição Teórica
Tecnologia *Blockchain*	d) a blockchain permissionada do tipo consórcio, baseada na plataforma *Hyperledger Fabric*, é apresentada como alternativa de equilíbrio entre controle, auditabilidade e conformidade regulatória. (Gonçalves; Da Silva; Da Cunha, 2024); e e) soluções como o armazenamento *off-chain* têm sido utilizadas para resolver conflitos resultantes da imutabilidade, possibilitando a retificação e apagamento de dados pessoais com maior facilidade, tornando a *blockchain* compatível com o próprio direito ao apagamento ou à eliminação de dados, positivado na LGPD brasileira no artigo 16. (Krey, 2021, p. 50).
Matriz SWOT e TOWS	a) enquanto a análise SWOT organiza os elementos do ambiente interno e externo da organização, a matriz TOWS orienta a formulação de estratégias ao cruzar esses fatores, promovendo ações práticas a partir do diagnóstico situacional. (Weihrich, 1982); e b) "a força do modelo TOWS reside na sua capacidade de transformar o diagnóstico estratégico em planos de ação concretos, direcionando decisões e priorizando recursos com base na interação entre ambiente interno e externo" (Gurel e Tat, 2017, p. 100, tradução nossa).

Fonte: O autor.

3 METODOLOGIA

Esta pesquisa, quanto ao método, caracterizou-se como indutiva, uma vez que, ao adotar a arquitetura *blockchain* proposta, buscou-se analisar de que maneira a implementação da tecnologia *blockchain* pode impactar os *gaps* no tratamento de dados pessoais identificados no Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), elaborado pelo COMAER.

No que se refere à técnica de obtenção de dados e informações, foram utilizados levantamentos bibliográficos e documentais. As fontes normativas – como o PCA 16-14/2022 e a LGPD – foram obtidas por meio da ferramenta de busca da Google. Para a pesquisa bibliográfica, utilizou-se o Google Acadêmico, sendo inicialmente empregados os termos: *blockchain,* LGPD e GDPR – *General Data Protection Regulation*, norma europeia de proteção de dados que serviu de referência para a formulação da LGPD. A partir dos resultados iniciais da busca, destacaram-se, em português, as palavras-chave: *blockchain*, LGPD, GDPR, proteção de dados, privacidade, imutabilidade e regulamentação. Em artigos de língua inglesa, observaram-se: *blockchain*, *GDPR*, *privacy*, *data protection e personal data*.

Esses termos orientaram a seleção de artigos, teses e livros sobre *blockchain* e proteção de dados pessoais, tendo como principais autores de referência: Satoshi Nakamoto (2018), Tapscott e Tapscott (2016), Bhutta *et al*. (2021), Suripeddi e Purandare (2021), Gonçalves, Da Silva e Da Cunha (2024), Han e Park (2023), Niranjanamurthy (2018), Krey (2021). Além da base temática sobre *blockchain*, foram adotados autores clássicos, como Weihrich (1982) e Gurel e Tat (2017), que forneceram o embasamento metodológico das matrizes SWOT e TOWS, fundamentais para a estrutura analítica desta pesquisa. Essas ferramentas foram aplicadas no tratamento dos dados obtidos a partir do levantamento das características dos elementos do ambiente interno e externo (matriz SWOT) e do cruzamento entre esses elementos (matriz TOWS), gerando as ações estratégicas necessárias à análise.

O desenvolvimento metodológico seguiu os três objetivos específicos delineados neste trabalho. Para o Objetivo Específico 1 (OE1), procedeu-se à identificação dos *gaps* no tratamento de dados pessoais no âmbito do COMAER, conforme disposto no PCA 16-14/2022. Essa etapa baseou-se nas fichas de controle classificadas em duas categorias existentes no documento – segurança e privacidade – e permitiu quantificar as inconformidades, organizando os dados em um quadro-resumo que subsidiou as etapas subsequentes. Além disso, de posse dos dados, foi realizada uma análise quantitativa para verificar a ocorrência do Princípio de Pareto (regra 80/20). Tal verificação é importante para que a organização possa concentrar esforços nas causas mais relevantes dos problemas, otimizando tempo, recursos e decisões estratégicas. Essa priorização evidencia os desafios mais impactantes e orienta, de forma clara, onde os gestores devem aplicar ações corretivas para alcançar o maior retorno possível (Santos *et al*., 2015).

Para o Objetivo Específico 2 (OE2), identificaram-se os elementos de força e fraqueza do ambiente interno, com base nas características da tecnologia *blockchain* descritas por Gonçalves, Da Silva e Da Cunha (2024). Em seguida, mapearam-se as oportunidades e ameaças do ambiente externo, considerando aspectos institucionais, normativos e contextuais. Com esses dados, estruturou-se a matriz SWOT, que, segundo Weihrich (1982), fornece insumos para a formulação da matriz TOWS. Essa, por sua vez, foi utilizada para o cruzamento dos elementos internos e externos da matriz SWOT, gerando os quatro tipos de ações estratégicas: ofensiva (SO), confrontativa (ST), de reforço (WO) e defensiva (WT). Essas ações, também consideradas por Weihrich (1982) como estratégias, foram organizadas em um quadro específico, contendo seus respectivos códigos identificadores, e serviram de base para a etapa seguinte da pesquisa.

Por fim, o terceiro objetivo (OE3) consistiu em correlacionar cada uma das ações estratégicas geradas a partir da matriz TOWS com os *gaps* identificados no tratamento de dados pessoais no COMAER. O processo de correlação permitiu classificar as **aderências** em quatro níveis: alta, média, baixa e nula. Com isso, foi possível analisar a relação entre as variáveis independente e dependente da pesquisa, gerando os resultados necessários para alcançar o objetivo geral e responder o problema proposto.

Quanto ao recorte temporal da investigação, este foi delimitado com base na versão vigente do PCA 16-14, publicada em 2022, a qual foi adotada como referência oficial e representativa da situação atual de conformidade do COMAER com a LGPD.

Além disso, por se tratar de um estudo documental e bibliográfico, não houve coleta de dados em campo e nem amostragem, restringindo-se somente à análise da arquitetura *blockchain* adotada neste trabalho e à identificação dos dados no PCA 16-14/2022.

Quanto ao universo desta pesquisa, adotou-se como objeto de estudo o PCA 16-14/2022, documento oficial que fundamentou o levantamento dos *gaps* no tratamento de dados pessoais, apresentados no formato de fichas de controle.

Entre os principais limites desta pesquisa, destaca-se a adoção exclusiva de uma abordagem documental e teórica, sem a realização de testes empíricos, entrevistas com especialistas ou validação prática das soluções propostas. A análise foi restrita às fichas de controle do PCA 16-14/2022, o que limita a generalização dos resultados e impossibilita a aferição, em campo, da aplicabilidade das estratégias formuladas. Embora fundamentada em autores especializados, a escolha pela plataforma Hyperledger Fabric não envolveu a análise de sistemas adjuntos nem a comparação com outras implementações possíveis. Essa limitação indica a necessidade de estudos futuros mais abrangentes e tecnicamente aprofundados para o contexto do COMAER.

4 APRESENTAÇÃO DOS DADOS E ANÁLISES DOS RESULTADOS

Os dados obtidos por meio da pesquisa bibliográfica e documental foram analisados à luz dos referenciais teóricos e foram dispostos em quatro subseções.

4.1 *GAPS* NO TRATAMENTO DE DADOS PESSOAIS

O COMAER, em conformidade com o disposto na Resolução do Conselho Diretor da Autoridade Nacional de Proteção de Dados (CD/ANPD nº1, de 28 de outubro de 2021),

elaborou o Plano de Ação de Conformidade (PCA 16-14/2022), no qual realizou o diagnóstico de seus macroprocessos e identificou 15 tipos de *gaps* relacionados às operações de tratamento de dados. Como resultado, foram propostas 129 fichas de controle, destinadas a orientar os ODGSA – que apresentavam esses *gaps* no tratamento de dados pessoais em suas organizações – na adequação aos requisitos estabelecidos pela LGPD (Brasil, 2022).

Nessas fichas, além da identificação de responsabilidades, prazos e métodos, constavam a classificação dos *gaps* (segurança e privacidade) e as respectivas ausências de controles, mecanismos, procedimentos ou tabelas, caracterizando os tipos de *gaps* no tratamento de dados pessoais do COMAER.

Ao identificar os dados no PCA 16-14/2022, observou-se que os *gaps* classificados como relacionados à segurança correspondiam a sete tipos, distribuídos em 16 fichas de controle, o que representa 12% do total. Em contrapartida, os *gaps* relacionados à privacidade somavam oito tipos, abrangendo 113 fichas, correspondentes a 88% do universo avaliado. Com o objetivo de apresentar e organizar essas informações para posterior análise, foi estruturado o Quadro 2 e determinado os respectivos códigos para cada *gap*.

Quadro 2 - *Gaps* no tratamento de dados pessoais.

Classificação	**Tipos *gap* no tratamento de dados pessoais (código)**	**Ficha de controle (quantidade)**	**Proporção**
Segurança 12% (16)	Ausência de controles criptográficos (G1)	1	1%
	Ausência de controles de acesso lógico (G2)	2	2%
	Ausência de controles de segurança em redes, proteção física e do ambiente (G3)	3	2%
	Ausência de mecanismos de desenvolvimento seguro (G4)	2	2%
	Ausência de mecanismos para registro de eventos, rastreabilidade e salvaguarda de logs (G5)	3	2%
	Ausência de mecanismos para garantir a segurança web (G6)	4	3%
	Ausência de procedimento de resposta a incidentes (G7)	1	1%
Privacidade 88% (113)	Ausência de mecanismos de conscientização sobre a importância da privacidade e segurança da informação (G8)	2	2%
	Ausência de mecanismos de consentimento e escolha (G9)	3	2%
	Ausência de mecanismos para garantir a precisão e a qualidade (G10)	3	2%
	Ausência de medidas de responsabilização (G11)	7	5%
	Ausência de medidas para assegurar a limitação da coleta (G12)	1	1%
	Ausência de medidas para assegurar o compliance com a privacidade (G13)	34	26%
	Ausência de medidas para garantir a abertura, transparência e notificação (G14)	31	24%
	ausência de tabela de temporalidade e destinação final definidas (G15)	32	25%
Total de fichas de controle de *gaps*		129	

Fonte: O autor.

Dessa forma, a identificação dos *gaps* com base no PCA 16-14/2022, permitiu o alcance do OE1 deste trabalho.

4.2 MATRIZ SWOT, MATRIZ TOWS E ESTRATÉGIAS

Nessa seção, para gerar as ações estratégicas definidas por Weihrich (1982), foi necessário, inicialmente, elaborar a matriz SWOT, considerando o COMAER e a tecnologia *blockchain* descrita por Gonçalves, Da Silva e Da Cunha (2024).

Para a estruturação da matriz SWOT, o processo iniciou-se com a identificação das qualidades da tecnologia *blockchain* que correspondiam ao elemento forças (*strengths*). Nesse sentido, foram considerados os atributos destacados por Gonçalves, Da Silva e Da Cunha (2024), tais como: imutabilidade condicional; descentralização dos dados; auditabilidade e rastreabilidade; flexibilidade, proporcionada por sua arquitetura modular e configurável; capacidade de armazenamento *off-chain*; e mecanismos de identificação e controle de acesso.

Em relação às fraquezas (*weaknesses*), estas foram identificadas a partir das limitações técnicas, operacionais e jurídicas associadas à tecnologia. Mesmo com as soluções propostas por Gonçalves, Da Silva e Da Cunha (2024) para contornar os desafios da imutabilidade, sua implementação envolve dificuldades como: elevada complexidade técnica; necessidade de profissionais qualificados; questões de escalabilidade (apesar dos avanços proporcionados pela plataforma *Hyperledger Fabric*); desafios relacionados à governança descentralizada; e resistência institucional, conforme salientado por Kossow (2019).

Quanto às oportunidades (*opportunities*), foram relacionados fatores do ambiente externo que favorecem a implementação da *blockchain* no COMAER. Destacam-se entre eles: o alinhamento com as exigências da LGPD; o acesso à expertise de outras organizações públicas que já desenvolvem ou aplicam a tecnologia, como o TCU, o BNDES e a ANAC; a integração digital com o Governo Federal, em conformidade com a Estratégia de Governo Digital e com o Plano de Transformação Digital; e a integração com tecnologias emergentes, como inteligência artificial – por meio de utilização de base de dados seguras e imutáveis – e a preparação para a Web 3.0, caracterizada pela descentralização da internet, conforme destaca Tapscott (2023).

Em relação às ameaças (*threats*), Han e Park (2023) destacam a insegurança jurídica decorrente da ausência de regulamentações específicas para a tecnologia *blockchain.* Somam-se a esse cenário os desafios impostos por tecnologias emergentes, como a computação quântica e a inteligência artificial, além da crescente complexidade dos ataques cibernéticos. Outro

aspecto que merece atenção é o risco de incompatibilidade com sistemas legados (software ou tecnologia ultrapassada que ainda continua em uso) utilizados pelas organizações, os quais muitas vezes não foram concebidos para se integrar a soluções modernas como a *blockchain* (Gonçalves; Da Silva; Da Cunha, 2024).

A partir da identificação e organização dos fatores internos (forças e fraquezas) e externos (oportunidades e ameaças), foi possível consolidar a matriz SWOT, representada no Quadro 3. Essa estrutura analítica sintetiza, de forma sistematizada, os principais elementos relacionados ao COMAER e à tecnologia *blockchain*. A consolidação da matriz permitiu visualizar o cenário estratégico da pesquisa e serviu como base para o desenvolvimento da matriz TOWS e das estratégias subsequentes.

Quadro 3 - Matriz SWOT.

	Forças (*Strengths*)	**Fraquezas (*Weaknesses*)**
Ambiente Interno	**(S1)** Imutabilidade condicional – resistência à adulteração.	**(W1)** Complexidade técnica (arquitetura ajustada).
	(S2) Descentralização – ausência de um único ponto de falha, maior resiliência cibernética.	**(W2)** Necessidade de mão de obra qualificada.
	(S3) Auditabilidade e rastreabilidade.	**(W3)** Escalabilidade da rede (número de transações).
	(S4) Arquitetura modular e configurável por meio da plataforma *hyperledger fabric*.	**(W4)** Necessidade de governança descentralizada.
	(S5) Dados pessoais off-chain (direito à exclusão e retificação – anonimização).	**(W5)** Resistência institucional.
	(S6) Identidade verificável e controle de acesso.	
	Oportunidades (*opportunities*)	**Ameaças (*threats*)**
Ambiente Externo	**(O1)** Adequação às exigências lgpd e fortalecimento da estrutura de proteção de dados.	**(T1)** Ausência de regulação específica.
	(O2) Expertise de organizações públicas que pesquisam, desenvolvem ou aplicam a tecnologia (tcu, bndes e rfb).	**(T2)** Desafios tecnológicos da era digital (computação quântica e inteligência artificial).
	(O3) Integração digital com o governo federal – alinhamento com a estratégia de governo digital e cumprimento do plano de transformação digital (pdt).	**(T3)** Ataques cibernéticos.
	(O4) Integração com inteligência artificial (utilização de base de dados segura e imutável) e preparação para a web 3.0 (descentralização da internet).	**(T4)** Desafios de integração com sistemas legados.

Fonte: O autor.

Em continuidade à análise, procedeu-se ao cruzamento dos elementos da matriz SWOT, resultando na formulação da matriz TOWS, que permitiu combinar os fatores internos com os fatores externos. A partir dessa matriz, foram gerados códigos identificadores e ações estratégicas específicas, as quais foram organizadas em quatro categorias principais: ofensivas (SO), confrontativas (ST), de reforço (WO) e defensivas (WT), conforme modelo proposto por Weihrich (1982). O desenvolvimento dessas estratégias teve como base a busca por soluções que apresentassem coerência técnica, viabilidade institucional e aderência às necessidades

identificadas no COMAER. Assim, conforme estruturado no Quadro 4, foram selecionadas apenas as estratégias que demonstraram sentido semântico claro e lógica de aplicação prática. Essas ações estratégicas foram posteriormente relacionadas aos *gaps* diagnosticados no Plano de Adequação à LGPD (PCA 16-14/2022), permitindo o alcance do OE2 deste trabalho.

Quadro 4 - Matriz TOWS.

		Análise Interna	
		Forças (*Strengths*)	**Fraquezas (*Weaknesses*)**
Análise Externa	**Oportunidades (*opportunities*)**	**(S1O1)** Aproveitar a imutabilidade para fortalecer a estrutura de proteção dos dados pessoais exigidos pela LGPD	**(W1O2)** Superar a complexidade técnica da arquitetura *blockchain* aproveitando a expertise de organizações públicas que já aplicam a tecnologia.
		(S1O4) Aproveitar a imutabilidade da cadeia de blocos para potencializar a possibilidade de integração com soluções de inteligência artificial.	**(W2O2)** Superar a carência de mão de obra qualificada para operar *blockchain* aproveitando a expertise de organizações públicas que já aplicam a tecnologia.
		(S2O3) Aproveitar a descentralização da rede *blockchain* para potencializar o alinhamento com a Estratégia de Governo Digital.	**(W5O3)** Superar a resistência institucional à adoção de novas tecnologias aproveitando o alinhamento com a Estratégia de Governo Digital.
		(S4O1) Aproveitar a arquitetura modular e configurável da plataforma *Hyperledger Fabric* para ampliar a conformidade com a LGPD e potencializar a governança e fortalecer a estrutura de proteção de dados pessoais.	
		(S4O5) Aproveitar a arquitetura modular e configurável da *blockchain* para promover o alinhamento do COMAER ao Plano de Transformação Digital (PDT)	
		(S5O1) Aproveitar a capacidade de armazenamento *off-chain* para cumprir a anonimização dos dados pessoais e potencializar as conformidades legais junto à LGPD.	
		(S6O1) Aproveitar a identidade verificável e controle de acesso da tecnologia *blockchain* para potencializar as conformidades legais junto à LGPD.	
	Ameaças (*Threats*)	**(S1T3)** Utilizar a imutabilidade da cadeia de blocos para mitigar os efeitos dos ataques cibernéticos contra os sistemas de dados.	**(W1T2)** Minimizar a complexidade técnica da arquitetura *blockchain* para reduzir os impactos dos desafios tecnológicos impostos por novas tecnologias.
		(S2T2) Utilizar a descentralização da rede *blockchain* para aumentar a resiliência cibernética e mitigar os desafios tecnológicos impostos por novas tecnologias.	**(W2T3)** Minimizar a carência de mão de obra qualificada em *blockchain* para reduzir os impactos de os ataques cibernéticos contra sistemas de dados.
		(S3T1) Utilizar a auditabilidade e rastreabilidade da *blockchain* para mitigar os efeitos da ausência de regulação específica sobre *blockchain* e fortalecer a governança interna.	**(W4T1)** Minimizar a ausência de um modelo consolidado de governança descentralizada para reduzir os impactos da ausência de regulação específica sobre *blockchain.*
		(S4T4) Utilizar a arquitetura modular e configurável da *blockchain* para mitigar efeitos dos desafios de integração com sistemas legados.	

Fonte: O autor.

4.3 CORRELAÇÃO E NÍVEL DE ADERÊNCIA

Nesta etapa, foram analisadas as correlações entre os *gaps* no tratamento de dados pessoais identificados (OE1) e as ações estratégicas geradas a partir da matriz TOWS (OE2), resultando nos seguintes níveis de aderência entre eles: alta, média, baixa ou nula.

Para fins de organização e sistematização dos dados, optou-se por elaborar o Quadro 5 para apresentar uma alínea para cada tipo de *gap*, na qual são indicadas as ações estratégicas associadas, a respectiva classificação do nível de aderência e a análise justificativa. Além disso, os níveis de aderência foram identificados pelas seguintes cores: alta (verde), média (azul), baixa (amarela) e nula (laranja).

Quadro 5 – Correlação e aderência das ações estratégicas.

Correlação dos *Gaps* com as Ações Estratégicas	**Qtd.**	**Aderência**
a) Ausência de controles criptográficos (G1); − Estratégia(s): Nenhuma. − Aderência: Nula. − Análise: O controle criptográfico nesse caso é para informar aos titulares em quais circunstâncias que foram utilizadas as criptografias para a proteção dos dados.	1	Nula
b) Ausência de controles de acesso lógico (G2); − Estratégia(s): • Ofensiva(s):S4O1 e S6O1; • Confrontativa(s): S3T1; • Reforço: W1O2 e W2O2; e • Defensiva: W4T1. − Aderência: Alta. − Análise: O tipo de arquitetura modular e configurável, somada à capacidade de identidade verificável, controle de acesso, auditoria e rastreabilidade, fortalecem a governança e a segurança de acesso. Além disso, as estratégias apontam para superação da complexidade técnica da capacitação de mão de obra com o apoio de organizações com expertise no desenvolvimento da tecnologia. Por fim, a criação de normativos internos e de protocolos de governança evidencia o esforço institucional do COMAER em aperfeiçoar seus processos de controle e acesso lógico.	2	Alta
c) Ausência de controles de segurança em redes, proteção física e do ambiente (G3); − Estratégia(s): • Ofensiva(s): S1O1; e • Confrontativa(s): S2T2 e S1T3. − Aderência: Alta. − Análise: Esse controle refere-se à ausência de medidas de segurança tanto no plano físico quanto no lógico. A tecnologia blockchain, por sua arquitetura descentralizada, contribui significativamente para a elevação da resiliência cibernética, reduz a possibilidade de corrupção dos dados, viabiliza trilhas de auditoria imutáveis e elimina o ponto único de falha – característica comum em ambientes em que servidores e backups coexistem fisicamente. No que se refere às informações armazenadas em formato físico (papel), recomenda-se a digitalização e posterior integração à rede blockchain.	3	Alta

d) ausência de mecanismos de desenvolvimento seguro (G4); − Estratégia(s): • Ofensiva(s): S4O1 e S6O1; • Confrontativa(s): S4T4; e • Defensiva: W2T3. − Aderência: Alta. − Análise: Esse controle refere-se à inexistência de práticas e mecanismos voltados ao desenvolvimento seguro de sistemas e softwares utilizados no ambiente organizacional. O modelo proposto nesta pesquisa – baseado na blockchain permissionada do tipo consórcio, com uso da plataforma Hyperledger Fabric – configura-se como uma alternativa tecnológica viável, passível de ser explorada pelo COMAER, desde que observados critérios técnicos e orçamentários. As estratégias selecionadas indicam aderência tanto sob o ponto de vista da coerência técnica quanto da conformidade legal, demonstrando o potencial da solução para mitigar o gap em questão de forma estruturada e alinhada às exigências da LGPD.	2	Alta
e) ausência de mecanismos para registro de eventos, rastreabilidade e salvaguarda de logs (G5); − Estratégia(s): • Ofensiva(s): S1O1 e S6O1; • Confrontativa(s): S4T4; e • Defensiva: W4T1. − Aderência: Alta. − Análise: A tecnologia blockchain, ao incorporar atributos como imutabilidade, descentralização, criptografia e encadeamento de blocos por meio de hashes, assegura a integridade dos registros, impedindo sua exclusão ou alteração não autorizada. Isso permite a criação de trilhas de auditoria robustas, com registro automático e confiável de todos os eventos de acesso e autorização. No contexto da LGPD, a exclusão ou modificação de dados pessoais (como no caso da anonimização) deve ocorrer fora da cadeia de blocos, exigindo que as organizações estabeleçam normativos internos que regulamentem, de forma clara, as ações dos agentes de tratamento (controladores, operadores e encarregados). Além disso, a arquitetura modular e configurável da blockchain analisada pode facilitar sua integração com sistemas legados, contribuindo para a adequação progressiva da infraestrutura do COMAER às exigências legais.	3	Alta
f) Ausência de mecanismos para garantir a segurança web (G6); − Estratégia(s): • Ofensiva(s): S1O1, S4O1 e S6O1; • Confrontativa(s): S2T2; e • Reforço: W1O2 e W2O. − Aderência: Alta. − Análise: A característica de imutabilidade da blockchain contribui para o fortalecimento da proteção dos dados, assegurando que informações registradas não possam ser alteradas ou excluídas de forma indevida. Além disso, a adoção de contratos inteligentes possibilita a criação de regras automatizadas de acesso, rastreamento e autorização de dados, especialmente em contextos que envolvam o uso de redes externas, como a internet pública. A arquitetura modular e configurável da blockchain proposta nesta pesquisa permite sua adaptação às exigências normativas e técnicas relacionadas à segurança digital, oferecendo flexibilidade na implementação de camadas adicionais de proteção.	4	Alta
g) Ausência de procedimento de resposta a incidentes (G7); − Estratégia(s): • Defensiva: W4T1 − Aderência: Baixa − Análise: Embora a tecnologia blockchain possua características que fortaleçam a proteção dos dados – como imutabilidade, rastreabilidade e descentralização –, sua aplicação isolada não é suficiente para suprir a ausência de procedimentos formais de resposta a incidentes. A LGPD exige que as organizações estabeleçam protocolos claros para o tratamento de eventos que comprometam a segurança dos dados pessoais. Assim, torna-se imprescindível a criação de normativos internos e planos de ação específicos, que definam responsabilidades, prazos e medidas corretivas.	1	Baixa

h) Ausência de mecanismos de conscientização sobre a importância da privacidade e segurança da informação (G8); − Estratégia(s): • Reforço: W5O3; e • Defensiva: W2T3. − Aderência: Nula; − Análise: Embora algumas estratégias selecionadas proponham o enfrentamento da resistência institucional e a implementação de programas contínuos de capacitação, não foi observada, na prática, uma aderência efetiva às exigências específicas desse controle. Isso ocorre porque tais estratégias carecem de ações estruturadas que promovam, de forma contínua e institucionalizada, a mudança de cultura organizacional necessária para o cumprimento dos princípios da LGPD.	2	Nula
i) Ausência de mecanismos de consentimento e escolha (G9); − Estratégia(s): • Ofensiva(s): S4O1; e • Confrontativa(s): S4T4. − Aderência: Média. − Análise: A arquitetura modular e configurável da blockchain baseada no Hyperledger Fabric possibilita a criação de mecanismos que conferem maior autonomia ao titular dos dados, permitindo, por exemplo, o gerenciamento de consentimentos e a modificação ou revogação de permissões previamente concedidas. No entanto, este controle exige, além da solução tecnológica, a implementação de procedimentos normativos específicos por parte do COMAER para registrar e comprovar o consentimento. Conforme disposto na LGPD, "o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (Brasil, 2018).	3	Média
j) Ausência de mecanismos para garantir a precisão e a qualidade (G10); − Estratégia(s): • Ofensiva(s): S1O1, S2O3, S4O1, S4O5 e S6O1; • Confrontativa(s): S3T1, S2T2, S4T4; • Reforço:W1O2 e W2O2; e • Defensiva: W1T2, W2T3 e W4T1. − Aderência: Alta. − Análise: As estratégias associadas apresentam alta aderência por estarem fortemente alinhadas às propriedades técnicas da blockchain proposta neste estudo. A imutabilidade garante que os dados registrados não sejam alterados indevidamente; a criptografia e a proteção dos dados asseguram sua integridade; a rastreabilidade e a auditabilidade permitem o acompanhamento e verificação dos registros ao longo do tempo; e a possibilidade de anonimização, conforme previsto na LGPD, contribui para a preservação da privacidade. Além disso, a arquitetura modular e configurável favorece a adequação da solução às exigências institucionais e legais específicas.	3	Alta
k) Ausência de medidas de responsabilização (G11); − Estratégia(s): • Ofensiva(s): S6O1; • Confrontativa(s): S3T1; e − Defensiva: W4T1. − Aderência: Alta. − Análise: A arquitetura de blockchain proposta nesta pesquisa permite a verificação de identidade, o registro imutável das ações executadas e a rastreabilidade completa das operações. Esses atributos possibilitam a criação de trilhas de auditoria seguras e confiáveis, que vinculam ações a responsáveis identificáveis. Dessa forma, as estratégias contribuem para a transparência, promovendo maior controle, supervisão e governança sobre o ciclo de vida dos dados pessoais.	7	Alta
l) Ausência de medidas para assegurar a limitação da coleta (G12); − Estratégia(s): Não há. − Aderência: Nula. − Análise: Este controle refere-se à aplicação do princípio da necessidade previsto na LGPD, segundo o qual apenas os dados estritamente necessários à finalidade do tratamento devem ser coletados. A definição de quais dados são essenciais cabe aos ODGSA, por meio da formalização de critérios e diretrizes internas. Embora a	1	Nula

tecnologia blockchain proposta possua mecanismos que permitem a anonimização e a atualização de dados, sua aplicação não atua diretamente na etapa inicial de coleta dos dados.		
m) Ausência de medidas para assegurar o compliance com a privacidade (G13); − Estratégia(s): • Ofensiva(s):S1O1 e S5O1; • Confrontativa(s): S3T1; • Reforço(s): W5O3; e • Defensiva(s): W4T1. − Aderência: Alta. − Análise: O cumprimento das exigências legais relacionadas à privacidade, conforme estabelecido pela LGPD, requer a adoção de mecanismos que garantam o controle, a rastreabilidade e a limitação no tratamento de dados pessoais. A tecnologia blockchain, por meio da imutabilidade dos registros, possibilita a verificação de acessos e a identificação dos agentes que realizaram operações sobre os dados, assegurando transparência e prestação de contas. Além disso, a possibilidade de armazenamento de dados sensíveis em ambientes off-chain permite a adoção de medidas como a anonimização ou pseudonimização, conforme previsto na legislação, atendendo às exigências relativas ao ciclo de vida do dado.	34	Alta
n) Ausência de medidas para garantir a abertura, transparência e notificação (G14); − Estratégia(s): • Ofensiva(s):S4O1 e S5O1; • Confrontativa(s):S3T1 e S1T5; e • Defensiva(s):W1T2. − Aderência: Alta. − Análise: Este controle refere-se à obrigatoriedade de garantir abertura, transparência e notificação aos titulares de dados pessoais, conforme determina a LGPD. Parte dessa lacuna pode ser suprida por medidas administrativas, como a inclusão de avisos de privacidade (privacy notices) em formulários físicos, eletrônicos ou páginas web, o que não demanda, necessariamente, uma solução tecnológica. Contudo, no que se refere à efetiva abertura para que o titular visualize, altere ou solicite a exclusão de seus dados, a arquitetura modular e configurável da blockchain permissionada Hyperledger Fabric permite a integração com camadas externas (off-chain). Adicionalmente, a criação de protótipos antes da implementação final da solução contribui para a identificação e correção de falhas críticas, promovendo maior transparência e previsibilidade no processo.	31	Alta
o) Ausência de tabela de temporalidade e destinação final definidas (G15); − Estratégia(s): • Ofensiva(s): S5O1; e • Confrontativa(s):S3T1, S4T4 S1T5; − Aderência: Média. − Análise: Este controle diz respeito à ausência de definição formal sobre a temporalidade dos dados pessoais – ou seja, o prazo de retenção e a destinação final após o término do tratamento, conforme preconiza a LGPD. A responsabilidade por estabelecer tais prazos cabe a cada ODGSA, por meio da elaboração de tabelas de temporalidade e critérios claros de descarte ou anonimização. A tecnologia blockchain, embora não permita a exclusão de dados armazenados na própria cadeia de blocos (on-chain), possibilita o uso de estruturas complementares fora da cadeia de blocos (off-chain), permitindo a anonimização ou descarte dos dados quando ultrapassado o período necessário. Além disso, os mecanismos de rastreabilidade e auditabilidade inerentes à arquitetura blockchain fornecem a transparência e a credibilidade necessárias para comprovar o cumprimento das políticas de retenção de dados. Diante disso, a tecnologia oferece meios auxiliares ao atendimento do controle, mas exige, a implementação de medidas administrativas e normativas específicas por parte da organização.	32	Média

Fonte: O autor.

Com base na análise de correlação entre os *gaps* identificados no tratamento de dados pessoais no COMAER e as ações estratégicas derivadas da matriz TOWS, foi possível atingir

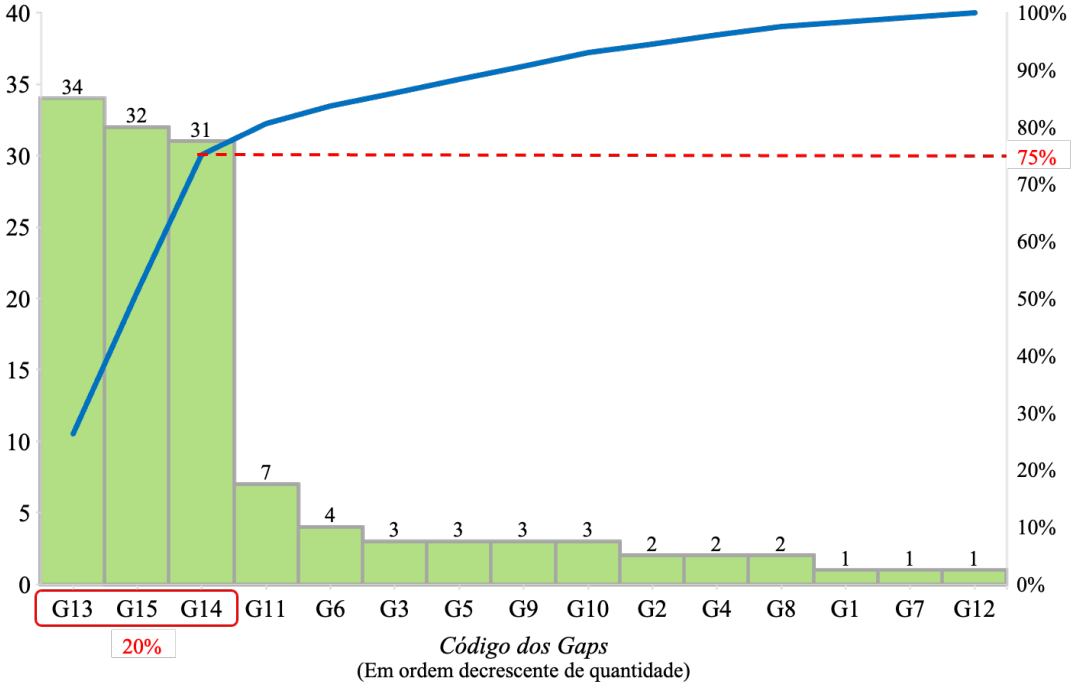
o OE3 e classificar os níveis de aderência observados no universo das 129 fichas de controle do PCA 16-14/2022. Assim, os resultados obtidos foram:

a) 89 fichas de controle apresentaram alta aderência, correspondendo a 68,9%;
b) 35 fichas de controle apresentaram aderência média, representando 27,1%;
c) 1 ficha de controle apresentou baixa aderência, equivalente a 0,8%; e
d) 4 fichas de controle apresentaram aderência nula, totalizando 3,2%.

4.4 ANÁLISE DOS RESULTADOS

Durante o processo de identificação dos *gaps* no tratamento de dados pessoais no COMAER com base no PCA 16-14/2022 (OE1), observou-se a ocorrência do fenômeno descrito pela regra 80/20. Conhecida também como princípio de Pareto, essa regra estabelece que, em muitos sistemas, cerca de 80% dos efeitos decorrem de aproximadamente 20% das causas. (Santos *et al*., 2015). Assim, conforme Quadro 2, verificou-se que três dos quinze tipos de *gaps* (20%) no tratamento de dados pessoais – G13, G14 e G15 – corresponderam a 75% das fichas de controle, conforme demonstrado no Gráfico 1. Essa interpretação dos resultados vinculados ao OE1, ainda que analisada de forma isolada em relação aos demais objetivos específicos, resultou em uma inferência que oferece ao COMAER uma possibilidade de ação autônoma, não condicionada à adoção da tecnologia *blockchain*, permitindo a priorização de esforços na mitigação dos *gaps* mais recorrentes.

Gráfico 1 - Diagrama de pareto



Fonte: O autor.

Em seguida, ao analisar os dados referentes aos níveis de aderência, constatou-se que os controles inicialmente classificados com aderência média concentravam-se, principalmente, nos *gaps* G9 e G15. Esses *gaps*, relacionados, respectivamente, à ausência de mecanismos de consentimento e escolha, e à ausência de tabela de temporalidade e destinação final definidas, foram influenciados por fatores ligados à governança e aos processos internos dos ODGSA, cuja superação dependia da implementação de ações administrativas simples. Dessa forma, considerando-se a adoção dessas ações por parte dos ODGSA, procedeu-se à reavaliação dos 35 controles inicialmente classificados com aderência média. Após essa análise, tais controles passaram a ser considerados como de alta aderência, elevando o total para 124, o que representa 96,1% do universo avaliado. Assim, o Quadro 6 representa uma síntese da correlação das ações estratégicas e os *gaps* identificados no tratamento de dados pessoais com os níveis de aderência reavaliados.

Quadro 6 - Nível de aderência das estratégias.

Classificação	**Tipos *gap* no tratamento de dados pessoais (código)**	**Ficha de Controle (frequência)**	**Nível de Aderência**
Segurança 12% (16)	Ausência de controles criptográficos (G1)	1	Nula
	Ausência de controles de acesso lógico (G2)	2	Alta
	Ausência de controles de segurança em redes, proteção física e do ambiente (G03)	3	Alta
	Ausência de mecanismos de desenvolvimento seguro (G4)	2	Alta
	Ausência de mecanismos para registro de eventos, rastreabilidade e salvaguarda de logs (G5)	3	Alta
	Ausência de mecanismos para garantir a segurança web (G6)	4	Alta
	Ausência de procedimento de resposta a incidentes (G7)	1	Baixa
Privacidade 88% (113)	Ausência de mecanismos de conscientização sobre a importância da privacidade e segurança da informação (G8)	2	Nula
	Ausência de mecanismos de consentimento e escolha (G9)	3	Alta
	Ausência de mecanismos para garantir a precisão e a qualidade (G10)	3	Alta
	Ausência de medidas de responsabilização (G11)	7	Alta
	Ausência de medidas para assegurar a limitação da coleta (G12)	1	Nula
	Ausência de medidas para assegurar o compliance com a privacidade (G13)	34	Alta
	Ausência de medidas para garantir a abertura, transparência e notificação (G14)	31	Alta
	Ausência de tabela de temporalidade e destinação final definidas (G15)	32	Alta
Total de fichas de controle de *gaps*		129	

Fonte: O autor.

O resultado obtido corrobora a ideia destacada por Gurel e Tat (2017, p. 100, tradução nossa) sobre “a capacidade de transformar o diagnóstico em planos de ação concretos, direcionando decisões e priorizando os recursos”.

Por fim, a arquitetura da tecnologia *blockchain* adotada nesta pesquisa, conforme proposta de Gonçalves, Da Silva e Da Cunha (2024), apresentou potencial para impactar positivamente, com **alta aderência**, em **96,1%** dos *gaps* relativos ao tratamento de dados pessoais identificados no PCA 16-14/2022. Com esse resultado, o objetivo geral deste trabalho foi plenamente alcançado e o problema de pesquisa respondido.

5 CONCLUSÃO

O objetivo deste trabalho foi analisar de que maneira a implementação da tecnologia *blockchain* pode impactar os *gaps* no tratamento de dados pessoais identificados no Plano de Adequação à Lei Geral de Proteção de Dados (PCA 16-14/2022), elaborado pelo COMAER.

Quanto à fundamentação teórica, este trabalho foi estruturado em três eixos: o primeiro abordou os principais fundamentos legais da LGPD e o embasamento e diagnóstico realizado pelo PCA 16-14/2022. O segundo analisou a tecnologia *blockchain*, tendo como principal referência a proposta de Gonçalves, Da Silva e Da Cunha (2024), propondo um modelo capaz de garantir segurança, rastreabilidade e conformidade legal. O terceiro eixo apresentou as matrizes SWOT e TOWS como instrumentos metodológicos para gerar estratégias de mitigação dos *gaps* mapeados, fundamentadas em autores como Weihrich (1982) e Gurel e Tat (2017).

Para responder ao problema de pesquisa, foram definidos três objetivos específicos. O primeiro consistiu na identificação dos *gaps* no tratamento de dados pessoais do COMAER com base no PCA 16-14/2022 (OE1). Durante a identificação dos *gaps* foram observados 15 tipos de inconformidades organizadas em 129 fichas de controle. Destas, 88% referiam-se à privacidade e 12% à segurança da informação, o que proporcionou o alcance do objetivo específico 1.

O segundo objetivo específico identificou as ações estratégicas para a mitigação dos *gaps* identificados no tratamento de dados pessoais no COMAER (OE2). Nesta etapa, com base nas características da *blockchain* propostas por Gonçalves, Da Silva e Da Cunha (2024), foi estruturada uma matriz SWOT para identificar forças, fraquezas, oportunidades e ameaças relacionadas à adoção da tecnologia no contexto institucional do COMAER. O cruzamento

entre esses fatores resultou na matriz TOWS, resultando nas ações estratégicas ofensivas, confrontativas, de reforço e defensivas.

O terceiro objetivo consistiu em correlacionar as ações estratégicas, geradas a partir da matriz TOWS, com os *gaps* no tratamento de dados pessoais no COMAER (OE3). Essa etapa permitiu classificar, por meio de análise, as **aderências** entre as estratégias e os *gaps* em quatro níveis: alta, média, baixa e nula. Dessa maneira, observou-se que 89 controles apresentaram alta aderência (68,9%), 35 resultaram em aderência média (27,1%), 1 controle foi classificado com baixa aderência (0,8%) e 4 controles apresentaram aderência nula (3,2%).

Posteriormente, quanto à análise dos dados obtidos, observou-se a incidência do Princípio de Pareto (80/20), com os *gaps* G13, G14 e G15 concentrando 75% das fichas de controle, evidenciando uma prioridade estratégica para o processo de mitigação dos *gaps*. Em seguida, ao analisar os dados referentes aos níveis de aderência, constatou-se que os controles inicialmente classificados como de aderência média associados a fatores relacionados à governança e a processos internos dos ODGSA, dependiam de ações administrativas simples. A partir dessa reclassificação, constatou-se que 124 controles (96,1%) apresentavam alta aderência com a implementação do modelo de tecnologia *blockchain* proposta por Gonçalves, Da Silva e Da Cunha (2024). Dessa forma, concluiu-se que a arquitetura da *blockchain* adotada nesta pesquisa apresentou potencial para impactar positivamente, com **alta aderência**, em **96,1%** dos *gaps* no tratamento de dados pessoais identificados no PCA 16-14/2022. Assim, o objetivo geral deste trabalho foi plenamente alcançado e o problema de pesquisa respondido.

Como contribuição para a Força Aérea Brasileira, este trabalho propõe uma tecnologia ainda pouco explorada no ambiente militar, mas que tem demonstrado potencial de desenvolvimento e superação de desafios na era digital. A proposta de implementação da *blockchain* para enfrentar os desafios impostos pela LGPD representa apenas uma das possibilidades de aplicação dessa ferramenta, cujas características incluem imutabilidade, resiliência cibernética, rastreabilidade e transparência dos registros. Os resultados também fortalecem a governança digital institucional e alinham o COMAER às diretrizes da Estratégia de Governo Digital, promovendo maior controle, eficiência e governança.

Entre as principais limitações desta pesquisa, destaca-se a ausência de validação prática da solução proposta e a não realização de entrevistas com especialistas ou operadores da LGPD, o que restringe a generalização dos resultados. Além disso, a escolha por uma única arquitetura de *blockchain* e a não exploração de outras soluções indicam outra limitação desta pesquisa.

Como sugestões para pesquisas futuras, recomenda-se a realização de estudos empíricos com testes práticos da tecnologia em ambientes institucionais da FAB, bem como comparações

entre diferentes arquiteturas *blockchain* e suas integrações com sistemas adjuntos já utilizados pelo COMAER. Além disso, as análises realizadas neste estudo evidenciaram a viabilidade de aplicação da tecnologia blockchain em outras áreas institucionais, tais como: na logística, com foco no rastreamento e controle de materiais e componentes de interesse do COMAER; no setor de saúde, para apoiar a gestão de prontuários dos usuários do Fundo de Saúde de Aeronáutica (FUNSA); e na área de gestão de recursos humanos, com vistas à integridade, segurança e rastreabilidade das informações e histórico de todos os militares. Ademais, estudos futuros para a adoção da *blockchain* em conjunto pelos ODGSA poderá viabilizar sua exploração como uma solução de arquitetura mais descentralizada, promovendo maior segurança da informação e resiliência cibernética. Tais atributos tornam-se especialmente relevantes para sua aplicação em sistemas estratégicos da Força Aérea Brasileira, como o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA) e o Sistema de Material Aeronáutico e Bélico (SISMAB), à semelhança do que já vem sendo desenvolvido por instituições como a DARPA e a OTAN (Ahmad, 2021).

REFERÊNCIAS

AHMAD, R. W. *et al*. Blockchain for aerospace and defense: Opportunities and open research challenges. **Computers & Industrial Engineering**, v. 151, p. 106982, jan. 2021.

BNDES e TCU se unem para criar a Rede Blockchain Brasil. Exame, 30 maio 2022. Disponível em: https://exame.com/future-of-money/bndes-e-tcu-se-unem-para-criar-a-rede-blockchain-brasil/. Acesso em: 4 jun. 2025.

BHUTTA, M. N. M. *et al*. A Survey on Blockchain Technology: Evolution, Architecture and Security. **IEEE Access**, v. 9, p. 61048–61073, 2021.

BRASIL. Agência Nacional de Aviação Civil. **ANAC autoriza Diário de Bordo Eletrônico para aviação geral**. Brasília, 22 nov. 2022. Disponível em: https://www.gov.br/anac/pt-br/noticias/2022/anac-autoriza-diario-de-bordo-eletronico-para-aviacao-geral. Acesso em: 14 jun. 2025.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria nº31/CEMAER, de 25 de agosto de 20222. Aprova a reedição do Plano que dispõe sobre a adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados Pessoais - PCA 16-14/2022. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 163, f. 12510, 30 ago. 2022.

BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Aprova a Estratégia de Governo Digital para o período de 2020 a 2022 e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 29 abr. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254711358. Acesso em: 22 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709 compilado.htm. Acesso em: 10 mar. 2025.

GONÇALVES, R. M.; DA SILVA, M. M.; DA CUNHA, P. R. Olympus: a GDPR compliant blockchain system. **International Journal of Information Security**, v. 23, n. 2, p. 1021–1036, 1 abr. 2024. Disponível em: https://link.springer.com/article/10.1007/s10207-023-00782-z. Acesso em: 4 mar. 2025.

GUREL, E.; TAT, M. SWOT Analysis: a Theoretical Review. **Journal of International Social Research**, v. 10, n. 51, p. 994–1006, ago. 2017.

HAN, Sejin; PARK, Sooyong. A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review. **IEEE Access**, v. 10, p. 103888–103905, 2022.

KOSSOW, Niklas. **Beyond the Hype: Distributed Ledger Technology in the Field of Public Administration**. 2019.

KREY, V. G. **Impactos das legislações de proteção de dados pessoais a tecnologia blockchain**. 2021.

MARTÍNEZ LAOSA, Belén. **Blockchain within Logistics: a SWOT analysis**. 2019. Dissertação de Mestrado. Universitat Politècnica de Catalunya.

NAKAMOTO, S. **Bitcoin: a peer-to-peer electronic cash system**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 7 mar. 2025.

NIRANJANAMURTHY, M.; NITHYA, B. N.; JAGANNATHA, S. Analysis of Blockchain technology: pros, cons and SWOT. **Cluster Computing**, v. 22, n. S6, p. 14743–14757, nov. 2019.

SANTOS, A. *et al.* **Utilização da ferramenta Diagrama de Pareto para auxiliar na identificação dos principais problemas nas empresas**. Disponível em: https://unisalesiano.com.br/aracatuba/wp-content/uploads/2020/12/Artigo-Utilizacao-da-ferramenta-Diagrama-de-Pareto-para-auxiliar-na-identificacao-dos-principais-problemas-nas-empresas-Pronto.pdf. Acesso em: 7 jun. 2025.

SURIPEDDI, M. K. S.; PURANDARE, P. Blockchain and GDPR: A study on compatibility issues of the distributed ledger technology with GDPR data processing. **Journal of Physics: Conference Series**, v. 1964, n. 4, p. 42005, 2021.

SWAN, Melanie. **Blockchain: blueprint for a new economy**. First edition ed. Sebastopol, Calif: O'Reilly, 2015.

TAPSCOTT, A. **Web3: charting the internet's next economic and cultural frontier**. New York: Harper Business, 2023.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world**. New York: Portfolio Penguin, 2016.

WEIHRICH, Heinz. The TOWS matrix – A tool for situational analysis. **Long Range Planning**, v. 15, n. 2, p. 54–66, 1 abr. 1982.

ZAFAR, A. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. **Journal of Cybersecurity**, v. 11, n. 1, 17 jan. 2025.