

UNIVERSIDADE FEDERAL DE OURO PRETO  
Centro de Educação Aberta e a Distância  
Departamento de Gestão Pública

Marcos Henrique Pereira da Silva  
Augusto Ferreira Tassar

GOVERNANÇA DIGITAL E TRANSPARÊNCIA PÚBLICA NO BRASIL: Desafios,  
Oportunidades e Impactos da Implementação de Tecnologias na Gestão Pública.

Ouro Preto  
2025

Marcos Henrique Pereira da Silva  
Augusto Ferreira Tassar

GOVERNANÇA DIGITAL E TRANSPARÊNCIA PÚBLICA NO BRASIL: Desafios,  
Oportunidades e Impactos da Implementação de Tecnologias na Gestão Pública.

Trabalho de Conclusão apresentado na modalidade de Trabalho de Conclusão de Curso ao Curso de Administração Pública da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Administração Pública.

Orientador: Prof. Dr. Wellington Tavares

Ouro Preto  
2025

## SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

T211g Tassar, Augusto Ferreira.

Governança digital e transparência pública no Brasil [manuscrito]: desafios, oportunidades e impactos da implementação de tecnologias na gestão pública. / Augusto Ferreira Tassar. Marcos Henrique Pereria da Silva. - 2025.

26 f.: il.: tab..

Orientador: Prof. Dr. Wellington Tavares.

Monografia (Bacharelado). Universidade Federal de Ouro Preto. Centro de Educação Aberta e a Distância. Graduação em Administração Pública .

1. Governança pública - Brasil. 2. Tecnologia da informação - Brasil. 3. Transparência na administração pública - Brasil. I. Silva, Marcos Henrique Pereria da. II. Tavares, Wellington. III. Universidade Federal de Ouro Preto. IV. Título.

CDU 35(815.1)

Bibliotecário(a) Responsável: Essevalter De Sousa - Bibliotecário Coordenador  
CBICSA/SISBIN/UFOP-CRB6a1407



## FOLHA DE APROVAÇÃO

**Augusto Ferreira Tassar**  
**Marcos Henrique Pereira da Silva**

### **Governança digital e transparência pública no Brasil: desafios, oportunidades e impactos da implementação de tecnologias na gestão pública**

Monografia apresentada ao Curso de Administração Pública, modalidade a distância, da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Administração Pública

Aprovada em 07 de julho de 2025

#### Membros da banca

Prof. Dr. Wellington Tavares - Orientador (Universidade Federal de Ouro Preto)  
Prof. Dr. Lelis Maia de Brito - (Universidade Federal de Ouro Preto)

Wellington Tavares, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 07/07/2025



Documento assinado eletronicamente por **Wellington Tavares, PROFESSOR DE MAGISTERIO SUPERIOR**, em 18/07/2025, às 16:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [http://sei.ufop.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0944396** e o código CRC **7E8D53F9**.

## RESUMO

Este trabalho tem como objetivo analisar os impactos da governança digital na promoção da transparência pública no Brasil, destacando os desafios, oportunidades e impactos da implementação de tecnologias na gestão pública. A pesquisa parte da premissa de que a adoção de ferramentas digitais pode contribuir significativamente para o fortalecimento da democracia, ao proporcionar maior acesso à informação e possibilitar uma gestão mais eficiente e participativa. A metodologia utilizada foi qualitativa, fundamentada na análise documental de legislações, relatórios oficiais e plataformas governamentais, além da revisão bibliográfica de autores nacionais e internacionais. Os resultados indicam que houve avanços institucionais importantes, como a criação da plataforma Gov.br e a aplicação de normas como a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD). No entanto, ainda persistem desafios como a desigualdade no acesso à internet, a defasagem tecnológica, a resistência institucional à mudança e a ausência de uma cultura de segurança digital. A análise também evidenciou que a participação cidadã é impactada pela forma como os dados públicos são disponibilizados, sendo necessário investir em acessibilidade e educação digital. Comparações com experiências internacionais demonstram que o Brasil ainda está em processo de consolidação de sua governança digital, especialmente no que se refere à integração de sistemas e à centralidade do cidadão. Conclui-se que, embora o país tenha avançado em termos normativos e tecnológicos, a plena efetivação da transparência pública digital requer planejamento estratégico, capacitação de servidores e engajamento social contínuo. Este estudo contribui para a compreensão do papel das tecnologias na transformação da administração pública, destacando a importância de políticas públicas inclusivas, seguras e orientadas à participação cidadã.

**Palavras-chave:** governança digital; transparência pública; administração pública; tecnologia da informação; participação cidadã.

## ABSTRACT

This paper aims to analyze the impacts of digital governance on the promotion of public transparency in Brazil, highlighting the challenges, opportunities, and effects of implementing technologies in public administration. The research is based on the premise that the adoption of digital tools can significantly contribute to strengthening democracy by providing greater access to information and enabling more efficient and participatory management. The methodology used was qualitative, based on document analysis of legislation, official reports, and government platforms, as well as a literature review of national and international authors. The results indicate significant institutional progress, such as the creation of the Gov.br platform and the enforcement of laws like the Access to Information Law (LAI) and the General Data Protection Law (LGPD). However, challenges remain, such as inequality in internet access, technological obsolescence, institutional resistance to change, and the lack of a digital security culture. The analysis also revealed that citizen participation is affected by how public data is made available, making it necessary to invest in accessibility and digital education. Comparisons with international experiences show that Brazil is still in the process of consolidating its digital governance, especially regarding system integration and citizen-centric policies. It is concluded that, although the country has made progress in regulatory and technological terms, the full realization of digital public transparency requires strategic planning, continuous training of public servants, and active social engagement. This study contributes to the understanding of the role of technology in transforming public administration, highlighting the importance of inclusive, secure, and citizen-oriented public policies.

**Keywords:** digital governance; public transparency; public administration; information technology; citizen participation.

## LISTA DE ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados

CGU – Controladoria-Geral da União

DPO – Data Protection Officer (Encarregado pelo Tratamento de Dados Pessoais)

Ex. – Exemplo

FGV – Fundação Getúlio Vargas

IBGE – Instituto Brasileiro de Geografia e

Estatística ISO – International Organization for

Standardization LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados

ONU – Organização das Nações Unidas

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OEA – Organização dos Estados Americanos

Org. – Organizador

EGD – Estratégia de Governo Digital

## **LISTA DE SIGLAS**

ABNT – Associação Brasileira de Normas Técnicas  
ANPD – Autoridade Nacional de Proteção de  
Dados CGU – Controladoria-Geral da União  
CSIRT – Computer Security Incident Response  
Team DDoS – Distributed Denial of Service  
DPO – Data Protection Officer  
GDPR – General Data Protection Regulation  
IBGE – Instituto Brasileiro de Geografia e Estatística  
ISO/IEC 27001 – Norma Internacional de Gestão de Segurança da Informação  
LAI – Lei de Acesso à Informação  
LGPD – Lei Geral de Proteção de Dados  
OCDE – Organização para a Cooperação e Desenvolvimento Econômico  
OEA – Organização dos Estados Americanos  
ONU – Organização das Nações Unidas  
SOC – Security Operations Center  
STJ – Superior Tribunal de Justiça  
TJRS – Tribunal de Justiça do Estado do Rio Grande do Sul

## SUMÁRIO

<b>1 INTRODUÇÃO</b>	7
<b>2 REFERENCIAL TEÓRICO</b>	8
2.1 Evolução Histórica da Governança Digital	8
2.2 Modelos e Abordagens na Administração Pública	9
2.3 Segurança da Informação e Proteção de Dados na Gestão Pública	11
2.4 Impactos e Benefícios da Governança Digital	12
2.5 Ameaças Cibernéticas	13
<b>3 METODOLOGIA</b>	15
<b>4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS</b>	18
4.1 Avanços Institucionais na Governança Digital	18
4.2 Desafios Estruturais e Regionais	19
4.3 Transparência Ativa e Participação Cidadã	19
4.4 Segurança da Informação e Conformidade com a LGPD	19
<b>5 CONSIDERAÇÕES FINAIS</b>	20
<b>REFERÊNCIAS</b>	23

## 1 INTRODUÇÃO

A modernização dos processos administrativos e a busca por transparência na gestão pública tornaram-se temas centrais no debate acadêmico e governamental, especialmente com a ascensão das tecnologias digitais (Meijer, 2015; Zuiderwijk & Janssen, 2014). No Brasil, a implementação de ferramentas tecnológicas voltadas à melhoria da transparência e da governança pública tem sido impulsionada por exigências legais e demandas sociais cada vez mais complexas (SOUZA, 2022).

A transparência na administração pública, embora não seja um conceito recente, assume novas dimensões com o uso das tecnologias da informação e comunicação (TICs). Essas tecnologias ampliam o acesso da sociedade às informações governamentais e possibilitam novas formas de participação social (JANSSEN; MATHEUS; WEERAKKODY, 2017). No entanto, essa evolução tecnológica levanta questões importantes sobre como e em que medida as ferramentas digitais realmente favorecem práticas mais transparentes e democráticas na gestão pública.

Nesse sentido, a presente pesquisa parte do seguinte problema: Como a adoção de tecnologias digitais na administração pública pode contribuir para o fortalecimento da transparência e da participação cidadã no Brasil? A formulação dessa questão busca compreender o papel das ferramentas digitais sem pressupor previamente suas limitações ou virtudes, permitindo uma análise crítica e fundamentada sobre o tema.

O objetivo geral deste estudo é compreender de que forma as tecnologias digitais estão sendo utilizadas para promover a transparência pública no Brasil, especialmente no contexto da administração pública. Os objetivos específicos incluem: (I) investigar o papel das tecnologias digitais na modernização dos processos administrativos; (II) identificar os principais desafios enfrentados pelos órgãos públicos na adoção de práticas digitais transparentes; (III) analisar o papel das legislações como a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD); (IV) examinar experiências nacionais e internacionais que possam servir de referência; e (V) propor caminhos e recomendações para o aprimoramento da governança digital no setor público brasileiro.

A relevância do tema se justifica pela urgência em aprimorar a gestão pública frente a um cenário de desconfiança institucional e crescente cobrança social por maior eficiência e prestação de contas (OCDE, 2021). Além disso, a transformação digital no setor público

constitui um campo em expansão, que carece de análises críticas sobre suas práticas, limitações e potencialidades (SILVA, 2015).

Modelos internacionais, como o da Estônia, servem como referência para o debate global sobre governo digital (OEA, 2022). No Brasil, plataformas como o Portal da Transparência e o Gov.br têm sido destacados como marcos importantes no avanço da governança eletrônica (CGU, 2024). No entanto, persistem lacunas que precisam ser investigadas, especialmente no que diz respeito à acessibilidade, à inclusão digital e à capacidade dos entes públicos de utilizarem adequadamente essas ferramentas.

Este Trabalho de Conclusão de Curso está estruturado em cinco capítulos. O Capítulo 1 apresenta a introdução, abordando o tema, a delimitação da problemática, os objetivos, a justificativa e a organização do trabalho. O Capítulo 2 trata do referencial teórico, discutindo os principais conceitos relacionados à governança digital, transparência pública e proteção de dados. O Capítulo 3 descreve a metodologia adotada, detalhando as etapas de coleta e análise de dados. O Capítulo 4 apresenta e discute os principais resultados, com foco nos avanços, limitações e implicações práticas observadas. Por fim, o Capítulo 5 apresenta as considerações finais, com reflexões sobre os achados e sugestões para futuras pesquisas.

## **2 REFERENCIAL TEÓRICO**

Este capítulo tem como objetivo apresentar a fundamentação teórica que embasa a pesquisa, explorando conceitos essenciais para a compreensão da transparência na gestão pública e os desafios da implementação digital. Serão abordados temas como governança digital, transparência pública, segurança da informação e os impactos da tecnologia na administração pública.

### **2.1 Evolução Histórica da Governança Digital**

A governança digital surgiu como uma resposta à crescente demanda por transparência, eficiência e participação cidadã na administração pública, especialmente a partir do advento da internet nos anos 1990. De acordo com Janowski (2015), a governança digital deve ser entendida como um estágio mais avançado do governo eletrônico, ao incorporar elementos como interatividade, dados abertos, interoperabilidade e inovação cívica.

Nos anos 2000, a implantação do *e-government* consolidou-se em muitos países como parte de estratégias de modernização administrativa. O uso intensivo de Tecnologias da Informação e Comunicação (TICs) passou a integrar as políticas públicas com o objetivo de

reestruturar processos burocráticos, promover maior accountability e ampliar o acesso à informação pública (CRUZ; SILVA; LIMA, 2024).

Na década de 2010, o avanço de tecnologias como computação em nuvem, *big data* e inteligência artificial expandiu significativamente as possibilidades de digitalização governamental. Países como Estônia e Dinamarca tornaram-se referências globais ao integrar serviços públicos em plataformas digitais unificadas, com foco em interoperabilidade, segurança e acessibilidade (OCDE, 2021). Esse movimento reforça a necessidade de os governos adotarem uma abordagem centrada no cidadão e orientada por dados, em busca de uma administração mais eficiente, responsiva e transparente.

Segundo Zuiderwijk e Janssen (2014), a abertura de dados governamentais, quando combinada à governança digital, potencializa a inovação no setor público, ao permitir o reuso da informação por cidadãos, empresas e instituições. Essa tendência é reforçada pelas diretrizes da OCDE (2021), que orientam a adoção de governos digitais abertos, responsivos e centrados no usuário.

No Brasil, a trajetória da governança digital acompanha as tendências internacionais, embora apresente assimetrias significativas entre os diferentes entes federativos. O Governo Federal tem investido em iniciativas estruturantes, como a plataforma Gov.br, que centraliza o acesso a diversos serviços públicos digitais e busca promover maior eficiência e integração (MINISTÉRIO DA ECONOMIA, 2020). No entanto, estados e municípios demonstram níveis variados de maturidade digital, refletindo desigualdades regionais em termos de infraestrutura tecnológica, conectividade e recursos humanos.

Assim, a evolução da governança digital deve ser compreendida como um processo histórico em constante transformação, atravessado por fatores políticos, tecnológicos e institucionais, cujos desdobramentos impactam diretamente a transparência pública e a qualidade da gestão governamental.

## **2.2 Modelos e Abordagens na Administração Pública**

A adoção da governança digital pelos diferentes países têm seguido modelos diversos, influenciados por fatores institucionais, culturais e tecnológicos. Segundo Castells (2010), o desenvolvimento de políticas públicas digitais ocorre em meio a uma sociedade em rede, na qual o poder se reorganiza por meio da informação e do fluxo digital. Isso implica que os modelos de administração digital variam conforme a estrutura de governança de cada país.

Há os modelos de governo digital em três principais abordagens: centralizada, descentralizada e híbrida. No modelo centralizado, exemplificado pelo caso da Estônia, os serviços públicos digitais são organizados em uma única plataforma, que assegura elevada interoperabilidade, segurança e eficiência. Esse modelo é viabilizado por infraestruturas tecnológicas avançadas, como o sistema X-Road, que permite o intercâmbio seguro de dados entre diferentes instituições governamentais.

De acordo com Santos (2021), essa abordagem promove uma gestão integrada da informação e favorece a prestação de serviços públicos centrados no cidadão, alinhando-se às diretrizes da OCDE para uma governança digital eficiente. No entanto, sua implementação demanda uma arquitetura digital sólida, padronização de sistemas e uma estreita cooperação interinstitucional, fatores que se tornam particularmente desafiadores em países de estrutura federativa complexa, como o Brasil, onde coexistem diferentes níveis de autonomia administrativa e tecnológica entre União, estados e municípios.

O modelo descentralizado, comum nos Estados Unidos, concede autonomia às agências e aos diferentes níveis de governo para desenvolverem seus próprios sistemas e interfaces. Embora promova inovação local e flexibilidade, esse modelo enfrenta desafios de padronização e de compartilhamento de dados entre órgãos.

Por sua vez, o modelo híbrido combina elementos centralizados e descentralizados, sendo o mais comum em países federativos como o Brasil, onde há esforços de centralização em nível federal (como o Portal Gov.br), coexistindo com soluções independentes em estados e municípios (CGU, 2022). Essa configuração demanda governança colaborativa e mecanismos de coordenação eficazes.

De acordo com Zuiderwijk e Janssen (2014), não há um modelo de governança digital universalmente superior; sua efetividade está diretamente relacionada à compatibilidade entre o modelo adotado e o contexto institucional, tecnológico e sociopolítico em que se insere. A escolha da abordagem deve considerar os objetivos estratégicos da administração pública, especialmente no que se refere à promoção da transparência, da eficiência administrativa e da inclusão digital.

Dessa forma, compreender os diferentes modelos de governança digital é fundamental para avaliar as condições estruturais e operacionais necessárias à sua implementação e sustentabilidade. Além disso, essa compreensão possibilita a identificação de boas práticas e o delineamento de caminhos viáveis para o fortalecimento da transparência pública e da

prestação de serviços mais acessíveis e eficazes.

### **2.3 Segurança da Informação e Proteção de Dados na Gestão Pública**

A crescente digitalização dos serviços públicos impõe novos desafios à segurança da informação e à proteção de dados pessoais na administração pública. A necessidade de garantir a confidencialidade, integridade e disponibilidade das informações governamentais tornou-se estratégica frente ao aumento de ameaças cibernéticas e ao volume exponencial de dados tratados pelas instituições públicas. Segundo Santos (2021), o Brasil, alinhado às orientações da OCDE, precisa fortalecer suas estruturas de governança digital com foco na segurança da informação, interoperabilidade e proteção de dados.

Segundo Doneda (2018), a proteção de dados deve ser vista como um direito fundamental, sendo a administração pública responsável por garantir que o tratamento de informações pessoais ocorra em conformidade com princípios éticos e legais. A entrada em vigor da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) marca um novo paradigma na relação entre Estado, cidadão e tecnologia, exigindo adaptações nos processos administrativos e maior responsabilização das instituições públicas.

Relatórios da Organização dos Estados Americanos (OEA, 2022) apontam que cerca de 85% dos países da América Latina, incluindo o Brasil, identificam as ameaças cibernéticas como um dos principais riscos à governança digital. Além disso, dados da Fortinet (2021) indicam que o Brasil sofreu mais de 100 milhões de tentativas de ataques cibernéticos apenas no primeiro semestre daquele ano, evidenciando a vulnerabilidade dos sistemas públicos.

A adoção de normas internacionais, como a ISO/IEC 27001, tem sido recomendada para padronizar as práticas de segurança da informação e elevar o grau de maturidade institucional. No setor público brasileiro, iniciativas como a Estratégia de Governo Digital (EGD) e os guias da Secretaria de Governo Digital buscam orientar os órgãos quanto à proteção de dados e à gestão de riscos tecnológicos (BRASIL, 2020).

A capacitação dos servidores públicos também é essencial. Conforme relatório da Escola Nacional de Administração Pública (ENAP, 2021), mais de 60% dos servidores federais não possuíam, até recentemente, formação básica em proteção de dados, o que compromete a implementação efetiva da LGPD.

Assim, a segurança da informação e a proteção de dados não são apenas requisitos técnicos, mas elementos centrais para a construção de uma governança digital confiável,

transparente e orientada ao cidadão.

## **2.4 Impactos e Benefícios da Governança Digital**

A adoção da governança digital tem provocado transformações profundas na administração pública, impactando diretamente a forma como os serviços públicos são ofertados, como as instituições operam internamente e como o cidadão interage com o Estado. Trata-se de um processo que transcende a simples digitalização de serviços, englobando mudanças estruturais, culturais e organizacionais que visam gerar maior valor público (WIRTZ et al., 2018).

Um dos principais benefícios da governança digital é a promoção de uma administração pública mais eficiente, transparente e orientada por dados. A utilização intensiva das Tecnologias da Informação e Comunicação (TICs) permite a automação de processos, a redução da burocracia e o aumento da produtividade dos serviços públicos (SANTOS, 2021). Além disso, ao integrar dados e sistemas, os governos conseguem responder com maior agilidade às demandas sociais, ampliando a capacidade de planejamento, monitoramento e avaliação de políticas públicas.

Nesse sentido, a experiência de países como Estônia e Dinamarca, que implementaram plataformas digitais unificadas, serve de referência global. Essas nações demonstram que, ao investir em interoperabilidade, acessibilidade e segurança da informação, é possível oferecer serviços públicos mais inclusivos e centrados no cidadão (SANTOS, 2021; WIRTZ et al., 2018). A plataforma X-Road, por exemplo, utilizada na Estônia, promove uma troca segura de dados entre instituições, garantindo eficiência administrativa com respeito à privacidade dos usuários.

No contexto brasileiro, a plataforma Gov.br representa um esforço federal em direção à centralização dos serviços públicos digitais. Embora enfrente os desafios típicos de um modelo híbrido (como a coexistência de soluções estaduais e municipais independentes), essa iniciativa aponta para uma direção promissora de integração digital (SANTOS, 2021). Ainda, como destaca Silveira (2002), a governança digital no Brasil deve ser acompanhada por políticas de inclusão digital para garantir que os benefícios da tecnologia sejam estendidos à população de forma equitativa, sobretudo aos grupos historicamente excluídos do acesso às tecnologias da informação.

Outro impacto relevante está relacionado à transparência e ao fortalecimento da participação cidadã. Governos digitais bem estruturados oferecem maior acesso a dados

públicos, viabilizam canais de escuta e fomentam a coprodução de políticas públicas. De acordo com Silveira (2002), o governo eletrônico, ao ampliar o acesso à informação e simplificar a comunicação com a administração pública, contribui para o empoderamento do cidadão e para o controle social das ações governamentais.

No entanto, a crescente digitalização dos serviços impõe novos desafios, especialmente no campo da segurança da informação e da proteção de dados pessoais. Como destaca Santos (2021), é necessário garantir a confidencialidade, integridade e disponibilidade das informações frente ao aumento das ameaças cibernéticas e ao volume crescente de dados sensíveis. Isso exige uma governança robusta, com diretrizes claras sobre o uso ético e responsável das informações públicas, conforme discutido por Doneda (2018), que aponta a necessidade de uma cultura institucional voltada à proteção da privacidade e à observância da Lei Geral de Proteção de Dados (LGPD).

Assim, os impactos da governança digital se revelam multifacetados: promovem maior eficiência administrativa, ampliam a transparência pública, incentivam a participação cidadã e exigem novas capacidades estatais voltadas à segurança e à ética na gestão da informação. A adoção dessa abordagem, quando alinhada ao contexto institucional e às boas práticas internacionais, representa um caminho viável para a construção de um Estado mais responsivo, democrático e inclusivo.

## **2.5 Ameaças Cibernéticas**

Os ataques cibernéticos contra instituições governamentais têm crescido significativamente nos últimos anos, representando uma das principais ameaças à segurança da informação na esfera pública. Esse cenário se agrava com o aumento da digitalização de serviços e a maior exposição dos sistemas governamentais na internet, o que amplia consideravelmente a superfície de ataque (FORTINET, 2021).

Dentre as técnicas mais utilizadas pelos cibercriminosos destacam-se o *ransomware*, o *phishing* e os ataques de negação de serviço distribuído (DDoS). O *ransomware* se caracteriza pela criptografia maliciosa de dados e a exigência de pagamento de resgates para sua liberação, o que pode paralisar órgãos essenciais. Já o *phishing* explora vulnerabilidades humanas por meio de mensagens enganosas, buscando a coleta de informações sensíveis, como logins e senhas. Os ataques DDoS, por sua vez, visam tirar sistemas do ar, tornando indisponíveis os serviços digitais por meio de sobrecarga de servidores. Esses riscos evidenciam a importância da adoção de políticas robustas de segurança da informação, como

as previstas na norma NBR ISO/IEC 27001:2013, que estabelece requisitos para a proteção da confidencialidade, integridade e disponibilidade dos dados tratados pelos órgãos públicos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Essas ameaças têm se tornado mais sofisticadas, com o surgimento de ataques persistentes avançados (APT – *Advanced Persistent Threats*), que envolvem infiltrações de longa duração com objetivos estratégicos, muitas vezes articulados por grupos criminosos organizados ou patrocinados por Estados. Tais ataques ameaçam não apenas a segurança da informação, mas também a soberania nacional e a estabilidade institucional (OEA, 2022).

Casos reais reforçam a necessidade de ação estratégica. Em 2020, o Superior Tribunal de Justiça (STJ) foi alvo de um severo ataque de *ransomware* que comprometeu todo o sistema de tramitação eletrônica de processos. O caso exigiu a mobilização de equipes de emergência, a restauração de sistemas a partir de backups e medidas judiciais para conter os danos. Situação semelhante ocorreu com o Tribunal de Justiça do Estado do Rio Grande do Sul em 2021, quando outro ataque cibernético afetou serviços essenciais, atrasando o andamento processual e evidenciando a vulnerabilidade da infraestrutura digital da Justiça brasileira (SOUZA, 2022; OEA, 2022).

Doneda (2018) ressalta que a vulnerabilidade digital do setor público decorre, em grande parte, da ausência de uma cultura consolidada de proteção de dados e da insuficiência de recursos tecnológicos e humanos. Ainda, a construção de uma política de governança da informação deve ir além da normatização legal e envolver mudanças estruturais e organizacionais capazes de garantir os direitos fundamentais dos cidadãos (DONEDA, 2018, p. 11).

Diante desse cenário, torna-se urgente a adoção de políticas públicas robustas de cibersegurança. A implementação de normas internacionais, como a ISO/IEC 27001, tem se mostrado uma boa prática, padronizando a gestão da segurança da informação e elevando o grau de maturidade institucional (ABNT, 2013). A Estratégia de Governo Digital (EGD) também incentiva a criação de estruturas como Centros de Operações de Segurança (SOC) e Equipes de Resposta a Incidentes (CSIRTs), que devem ser fortalecidas em todas as esferas de governo.

Ademais, é necessário fomentar uma governança colaborativa em nível nacional, com o compartilhamento de informações sobre incidentes, boas práticas e respostas entre os entes federativos, órgãos de controle, universidades e setor privado. Esse ecossistema de cooperação fortalece a resiliência coletiva do Estado brasileiro diante das ameaças digitais que desafiam a segurança pública e a confiança social nas instituições. Segundo Santos

(2021), a governança digital eficaz exige a articulação entre diferentes atores e níveis administrativos, o que demanda estratégias coordenadas e transparentes, em consonância com os princípios recomendados pela OCDE.

Portanto, as ameaças cibernéticas representam um risco sistêmico para a governança digital e exigem abordagens integradas, preventivas e contínuas. O enfrentamento desse desafio passa pela modernização tecnológica, pela capacitação humana e pela construção de uma cultura organizacional comprometida com a segurança da informação e a defesa do interesse público. Como destaca Doneda (2018), a proteção de dados não é apenas uma questão técnica, mas um elemento central da cidadania digital e do exercício pleno dos direitos fundamentais. Nesse sentido, a segurança cibernética deve ser compreendida como parte integrante da política pública de transformação digital, devendo ser tratada de forma estratégica e transversal na administração pública.

### **3 METODOLOGIA**

Esta pesquisa adota uma abordagem qualitativa, de caráter exploratório e descritivo, orientada pelo método de análise documental e revisão de literatura científica. A principal estratégia metodológica utilizada foi o mapeamento do "estado da arte" relacionado à governança digital e à transparência pública no Brasil, com foco específico na legislação e em instrumentos normativos que regulam o uso de tecnologias digitais na administração pública.

A escolha da abordagem qualitativa justifica-se pela natureza interpretativa e crítica do objeto de estudo, que requer uma análise aprofundada das práticas, normativas e contextos institucionais relacionados à digitalização da gestão pública. Conforme Gil (2010), esse tipo de abordagem é indicado quando o objetivo da pesquisa é compreender fenômenos sociais complexos a partir da análise de significados e relações construídas historicamente.

Para isso, foram adotadas duas etapas principais de investigação:

1. Revisão do estado da arte sobre a legislação e os marcos regulatórios da transparência e da governança digital:

Além da revisão teórica, o estudo incluiu a análise de documentos oficiais, como relatórios da Controladoria-Geral da União (2024), Ministério da Economia (2020), e legislações fundamentais como a Lei de Acesso à Informação (BRASIL, 2011) e a Lei Geral de Proteção de Dados (BRASIL, 2018). Também foram examinados casos emblemáticos de

incidentes cibernéticos, como os ataques ao Superior Tribunal de Justiça (2020) e ao Tribunal de Justiça do Rio Grande do Sul (2021), com base em dados públicos e relatórios técnicos (FORTINET, 2021), como forma de ilustrar os riscos reais enfrentados pelo setor público.

## 2. Análise documental orientada por critérios de relevância institucional e atualidade:

Foi realizada uma seleção criteriosa de documentos produzidos por instituições públicas, organismos internacionais e centros de pesquisa reconhecidos. Os critérios de inclusão dos documentos foram: (a) atualidade da publicação; (b) aderência direta ao tema da pesquisa; (c) relevância no cenário da administração pública digital; e (d) acesso público e confiável. A Tabela 1 a seguir sintetiza os principais documentos analisados:

**Tabela 1:** Documentos analisados na pesquisa

<b>Documento</b>	<b>Órgão Responsável</b>	<b>Data de Publicação</b>	<b>Endereço de Acesso</b>
Lei de Acesso à Informação (Lei nº 12.527)	Presidência da República	2011	<a href="https://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/112527.htm">https://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/112527.htm</a>

Lei Geral de Proteção de Dados (LGPD)	Presidência da República	2018	<a href="https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm">https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm</a>
Portal da Transparência	Controladoria-Geral da União (CGU)	Atualizado	<a href="https://www.portalttransparencia.gov.br/">https://www.portalttransparencia.gov.br/</a>
Plataforma Gov.br	Secretaria de Governo Digital	Atualizado	<a href="https://www.gov.br/">https://www.gov.br/</a>
Relatório de Transformação Digital no Brasil	Ministério da Economia	2020	<a href="https://www.gov.br/economia/documentos/relatorio-transformacao-digital">https://www.gov.br/economia/documentos/relatorio-transformacao-digital</a>
Relatório de Cibersegurança na América Latina	Organização dos Estados Americanos (OEA)	2022	<a href="https://www.oas.org/iberseguridad">https://www.oas.org/iberseguridad</a>

Fonte: Elaborada pelos autores

Além dos documentos oficiais, foram examinados estudos acadêmicos que dialogam com a temática da governança digital, tanto no contexto brasileiro quanto internacional. Foram priorizados trabalhos que abordam os impactos das tecnologias da informação na gestão pública, os desafios da proteção de dados e os mecanismos de participação e accountability digital. Entre os principais autores consultados estão Meijer (2015), Zuidervijk e Janssen (2014), Janssen, Matheus e Weerakkody (2017), Silva (2015), Souza (2022), Santos (2021), OCDE (2021) e OEA (2022).

Essa estratégia de levantamento do estado da arte foi essencial para construir um panorama consistente da evolução normativa e institucional da governança digital no Brasil. A metodologia adotada contribuiu para identificar padrões, lacunas e boas práticas na gestão pública digital, oferecendo subsídios para a formulação de recomendações baseadas em evidências e em marcos legais já existentes.

Assim, a análise qualitativa, sustentada na triangulação entre marcos normativos, documentos institucionais e literatura acadêmica, constitui a base metodológica deste trabalho e orienta a interpretação crítica dos resultados apresentados nos capítulos seguintes.

## **4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS**

A análise dos dados obtidos por meio da revisão bibliográfica e documental permitiu identificar diversos aspectos fundamentais sobre o estado atual da governança digital e da transparência pública no Brasil. A seguir, são apresentados e discutidos os principais resultados, organizados de acordo com os eixos temáticos que orientaram esta pesquisa.

### **4.1 Avanços Institucionais na Governança Digital**

A análise evidencia que a governança digital tem promovido avanços significativos em transparência, eficiência administrativa e participação cidadã, conforme indicam relatórios da OCDE (2021) e da CGU (2024). A centralização de serviços no portal Gov.br e a expansão do acesso à informação por meio do Portal da Transparência são exemplos práticos desses avanços, alinhados aos princípios de interoperabilidade e accountability defendidos por Meijer (2015) e Zuiderwijk e Janssen (2014).

Além disso, o lançamento de iniciativas como o Plano de Transformação Digital da Administração Pública Federal, a criação de estruturas específicas como Secretarias de Governo Digital, e a modernização de legislações (a exemplo da Lei Geral de Proteção de Dados (LGPD) e da Lei de Acesso à Informação (LAI)) indicam uma institucionalização progressiva das práticas de governança digital (SOUZA, 2022; OCDE, 2021).

Estudos como os de Zuiderwijk e Janssen (2014) e Meijer (2015) destacam que a consolidação da governança digital depende não apenas de investimentos tecnológicos, mas também de mudanças culturais nas instituições públicas, algo que tem sido um desafio recorrente no Brasil.

A transformação digital no setor público não ocorre de maneira uniforme ou meramente técnica; ela exige adaptação aos contextos institucionais e sociais específicos. Janowski (2015) argumenta que a evolução da governança digital passa da simples digitalização de serviços para uma fase de contextualização, em que as políticas públicas digitais devem refletir valores locais, capacidades administrativas e a participação dos cidadãos. No Brasil, entretanto, essa participação ainda enfrenta barreiras estruturais. Como mostram Sampaio et al. (2019), as iniciativas de democracia digital no país foram numerosas entre 1999 e 2016, mas muitas não sobreviveram por falta de institucionalização, financiamento ou engajamento social.

## 4.2 Desafios Estruturais e Regionais

Apesar dos avanços, a análise revelou desafios significativos para a plena implementação da governança digital no Brasil. Dados do Relatório de Transformação Digital no Brasil (Ministério da Economia, 2020) e do Relatório de Cibersegurança na América Latina (OEA, 2022) evidenciam que a desigualdade regional no acesso à tecnologia e à internet limita a efetividade das políticas digitais, especialmente em municípios de pequeno porte, com baixa infraestrutura tecnológica.

Outro ponto crítico é a falta de capacitação técnica dos servidores públicos, também apontada por Silva (2015) e Souza (2022), que destacam a ausência de políticas estruturadas para formação contínua em tecnologia e segurança da informação. Ainda, a Escola Nacional de Administração Pública (ENAP, 2021) identificou que mais de 60% dos servidores públicos federais ainda não possuem capacitação básica sobre proteção de dados. Essa lacuna de conhecimento fragiliza a administração pública frente a ataques de engenharia social, *phishing* e vazamentos de dados sensíveis.

Além disso, observou-se uma desigualdade na maturidade digital entre os entes federativos, refletindo um modelo híbrido de governança digital, conforme classificado por Santos (2021). Embora o governo federal apresente avanços, muitos estados e municípios carecem de infraestrutura adequada, cultura digital institucionalizada e recursos humanos qualificados, o que dificulta a plena integração e interoperabilidade dos sistemas.

## 4.3 Transparência Ativa e Participação Cidadã

A análise dos documentos legais e das plataformas digitais demonstra que houve avanços na transparência ativa, especialmente com a disponibilização de dados em portais como o Portal da Transparência, o Painel de Cidadania Ativa e a própria plataforma Gov.br (CGU, 2024).

Contudo, estudos como o de Janssen, Matheus e Weerakkody (2017) apontam que a disponibilização dos dados nem sempre ocorre de forma acessível, afetando diretamente a participação social. Além disso, a transparência passiva, que depende de respostas a solicitações feitas pelos cidadãos, ainda enfrenta barreiras burocráticas e operacionais, como também analisado por Zuiderwijk e Janssen (2014).

## 4.3 Segurança da Informação e Conformidade com a LGPD

O impacto da Lei Geral de Proteção de Dados (LGPD) na gestão pública foi um dos

achados mais relevantes da pesquisa. A necessidade de adequação à lei tem impulsionado mudanças organizacionais, como a nomeação de encarregados pelo tratamento de dados (DPOs) e a elaboração de políticas de privacidade (OEA, 2022; OCDE, 2021).

Contudo, muitos órgãos públicos ainda enfrentam dificuldades na adaptação às exigências legais, especialmente no que se refere à infraestrutura tecnológica defasada e à falta de planejamento estratégico para segurança da informação, como destacam Meijer (2015). Casos como os ataques de *ransomware* ao STJ (2020) e ao TJ-RS (2021) revelam a vulnerabilidade dos sistemas públicos frente às ameaças cibernéticas, o que contrasta com os padrões de segurança previstos na norma ISO/IEC 27001 (ABNT, 2013). Segundo Doneda (2018), a proteção de dados deve ser tratada como dimensão estratégica da cidadania digital, o que ainda não se verifica plenamente no setor público brasileiro.

## 5 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar os impactos da governança digital na promoção da transparência pública no Brasil, bem como identificar os desafios e oportunidades advindos da implementação de tecnologias na gestão pública. A partir da análise teórica e documental realizada, foi possível compreender que a digitalização da administração pública representa uma estratégia essencial para o fortalecimento da democracia, da eficiência administrativa e da participação cidadã.

Os resultados apontaram avanços relevantes, como a criação de plataformas digitais integradas, a exemplo do Gov.br, e a adoção de políticas públicas voltadas à transformação digital do Estado. Instrumentos legais como a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) foram fundamentais para estabelecer diretrizes claras sobre transparência e responsabilidade na gestão de dados governamentais.

Entretanto, também foram identificados desafios estruturais e institucionais que comprometem a efetividade dessas iniciativas, tais como a desigualdade no acesso à internet, a escassez de recursos técnicos e humanos, a resistência cultural à adoção de novas tecnologias e as fragilidades na segurança da informação. Tais barreiras evidenciam a necessidade de ações coordenadas e investimentos contínuos por parte do Estado, especialmente nos níveis locais e regionais, onde as disparidades são ainda mais acentuadas.

A análise também demonstrou que, para que a governança digital alcance seu potencial máximo, é imprescindível que os dados públicos sejam não apenas acessíveis, mas também compreensíveis e utilizáveis pelos cidadãos. Isso exige uma comunicação mais clara por parte dos órgãos públicos, bem como o fortalecimento da educação digital e da cultura de

participação social.

A experiência de países que se destacam na área de governo digital revela que o sucesso dessas iniciativas está diretamente relacionado ao planejamento estratégico, à interoperabilidade entre sistemas e à centralidade do cidadão nas políticas públicas. Nesse sentido, o Brasil pode se beneficiar ao adotar modelos mais integrados e ao promover a cooperação entre os diferentes entes federativos e instituições públicas.

Do ponto de vista teórico, este estudo contribui ao consolidar uma compreensão abrangente sobre governança digital e transparência pública no contexto brasileiro, ao articular conceitos, legislações e práticas a partir de uma perspectiva crítica. Ao reunir referências nacionais e internacionais, como os estudos de Meijer (2015), Zuiderwijk e Janssen (2014) e a OCDE (2021), a pesquisa oferece uma análise comparativa que amplia a compreensão acadêmica sobre os desafios e oportunidades na adoção de tecnologias no setor público.

Em termos empíricos, o estudo também se destaca por sistematizar e analisar documentos oficiais, legislações e plataformas digitais relevantes, contribuindo para a construção de um panorama atualizado sobre a governança digital no Brasil. A elaboração da tabela de análise documental, bem como a discussão dos principais marcos legais e das práticas institucionais, serve como um referencial prático para gestores públicos, pesquisadores e formuladores de políticas públicas interessados na transformação digital do Estado.

Portanto, esta pesquisa contribui para o debate sobre o papel da tecnologia na gestão pública, ao evidenciar que a transparência e a *accountability* não dependem apenas de ferramentas digitais, mas de uma mudança estrutural e cultural no modo como o Estado se relaciona com seus cidadãos.

Adicionalmente, este estudo apresenta as seguintes contribuições teóricas e práticas: fornece uma visão consolidada sobre o estado da governança digital e da transparência pública no Brasil; oferece subsídios para a formulação de políticas públicas mais eficazes, centradas na participação cidadã e na proteção de dados, e; contribui para o desenvolvimento de práticas administrativas mais alinhadas com os princípios da transparência, segurança da informação e eficiência pública.

No entanto, é importante destacar algumas limitações deste estudo. A análise foi baseada em uma abordagem documental e bibliográfica, sem a realização de entrevistas, questionários ou análises de dados empíricos diretos, o que poderia proporcionar uma visão mais aprofundada sobre a percepção dos usuários e dos gestores públicos em relação às

plataformas digitais e às políticas de transparência.

Ademais, como a área de governança digital é extremamente dinâmica, marcada por rápidas inovações tecnológicas e mudanças normativas constantes, parte das informações analisadas pode se tornar defasada em médio prazo. Portanto, os resultados aqui apresentados refletem o contexto vigente até o momento da realização da pesquisa, sendo recomendada a atualização contínua dos dados e da análise.

Como sugestões para pesquisas futuras, recomenda-se a realização de estudos de natureza empírica, que envolvam análise de casos específicos em municípios brasileiros, entrevistas com gestores públicos e usuários dos serviços digitais, bem como a investigação do impacto direto da transformação digital na efetividade dos serviços públicos e na percepção dos cidadãos sobre a transparência governamental. Além disso, novos estudos podem focar na avaliação da efetividade das ferramentas de governança digital, como o Gov.br e o Portal da Transparência, verificando se realmente estão contribuindo para o fortalecimento da participação social e da accountability.

Outra vertente interessante para futuras pesquisas é a análise das desigualdades regionais na adoção da governança digital, buscando entender como municípios de diferentes portes e realidades econômicas estão lidando com os desafios da transformação digital. Investigações que explorem a percepção dos servidores públicos, os impactos da LGPD na gestão pública, além de estudos comparativos internacionais, especialmente com modelos bem-sucedidos como os da Estônia e Dinamarca, também são caminhos relevantes para ampliar e aprofundar o debate sobre o tema no contexto brasileiro.

Por fim, conclui-se que a governança digital, quando implementada de forma estratégica, transparente e segura, pode transformar significativamente a administração pública brasileira, tornando-a mais eficiente, participativa e confiável. Para isso, é essencial que os gestores públicos estejam comprometidos com a inovação, que os servidores sejam continuamente capacitados e que a sociedade esteja engajada na utilização e fiscalização das ferramentas digitais.

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013 – **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2013.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto na Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, ano CXLVIII, n. 222, p. 1, 18 nov. 2011. Disponível em:

<[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm)>. Acesso em: 10 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Lei Geral de Proteção de Dados - LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:

<[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 10 abr. 2025.

BRASIL. **Estratégia de Governo Digital 2020–2022**. Secretaria de Governo Digital. Brasília: Ministério da Economia, 2020.

CRUZ, L. S; SILVA, N. A; LIMA, T. G. GOVERNANÇA DIGITAL NA GESTÃO PÚBLICA: ANÁLISE DA EFICÁCIA. RECIMA21 - **REVISTA CIENTÍFICA MULTIDISCIPLINAR** - v.5, n.5, 2024.

CONTROLADORIA-GERAL DA UNIÃO (Brasil). **Painel de Cidadania Ativa**. Brasília, DF: CGU, 2024. Disponível em: <<https://www.gov.br/cgu>>. Acesso em: 10 abr. 2025.

CASTELLS, M. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 2010.

DONEDA, D. Da privacidade à proteção de dados pessoais. **Revista Brasileira de Políticas Públicas**, v. 8, n. 2, p. 507–528, 2018.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (Brasil). **Capacitação dos**

**servidores públicos sobre a LGPD: relatório técnico 2021.** Brasília, DF: ENAP, 2021. Disponível em: <<https://www.enap.gov.br>>. Acesso em: 10 abr. 2025.

FORTINET. **Relatório de ameaças globais: panorama de ataques cibernéticos ao setor público.** Sunnyvale, CA: Fortinet, 2021. Disponível em: <<https://www.fortinet.com>>. Acesso em: 10 abr. 2025.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2010.

JANSSEN, Marijn; MATHEUS, Ricardo; WEERAKKODY, Vishanth. Big and open linked data (BOLD) in government: a challenge to transparency and privacy? **Information Systems Frontiers**, v. 19, n. 2, p. 263–283, 2017.

JANOWSKI, T. Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, v. 32, n.3, p. 221-236, 2015.

MEIJER, Albert. Government transparency in historical perspective: from the ancient regime to open data in the Netherlands. **International Journal of Public Administration**, v. 38, n. 3, p. 189–199, 2015.

MINISTÉRIO DA ECONOMIA (Brasil). **Relatório de Transformação Digital no Brasil: 2020.** Brasília, DF: Ministério da Economia, 2020. Disponível em: <<https://www.gov.br/economia/documentos/relatorio-transformacao-digital>>. Acesso em: 10 abr. 2025.

OCDE – ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Digital Government Index: 2021 results.** Paris: OECD Publishing, 2021. Disponível em: <<https://www.oecd.org/governance/digital-government-index.htm>>. Acesso em: 10 abr. 2025.

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe.** Washington, D.C., 2022. Disponível em: <<https://www.oas.org/iberseguridad>>. Acesso em: 10 abr. 2025.

PORTAL DA TRANSPARÊNCIA. **Portal da Transparência.** Brasília, DF: Controladoria-Geral da União, [s.d.]. Disponível em: <<https://www.portaltransparencia.gov.br>>. Acesso em: 10 abr. 2025.

SILVA, E. R. A. **Continuidades, Inovações e Retrocessos na Evolução do Governo Digital em Pernambuco**. Programa de Pós-Graduação em Administração – Universidade Federal de Pernambuco, 2015.

SOUZA, Patrícia Ferreira. A LGPD no setor público: desafios e oportunidades para a proteção de dados pessoais. **Revista Brasileira de Administração Pública Digital**, v. 2, n. 1, p. 33–47, 2022.

SAMPAIO, R. C; BRAGA, S; CARLOMAGNO, M. C; MARIOTO, D. J. F; ALISON, M. B; SILVA, T. P. F. B. Estado da arte da democracia digital no Brasil: oferta e sobrevivência das iniciativas (1999-2016). **Rev. Serv. Público Brasília**, v. 70, n. 4, p. 693-734, out/dez, 2019.

SILVEIRA, S. A. Governo Eletrônico e Inclusão Digital. In: HERMANNNS, Klaus (org). **Governo Eletrônico: os desafios da participação cidadã**. Fortaleza: Fundação Konrad Adenauer, 2002. p. 69-81.

SANTOS, M. H. S. Aspectos da governança digital da administração pública federal do Brasil sob a luz das orientações da OCDE. **Revista tempo do mundo - RTM**, n. 25, abr. 2021.

WIRTZ, B. W., DAISER, P., BINKOWSKA, B. Smart governance: A conceptual framework. **Information Polity**, v. 23, p.1, p. 43–60, 2018.

ZUIDERWIJK, Anneke; JANSSEN, Marijn. Open data policies, their implementation and impact: a framework for comparison. **Government Information Quarterly**, v. 31, n. 1, p. 17–29, 2014.