iSys - Journal of Information Systems, 2026, 19:1
ISSN: 1984-2902 • doi: 10.5753/isys.2026.8971
This work is licensed under a Creative Commons Attribution 4.0 International License.

Research Paper

Personal data governance in municipal e-government information systems: an instrument for assessing observable compliance with the Brazilian LGPD and its application to public portals

Vitor Felipe Bastos de Arruda Carneiro [**Universidade Federal de Mato Grosso** | ***vitorfelip@gmail.com***]
Nelcileno Virgilio de Souza Araujo [**Universidade Federal de Mato Grosso** | ***nelcileno@ic.ufmt.br***]
Constantino Dias da Cruz Neto [**Universidade Federal de Mato Grosso** | ***tino197504@gmail.com***]
Programa de Pós-Graduação em Computação Aplicada, Instituto de Computação, Universidade Federal de Mato Grosso, Cuiabá, MT, Brasil.

Instituto de Computação, Universidade Federal de Mato Grosso, Av. Fernando Corrêa da Costa, 2367, Cuiabá, MT, 78060-900, Brasil.

Resumo. [Contexto] A digitalização dos serviços públicos municipais transformou os portais institucionais nos principais sistemas de informação que mediam a relação entre cidadão e poder público local, intensificando a necessidade de governar os dados pessoais que eles tratam sob a Lei Geral de Proteção de Dados. [Objetivo] Este estudo desenvolve, valida e aplica um instrumento de avaliação, um índice de conformidade baseado em rubrica, para mensurar a conformidade observável dos portais de governo eletrônico municipal à LGPD, isto é, aquilo que pode ser verificado por inspeção externa da interface, em quatro dimensões sociotécnicas: conformidade legal e governança, segurança da informação, usabilidade e acessibilidade digital. [Método] Derivou-se uma rubrica de treze indicadores pontuáveis a partir do cruzamento de fontes legais, técnicas, de acessibilidade e de interação humano-computador. O instrumento foi validado por painel de especialistas, com Índice de Validade de Conteúdo de 1,00, e aplicado por três avaliadores independentes aos portais dos seis municípios mato-grossenses com mais de 100 mil habitantes; as notas foram consolidadas pela mediana em um Índice de Conformidade, cuja robustez foi examinada por análise de sensibilidade. [Resultados] O Índice de Conformidade médio foi de 55,8%, indicando conformidade observável apenas parcial, sem nenhum portal com pontuação máxima e com variação de 30,8% na capital a 84,6%. Conformidade legal e governança, com 51,4%, e acessibilidade, com 54,2%, obtiveram pontuações inferiores às de segurança e usabilidade, e a ordenação dos portais manteve-se sob esquemas alternativos de ponderação. A concordância entre avaliadores foi limitada (Fleiss *kappa* 0,260; alfa de Krippendorff ordinal 0,427), e a análise das divergências indicou pontos específicos de refinamento dos descritores. [Conclusão/Contribuições] O estudo contribui com um instrumento replicável para a avaliação externa da governança de dados em portais de governo eletrônico e com evidências, restritas à amostra analisada, de que as pontuações são mais altas nos controles técnicos visíveis do que nos requisitos que dependem de rotinas contínuas de governança.

Abstract. [Context] The digitalization of municipal public services has turned institutional portals into the main information systems mediating the relationship between citizens and local government, intensifying the need to govern the personal data these systems process under the Brazilian General Data Protection Law (LGPD). [Objective] This study develops, validates, and applies an evaluation instrument, structured as a rubric-based compliance index, to assess the observable compliance of municipal e-government portals with the LGPD, that is, what can be verified through external inspection of the interface, across four sociotechnical dimensions: legal compliance and information governance, information security, usability, and digital accessibility. [Method] Through a structured development-and-validation process, we derived a rubric of thirteen scorable indicators through cross-mapping of legal, technical, accessibility, and human-computer interaction sources. The instrument was validated by an expert panel, reaching a Content Validity Index of 1.00, and independently applied by three evaluators to the portals of the six municipalities in Mato Grosso, Brazil, with more than 100,000 inhabitants; scores were consolidated by the median into a Compliance Index, whose robustness was examined through sensitivity analysis. [Results] The mean Compliance Index was 55.8%, indicating only partial observable compliance, with no portal reaching the maximum score and scores ranging from 30.8% in the state capital to 84.6%. Legal compliance and governance, at 51.4%, and accessibility, at 54.2%, scored lower than security and usability, and the ranking of portals held under alternative weighting schemes. Inter-rater agreement was limited (Fleiss' kappa 0.260; ordinal Krippendorff's alpha 0.427), and the analysis of disagreements identified specific points for refining the descriptors. [Conclusion/Contribution] The paper contributes a replicable instrument for the external assessment of data governance in e-government portals and evidence, limited to the sample analyzed, that scores are higher for visible technical controls than for requirements that depend on continuous governance routines.

Palavras-chave: governo eletrônico, governança de sistemas de informação, proteção de dados pessoais, LGPD, avaliação de conformidade

Keywords: e-government, information systems governance, personal data protection, LGPD, compliance assessment

Received: 16 August 2026 • **Accepted:** 20 October 2026 • **Published:** 06 November 2026

1 Introdução

A adoção de tecnologias de informação e comunicação pela administração pública converteu os portais institucionais das prefeituras em sistemas de informação de fato: interfaces que coletam, processam e disponibilizam dados pessoais dos cidadãos e que materializam, no âmbito local, a agenda de governo eletrônico. Esse movimento amplia o alcance dos serviços públicos, mas também expande a superfície de exposição de informações sensíveis e transfere para o município deveres de governança da informação antes difusos. No Brasil, a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, estabeleceu princípios de transparência, finalidade, segurança e responsabilização que passam a reger o tratamento de dados por esses sistemas, com deveres reforçados pelos guias da Agência Nacional de Proteção de Dados, a ANPD [Brasil, 2018; Agência Nacional de Proteção de Dados, 2022b].

Do ponto de vista de Sistemas de Informação, avaliar a adequação desses portais à LGPD não é uma questão puramente jurídica nem puramente técnica: trata-se de um problema sociotécnico, que articula tecnologia, pessoas e organizações. A dimensão tecnológica compreende os controles de segurança e a arquitetura da informação; a dimensão humana envolve a experiência e os direitos do cidadão que usa o sistema; a dimensão organizacional abrange as práticas de governança da informação da prefeitura. Essa tríade constitui precisamente o eixo de análise da pesquisa em SI, e é sob essa lente que este trabalho se posiciona [Gil-Garcia *et al*., 2018].

Apesar da centralidade do tema, persiste uma lacuna instrumental. Falta, na literatura de SI e de governo eletrônico, um instrumento replicável que permita mensurar, por inspeção externa e de forma comparável entre organizações, o grau de conformidade de portais públicos à proteção de dados, integrando em uma única ferramenta as dimensões legal, de segurança, de usabilidade e de acessibilidade. A ausência desse instrumento dificulta o diagnóstico, o *benchmarking* entre municípios e o direcionamento de investimentos em governança digital.

O contexto empírico escolhido acentua a relevância do problema. Segundo a pesquisa TIC Domicílios do Comitê Gestor da Internet no Brasil, cerca de 84% da população brasileira tem acesso à internet, o que representa mais de 156 milhões de pessoas conectadas, e em Mato Grosso a proporção de domicílios com acesso supera 90% [Comitê Gestor da Internet no Brasil, 2024; Instituto Brasileiro de Geografia e Estatística, 2024]. O estado, contudo, reúne 141 municípios com realidades socioeconômicas diversas e infraestrutura tecnológica desigual, e as cidades de maior densidade populacional concentram tanto o maior número de usuários quanto as maiores demandas por serviços digitais de qualidade. Esse quadro justifica o recorte analítico do estudo nos seis municípios com mais de 100 mil habitantes, que combinam representatividade populacional, dinamismo econômico e estruturas administrativas mais consolidadas, condições que tornam a comparação entre portais metodologicamente equilibrada.

Diante disso, este estudo responde à seguinte questão de pesquisa: **em que medida os sistemas de informação de governo eletrônico municipal, isto é, os portais institucionais das prefeituras, atendem, no que é observável por inspeção externa, aos princípios e requisitos da LGPD, considerando conjuntamente conformidade legal e governança da informação, segurança da informação, usabilidade e acessibilidade digital?**

Para responder a essa questão, o estudo desenvolve, valida e aplica um instrumento de avaliação em três etapas: constrói-se uma rubrica de avaliação convertida em um Índice de Conformidade; valida-se o instrumento por painel de especialistas; e aplica-se o instrumento, de forma empírica e independente, aos portais dos seis municípios de Mato Grosso com mais de 100 mil habitantes, a saber, Cuiabá, Várzea Grande, Rondonópolis, Sinop, Sorriso e Tangará da Serra, que juntos concentram cerca de 44% da população estadual.

É necessário delimitar desde já o construto avaliado. O instrumento mede a *conformidade observável* dos portais, isto é, o grau em que os requisitos de proteção de dados se manifestam de forma verificável na interface pública, acessível a qualquer cidadão sem autenticação. Ele não mede a conformidade institucional da prefeitura, que depende de processos internos, como registros de operações, contratos com operadores e atuação efetiva do encarregado, inacessíveis à inspeção externa. Assim, as expressões "conformidade" e "Índice de Conformidade" designam, ao longo deste artigo, a conformidade observável no portal, e o índice não deve ser interpretado como auditoria global de conformidade legal. Parte dos indicadores decorre diretamente de dispositivos da LGPD; outra parte operacionaliza as condições de usabilidade e acessibilidade sem as quais a informação exigida pela lei não chega de forma efetiva ao titular, vínculo justificado na Seção 3.4.

As contribuições do artigo para o campo de SI são três. A primeira é um instrumento de avaliação replicável e teoricamente rastreável, que operacionaliza requisitos normativos heterogêneos em indicadores observáveis por inspeção externa. A segunda é a evidência empírica, restrita aos seis portais analisados, de que as pontuações são mais altas nos controles técnicos mais visíveis, como a comunicação cifrada e a existência formal de política de privacidade, e mais baixas nos requisitos que dependem de rotinas contínuas de governança da informação, acompanhada de uma análise da confiabilidade da aplicação que identifica os descritores que requerem refinamento. A terceira é um conjunto de recomendações priorizadas para gestores públicos e equipes de tecnologia da informação, conectando os achados da avaliação a decisões de governança de SI.

O restante do artigo está organizado da seguinte forma. A Seção 2 discute o referencial teórico e os trabalhos relacionados. A Seção 3 detalha a construção e a validação do instrumento. A Seção 4 apresenta os resultados. A Seção 5 discute implicações, recomendações e ameaças à validade. A Seção 6 conclui.

2 Referencial teórico e trabalhos relacionados

2.1 Governo eletrônico como sistema de informação e governança de dados

O governo eletrônico é entendido como o uso estratégico de tecnologias de informação e comunicação para modernizar processos estatais, ampliar a oferta de serviços públicos

digitais e fortalecer a participação social [Silva and Rover, 2010]. Sob a perspectiva de Sistemas de Informação, o portal municipal é o sistema de informação de linha de frente da organização pública: é por ele que o cidadão acessa serviços, fornece dados pessoais e exerce direitos. A adequação desse sistema à LGPD é, portanto, uma expressão concreta de governança da informação, entendida como a definição de responsabilidades, políticas e controles sobre o ciclo de vida dos dados pessoais [Tallon *et al*., 2013; Abraham *et al*., 2019].

O contexto brasileiro reforça a relevância do tema. Segundo o *GovTech Maturity Index* do Banco Mundial [World Bank, 2022], o Brasil figura entre os países latino-americanos mais avançados em governo digital, e o Painel de Serviços Digitais do Governo Federal indica que mais de 90% dos serviços federais já são ofertados em formato digital [Brasil, 2024]. Esse avanço, contudo, é assimétrico: enquanto a esfera federal consolida plataformas integradas, as prefeituras enfrentam desafios de padronização, infraestrutura e capacitação, sobretudo fora dos grandes centros. Quanto mais o Estado se digitaliza, mais cresce sua responsabilidade sobre a proteção, a integridade e a transparência dos dados pessoais que coleta, e essa responsabilidade recai de forma desigual sobre os entes municipais.

Há ainda uma tensão normativa que os portais municipais precisam equacionar. A Lei de Acesso à Informação impõe ao poder público o dever de divulgar informações de interesse coletivo [Brasil, 2011], enquanto a LGPD exige o resguardo dos dados pessoais. As duas leis não se opõem: complementam-se ao delinear os limites e as responsabilidades do Estado na era digital, definindo o que a ANPD denomina governo digital responsável, conceito que associa o uso de tecnologias à observância de princípios éticos, legais e de inclusão social. A conformidade digital, nesse sentido, ultrapassa o cumprimento formal de normas e envolve o desenvolvimento de uma cultura institucional de governança da informação, baseada em políticas de segurança, gestão de riscos e design centrado no cidadão.

A comunidade brasileira de Sistemas de Informação vem tratando a conformidade à LGPD como um problema próprio da área. No âmbito do Simpósio Brasileiro de Sistemas de Informação, Barros *et al*. [2023] propõem estratégias para modelar e avaliar a conformidade entre sistemas de informação e a LGPD, e Araújo *et al*. [2021] apresentam o método LGPD4BP para avaliar a aderência de processos de negócio à lei. No campo correlato de engenharia de software e requisitos, há frameworks e checklists de inspeção de conformidade, como os de Carturan *et al*. [2022], Mendes *et al*. [2021] e Cerqueira *et al*. [2023]. Esses trabalhos, contudo, concentram-se em artefatos internos de software, como processos de negócio, requisitos e bancos de dados, e não na avaliação externa, observável pela interface, de portais de governo eletrônico em produção. Essa é a lacuna que este estudo endereça. Trabalhos relacionados indexados na SBC OpenLib, a SOL, foram consultados conforme a política da iSys.

2.2 Fundamentos legais e de segurança da informação

A consolidação da era digital transformou a informação em ativo estratégico tanto para a gestão pública quanto para o exercício da cidadania, e fez emergir a necessidade de regulamentar o tratamento de dados pessoais para que a coleta, o armazenamento e o compartilhamento de informações ocorram dentro de parâmetros éticos, técnicos e jurídicos. A LGPD representa o principal marco regulatório brasileiro nesse campo e inspira-se diretamente no Regulamento Geral sobre a Proteção de Dados da União Europeia, o GDPR [Brasil, 2018; União Europeia, 2016].

A lei estabelece princípios fundamentais de finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção e responsabilização, que norteiam o tratamento de dados pessoais em qualquer esfera pública ou privada. Ao colocar o titular dos dados no centro do processo e conferir-lhe poder de decisão sobre suas informações, a LGPD protege direitos essenciais como a liberdade, a privacidade e o livre desenvolvimento da personalidade. Além de fixar obrigações aos agentes de tratamento, a lei institui um sistema de governança da informação que articula responsabilidades entre controladores, operadores e encarregados, sob a supervisão da ANPD, órgão responsável por regulamentar e fiscalizar sua aplicação. A herança europeia é visível na adoção dos conceitos de *privacy by design* e *privacy by default*, que orientam a incorporação da privacidade desde a concepção dos sistemas, e na lógica de *accountability*, isto é, de responsabilização ativa das organizações pelo cumprimento da lei e pela adoção de medidas efetivas de proteção [Castro *et al*., 2022].

A dimensão técnica da conformidade encontra sustentação no campo da segurança da informação, que antecede historicamente a LGPD e fornece os fundamentos para sua implementação prática. A segurança da informação busca preservar a confidencialidade, a integridade e a disponibilidade dos dados, tríade consolidada em normas internacionais como a ISO/IEC 27002:2022, que estabelece controles aplicáveis a políticas organizacionais, gestão de ativos, criptografia, controle de acessos e gestão de incidentes [Associação Brasileira de Normas Técnicas, 2022]. A incorporação desses padrões é condição para que a proteção de dados não fique restrita à esfera normativa e se traduza em procedimentos técnicos concretos: sem controles de segurança operantes, os princípios da lei permanecem declarações de intenção.

No contexto da administração pública, essa articulação entre norma jurídica e controle técnico assume relevância adicional, pois o Estado é depositário de grandes volumes de dados sensíveis e o cidadão não pode optar por não fornecê-los. A ANPD tem publicado guias específicos para órgãos públicos e para agentes de tratamento de pequeno porte, com orientações práticas para a aplicação proporcional das medidas de segurança e para o atendimento aos direitos dos titulares [Agência Nacional de Proteção de Dados, 2022b]. A relação entre a legislação e a segurança da informação é, portanto, de complementaridade: a primeira fornece a estrutura normativa e os valores que orientam o tratamento ético e transparente dos dados; a segunda oferece os processos técnicos que tornam essa proteção efetiva. Essa complementaridade fundamenta dois dos quatro eixos do instrumento proposto neste trabalho, o eixo de conformidade legal e governança da informação e o eixo de segurança da informação.

2.3 Usabilidade, design centrado no usuário e *privacy by design*

A efetividade das políticas de proteção de dados não depende apenas de boas leis e de sólidas práticas de segurança. Para que os princípios da LGPD se concretizem, é indispensável que o cidadão compreenda e consiga exercer seus direitos de forma simples, intuitiva e acessível. Essa dimensão prática e comunicacional insere a discussão no campo da Interação Humano-Computador, a IHC, que investiga como as pessoas interagem com sistemas computacionais e como o design dessas interfaces pode favorecer a compreensão, a transparência e a confiança [Cybis *et al*., 2007]. Surgida na década de 1980 na articulação entre computação, psicologia cognitiva e design, a IHC ampliou progressivamente seu escopo para tratar de usabilidade, experiência do usuário, acessibilidade e ética no design, à medida que os sistemas digitais passaram a mediar atividades cotidianas e processos públicos essenciais [Nielsen, 1994; Norman, 2013].

O conceito de usabilidade é central nessa perspectiva. Para Nielsen [1994], sistemas usáveis são aqueles que podem ser aprendidos com facilidade, operados de modo eficiente e lembrados sem esforço, com baixo índice de erros e satisfação do usuário. A norma ISO 9241-11:2018 complementa essa definição ao caracterizar a usabilidade como a medida em que um sistema pode ser utilizado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação em um contexto de uso determinado [International Organization for Standardization, 2018]. Ao vincular a usabilidade a contextos particulares, a norma reforça que portais públicos devem ser avaliados considerando o perfil real de seus usuários: cidadãos com diferentes níveis de letramento digital, diferentes capacidades e diferentes necessidades informacionais. Um portal que apresenta políticas de privacidade confusas, termos longos e linguagem técnica inacessível cria barreiras práticas à efetividade da LGPD, ainda que seja juridicamente correto. Nesse sentido, a aplicação de heurísticas como visibilidade do status do sistema, correspondência com o mundo real, consistência, prevenção de erros e linguagem simples é essencial para uma comunicação transparente entre governo e cidadão [Nielsen and Loranger, 2007]. As oito regras de ouro de Shneiderman *et al*. [2018] apontam na mesma direção ao destacar a consistência, o feedback informativo e a redução da carga de memória, diretrizes que dialogam diretamente com os indicadores de usabilidade adotados na rubrica desta pesquisa.

O paradigma do design centrado no usuário amplia essa noção ao propor que o desenvolvimento de interfaces parta das necessidades, capacidades e expectativas das pessoas, e não apenas dos requisitos técnicos ou legais [Preece *et al*., 2015]. Norman [2013] ressalta que o bom design se alinha à forma como os usuários pensam e agem, permitindo que a tarefa, e não o sistema, se torne o foco da atenção. Rosson and Carroll [2002] aprofundam essa articulação ao propor o design baseado em cenários, que permite antecipar a experiência do usuário e identificar barreiras de interação antes da implementação. Essa abordagem conecta-se diretamente ao princípio de *privacy by design*: se a proteção de dados deve ser incorporada desde a concepção dos sistemas, os cenários de interação entre o cidadão e o portal precisam considerar, desde o início, como as informações sobre tratamento de dados serão percebidas, compreendidas e utilizadas pelos diferentes perfis de usuários. Evidências empíricas sustentam essa conexão entre design e conformidade: Chalhoub and Flechais [2022] demonstram que usuários tendem a desconfiar de portais com termos longos e incompreensíveis, enquanto interfaces com linguagem simples e feedback imediato aumentam a sensação de controle e segurança. A experiência do usuário deixa de ser questão apenas estética ou funcional e se transforma em elemento de conformidade legal.

A IHC oferece ainda o fundamento metodológico da avaliação conduzida neste trabalho. Barbosa and Silva [2010] sistematizam os métodos de avaliação de interfaces em dois grandes grupos: os métodos de inspeção, nos quais avaliadores com formação técnica examinam a interface com base em critérios ou heurísticas predefinidos, e os métodos empíricos, nos quais usuários reais executam tarefas em ambiente controlado. Os autores destacam que os métodos de inspeção apresentam vantagens operacionais significativas quando o objetivo é verificar a conformidade de uma interface a diretrizes normativas específicas, pois dispensam o recrutamento de usuários finais e permitem a aplicação padronizada de critérios objetivos. A avaliação heurística de Nielsen [1994] é o exemplo clássico desse tipo de método. Essa distinção é particularmente relevante para a presente pesquisa, na qual a avaliação dos portais é conduzida por avaliadores que inspecionam as interfaces com base em indicadores predefinidos, e não por cidadãos em situação real de uso. Ao adotar a inspeção como estratégia central, o trabalho filia-se a uma tradição consolidada da IHC que reconhece a legitimidade e a eficácia dessa abordagem para identificar problemas de usabilidade e de conformidade normativa. Rubin and Chisnell [2008] reforçam que a qualidade de uma interface não se mede apenas pela presença de elementos normativos, mas pela forma como esses elementos são comunicados e compreendidos, princípio que informou a construção dos descritores da rubrica.

2.4 Acessibilidade digital e inclusão informacional

A discussão sobre usabilidade e design centrado no usuário conduz naturalmente à acessibilidade digital, que representa a ampliação ética e social desses conceitos. Se a usabilidade garante que um sistema seja eficiente e compreensível, a acessibilidade assegura que ele seja universalmente utilizável, incluindo pessoas com diferentes tipos de deficiência ou limitação. No contexto dos portais públicos essa dimensão adquire relevância especial, pois o acesso às informações governamentais é um direito fundamental vinculado à cidadania, à transparência e à inclusão social, e o cidadão não é um cliente que pode escolher outra plataforma: é um titular de direitos que depende das interfaces estatais para acessar serviços essenciais.

A acessibilidade digital compreende o conjunto de práticas, normas e técnicas que permitem a qualquer indivíduo, independentemente de suas condições físicas, sensoriais ou cognitivas, perceber, compreender, navegar e interagir com conteúdos digitais. O W3C consolidou essas diretrizes nas *Web Content Accessibility Guidelines*, cuja versão 2.2 define quatro princípios que devem orientar todo conteúdo digital: perceptível, operável, compreensível e robusto [World Wide

Web Consortium, 2023]. No Brasil, o Modelo de Acessibilidade em Governo Eletrônico, o eMAG, adapta as recomendações internacionais à realidade nacional e estabelece diretrizes sobre contraste de cores, alternativas textuais para imagens, controle por teclado e estrutura semântica do conteúdo [Brasil, 2014]. O arcabouço legal reforça essa exigência: a Lei nº 13.146/2015, o Estatuto da Pessoa com Deficiência, e a Lei de Acesso à Informação preveem o acesso universal às informações públicas [Brasil, 2015, 2011].

A conformidade à LGPD depende diretamente da observância desses princípios. Quando uma política de privacidade é apresentada em linguagem técnica e sem alternativas acessíveis, ela exclui parte da população do direito de compreender e controlar o uso de seus dados pessoais. Acessibilidade e proteção de dados não são, portanto, temas paralelos, mas complementares: a falta de acessibilidade compromete a efetividade dos direitos garantidos pela lei, pois impede que titulares com deficiência visual, auditiva ou cognitiva compreendam plenamente as finalidades e os riscos do tratamento de suas informações [Chaves and Benitti, 2025]. Estudos recentes reforçam essa conexão ao demonstrar que interfaces com design inclusivo e linguagem simplificada aumentam significativamente a compreensão das políticas de privacidade, além de melhorar a experiência do usuário e a credibilidade institucional [Moreira *et al*., 2024].

No contexto das prefeituras brasileiras, a aplicação efetiva das normas de acessibilidade ainda enfrenta obstáculos como a falta de padronização, as limitações orçamentárias e a carência de profissionais especializados [Mendonça and Pereira Neto, 2015]. Ao mesmo tempo, índices internacionais de maturidade digital passaram a incorporar práticas inclusivas entre seus critérios, o que indica que a acessibilidade deixou de ser exigência meramente normativa e se tornou critério de qualidade e eficiência administrativa. Por essas razões, o instrumento proposto neste trabalho dedica um de seus quatro eixos à acessibilidade digital, avaliando tanto os aspectos perceptivos da interface quanto a operabilidade por tecnologias assistivas.

2.5 Privacidade e governança de dados na literatura internacional de SI

O problema tratado neste artigo não é uma particularidade brasileira, e situá-lo na produção internacional de Sistemas de Informação ajuda a esclarecer tanto a natureza do construto medido quanto o tipo de contribuição que um instrumento de avaliação pode oferecer. A privacidade da informação é um dos temas mais consolidados da agenda de SI, e as duas revisões seminais publicadas na *MIS Quarterly* em 2011 delimitam bem o campo. Smith *et al*. [2011] organizam a literatura em torno da tríade *antecedentes–preocupações com privacidade–resultados* e mostram que a maior parte dos estudos mede a preocupação declarada do indivíduo, e não a prática efetiva das organizações que tratam seus dados. Bélanger and Crossler [2011] chegam a diagnóstico convergente e apontam explicitamente o predomínio de *surveys* com estudantes e o déficit de pesquisas que examinem organizações reais e artefatos em produção. Essa lacuna metodológica é diretamente relevante para o presente trabalho: ao inspecionar sistemas efetivamente em operação, em vez de coletar percepções de usuários, o instrumento aqui proposto se posiciona no lado menos povoado dessa divisão.

Um segundo corpo de literatura fornece o vocabulário conceitual do estudo. A governança de dados é definida por Abraham *et al*. [2019], em revisão estruturada publicada no *International Journal of Information Management*, como o arranjo de estruturas de decisão, papéis e responsabilidades que determina quem decide o quê sobre os ativos de dados de uma organização. Tallon *et al*. [2013] haviam proposto no *Journal of Management Information Systems* a noção correlata de governança da informação, deslocando o foco da infraestrutura de TI para o próprio artefato informacional e seu ciclo de vida. Essa distinção esclarece por que o achado central deste estudo, a defasagem entre controles técnicos maduros e governança documental frágil, é teoricamente esperado e não meramente anedótico: controles como HTTPS pertencem à camada de infraestrutura, cuja adoção é pontual e de baixo custo marginal, ao passo que datar políticas, mapear bases legais e manter canais de incidentes são práticas de governança da informação, que exigem papéis definidos e rotinas organizacionais continuadas. Essa distinção sugere que as duas camadas podem apresentar níveis distintos de desenvolvimento em uma mesma organização, e os dados aqui apresentados permitem observar essa diferença, em contexto municipal, no nível daquilo que é visível no portal.

A pesquisa sobre governo digital acrescenta a dimensão de valor público. Twizeyimana and Andersson [2019] identificam, em revisão publicada no *Government Information Quarterly*, seis dimensões de valor público do governo eletrônico, entre as quais figuram a melhoria da administração pública, a confiança do cidadão e a inclusão social, precisamente os elementos que os eixos de governança, usabilidade e acessibilidade do instrumento procuram capturar. Gil-Garcia *et al*. [2018] argumentam, por sua vez, que a pesquisa em governo digital só produz conhecimento cumulativo quando articula a perspectiva tecnológica com a de gestão pública, evitando tanto o determinismo técnico quanto a análise institucional desconectada do artefato. O instrumento proposto neste artigo opera exatamente nessa interseção: mede propriedades observáveis de um artefato digital e as interpreta como indicadores de capacidade organizacional.

Vale registrar, por fim, uma tensão que a literatura internacional expõe e que limita o alcance de qualquer avaliação por inspeção. O modelo de *privacy calculus* de Dinev and Hart [2006], publicado na *Information Systems Research*, descreve a decisão de divulgar dados como um cálculo entre risco percebido e benefício esperado. Esse modelo pressupõe que o indivíduo possa optar por não transacionar, condição que não se verifica na relação entre cidadão e prefeitura: quem precisa emitir uma certidão ou consultar um tributo não dispõe de portal alternativo. A ausência de escolha desloca integralmente o ônus da proteção para o lado da organização e é o que justifica, no plano teórico, avaliar o portal público por padrões normativos externos em vez de por satisfação declarada do usuário. Trata-se de uma diferença de contexto que a literatura de comércio eletrônico não precisa enfrentar e que reforça a pertinência de instrumentos de auditoria externa como o aqui desenvolvido.

Em conjunto, essa produção internacional sustenta três decisões deste trabalho: avaliar organizações e artefatos, e não percepções; tratar conformidade como capacidade de

governança, e não como atributo técnico; e adotar critério normativo externo, dada a ausência de escolha do cidadão. Ela também indica o caminho de generalização discutido na Seção 5: como LGPD e GDPR compartilham arquitetura de princípios, bases legais e direitos do titular, a rastreabilidade normativa do instrumento permite sua adaptação a outras jurisdições.

2.6 Trabalhos empíricos sobre adequação à LGPD no setor público

A literatura empírica sobre a adequação de organizações brasileiras à LGPD indica um cenário de maturidade ainda incipiente. Canedo *et al*. [2021], em *survey* com organizações públicas e privadas, identificam desafios estruturais de conformidade, como a dificuldade de mapear dados pessoais, a ausência de processos formais e a escassez de pessoal especializado, problemas que se agravam em municípios de médio e pequeno porte. Neitzke *et al*. [2023] avaliam um *checklist* de atributos de qualidade de conformidade à LGPD aplicado em um órgão governamental e demonstram a utilidade de instrumentos estruturados para identificar falhas e orientar correções, abordagem coerente com a adotada nesta pesquisa. No plano da engenharia de software, Rocha *et al*. [2023] propõem um guia para implementar os princípios da lei no desenvolvimento, e Cerqueira *et al*. [2023] apresentam um *checklist* de inspeção de privacidade para artefatos de software. Na perspectiva do usuário, Chalhoub and Flechais [2022] evidenciam que a forma de comunicação das práticas de proteção de dados afeta a confiança, e que controles técnicos corretos convivem com transparência deficiente.

Há, ainda, uma linha internacional de estudos que mede a conformidade de *websites* por observação externa, e não por percepção declarada ou por inspeção de artefatos internos. Degeling *et al*. [2019] mediram, em larga escala e de forma automatizada, as mudanças em políticas de privacidade e avisos de *cookies* de *websites* europeus após a entrada em vigor do GDPR; Matte *et al*. [2020] verificaram se os *banners* de consentimento respeitavam a escolha do usuário; e Linden *et al*. [2020] analisaram, com apoio de processamento automatizado de texto, a evolução do conteúdo das políticas de privacidade após o regulamento. Esses estudos compartilham com o presente trabalho a perspectiva externa, mas diferem dele em três aspectos: concentram-se em *websites* predominantemente privados; tratam uma única dimensão, a jurídica ou a de consentimento; e dependem de medição automatizada, que não alcança julgamentos como a clareza da linguagem ou a explicitação das bases legais por finalidade.

A Tabela 1 sintetiza o posicionamento deste estudo frente aos trabalhos relacionados mais próximos, comparando a unidade de análise, o contexto, as dimensões cobertas, a estratégia e a perspectiva de avaliação e o tipo de validação reportado.

Em síntese, os trabalhos existentes ou tratam isoladamente de uma dimensão da conformidade, seja a segurança, a acessibilidade ou os aspectos jurídicos, ou avaliam artefatos internos do ciclo de desenvolvimento, como requisitos, processos e código, ou ainda medem externamente um único requisito em *websites* privados. O que o instrumento proposto permite avaliar, e os anteriores não permitiam, é a combinação de três propriedades: a comparação entre organizações públicas sem depender de acesso interno; a avaliação conjunta de requisitos jurídicos e das condições de usabilidade e acessibilidade que determinam se a informação chega ao titular; e o julgamento de itens que não são automatizáveis, como a clareza da linguagem e a explicitação das bases legais por finalidade. Não se identificou instrumento validado e replicável que integre as quatro dimensões sociotécnicas da conformidade e seja aplicável por inspeção externa a portais públicos em produção, permitindo comparação direta entre organizações. Este estudo se distingue precisamente por desenvolver, validar quanto ao conteúdo e aplicar empiricamente um instrumento com essas características, sob a ótica de governança de Sistemas de Informação.

2.7 Integração dos eixos teóricos

Os fundamentos discutidos nas subseções anteriores convergem para uma constatação: a conformidade digital em ambientes públicos requer uma abordagem integrada, capaz de articular dimensões jurídicas, técnicas e humanas que, isoladamente, não a explicam. A legislação de proteção de dados estabelece os princípios e define os direitos dos titulares e as responsabilidades dos agentes de tratamento, formando a base normativa da avaliação. A segurança da informação fornece a camada operacional que viabiliza o cumprimento desses princípios, por meio dos controles de confidencialidade, integridade e disponibilidade. A IHC e o design centrado no usuário introduzem a dimensão da experiência e da comunicação entre cidadão e Estado: interfaces intuitivas, linguagem acessível e fluxos de consentimento claros não são apenas recursos de design, mas componentes da própria conformidade, na medida em que a lei pressupõe que o titular tenha condições reais de entender e decidir sobre o uso de suas informações. A acessibilidade digital, por fim, universaliza esses direitos ao garantir que cidadãos com diferentes capacidades possam usufruir equitativamente dos serviços públicos digitais.

Essa integração fundamenta diretamente a proposta metodológica deste trabalho. O instrumento apresentado na Seção 3 traduz princípios legais, requisitos técnicos e diretrizes de usabilidade e acessibilidade em indicadores objetivos, estruturados em uma rubrica que procura captar a natureza multifacetada da conformidade digital em portais públicos, de maneira sistêmica, mensurável e replicável.

3 Método

3.1 Delineamento: desenvolvimento e validação de instrumento

O estudo estrutura-se como o desenvolvimento e a validação empírica de um instrumento de avaliação, seguido de sua aplicação a casos reais. A pesquisa possui natureza aplicada, pois gera conhecimento voltado à solução de um problema concreto, a mensuração da conformidade de portais públicos à LGPD, em um contexto específico [Gil, 2008]. A abordagem é predominantemente quantitativa: os fenômenos investigados são traduzidos em indicadores observáveis e mensuráveis, o que permite atribuir escores a cada critério, comparar unidades de análise e tratar estatisticamente os resultados, características típicas de pesquisas que utilizam instrumentos padronizados de coleta [Lakatos and Marconi, 2017]. O

Tabela 1. Comparação entre os trabalhos relacionados e o presente estudo.

Estudo	Unidade de análise	Contexto	Dimensões	Estratégia e perspectiva	Validação reportada
Araújo *et al*. [2021]	Processos de negócio	Organizacional	Legal	Questionário e modelagem; interna	Proposição do método
Carturan *et al*. [2022]	Áreas de TI	Organizacional	Legal e técnica	*Framework* de implementação; interna	Proposta conceitual, sem avaliação empírica
Canedo *et al*. [2021]	Organizações	Público e privado	Legal e organizacional	*Survey* com profissionais; percepção	Não se aplica (levantamento)
Mendes *et al*. [2021]	Artefatos de software	Desenvolvimento	Legal e privacidade	*Checklist* de inspeção; interna	Proposta inicial
Cerqueira *et al*. [2023]	Artefatos de software	Desenvolvimento	Privacidade	*Checklist* de inspeção; interna	Validação conceitual
Neitzke *et al*. [2023]	Sistemas web de um órgão	Público	Legal e qualidade	*Checklist*; interna	Estudo de caso com profissionais de TI e grupo focal
Barros *et al*. [2023]	Sistemas de informação	Geral	Legal e dados	Estratégias de modelagem; interna	Sem avaliação empírica (minicurso)
Degeling *et al*. [2019]; Linden *et al*. [2020]	*Websites* e políticas	Privado, UE	Legal (políticas e *cookies*)	Medição automatizada; externa	Medição em larga escala; sem rubrica multidimensional
Matte *et al*. [2020]	*Banners* de consentimento	Privado, UE	Consentimento	Medição automatizada e manual; externa	Verificação de conformidade de um único requisito
Este estudo	**Portais municipais em produção**	**Público municipal**	**Legal, segurança, usabilidade e acessibilidade**	**Rubrica; inspeção externa por três avaliadores**	**Validade de conteúdo (IVC) e análise de concordância**

caráter analítico decorre do interesse em examinar como as diferentes dimensões da conformidade se relacionam entre si, e não apenas em descrever a situação de cada portal.

O delineamento é, ainda, exploratório e descritivo. Exploratório porque a adequação de portais municipais à LGPD é um campo em consolidação, no qual é necessário ganhar familiaridade com o problema para torná-lo mais explícito; descritivo porque o estudo caracteriza de forma sistemática o nível de conformidade dos portais por meio de indicadores e sínteses comparativas entre municípios [Gil, 2008; Lakatos and Marconi, 2017].

O instrumento proposto é uma rubrica de avaliação de conformidade à LGPD para portais institucionais, operacionalizada em um Índice de Conformidade. A opção metodológica pela inspeção por avaliadores, em vez de testes com usuários finais, fundamenta-se na tradição de métodos de inspeção da IHC discutida na Seção 2.3: quando o objetivo é verificar a conformidade de uma interface a diretrizes normativas específicas, a inspeção padronizada por avaliadores treinados oferece objetividade, replicabilidade e viabilidade operacional [Barbosa and Silva, 2010]. O percurso metodológico compreendeu três etapas: a construção do instrumento a partir de rastreabilidade normativa; a validação de conteúdo por painel de especialistas; e a aplicação empírica, por três avaliadores independentes, a seis portais reais.

3.2 Hipóteses de pesquisa

Com base no problema de pesquisa e no referencial teórico, formulou-se a seguinte hipótese principal: os portais institucionais das prefeituras mato-grossenses com população superior a 100 mil habitantes apresentam nível insuficiente de conformidade à LGPD, com fragilidades mais acentuadas nas dimensões de transparência e governança da informação e de acessibilidade digital do que nas dimensões de segurança técnica e usabilidade.

Essa hipótese fundamenta-se em três pressupostos extraídos da literatura. O primeiro decorre da observação de que, embora a LGPD esteja vigente desde 2020, a adequação de órgãos públicos aos seus princípios permanece incipiente, sobretudo em municípios de médio porte [Canedo *et al*., 2021; Neitzke *et al*., 2023]. O segundo baseia-se na constatação de que a transparência sobre o tratamento de dados exige não apenas medidas técnicas, mas políticas claras de comunicação com o cidadão, aspecto que tende a ser negligenciado em comparação com a implementação de controles de segurança [Chalhoub and Flechais, 2022]. O terceiro apoia-se na literatura sobre acessibilidade em portais governamentais brasileiros, que aponta deficiências recorrentes na aplicação das diretrizes do eMAG e da WCAG, especialmente fora dos grandes centros metropolitanos [Mendonça and Pereira Neto, 2015]. Do ponto de vista teórico, os três pressupostos são consistentes com a distinção entre infraestrutura de TI e governança da informação discutida na Seção 2.5 [Tallon *et al*., 2013; Abraham *et al*., 2019].

Formularam-se ainda quatro hipóteses secundárias, cada uma alinhada a indicadores específicos da rubrica, de modo que os dados coletados permitissem sua verificação direta.

- **H1**: os portais apresentam políticas de privacidade genéricas ou ausentes, sem identificação clara do encarregado e sem descrição das finalidades específicas do tratamento.
- **H2**: a maioria dos portais adota protocolo seguro HTTPS, porém apresenta deficiências nos mecanismos de consentimento para *cookies* e na comunicação sobre tecnologias de rastreamento.
- **H3**: as informações relativas à proteção de dados encontram-se dispersas nos portais, com linguagem técnica e fluxos de navegação que dificultam a compreensão e o exercício dos direitos pelo cidadão.
- **H4**: os portais não atendem plenamente às diretrizes de acessibilidade do eMAG e da WCAG 2.2, restringindo o acesso de pessoas com deficiência às informações sobre tratamento de dados pessoais.

A verificação dessas hipóteses é apresentada na Seção 4.7.

3.3 Considerações éticas

O projeto foi submetido ao Comitê de Ética em Pesquisa da área de Humanidades da Universidade Federal de Mato Grosso, por meio da Plataforma Brasil, em conformidade com a Resolução nº 510/2016 do Conselho Nacional de Saúde, e foi aprovado (CAAE 90651225.4.0000.5690; Parecer nº 7.900.910). Embora o estudo utilize exclusivamente dados de acesso público provenientes de portais institucionais, a submissão ao comitê justificou-se pelo contexto de análise, que envolve tratamento de dados pessoais e princípios de proteção à privacidade. Os três avaliadores são voluntários externos que assinaram Termo de Consentimento Livre e Esclarecido, autorizando a divulgação dos resultados com sigilo absoluto de suas identidades; seus nomes foram substituídos pelos códigos A, B e C em todos os registros da pesquisa.

3.4 Construção do instrumento: rubrica com rastreabilidade normativa

A escolha da rubrica como formato do instrumento possui fundamentação consolidada na literatura de avaliação. Rubricas organizam critérios, descritores e níveis graduais de qualidade para orientar julgamentos consistentes, reduzindo subjetividades e permitindo análises comparáveis entre avaliadores [Stevens and Levi, 2013]. Brookhart [2018] destaca que rubricas transformam expectativas abstratas em indicadores observáveis e graduados, favorecendo transparência, reprodutibilidade e rigor metodológico, e Andrade [2005] reconhece sua utilidade em contextos que exigem clareza de critérios e documentação sistemática de evidências. Ao adotar uma rubrica, buscou-se um formato capaz de traduzir exigências legais, normativas e conceituais em parâmetros mensuráveis.

Os critérios foram derivados por rastreabilidade normativa: cada item da rubrica foi vinculado a pelo menos uma fonte legal, técnica ou conceitual, por meio de um mapeamento cruzado entre os dispositivos da LGPD, em especial os artigos 6º, 7º, 9º, 18, 41, 46 e 50, os controles das seções 5, 6 e 8 da ISO/IEC 27002:2022, as diretrizes de nível A a AAA da WCAG 2.2, as recomendações do eMAG e os princípios de usabilidade consolidados na literatura de IHC. Esse mapeamento resultou em uma matriz de correspondência que permitiu identificar quais aspectos da conformidade eram contemplados por mais de um referencial, conferindo robustez aos critérios selecionados.

Partiu-se de dezoito critérios potenciais. Após análise de sobreposição, de viabilidade de observação por inspeção externa e do retorno dos especialistas na etapa de validação, consolidaram-se treze indicadores pontuáveis, uma vez que o indicador 10 foi desdobrado em 10A e 10B, com pontuação máxima de 26 pontos. Os critérios descartados referiam-se a aspectos que exigiam acesso a informações internas das prefeituras, como a existência de relatórios de impacto à proteção de dados, elementos que não são verificáveis pela inspeção externa do portal.

Cada indicador recebeu uma pergunta orientadora, descritores por nível de conformidade, a referência normativa correspondente e o princípio de design associado. Adotou-se uma escala ordinal de três níveis: 0 quando o requisito não é evidenciado, 1 quando aparece de forma parcial, limitada ou pouco clara, e 2 quando é atendido de forma clara, completa e alinhada às boas práticas. A escala de três níveis foi preferida à lógica binária típica de *checklists* porque permite registrar situações de conformidade parcial, frequentes em portais que apresentam elementos normativos de forma incompleta. Uma escala de cinco níveis chegou a ser considerada e foi descartada após o pré-teste, por gerar ambiguidade na diferenciação entre níveis intermediários e comprometer a concordância entre avaliadores, decisão alinhada à recomendação de Brookhart [2018] de que escalas com três a quatro níveis equilibram capacidade discriminante e clareza dos descritores.

Os treze indicadores organizam-se em quatro critérios, que constituem os eixos temáticos da avaliação:

- **Conformidade legal e governança da informação**, com os indicadores 1, 3, 5, 8, 11 e 12 e máximo de 12 pontos: política de privacidade, identificação do encarregado, bases legais, data de atualização, retenção e compartilhamento de dados.
- **Segurança da informação**, com os indicadores 6, 7 e 9 e máximo de 6 pontos: consentimento e *cookies*, protocolo HTTPS e canal de incidentes.
- **Usabilidade e design centrado no usuário**, com os indicadores 2 e 4 e máximo de 4 pontos: acesso à página de LGPD e clareza na comunicação dos direitos do titular.
- **Acessibilidade digital e inclusão informacional**, com os indicadores 10A e 10B e máximo de 4 pontos: contraste e alternativas textuais, e navegação por teclado com suporte a leitores de tela.

Os indicadores dos eixos de usabilidade e de acessibilidade merecem justificativa específica, pois não correspondem a requisitos formais da LGPD no mesmo sentido que, por exemplo, a identificação do encarregado. Sua inclusão decorre de dois fundamentos. O primeiro é que a própria LGPD exige que as informações sobre o tratamento sejam disponibilizadas "de forma clara, adequada e ostensiva" (art. 9º) e garante aos titulares informações claras, precisas e facilmente acessíveis (art. 6º, VI); a localização da página de privacidade (indicador 2) e a linguagem com que os direitos são explicados (indicador 4) operacionalizam essas exigências no nível da interface. O segundo é que a Lei nº 13.146/2015 torna obrigatória a acessibilidade dos sítios mantidos por órgãos de governo (art. 63), de modo que uma informação de privacidade inacessível a pessoas com deficiência não é "facilmente acessível" a todos os titulares [Brasil, 2015]. Esses indicadores medem, portanto, as condições de efetividade da transparência exigida pela lei, e não boas práticas de usabilidade em geral; por essa razão, avaliam apenas as seções do portal relacionadas à privacidade e à LGPD. A Seção 4.5 examina como os resultados se alteram quando esses indicadores são excluídos do índice.

A rubrica completa, com os treze indicadores, os descritores por nível, a base normativa e o princípio de design associado a cada item, é reproduzida no Apêndice A, permitindo sua replicação em outros contextos. A matriz completa das notas individuais dos três avaliadores é reproduzida no Apêndice B.

3.5 Validação do instrumento: validade de conteúdo

A validade de conteúdo foi aferida por um painel de especialistas, calculando-se o Índice de Validade de Conteúdo, o IVC, definido como a razão entre o número de especialistas que atribuíram nota igual ou superior a 3 a um item e o número total de especialistas que o avaliaram [Lynn, 1986; Alexandre and Coluci, 2011]. Adotou-se o ponto de corte de 0,80, conforme a recomendação de Lynn [1986] para painéis compostos por três a cinco juízes. Os especialistas julgaram cada critério segundo quatro dimensões: relevância, entendida como pertinência ao construto de conformidade à LGPD; clareza da redação; aplicabilidade, isto é, observabilidade por inspeção externa; e completude, entendida como ausência de lacunas ou redundâncias. Os pareceres foram registrados de forma narrativa integrada ao próprio instrumento, em consonância com a estratégia de validação contextualizada recomendada por Rubio *et al*. [2003], segundo a qual a qualidade da validação de conteúdo depende da análise integrada dos itens em seu contexto real de aplicação.

O IVC resultante foi 1,00 para todos os itens, e as sugestões qualitativas dos especialistas foram incorporadas antes da aplicação, incluindo o desdobramento do indicador de acessibilidade em dois itens distintos. Um pré-teste de aplicação precedeu a coleta definitiva, permitindo ajustar a redação dos descritores e confirmar a operacionalidade da escala.

3.6 Aplicação: coleta nos portais

O instrumento foi aplicado aos portais das seis prefeituras de Mato Grosso com população superior a 100 mil habitantes. O recorte justifica-se pela representatividade populacional desses municípios, que concentram cerca de 44% da população estadual, pelo seu dinamismo econômico e pela maior probabilidade de existência de estruturas formais de tecnologia da informação, condições que tornam a comparação entre portais mais equilibrada.

Cada portal foi avaliado de forma independente por três aplicadores, com registro sistemático de evidências por meio de capturas e gravações de tela. A coleta ocorreu entre 9 e 29 de maio de 2026. Cada aplicador registrou na ficha de avaliação as datas de início e de término da inspeção de cada portal: o aplicador A avaliou os seis portais entre 24 e 25 de maio; a aplicadora B, entre 9 e 24 de maio; e o aplicador C, entre 24 e 29 de maio. Como os portais são sistemas dinâmicos, o intervalo de até vinte dias entre as inspeções de um mesmo portal é tratado como fonte potencial de divergência na Seção 4.6. Para reduzir viés na consolidação, os portais foram identificados por códigos de anonimização durante o processamento das notas, e a correspondência entre código e município era conhecida apenas pelo pesquisador responsável.

Os três aplicadores são profissionais da área de tecnologia da informação, com formação e experiência em segurança da informação, redes e desenvolvimento de sistemas, e são identificados nesta pesquisa pelos códigos A, B e C, em coerência com a estratégia de anonimização adotada. O aplicador A é bacharel em Ciência da Computação, com pós-graduação em Segurança Cibernética e da Informação e 14 anos de experiência em cibersegurança e conformidade em órgãos públicos estaduais e federais. A aplicadora B é tecnóloga em Defesa Cibernética, com pós-graduações em Redes de Computadores e em Segurança de Redes e cerca de 6 anos de atuação em segurança e telecomunicações. O aplicador C é tecnólogo em Defesa Cibernética, com pós-graduações em Engenharia da Computação e em Análise e Desenvolvimento de Sistemas e cerca de 5 anos de experiência em desenvolvimento de sistemas em organizações públicas e privadas. A adoção de três avaliadores independentes com perfis técnicos complementares teve por finalidade permitir a consolidação das notas por tendência central e a verificação da dispersão entre julgamentos, conferindo robustez ao dado quantitativo.

3.7 Análise dos dados

As três notas de cada indicador foram consolidadas pela mediana, medida apropriada a escalas ordinais por preservar o valor central e neutralizar pontuações isoladas. O Índice de Conformidade de cada portal foi calculado como a razão entre a pontuação obtida e os 26 pontos possíveis, multiplicada por 100, e classificado nas três faixas definidas na Tabela 2, construídas pela divisão do intervalo percentual em terços iguais.

Duas decisões de construção do índice precisam ser explicitadas. A primeira é a ponderação uniforme por indicador. Na ausência de evidência empírica ou de orientação regulatória sobre a importância relativa de cada requisito, atribuir pesos diferenciados introduziria um julgamento arbitrário adicional, e a ponderação uniforme é a opção mais parcimoniosa e transparente [OECD and European Commission Joint Research Centre, 2008]. Essa escolha não é neutra quanto aos eixos: como o eixo de conformidade legal e governança reúne seis dos treze indicadores, ele responde por 12 dos 26 pontos, cerca de 46% do índice, o que é coerente com o fato de reunir os requisitos diretamente derivados da LGPD, mas deve ser considerado na leitura dos resultados. A segunda decisão são os pontos de corte das faixas. As faixas baixa, moderada e alta são classificações analíticas propostas por este estudo para facilitar a comparação, e não limiares de conformidade estabelecidos pela LGPD, pela ANPD ou por qualquer órgão regulador. Como ambas as decisões são convencionais, a robustez dos resultados a elas foi examinada por análise de sensibilidade [OECD and European Commission Joint Research Centre, 2008], recalculando-se o índice sob três esquemas alternativos: peso igual para os quatro eixos; exclusão dos indicadores de usabilidade e acessibilidade que não correspondem a requisitos formais da lei (2, 10A e 10B); e consolidação pela média, em vez da mediana, das três notas.

A concordância entre os três aplicadores foi examinada de duas formas complementares. A primeira consistiu na distribuição das amplitudes de divergência por par município–indicador, isto é, na verificação de quantos casos apresentaram consenso pleno, divergência de um ponto ou divergência de dois pontos na escala. A segunda consistiu no cálculo do coeficiente Fleiss *kappa*. Registra-se, desde já, uma ressalva metodológica relevante para a interpretação desse coeficiente: o Fleiss *kappa* não ponderado trata todas as discordâncias como equivalentes, de modo que uma divergência entre 1 e 2 recebe o mesmo peso de uma divergência entre 0 e 2. Em escalas ordinais curtas e com distribuição concentrada, essa propriedade penaliza fortemente o coeficiente. Por essa razão, calcularam-se também dois coeficientes que conside-

Tabela 2. Faixas de classificação do Índice de Conformidade.

Faixa	Intervalo do IC	Interpretação
Baixa	0% a 33,2%	Conformidade insuficiente; ausência da maioria dos requisitos substantivos.
Moderada	33,3% a 66,6%	Conformidade parcial; requisitos atendidos de forma incompleta ou heterogênea.
Alta	66,7% a 100%	Conformidade consistente; requisitos atendidos de forma ampla e regular.

ram a natureza ordinal da escala: o alfa de Krippendorff com métrica ordinal, aplicável a mais de dois avaliadores [Hayes and Krippendorff, 2007; Krippendorff, 2018], e o *kappa* de Cohen com ponderação quadrática para cada par de avaliadores. Os coeficientes ponderados são apresentados como complemento, e não como substitutos, do Fleiss *kappa*. Por fim, para identificar as causas das divergências, as observações escritas pelos avaliadores nas fichas de avaliação foram comparadas nos casos de divergência de dois pontos.

4 Resultados

4.1 Índice de Conformidade geral

O Índice de Conformidade médio foi de 55,8%, na faixa moderada, e nenhum portal alcançou conformidade plena. O desempenho variou de 30,8% em Cuiabá a 84,6% em Sinop, sendo este o único portal na faixa alta e aquele o único na faixa baixa. A ordenação completa foi: Sinop com 84,6%, Rondonópolis com 65,4%, Tangará da Serra com 61,5%, Sorriso com 53,8%, Várzea Grande com 38,5% e Cuiabá com 30,8%. Nos seis casos analisados, não se observou padrão entre porte populacional e pontuação: a capital, maior município do estado, obteve o menor índice do conjunto. Com seis casos, essa observação descreve a amostra e não permite afirmar a inexistência de relação entre as duas variáveis.

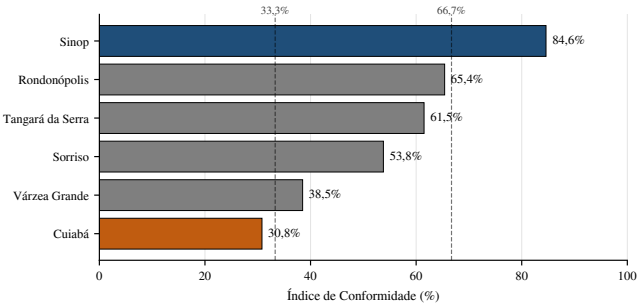


Figura 1. Índice de Conformidade geral por município, com as faixas baixa, moderada e alta.

4.2 Análise por eixo temático

Os índices parciais médios por eixo mostram que a conformidade legal e a governança da informação, com média de 51,4%, e a acessibilidade digital, com 54,2%, ficaram abaixo da segurança da informação, com 61,1%, e da usabilidade, com 62,5%. Na amostra analisada, portanto, os portais obtiveram pontuações mais altas nos aspectos técnicos e de navegação do que nos aspectos jurídicos e de inclusão.

A leitura por município reforça o diagnóstico. Sinop lidera nos quatro eixos, com destaque para a governança legal, na qual atinge 91,7%. Cuiabá, com 16,7%, e Várzea Grande, com 33,3%, concentram suas maiores fragilidades exatamente no eixo legal. A acessibilidade mostrou-se notavelmente uniforme: cinco dos seis municípios estacionaram em 50%, o que sugere um teto comum de atendimento apenas parcial às diretrizes do eMAG e da WCAG 2.2.



Figura 2. Mapa de calor do Índice de Conformidade parcial por eixo temático e município, com municípios ordenados pelo IC geral.

4.3 Análise individual dos portais

A leitura individual dos portais complementa os índices agregados ao revelar perfis distintos de conformidade. Sinop, com 84,6% e 22 dos 26 pontos possíveis, apresenta a distribuição mais favorável do conjunto: das treze notas consolidadas, nove são de conformidade plena e as quatro restantes são de conformidade parcial, sem nenhuma nota nula. Trata-se de um portal sem ausências completas de requisitos, que atende plenamente aos elementos centrais exigidos pela LGPD, como a identificação do encarregado, a explicitação das bases legais e a transparência sobre compartilhamento e retenção, restando-lhe avançar sobretudo na manutenção documental e na completude da acessibilidade.

Rondonópolis, com 65,4%, situa-se no limite superior da faixa moderada, com desempenho pleno na tríade de transparência e governança formada pela política de privacidade, pelo acesso rápido à página de LGPD e pelo contato do encarregado, além da política de retenção. Sua principal lacuna concentra-se na manutenção e atualização da política, único indicador em que registrou ausência total. Tangará da Serra, com 61,5%, destaca-se no eixo de segurança da informação, com conformidade plena tanto no consentimento e gestão de *cookies* quanto no protocolo HTTPS, mas apresenta ausências nos requisitos de ciclo de vida e governança dos dados, especificamente na atualização da política e na retenção. Sorriso, com 53,8%, demonstra solidez na camada de transparência, mas fragilidade na profundidade jurídica: não explicita as bases legais do tratamento nem oferece mecanismo adequado de consentimento para *cookies*.

Os dois últimos colocados apresentam perfis qualitativamente distintos. Várzea Grande, com 38,5%, é o portal com a distribuição mais concentrada no nível parcial: uma única nota plena, no protocolo HTTPS, oito notas parciais e quatro nulas. Esse perfil caracteriza um portal que implementa de forma incompleta a maior parte dos requisitos, sem consolidar conformidade plena em praticamente nenhum deles, e que registra o menor índice de usabilidade do conjunto, de 25%. Cuiabá, com 30,8%, é o único portal na faixa baixa

Tabela 3. Matriz consolidada de pontuações, obtidas pela mediana das três avaliações, por indicador e município, com o total e o Índice de Conformidade.

Indicador	Cuiabá	Várzea Grande	Rondonópolis	Sinop	Sorriso	Tangará da Serra
1. Transparência (existência)	2	1	2	2	2	2
2. Transparência (acesso)	2	1	2	1	2	2
3. Governança (encarregado)	0	1	2	2	2	2
4. Direitos do titular	0	0	1	2	1	1
5. Bases legais	0	1	1	2	0	1
6. Consentimento e *cookies*	0	0	1	2	0	2
7. Segurança mínima (HTTPS)	2	2	2	2	2	2
8. Atualização da política	0	0	0	1	0	0
9. Segurança e incidentes	0	1	1	1	1	1
10A. Acessibilidade (contraste)	1	1	1	1	1	1
10B. Acessibilidade (teclado)	1	1	1	2	1	1
11. Retenção de dados	0	0	2	2	1	0
12. Compartilhamento com terceiros	0	1	1	2	1	1
Total (máx. 26)	**8**	**10**	**17**	**22**	**14**	**16**
IC (%)	**30,8**	**38,5**	**65,4**	**84,6**	**53,8**	**61,5**

Tabela 4. Índice de Conformidade parcial por eixo temático e município, em porcentagem, e IC geral.

Município	Legal e gov.	Segurança	Usabilidade	Acessib.	IC geral
Cuiabá	16,7	33,3	50,0	50,0	30,8
Várzea Grande	33,3	50,0	25,0	50,0	38,5
Rondonópolis	66,7	66,7	75,0	50,0	65,4
Sinop	91,7	83,3	75,0	75,0	84,6
Sorriso	50,0	50,0	75,0	50,0	53,8
Tangará da Serra	50,0	83,3	75,0	50,0	61,5
Média	**51,4**	**61,1**	**62,5**	**54,2**	**55,8**

e apresenta a distribuição mais desfavorável: apenas três indicadores plenos, dois parciais e oito ausências totais, que abrangem requisitos centrais da lei, como o contato do encarregado, os direitos do titular, as bases legais, o consentimento de *cookies*, o canal de incidentes, a retenção e o compartilhamento. Em termos quantitativos, a capital atende apenas à camada mais superficial e visível da conformidade, composta pela existência de uma política e pela comunicação cifrada, com ausência da maioria dos elementos de substância jurídica.

4.4 Desempenho por indicador

A análise agregada por indicador identifica quais requisitos são mais e menos atendidos pelo conjunto dos portais, e o padrão que emerge é estratificado com clareza. No patamar superior situa-se o protocolo HTTPS, indicador 7, único requisito com nota máxima em todos os portais, seguido da existência de política de privacidade, com média 1,83, e do acesso à página de LGPD, com 1,67. Esses valores indicam que os elementos mais visíveis e estruturais da conformidade, ligados à existência formal da política e à comunicação cifrada, já se encontram amplamente incorporados.

No patamar inferior concentram-se os requisitos de maior densidade jurídica e de governança. A data de atualização da política, indicador 8, obteve a menor média de toda a avaliação, 0,17, com nota acima de zero em apenas um dos seis portais, o que evidencia ausência sistemática de controle sobre a vigência das políticas. Apresentaram igualmente médias baixas, todas em 0,83, os indicadores relativos às bases legais do tratamento, aos direitos do titular em linguagem acessível, ao consentimento e *cookies*, ao canal de incidentes e à retenção de dados. Os indicadores de acessibilidade mantiveram-se no nível intermediário, com 10A em 1,00 e 10B em 1,17, sem que nenhum portal atingisse desempenho pleno consistente. Na amostra, portanto, as menores pontuações não estão na existência formal da política, mas no seu conteúdo e na sua manutenção.

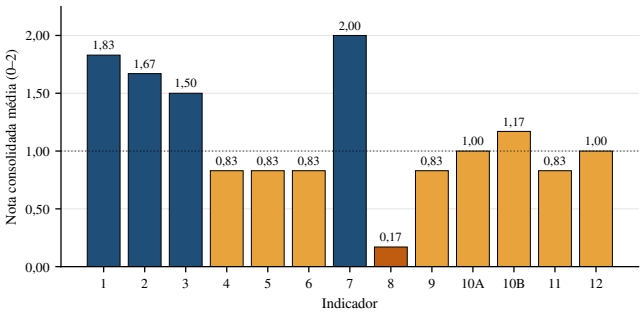


Figura 3. Desempenho médio por indicador nos seis municípios, calculado como média das medianas na escala de 0 a 2.

4.5 Sensibilidade do índice à ponderação e à consolidação

A Tabela 5 apresenta o Índice de Conformidade de cada portal sob o esquema original e sob os três esquemas alternativos descritos na Seção 3.7. A ordenação dos portais manteve-se praticamente inalterada: Sinop ocupa a primeira posição e Cuiabá a última em todos os esquemas, e a única alteração é o empate entre Rondonópolis e Tangará da Serra quando

os eixos recebem peso igual. A exclusão dos indicadores 2, 10A e 10B também preserva a ordenação, o que indica que os resultados não dependem dos itens de usabilidade e acessibilidade. A classificação em faixas é menos robusta que a ordenação: com peso igual por eixo, Cuiabá passa da faixa baixa para a moderada (37,5%), porque esse esquema reduz o peso do eixo legal, no qual o portal obteve sua menor pontuação. A afirmação de que Cuiabá é o único portal na faixa baixa depende, portanto, da ponderação adotada, ao passo que sua posição relativa não depende.

Tabela 5. Índice de Conformidade (%) sob esquemas alternativos de ponderação e de consolidação.

Município	Original	Eixos iguais	Sem 2, 10A, 10B	Média
Sinop	84,6	81,3	90,0	79,5
Rondonópolis	65,4	64,6	65,0	65,4
Tangará da Serra	61,5	64,6	60,0	59,0
Sorriso	53,8	56,3	50,0	52,6
Várzea Grande	38,5	39,6	35,0	43,6
Cuiabá	30,8	37,5	20,0	30,8

Original: 13 indicadores com peso igual e consolidação pela mediana. Eixos iguais: média simples dos quatro índices parciais. Sem 2, 10A, 10B: 10 indicadores, máximo de 20 pontos. Média: consolidação pela média das três notas.

4.6 Concordância entre aplicadores

Dos 78 pares município–indicador, 30,8% apresentaram consenso pleno, 55,1% divergência de um ponto e 14,1% divergência de dois pontos. O Fleiss *kappa* foi de 0,260. Os coeficientes que consideram a ordem da escala foram mais altos, mas ainda indicam concordância limitada: o alfa de Krippendorff ordinal foi de 0,427, abaixo do limiar de 0,667 que Krippendorff [2018] considera mínimo para conclusões provisórias, e o *kappa* de Cohen com ponderação quadrática variou entre 0,409 e 0,481 entre os pares de avaliadores, faixa descrita como concordância moderada por Landis and Koch [1977]. Esse resultado não é tratado aqui apenas como limitação estatística, mas como informação sobre o instrumento, examinada em três níveis.

Por indicador. A Tabela 6 mostra que a discordância não se distribui de modo uniforme. Os indicadores 1, 7, 8 e 10B, que verificam a presença de elementos objetivos, não tiveram nenhuma divergência de dois pontos. As maiores amplitudes médias ocorreram nos indicadores 4 (direitos do titular em linguagem simples) e 3 (dados do encarregado), seguidos de 5, 6, 10A e 11. A exclusão de qualquer indicador isolado altera pouco o alfa (de 0,369 a 0,459), o que indica que a baixa concordância não decorre de um único item defeituoso.

Por avaliador. Parte da discordância é sistemática, e não aleatória. A nota média atribuída foi de 1,15 pelo aplicador A, 0,94 pela aplicadora B e 1,22 pelo aplicador C, o que indica diferença de rigor na aplicação dos descritores. Apesar disso, a ordenação dos portais pelos totais de cada avaliador foi convergente (correlação de Spearman entre 0,74 e 0,90 entre os pares): Cuiabá obteve o menor total para os três avaliadores, e Sinop o maior para A e B, empatado com Rondonópolis para C. A divergência afeta mais as notas de cada item do que a posição relativa dos portais.

Pelas causas registradas. A comparação das observações escritas nos casos de divergência de dois pontos indicou cinco causas principais, cada uma associada a um refinamento do instrumento. (i) *Perímetro de inspeção indefinido.* Nos indicadores 3, 4 e 12, divergências de dois pontos ocorreram quando um avaliador examinou apenas o texto da política de privacidade e outro localizou a informação em páginas vinculadas, como uma página própria do encarregado ou uma política de retenção separada; no indicador 10A, um avaliador examinou apenas as seções de privacidade e outro incluiu elementos da página inicial, como logotipos e *banners*. O refinamento consiste em definir o perímetro: a página inicial, a página de privacidade ou LGPD e todos os documentos e páginas vinculados a ela, com registro obrigatório das URLs examinadas. (ii) *Fonte de informação conflitante.* No indicador 8, um portal exibia a data de revisão declarada no texto da política e, ao mesmo tempo, uma data de atualização gerada pela plataforma de publicação; os avaliadores adotaram datas diferentes. O refinamento consiste em estabelecer que prevalece a data declarada no documento. (iii) *Interpretação divergente do nível pleno.* Nos indicadores 5 e 6, um avaliador atribuiu nota 2 a elementos que os descritores classificam como parciais, como a lista genérica de hipóteses de compartilhamento tomada como explicitação das bases legais, ou a simples presença de um *banner* de *cookies* sem opção de recusa. O refinamento consiste em acrescentar aos descritores contraexemplos explícitos do que não constitui conformidade plena. (iv) *Julgamento de qualidade sem âncora.* O indicador 4, único sem nenhum consenso, depende da avaliação da clareza da linguagem. O refinamento consiste em ancorar os níveis na contagem dos direitos do art. 18 que são listados e explicados, com exemplos de referência para cada nível. (v) *Condições de coleta.* As inspeções de um mesmo portal ocorreram com até vinte dias de intervalo, e parte das notas não foi acompanhada de justificativa escrita, o que impediu reconstruir a razão de algumas divergências. O refinamento consiste em concentrar a coleta de cada portal em uma janela curta, exigir justificativa e evidência para cada nota e realizar sessão de calibração com um portal piloto antes da coleta.

Tabela 6. Distribuição das divergências entre os três aplicadores por indicador (seis municípios).

Indicador	Consenso	Div. 1 pt	Div. 2 pts	Ampl. média
1. Política (existência)	3	3	0	0,50
2. Acesso à página	2	3	1	0,83
3. Encarregado	2	1	3	1,17
4. Direitos do titular	0	4	2	1,33
5. Bases legais	1	4	1	1,00
6. *Cookies*	1	4	1	1,00
7. HTTPS	3	3	0	0,50
8. Atualização	3	3	0	0,50
9. Incidentes	2	4	0	0,67
10A. Contraste	1	4	1	1,00
10B. Teclado	3	3	0	0,50
11. Retenção	1	4	1	1,00
12. Compartilhamento	2	3	1	0,83
Total	**24**	**43**	**11**	**0,82**

Esses refinamentos não foram aplicados retroativamente às notas deste estudo, que permanecem as originalmente atribuídas. Eles constituem uma versão revisada dos procedimentos de aplicação, cuja efetividade para elevar a concordância deve ser verificada em aplicações futuras. A consolidação pela mediana atenua o efeito das divergências sobre os índices, como mostra a proximidade entre os resultados obtidos pela mediana e pela média na Tabela 5, mas não as elimina.

4.7 Verificação das hipóteses

A hipótese principal do estudo previa nível insuficiente de conformidade, com fragilidades mais acentuadas em transparência, governança da informação e acessibilidade digital do que em segurança técnica e usabilidade. Os resultados são compatíveis com essa hipótese na amostra analisada: o IC médio de 55,8% caracteriza conformidade observável apenas parcial, e a ordem dos índices por eixo corresponde à relação prevista, com governança legal e acessibilidade abaixo de segurança e usabilidade. Dado o caráter exploratório do estudo e o número de casos, trata-se de compatibilidade descritiva, e não de teste estatístico da hipótese.

Das quatro hipóteses secundárias, duas foram compatíveis com os dados e duas o foram parcialmente. H2 foi compatível com os dados, isto é, que os portais adotam majoritariamente HTTPS, mas apresentam deficiências no consentimento para *cookies*, contraste expresso pela média máxima do indicador 7 diante da média de 0,83 do indicador 6. H4 também foi compatível com os dados, o atendimento apenas parcial às diretrizes de acessibilidade, com cinco dos seis municípios em 50% no eixo. H1 e H3 foram compatíveis apenas em parte: a existência formal das políticas superou a expectativa de ausência, mas convive com a falta de especificação das bases legais e com a ausência quase total de controle de vigência; a página de LGPD mostrou-se localizável na média dos portais, mas a explicação dos direitos em linguagem simples e a indicação da data de atualização permanecem deficientes.

5 Discussão

5.1 Implicações para governança de SI e governo eletrônico

Nos portais analisados, as pontuações foram mais altas nos requisitos satisfeitos por decisões pontuais e verificáveis de uma só vez, como a comunicação cifrada e a existência de uma política localizável, e mais baixas nos requisitos que dependem de processos organizacionais contínuos: a explicitação das bases legais, a gestão do consentimento, a manutenção documental, os canais de incidentes e as políticas de retenção e compartilhamento. A distinção de Tallon *et al*. [2013] entre governança de TI, voltada à infraestrutura, e governança da informação, voltada ao ativo informacional e ao seu ciclo de vida, detalhada por Abraham *et al*. [2019] em estruturas de decisão, papéis e responsabilidades, oferece uma leitura para esse padrão. O indicador de maior média, o HTTPS, pertence à primeira camada; o de menor média, a datação e revisão da política (média de 0,17, ante 2,00 do HTTPS), pertence à segunda e só é satisfeito por uma rotina que se repete no tempo e requer responsável designado. Os dados não permitem afirmar que os municípios percorram uma sequência temporal entre as camadas, pois o estudo é transversal, nem determinar a maturidade dos processos internos que produziram essas diferenças; eles mostram a diferença entre as camadas no nível daquilo que o portal torna visível.

Para o conhecimento de SI, o estudo acrescenta duas contribuições que vão além de confirmar que governança envolve mais do que infraestrutura técnica. A primeira é operacional: as discussões de Tallon *et al*. [2013] e Abraham *et al*. [2019] tratam a governança da informação como arranjo interno da organização, observável por entrevistas ou documentos internos. Este trabalho mostra que parte desse arranjo deixa traços verificáveis no artefato voltado ao cidadão, como a data de revisão de uma política, a indicação das bases legais por finalidade ou a existência de um canal de incidentes, e que esses traços podem ser medidos de forma comparável entre organizações sem acesso interno. Em contextos nos quais o cidadão não pode deixar de usar o sistema, como discutido a partir de Dinev and Hart [2006], a visibilidade desses traços é ela própria uma condição de *accountability*. A segunda contribuição é metodológica e decorre da análise de concordância: os indicadores que verificam a presença de um elemento (1, 7, 8 e 10B) tiveram amplitude média de divergência de 0,50, enquanto os que exigem julgar a adequação do conteúdo (3, 4, 5, 6 e 11) tiveram amplitude média igual ou superior a 1,00. A avaliação externa da governança da informação é, portanto, mais confiável quanto à existência dos traços do que quanto à sua qualidade, o que indica onde instrumentos futuros, deste ou de outros autores, precisam concentrar o esforço de especificação.

O estudo também se relaciona com a agenda brasileira de pesquisa em SI. O relatório *II GranDSI-BR: Grandes Desafios de Sistemas de Informação no Brasil 2026–2036* [Araujo *et al*., 2025] inclui entre seus temas a governança digital e a proteção de dados, bem como a inclusão e a acessibilidade. O instrumento aqui proposto se situa na interseção desses temas: trata a proteção de dados em sistemas de governo digital como objeto de avaliação sociotécnica e incorpora a acessibilidade como condição de efetividade dos direitos do titular. Nesse sentido, a rubrica e o protocolo de aplicação revisado oferecem um ponto de partida verificável para estudos que acompanhem, ao longo da década coberta pelo relatório, a situação dos sistemas de governo digital municipal quanto à proteção de dados.

O resultado dialoga, ainda, com a agenda de valor público do governo digital. Twizeyimana and Andersson [2019] identificam a confiança do cidadão e a inclusão social entre as dimensões de valor que o governo eletrônico deveria gerar. Os eixos com menores pontuações, governança legal com 51,4% e acessibilidade com 54,2%, são os que sustentam essas duas dimensões: sem bases legais explícitas e sem canal de incidentes, a *accountability* não é verificável pelo cidadão, e sem acessibilidade não há inclusão. A convivência entre HTTPS pleno e consentimento de *cookies* deficiente é compatível com o descompasso apontado por Chalhoub and Flechais [2022] entre controles técnicos e transparência efetiva, e o atendimento parcial uniforme na acessibilidade é compatível com as deficiências relatadas por Mendonça and Pereira Neto [2015].

Quanto ao porte populacional, o fato de a capital ocupar a última posição e Sinop a primeira indica apenas que, nesta amostra, a pontuação não acompanhou o porte. Uma explicação plausível é que a conformidade observável dependa mais de fatores institucionais, como a prioridade atribuída pela gestão, a existência de competências internas e a continuidade das rotinas, do que da escala do município, explicação coerente com a ênfase de Abraham *et al*. [2019] em estruturas de decisão e responsabilidades. Esses fatores, porém, não foram medidos neste estudo, e a relação deve ser tratada como hipótese a ser investigada em amostras maiores. A implicação prática que os dados autorizam é mais limitada: programas de

adequação à LGPD não devem pressupor que os municípios maiores estejam necessariamente mais avançados.

Como a LGPD compartilha com o GDPR a arquitetura de princípios, bases legais e direitos do titular, a rastreabilidade normativa do instrumento facilita sua adaptação a outras jurisdições, pela substituição das referências aos artigos da lei brasileira pelos dispositivos correspondentes do regulamento europeu. Do ponto de vista gerencial, o índice pode operar como ferramenta de acompanhamento periódico, permitindo que uma prefeitura acompanhe sua evolução e priorize investimentos com base em lacunas mensuradas, e que órgãos de controle e associações municipalistas realizem levantamentos comparativos, desde que adotado o protocolo de aplicação revisado descrito na Seção 4.6.

5.2 Recomendações priorizadas para gestores públicos

As lacunas identificadas permitem formular recomendações práticas, priorizadas por um critério objetivo: a diferença entre a nota máxima possível e a nota média obtida em cada indicador. Quanto maior a lacuna, maior a prioridade de adequação. Sob esse critério, as ações de maior prioridade são, nesta ordem, a instituição de rotina de atualização e datação das políticas de privacidade, indicador de pior desempenho de toda a avaliação; a explicitação das bases legais do tratamento por finalidade, conforme o artigo 7º da LGPD; a descrição dos direitos do titular em linguagem simples, com indicação do canal para seu exercício, conforme o artigo 18; a adequação dos mecanismos de consentimento para *cookies* às orientações do guia da ANPD; a criação de canal formal de comunicação de incidentes, alinhado à ISO/IEC 27002; e a definição e publicação de políticas de retenção de dados.

No eixo de usabilidade, recomenda-se padronizar a localização da seção de privacidade e simplificar a comunicação com o cidadão. No eixo de acessibilidade, recomenda-se corrigir contraste, alternativas textuais e navegação por teclado conforme o eMAG e a WCAG 2.2, superando o teto de atendimento parcial observado em praticamente todos os portais.

A Tabela 7 organiza essas recomendações por eixo temático, associando cada lacuna identificada nos dados à ação corretiva correspondente e à referência normativa que a fundamenta, o que facilita sua incorporação a planos formais de adequação e sua defesa perante instâncias de controle.

De modo geral, recomenda-se que as administrações municipais tratem a conformidade à LGPD não como um requisito formal pontual, mas como um processo contínuo de governança, que envolve manutenção documental, transparência das bases legais e inclusão digital. A priorização proposta considera a realidade de municípios com recursos técnicos e orçamentários limitados: as lacunas de maior impacto, em especial a atualização das políticas e a explicitação das bases legais, apresentam alta relevância de conformidade e baixo custo de implementação, o que as torna o ponto de partida racional de qualquer plano de adequação.

5.3 Ameaças à validade

Validade de construto. Como delimitado na Introdução, o instrumento examina a camada pública dos portais, isto é, aquilo que é observável por qualquer cidadão. Aspectos internos do tratamento, como os registros de operações, a atuação efetiva do encarregado e os contratos com operadores, não são alcançados pela inspeção externa. A conformidade mensurada constitui, portanto, um indicador da adequação comunicada e observável, e não uma auditoria completa das práticas internas: um portal pode divulgar um canal de incidentes sem que ele opere adequadamente, situação que o instrumento não tem condições de verificar. Essa limitação é compartilhada por toda a tradição de métodos de inspeção da IHC [Barbosa and Silva, 2010] e é o preço de uma estratégia que, em contrapartida, permite comparação padronizada entre organizações sem depender de acesso interno.

Confiabilidade. A concordância entre avaliadores foi limitada (Fleiss *kappa* de 0,260; alfa de Krippendorff ordinal de 0,427). A ordenação dos portais foi convergente entre os avaliadores e robusta aos esquemas de consolidação, mas as notas de itens individuais, sobretudo os que exigem julgamento do conteúdo, devem ser lidas com cautela. A Seção 4.6 identifica as causas das divergências e propõe refinamentos do protocolo de aplicação, cuja efetividade ainda precisa ser verificada.

Validade externa. O corpus restringe-se aos seis municípios mato-grossenses com mais de 100 mil habitantes, escolhidos por representatividade populacional e pela maior probabilidade de estruturas formais de tecnologia da informação. Municípios menores, que constituem a maioria do estado e do país, tendem a apresentar realidades distintas de infraestrutura e pessoal, de modo que os padrões aqui identificados não podem ser automaticamente estendidos a eles; a generalização exige replicação.

Composição do índice. A ponderação uniforme e os pontos de corte das faixas são convenções do estudo. A ordenação dos portais mostrou-se robusta a esquemas alternativos, mas a classificação em faixas não o é integralmente (Seção 4.5).

Temporalidade. Portais são sistemas dinâmicos, sujeitos a atualizações de conteúdo e reformulações de interface. Os resultados retratam a situação observada entre 9 e 29 de maio de 2026 e valem como linha de base comparativa, e não como retrato permanente. A distância de até vinte dias entre as inspeções de um mesmo portal por avaliadores diferentes pode ter contribuído para parte das divergências.

6 Considerações finais

Este trabalho desenvolveu, validou quanto ao conteúdo e aplicou um instrumento de avaliação da conformidade observável à LGPD em portais de governo eletrônico municipal, respondendo, sob a ótica de Sistemas de Informação, em que medida esses sistemas atendem, no que é visível ao cidadão, à proteção de dados pessoais. Na amostra analisada, o atendimento é parcial e desigual: o Índice de Conformidade médio foi de 55,8%, nenhum portal alcançou a pontuação máxima, a variação foi de 30,8% a 84,6%, sem padrão aparente em relação ao porte populacional, e as menores pontuações ocorreram na governança legal e na acessibilidade. A ordenação dos portais manteve-se sob esquemas alternativos de ponderação, e a análise de concordância identificou os descritores que exigem refinamento.

As contribuições articulam-se em quatro planos. No

Tabela 7. Recomendações de adequação por eixo temático, com a lacuna identificada e a referência normativa.

Eixo (média)	Lacuna identificada	Ação recomendada e referência
Legal e governança (51,4%)	Bases legais, atualização da política e retenção com desempenho baixo; menor média do conjunto.	Publicar e datar revisões periódicas da política; mapear e informar as bases legais por finalidade, conforme o art. 7º, e a política de retenção.
Legal e governança (51,4%)	Direitos do titular pouco detalhados em linguagem acessível.	Descrever, em linguagem simples, os direitos do art. 18 e o canal para seu exercício.
Segurança (61,1%)	HTTPS pleno, porém consentimento de *cookies* e canal de incidentes deficientes.	Implementar *banner* de *cookies* com opção clara de recusa, conforme o guia da ANPD, e canal formal de incidentes, conforme a ISO/IEC 27002.
Usabilidade (62,5%)	Acesso e clareza variáveis entre portais.	Padronizar a localização da seção de privacidade e simplificar a comunicação ao cidadão.
Acessibilidade (54,2%)	Atendimento apenas parcial e uniforme; nenhum portal pleno.	Corrigir contraste, alternativas textuais e navegação por teclado conforme eMAG e WCAG 2.2.

plano metodológico, disponibiliza-se um instrumento de avaliação validado quanto ao conteúdo, com descritores, escala padronizada, protocolo de consolidação por mediana entre múltiplos avaliadores e um protocolo de aplicação revisado a partir da análise das divergências, reaplicável por pesquisadores, órgãos de controle e equipes municipais. No plano empírico, oferece-se um diagnóstico quantitativo inédito da conformidade dos maiores portais municipais de Mato Grosso, que constitui linha de base documentada para comparações futuras. No plano prático, entrega-se um conjunto de recomendações priorizadas por um critério objetivo de lacuna, adequado à realidade de municípios com recursos limitados. No plano acadêmico, o trabalho aproxima os campos do direito digital, da segurança da informação e da IHC, ao demonstrar que a conformidade à LGPD em ambientes governamentais é também um problema de comunicação, usabilidade e inclusão informacional, cuja avaliação exige instrumentos genuinamente multidisciplinares.

Para a comunidade de Sistemas de Informação em particular, o estudo mostra que parte da governança da informação, entendida como conjunto de rotinas, papéis e responsabilidades sobre o ciclo de vida dos dados, deixa traços verificáveis no artefato voltado ao cidadão, e que, na amostra analisada, esses traços obtiveram pontuações inferiores às dos controles de infraestrutura técnica. Mostra também que a avaliação externa desses traços é mais confiável quanto à sua existência do que quanto à sua qualidade. Medir essa diferença em artefatos reais, e não em percepções declaradas, é a contribuição que o instrumento pretende consolidar.

Trabalhos futuros seguem quatro direções principais. A primeira é a ampliação do corpus, aplicando o instrumento a municípios de menor porte, a outros estados e a outras esferas de governo, o que permitirá testar a generalidade dos padrões aqui identificados e investigar os fatores institucionais que explicam a variação de maturidade. A segunda é a evolução do próprio instrumento, com a automação parcial da coleta dos indicadores tecnicamente verificáveis, como o protocolo seguro e os critérios de acessibilidade mensuráveis por ferramentas de inspeção, e com a verificação empírica, em nova aplicação, do efeito do protocolo revisado sobre a concordância entre avaliadores. A terceira é a incorporação da perspectiva do usuário final, por meio de avaliações assistidas por cidadãos com deficiência e de estudos de compreensão das políticas de privacidade. A quarta é o acompanhamento longitudinal dos portais avaliados, transformando a linha de base aqui estabelecida em série histórica de maturidade em governança de dados no setor público.

Declarações complementares

Agradecimentos

Os autores agradecem aos avaliadores voluntários e aos especialistas que participaram da validação e da aplicação do instrumento.

Contribuições dos autores

Descrição conforme a taxonomia CRediT. V.F.B.A.C.: Metodologia, Investigação, Curadoria de dados, Análise formal, Visualização, Redação (rascunho original, revisão e edição). N.V.S.A.: Conceituação, Supervisão, Metodologia, Validação. C.D.C.N.: Supervisão, Validação. Todos os autores leram e aprovaram o manuscrito final.

Conflitos de interesse

Os autores declaram não haver conflitos de interesse.

Disponibilidade de dados e materiais

O instrumento de avaliação é reproduzido integralmente no Apêndice A. Os dados que apoiam este estudo consistem em notas atribuídas por avaliadores voluntários, coletadas sob Termo de Consentimento Livre e Esclarecido. Uma matriz completa das notas individuais, com os avaliadores identificados pelos códigos A, B e C, é reproduzida no Apêndice B, o que permite recalcular a consolidação, o Índice de Conformidade e os coeficientes de concordância. As capturas e gravações de tela que fundamentaram as pontuações não são publicadas, pois podem conter elementos que identificam os avaliadores, cuja identidade é protegida pelo Termo de Consentimento Livre e Esclarecido, e dados pessoais de terceiros exibidos nos portais, como nomes e contatos de servidores; esse material pode ser disponibilizado ao editor e aos revisores mediante solicitação. Os termos de consentimento assinados não são compartilhados por conterem dados pessoais.

Financiamento

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Brasil (CAPES), Código de Financiamento 001, por meio de bolsa de mestrado concedida ao primeiro autor.

Outras informações relevantes

Aprovação ética. A pesquisa foi aprovada pelo Comitê de Ética em Pesquisa da área de Humanidades da Universidade Federal de Mato Grosso, por meio da Plataforma Brasil, em conformidade com a Resolução nº 510/2016 do Conselho Nacional de Saúde (CAAE

90651225.4.0000.5690; Parecer nº 7.900.910).

Uso de IA/LLM. Os autores utilizaram as ferramentas de inteligência artificial generativa Claude (Anthropic) e ChatGPT (OpenAI) como apoio à preparação deste manuscrito, abrangendo a revisão linguística, a condensação do texto a partir do trabalho de origem e a formatação segundo o *template* da revista. Na revisão solicitada pelos pareceristas, o Claude foi utilizado também como apoio à redação das alterações e à execução dos cálculos complementares (coeficientes de concordância e análise de sensibilidade do índice) a partir da matriz de notas, cujos resultados foram conferidos pelos autores. As ferramentas não foram utilizadas para coletar os dados, atribuir as notas aos portais nem construir o instrumento de avaliação. Todo o material produzido com apoio dessas ferramentas foi revisado e verificado pelos autores, que assumem integral responsabilidade pelo conteúdo do trabalho.

Origem do trabalho. Este artigo deriva da dissertação de mestrado do primeiro autor, desenvolvida no Programa de Pós-Graduação em Computação Aplicada da Universidade Federal de Mato Grosso e ainda não publicada em periódico ou anais. O manuscrito não é versão estendida de artigo previamente publicado.

Referências

Abraham, R., Schneider, J., and vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49:424–438. DOI: 10.1016/j.ijinfomgt.2019.07.008.

Agência Nacional de Proteção de Dados (2021a). Guia orientativo de segurança da informação para agentes de tratamento de pequeno porte. Technical report, ANPD.

Agência Nacional de Proteção de Dados (2021b). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Technical report, ANPD.

Agência Nacional de Proteção de Dados (2022a). Guia orientativo sobre cookies e proteção de dados pessoais. Technical report, ANPD.

Agência Nacional de Proteção de Dados (2022b). Guia orientativo: tratamento de dados pessoais pelo poder público. Technical report, ANPD.

Agência Nacional de Proteção de Dados (2022c). Resolução CD/ANPD nº 2, de 27 de janeiro de 2022: aprova o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte. Diário Oficial da União.

Agência Nacional de Proteção de Dados (2024a). Resolução CD/ANPD nº 15, de 24 de abril de 2024: aprova o Regulamento de Comunicação de Incidente de Segurança (RCIS). Diário Oficial da União.

Agência Nacional de Proteção de Dados (2024b). Resolução CD/ANPD nº 18, de 16 de julho de 2024: aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União.

Alexandre, N. M. C. and Coluci, M. Z. O. (2011). Validade de conteúdo nos processos de construção e adaptação de instrumentos de medidas. *Ciência & Saúde Coletiva*, 16(7):3061–3068. DOI: 10.1590/S1413-81232011000800006.

Andrade, H. G. (2005). Teaching with rubrics: The good, the bad, and the ugly. *College Teaching*, 53(1):27–31. DOI: 10.3200/CTCH.53.1.27-31.

Araújo, E., Vilela, J., Silva, C., and Alves, C. (2021). Are my business process models compliant with LGPD? the LGPD4BP method to evaluate and to model LGPD aware business processes. In *Anais do XVII Simpósio Brasileiro de Sistemas de Informação (SBSI)*. ACM. DOI: 10.1145/3466933.3466982.

Araujo, R. M. d., Siqueira, S. W. M., Classe, T. M. d., Maciel, R. S. P., and Boscarioli, C. (2025). II GranDSI-BR: Grandes desafios de sistemas de informação no Brasil 2026–2036. Technical report, Sociedade Brasileira de Computação, Porto Alegre.

Associação Brasileira de Normas Técnicas (2022). ABNT NBR ISO/IEC 27002:2022 – segurança da informação, cibersegurança e proteção à privacidade: controles de segurança da informação. ABNT.

Barbosa, S. D. J. and Silva, B. S. (2010). *Interação Humano-Computador*. Elsevier.

Barros, P. V. d. S., Monteiro, J. M., and Machado, J. C. (2023). Estratégias para modelagem e avaliação da conformidade entre sistemas de informação e a Lei Geral de Proteção de Dados Pessoais – LGPD. In *Tópicos Especiais em Sistemas de Informação: Minicursos SBSI 2023*. Sociedade Brasileira de Computação. DOI: 10.5753/sbc.11837.0.2.

Bélanger, F. and Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4):1017–1041. DOI: 10.2307/41409971.

Brasil (2011). Lei nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação. Presidência da República.

Brasil (2014). eMAG: Modelo de Acessibilidade em Governo Eletrônico, versão 3.1. Ministério do Planejamento, Orçamento e Gestão.

Brasil (2015). Lei nº 13.146, de 6 de julho de 2015: Estatuto da Pessoa com Deficiência. Presidência da República.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República.

Brasil (2024). Painel de Serviços Digitais. Ministério da Gestão e da Inovação em Serviços Públicos.

Brookhart, S. M. (2018). Appropriate criteria: Key to effective rubrics. *Frontiers in Education*, 3:22. DOI: 10.3389/feduc.2018.00022.

Canedo, E. D. *et al*. (2021). Challenges regarding the compliance with the general data protection law by Brazilian organizations: A survey. In *Computational Science and Its Applications – ICCSA 2021*, volume 12951 of *Lecture Notes in Computer Science*. Springer. DOI: 10.1007/978-3-030-86970-0_31.

Carturan, S. B. O. G., Matsui, B. M. A., and Goya, D. H. (2022). LGPD framework: An implementation and compliance guide for technology areas. In *Anais do XLIX Seminário Integrado de Software e Hardware (SEMISH)*. Sociedade Brasileira de Computação. DOI: 10.5753/semish.2022.223289.

Castro, E. T. V., Silva, G. R. S., and Canedo, E. D. (2022). Ensuring privacy in the application of the Brazilian General Data Protection Law (LGPD). In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing (SAC)*. ACM. DOI: 10.1145/3477314.3507023.

Cerqueira, D. A., Mello, R. M. d., and Travassos, G. H. (2023). Um checklist para inspeção de privacidade e proteção de

dados pessoais em artefatos de software. In *Anais do XXVI Congresso Ibero-Americano em Engenharia de Software (CIbSE)*, pages 206–213. Sociedade Brasileira de Computação. DOI: 10.5753/cibse.2023.24704.

Chalhoub, G. and Flechais, I. (2022). Data protection at a discount: Investigating the UX of data protection from user, designer, and business leader perspectives. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2). DOI: 10.1145/3555537.

Chaves, S. A. d. and Benitti, F. B. V. (2025). User-centred privacy and data protection: An overview of current research trends and challenges for the human–computer interaction field. *ACM Computing Surveys*. DOI: 10.1145/3715903.

Comitê Gestor da Internet no Brasil (2024). Pesquisa TIC Domicílios 2023: indicadores de acesso e uso da Internet no Brasil. Technical report, Cetic.br/NIC.br.

Cybis, W. A., Betiol, A. H., and Faust, R. (2007). *Ergonomia e usabilidade: conhecimentos, métodos e aplicações*. Novatec.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. (2019). We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society. DOI: 10.14722/ndss.2019.23378.

Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80. DOI: 10.1287/isre.1060.0080.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social*. Atlas, 6 edition.

Gil-Garcia, J. R., Dawes, S. S., and Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. *Public Management Review*, 20(5):633–646. DOI: 10.1080/14719037.2017.1327181.

Hayes, A. F. and Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data. *Communication Methods and Measures*, 1(1):77–89. DOI: 10.1080/19312450709336664.

Instituto Brasileiro de Geografia e Estatística (2024). Pesquisa nacional por amostra de domicílios contínua: Tecnologia da informação e comunicação 2023. Technical report, IBGE.

International Organization for Standardization (2018). ISO 9241-11:2018 – ergonomics of human-system interaction. part 11: Usability: Definitions and concepts. ISO.

Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology*. SAGE, Thousand Oaks, 4 edition.

Lakatos, E. M. and Marconi, M. d. A. (2017). *Fundamentos de metodologia científica*. Atlas, 8 edition.

Landis, J. R. and Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174. DOI: 10.2307/2529310.

Linden, T., Khandelwal, R., Harkous, H., and Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1):47–64. DOI: 10.2478/popets-2020-0004.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research*, 35(6):382–386. DOI: 10.1097/00006199-198611000-00017.

Matte, C., Bielova, N., and Santos, C. (2020). Do cookie banners respect my choice? measuring legal compliance of banners from IAB Europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809. IEEE. DOI: 10.1109/SP40000.2020.00076.

Mendes, J., Viana, D., and Rivero, L. (2021). Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the Brazilian General Data Protection Law: An initial proposal. In *Anais do XXXV Simpósio Brasileiro de Engenharia de Software (SBES)*. ACM. DOI: 10.1145/3474624.3477069.

Mendonça, A. P. B. and Pereira Neto, A. (2015). Critérios de avaliação da qualidade da informação em sites de saúde: uma proposta. *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, 9(1). DOI: 10.29397/reciis.v9i1.930.

Moreira, C. V., Seabra, R. D., and Garcés, L. (2024). Modelo web para exibição de termos de uso e políticas de privacidade com foco na LGPD e em práticas de design de experiência do usuário. In *Anais do XXXV Simpósio Brasileiro de Informática na Educação (SBIE)*. Sociedade Brasileira de Computação. DOI: 10.5753/sbie.2024.239998.

Neitzke, C. A. *et al*. (2023). Enhancing LGPD compliance: Evaluating a checklist for LGPD quality attributes within a government office. In *Proceedings of the XXII Brazilian Symposium on Software Quality (SBQS)*. ACM. DOI: 10.1145/3629479.3629497.

Nielsen, J. (1994). *Usability Engineering*. Morgan Kaufmann.

Nielsen, J. and Loranger, H. (2007). *Prioritizing Web Usability*. New Riders.

Norman, D. A. (2013). *O design do dia a dia*. Rocco.

OECD and European Commission Joint Research Centre (2008). *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD Publishing, Paris.

Preece, J., Rogers, Y., and Sharp, H. (2015). *Interaction Design: Beyond Human-Computer Interaction*. Wiley, 4 edition.

Rocha, L. D., Silva, G. R. S., and Canedo, E. D. (2023). Privacy compliance in software development: A guide to implementing the LGPD principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC)*, pages 1352–1361. ACM. DOI: 10.1145/3555776.3577615.

Rosson, M. B. and Carroll, J. M. (2002). *Usability Engineering: Scenario-Based Development of Human-Computer Interaction*. Morgan Kaufmann.

Rubin, J. and Chisnell, D. (2008). *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. Wiley, 2 edition.

Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., and Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research*, 27(2):94–104. DOI: 10.1093/swr/27.2.94.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., and Elmqvist, N. (2018). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Pearson, 6 edition.

Silva, E. R. G. d. and Rover, A. J. (2010). O governo eletrônico

no suporte às políticas públicas com ações participativas. *Revista Democracia Digital e Governo Eletrônico*, 1(3).

Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4):989–1015. DOI: 10.2307/41409970.

Stevens, D. D. and Levi, A. J. (2013). *Introduction to Rubrics: An Assessment Tool to Save Grading Time, Convey Effective Feedback, and Promote Student Learning*. Stylus Publishing, 2 edition.

Tallon, P. P., Ramirez, R. V., and Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3):141–178. DOI: 10.2753/MIS0742-1222300306.

Twizeyimana, J. D. and Andersson, A. (2019). The public value of e-government – a literature review. *Government Information Quarterly*, 36(2):167–178. DOI: 10.1016/j.giq.2019.01.001.

União Europeia (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: Regulamento Geral sobre a Proteção de Dados (RGPD). Jornal Oficial da União Europeia.

World Bank (2022). GovTech maturity index 2022: Trends in public sector digital transformation. Technical report, World Bank Group.

World Wide Web Consortium (2023). Web content accessibility guidelines (WCAG) 2.2. W3C Recommendation.

A Rubrica de avaliação de conformidade à LGPD para portais institucionais

Este apêndice reproduz integralmente o instrumento aplicado na avaliação. Cada indicador é pontuado em escala ordinal de três níveis: 0 quando o requisito não é evidenciado, 1 quando há conformidade parcial e 2 quando há conformidade plena. A pontuação máxima é de 26 pontos, correspondentes aos treze indicadores. O Índice de Conformidade de cada portal é a razão entre a pontuação obtida e os 26 pontos possíveis, multiplicada por 100, classificada nas faixas da Tabela 2.

Na aplicação, cada indicador é acompanhado de um campo de registro da pontuação atribuída, de marcação do tipo de evidência coletada (captura ou gravação de tela) e de observações do avaliador. Esses campos integram a ficha de aplicação e foram suprimidos desta reprodução por não fazerem parte da definição dos critérios. A aplicação deve ser conduzida por, no mínimo, dois avaliadores independentes, com consolidação das notas pela mediana, e cada nota deve ser acompanhada de evidência registrada, de modo a permitir auditoria posterior.

A.1 Visão sintética dos critérios

A Tabela 8 apresenta a visão sintética dos treze indicadores e dos quatro eixos temáticos. Os eixos agrupam os indicadores da seguinte forma: conformidade legal e governança da informação (indicadores 1, 3, 5, 8, 11 e 12; máximo de 12 pontos); segurança da informação (6, 7 e 9; máximo de 6 pontos); usabilidade e design centrado no usuário (2 e 4; máximo de 4 pontos); e acessibilidade digital e inclusão informacional (10a e 10b; máximo de 4 pontos).

A.2 Descritores por indicador

Apresentam-se a seguir, para cada indicador, a pergunta orientadora (critério), os descritores dos três níveis da escala e a base legal, a base normativa e o princípio de design que fundamentam o item.

Indicador 1 — Categoria: Transparência. *Critério:* O portal institucional possui uma página ou seção dedicada à privacidade ou à LGPD, publicamente acessível sem necessidade de autenticação, login ou cadastro?

- **2** o portal apresenta uma página ou seção exclusivamente dedicada à privacidade ou à LGPD, identificável pelo título (ex.: "Privacidade", "LGPD", "Proteção de Dados"), acessível diretamente a qualquer visitante, sem exigir login, cadastro ou qualquer forma de autenticação.
- **1** o portal apresenta informações sobre privacidade ou LGPD, porém inseridas em páginas genéricas (ex.: "Sobre o site", "Termos de Uso") sem identificação clara como seção dedicada; ou a página existe, mas seu acesso está condicionado a alguma forma de autenticação.
- **0** o portal não apresenta nenhuma página, seção ou conteúdo dedicado à privacidade ou à LGPD.

Base legal: LGPD Art. 6º, inciso VI (transparência); Art. 9º, §1º e §2º; Art. 18. *Base normativa:* Res. CD/ANPD nº 2/2022 [Agência Nacional de Proteção de Dados, 2022c], art. 7º — agentes devem oferecer acesso facilitado às informações sobre tratamento de dados pessoais, inclusive em meio eletrônico. *Princípio de design:* Princípio da Transparência [Nielsen, 1994]; Visibilidade da informação [Norman, 2013].

Indicador 2 — Categoria: Transparência. *Critério:* Existe um link ou acesso exclusivo à página dedicada à privacidade ou à LGPD a partir da página inicial, localizável em até dois cliques, em posição de destaque ou com indicação clara de sua localização?

- **2** a página dedicada à LGPD está disponível diretamente no menu principal, no rodapé em posição destacada ou em link de destaque claramente visível na página inicial, podendo ser acessada em até um clique.
- **1** a página inicial oferece indicação da localização da seção LGPD (ex.: submenu, rodapé em posição secundária), exigindo no máximo dois cliques; o link existe, mas não está em posição de destaque.
- **0** não há link ou indicação de localização da página LGPD na página inicial, ou a localização exige mais de dois cliques para ser atingida.

Base legal: LGPD Art. 6º, inciso I (Princípio da Transparência). *Base normativa:* Res. CD/ANPD nº 2/2022 [Agência Nacional de Proteção de Dados, 2022c], art. 7º — acesso facilitado às informações sobre tratamento de dados pessoais, inclusive em meio eletrônico. *Princípio de design:* Visibilidade da informação; Reconhecimento em vez de memorização [Nielsen, 1994]; princípio de no máximo dois cliques para informações essenciais [Nielsen and Loranger, 2007].

Indicador 3 — Categoria: Governança. *Critério:* A página dedicada à LGPD apresenta, de forma clara e sem qualquer barreira, os dados completos de contato do Encarregado de Dados (DPO), incluindo nome, e-mail e demais meios de comunicação?

- **2** a página dedicada à LGPD apresenta de forma imediata e sem qualquer barreira todos os dados essenciais do Encarregado (DPO), incluindo nome completo e e-mail direto. CAPTCHAs, formulários intermediários ou redirecionamentos para centrais

Tabela 8. Síntese dos critérios, indicadores e significado do instrumento.

Nº	Critério	Indicador	Descrição sintética
1	Transparência	Existência de página/seção LGPD	Verifica se o portal possui uma página ou seção dedicada à privacidade ou à LGPD, publicamente acessível sem necessidade de autenticação.
2	Transparência	Localização e acesso rápido	Avalia se o link para a página LGPD está disponível de forma clara a partir da página inicial, com no máximo dois cliques.
3	Governança	Dados de contato do DPO	Verifica se os dados completos do Encarregado de Dados (nome, e-mail, telefone) estão apresentados sem barreiras de acesso.
4	Direitos do Titular	Linguagem simples e acessível	Avalia se os direitos do titular estão explicados em linguagem clara, sem jargões jurídicos, com exemplos compreensíveis para o público leigo.
5	Bases Legais	Bases legais do tratamento	Verifica se a política de privacidade identifica e justifica as bases legais aplicáveis ao tratamento de cada categoria de dados (art. 7º LGPD).
6	Consentimento & Cookies	Banner de cookies com opção de recusa	Avalia se o site exibe banner de cookies com opção clara de recusa antes de qualquer coleta, sem dark patterns.
7	Segurança Mínima	Protocolo HTTPS e certificado válido	Verifica o uso de HTTPS com certificado válido em todas as páginas que coletam ou transmitem dados pessoais.
8	Transparência & Atualização	Data da última revisão	Avalia se a política de privacidade indica a data de revisão e se esta ocorreu nos últimos 12 meses.
9	Segurança & Incidentes	Canal para reporte de incidentes	Verifica a existência de canal oficial para comunicação de incidentes de segurança, com instruções claras e linguagem acessível.
10a	Acessibilidade Digital	Contraste e alternativas textuais	Avalia contraste texto/fundo e presença de textos alternativos em imagens, conforme WCAG 2.2 e eMAG.
10b	Acessibilidade Digital	Navegação por teclado e leitores de tela	Avalia se a navegação por teclado e a compatibilidade com leitores de tela estão adequadas nos fluxos relacionados a dados pessoais.
11	Retenção de Dados	Prazos e critérios de retenção	Avalia se a política informa por quanto tempo os dados são retidos ou quais critérios definem esse prazo (ex.: obrigação legal, finalidade).
12	Compartilhamento	Compartilhamento com terceiros	Verifica se a política identifica as categorias de terceiros e operadores com quem os dados são compartilhados, com a respectiva finalidade.

genéricas de atendimento não são aceitos como conformidade plena.

1 a página exibe apenas parte das informações (ex.: somente o e-mail ou apenas o setor responsável) ou impõe obstáculo leve ao acesso, como rolagem excessiva ou clique adicional; formulários intermediários com campos identificados para contato ao DPO são aceitos como conformidade parcial.

0 não há nenhum dado de contato do DPO visível, ou o portal fornece apenas canais genéricos (ex.: "Fale Conosco", central de atendimento) sem identificar o Encarregado.

Base legal: LGPD Art. 41, §1º. *Base normativa:* Res. CD/ANPD nº 18/2024 [Agência Nacional de Proteção de Dados, 2024b] (Regulamento do Encarregado); Guia Orientativo "Atuação do Encarregado" (dez/2024) — divulgação "clara e objetiva, preferencialmente no site". *Princípio de design:* Reconhecimento em vez de memorização [Nielsen, 1994] — o usuário identifica os dados sem esforço ou busca extra.

Indicador 4 — Categoria: Direitos do Titular. *Critério:* Os direitos do titular estão explicados em linguagem simples e acessível, sem uso de jargões jurídicos não explicados, com frases curtas e, quando possível, com exemplos práticos?

2 todos os direitos do titular estão explicados em linguagem simples, clara e acessível, sem uso de termos jurídicos sem explicação. O texto utiliza frases curtas, voz ativa e, preferencialmente, exemplos do cotidiano (ex.: "Você pode pedir para corrigir seu nome em nosso cadastro"). Não se exige linguagem jurídica formal.

1 o texto apresenta mistura de linguagem técnica e linguagem simples, ou explica apenas parte dos direitos de forma adequada; termos jurídicos aparecem sem explicação em alguns trechos, mas não de forma predominante.

0 o texto utiliza linguagem predominantemente técnica e de difícil compreensão para o público leigo, com termos jurídicos sem explicação e frases longas e complexas.

Base legal: LGPD Art. 18. *Base normativa:* Res. CD/ANPD nº 2/2022 [Agência Nacional de Proteção de Dados, 2022c], art. 7º (clareza e precisão das informações); Guia Orientativo sobre Comunicação com o Titular (jan/2024). *Princípio de design:* Linguagem simples e UX Writing [Nielsen and Loranger, 2007]; leiturabilidade para público leigo [Shneiderman *et al.*, 2018].

Indicador 5 — Categoria: Bases Legais. *Critério:* A política de privacidade identifica claramente as bases legais utilizadas para cada finalidade de tratamento de dados pessoais, justificando sua aplicação no contexto do serviço público municipal?

2 a política identifica de forma explícita e clara as bases legais aplicáveis (ex.: cumprimento de obrigação legal, execução de políticas públicas, consentimento) para cada categoria de dados tratados, com justificativa objetiva de sua aplicação ao contexto municipal.

1 a política menciona bases legais de forma genérica, sem associá-las às finalidades específicas de cada tratamento, ou omite a justificativa para uma ou mais categorias de dados.

0 a política não faz qualquer referência às bases legais do tratamento, ou as menciona de forma puramente decorativa, sem associação às finalidades declaradas.

Base legal: LGPD Art. 7º (bases legais); Art. 6º, incisos I e X (finalidade e responsabilização). *Base normativa:* Guia Orientativo "Hipóteses Legais de Tratamento de Dados – Legítimo Interesse" (fev/2024); Enunciado ANPD nº 1/2023. *Princípio de design:* Consistência e padrões [Nielsen, 1994] — apresentar informação completa e padronizada por categoria de dado.

Indicador 6 — Categoria: Consentimento & Cookies. *Critério:* Na primeira visita, o portal exibe um banner de cookies que oferece opção clara de "Recusar" antes de qualquer coleta de cookies não essenciais, sem utilização de dark patterns ou nudges manipulativos?

- **2** já no primeiro carregamento do portal, é exibido um banner de cookies que aparece imediatamente sem necessidade de rolagem; apresenta a opção "Recusar" (ou equivalente) na mesma camada, com igual destaque visual ao botão "Aceitar"; não instala cookies não essenciais até que o usuário faça escolha explícita; não utiliza dark patterns (ex.: botão de recusa em cor cinza, menor tamanho ou posição desfavorável; ausência de caixa "Personalizar" como única alternativa à aceitação).
- **1** o banner está presente, mas a opção de recusa está em segunda camada, com menor destaque visual, ou exige clique adicional; ou cookies não essenciais são instalados antes da decisão do usuário, ainda que a opção "Recusar" esteja disponível.
- **0** não existe banner de cookies; o banner não apresenta opção de recusa; ou os cookies não essenciais são instalados automaticamente sem possibilidade de rejeição.

Base legal: LGPD Art. 8º (consentimento). *Base normativa:* Guia orientativo sobre cookies e proteção de dados pessoais [Agência Nacional de Proteção de Dados, 2022a] — proíbe design que oculte opção de rejeição. *Princípio de design:* Prevenção de erros e design ético [Nielsen, 1994]; anti-dark patterns — consentimento livre e informado [Shneiderman *et al*., 2018].

Indicador 7 — Categoria: Segurança Mínima. *Critério:* O portal utiliza protocolo seguro (HTTPS) com certificado digital válido em todas as páginas que coletam ou transmitem dados pessoais?

- **2** todo o portal utiliza HTTPS e apresenta certificado válido, sem avisos de segurança nos principais navegadores. Nota: a presença de HTTPS não garante a autenticidade do site nem dispensa demais controles de segurança; o critério avalia exclusivamente a criptografia do canal de comunicação.
- **1** a página principal utiliza HTTPS, mas há páginas ou formulários de coleta de dados sem criptografia, ou com redirecionamento inseguro.
- **0** o portal não utiliza HTTPS, apresenta certificado inválido ou expirado, ou exibe avisos de segurança nos navegadores em uso.

Base legal: LGPD Art. 46 (segurança e boas práticas). *Base normativa:* Guia de segurança da informação da ANPD [Agência Nacional de Proteção de Dados, 2021a]; ISO/IEC 27002:2022, seção 8 [Associação Brasileira de Normas Técnicas, 2022] (controles de proteção de dados em trânsito). *Princípio de design:* Segurança por padrão (privacy by default — GDPR art. 25 [União Europeia, 2016]; LGPD art. 46).

Indicador 8 — Categoria: Transparência & Atualização. *Critério:* A política de privacidade indica a data completa da última revisão, realizada há no máximo 12 meses em relação à data da avaliação?

- **2** a política apresenta a data completa da última revisão (dia, mês e ano) e essa revisão ocorreu há no máximo 12 meses. O prazo de 12 meses não é fixado em norma específica, mas fundamenta-se na recomendação de revisão periódica da ANPD e na prática editorial de atualização anual de políticas de privacidade, adotada como limiar operacional desta pesquisa.
- **1** a política indica que houve atualização, mas a data completa está entre 12 e 24 meses; ou a referência à data é vaga (ex.: apenas mês/ano ou apenas o ano), impossibilitando confirmar se a revisão ocorreu nos últimos 12 meses.
- **0** a política não apresenta qualquer data de revisão, ou a data indicada ultrapassa 24 meses em relação à data da avaliação.

Base legal: LGPD Art. 6º, inciso X (responsabilização e prestação de contas). *Base normativa:* Guia orientativo de segurança da informação para agentes de pequeno porte [Agência Nacional de Proteção de Dados, 2021a] — recomenda revisão periódica de políticas de privacidade e segurança. *Princípio de design:* Visibilidade do status do sistema [Nielsen, 1994] — o usuário precisa saber se o documento está atualizado.

Indicador 9 — Categoria: Segurança & Incidentes. *Critério:* O portal disponibiliza, de forma clara e em linguagem acessível ao cidadão leigo, um canal oficial para comunicação de incidentes de segurança envolvendo dados pessoais, com informações sobre procedimentos e prazos?

- **2** o portal disponibiliza um canal exclusivo ou claramente identificado para reporte de incidentes de segurança com dados pessoais, acompanhado de instruções redigidas em linguagem acessível ao cidadão leigo (ex.: passo a passo, prazo de resposta e identificação dos responsáveis). O texto menciona explicitamente "incidentes de segurança" ou "violação de dados pessoais".
- **1** há apenas um canal genérico de contato (ex.: e-mail, telefone, "Fale Conosco") sem referência clara a incidentes de segurança; ou existe canal dedicado, mas faltam informações essenciais como prazos, responsáveis ou orientações específicas.
- **0** o portal não oferece qualquer meio específico para o reporte de incidentes de segurança, ou a política não faz referência objetiva a esse tipo de comunicação.

Base legal: LGPD Art. 48. *Base normativa:* Res. CD/ANPD nº 15/2024 [Agência Nacional de Proteção de Dados, 2024a] — Regulamento de Comunicação de Incidente de Segurança (RCIS). *Princípio de design:* Visibilidade do estado crítico [Nielsen, 1994]; linguagem acessível ao cidadão leigo [Preece *et al*., 2015].

Indicador 10a — Categoria: Acessibilidade Digital — Contraste e Alternativas Textuais. *Critério:* O portal apresenta contraste adequado entre texto e fundo e fornece textos alternativos em imagens nas seções relacionadas à LGPD e à privacidade?

- **2** as seções relacionadas à LGPD e à privacidade apresentam relação de contraste $\geq$ 4,5:1 para texto normal e $\geq$ 3:1 para texto grande (WCAG 2.2 critério 1.4.3); todas as imagens com conteúdo informativo possuem texto alternativo descritivo (WCAG 2.2 critério 1.1.1).
- **1** o portal apresenta contraste adequado em parte das seções, mas não em todas; ou imagens informativas carecem de texto alternativo em alguns elementos.
- **0** o contraste é insuficiente em áreas centrais das seções de privacidade; ou imagens informativas não possuem texto alternativo.

Base legal: LGPD Art. 6º, VI (transparência); Lei nº 13.146/2015 [Brasil, 2015]. *Base normativa:* WCAG 2.2 [World Wide Web Consortium, 2023], critérios 1.1.1 (Texto Alternativo) e 1.4.3 (Contraste Mínimo); eMAG 3.1 [Brasil, 2014], recomendações 2.1 e 3.6. *Princípio de design:* Perceptibilidade [World Wide Web Consortium, 2023] — qualquer usuário deve perceber o conteúdo independentemente de suas capacidades sensoriais.

Indicador 10b — Categoria: Acessibilidade Digital — Navegação e Leitores de Tela. *Critério:* O portal permite navegação completa por teclado e apresenta estrutura semântica compatível com leitores de tela nos fluxos relacionados a dados pessoais?

2 todos os elementos interativos (links, formulários, botões, banners de cookies) nas seções de privacidade são acessíveis por teclado (Tab/Enter/Esc) e possuem rótulos identificáveis por leitores de tela (aria-label, for/id em campos de formulário); a ordem de foco é lógica e coerente com a sequência visual.

1 a maioria dos elementos é acessível por teclado e por leitores de tela, mas há lacunas em componentes específicos (ex.: banner de cookies sem navegação por teclado, campos sem rótulo identificável).

0 elementos essenciais das seções de privacidade não são acessíveis por teclado ou leitores de tela; o portal depende exclusivamente de interações por mouse.

Base legal: LGPD Art. 6º, VI (transparência); Lei nº 13.146/2015 [Brasil, 2015]. *Base normativa:* WCAG 2.2 [World Wide Web Consortium, 2023], critérios 1.3.1 (Informação e Relações), 2.1.1 (Teclado) e 4.1.2 (Nome, Função, Valor); eMAG 3.1 [Brasil, 2014], recomendações 4.1 e 6.3. *Princípio de design:* Operabilidade e robustez [World Wide Web Consortium, 2023] — o conteúdo deve ser operável por diferentes tecnologias assistivas.

Indicador 11 — Categoria: Retenção de Dados Pessoais. *Critério:* A política de privacidade informa de forma clara por quanto tempo os dados pessoais dos usuários são armazenados, ou apresenta os critérios utilizados para definir esse prazo (ex.: obrigação legal, finalidade específica do tratamento, prazo contratual)?

2 a política informa de forma clara os prazos de retenção ou os critérios para defini-los, associando-os às finalidades ou às categorias de dados (ex.: "dados de cadastro são retidos pelo prazo de vigência do serviço; dados fiscais são retidos por cinco anos conforme obrigação legal").

1 a política menciona retenção de dados, mas de forma genérica, sem especificar prazos ou critérios objetivos (ex.: "os dados são retidos pelo tempo necessário" sem explicação adicional).

0 a política não faz qualquer menção a prazos de retenção de dados pessoais nem aos critérios utilizados para defini-los.

Base legal: LGPD Art. 15 e Art. 16; Art. 6º, inciso III (necessidade). *Base normativa:* Enunciado ANPD nº 2/2023 — os agentes de tratamento devem observar o princípio da necessidade quanto à retenção de dados pessoais. *Princípio de design:* Visibilidade do status do sistema [Nielsen, 1994]; consistência e padrões — regras sobre uso e descarte devem ser claras e uniformes.

Indicador 12 — Categoria: Compartilhamento de Dados com Terceiros. *Critério:* A política de privacidade identifica claramente as categorias de terceiros ou operadores com quem os dados pessoais podem ser compartilhados, bem como as finalidades específicas desse compartilhamento?

2 a política identifica as categorias de terceiros (ex.: prestadores de serviços, órgãos públicos parceiros, operadores de sistemas) ou os operadores com quem os dados são compartilhados, indicando a finalidade específica de cada compartilhamento. Diferencia adequadamente terceiros controladores de operadores, quando aplicável.

1 a política informa genericamente que os dados podem ser compartilhados, sem identificar as categorias de terceiros ou sem justificar a finalidade; ou identifica os terceiros, mas não informa a finalidade do compartilhamento.

0 a política não menciona compartilhamento de dados com terceiros ou omite completamente essa informação.

Base legal: LGPD Art. 9º, §2º; Art. 18, inciso VII; Art. 6º, inciso VI (transparência). *Base normativa:* Guia orientativo sobre agentes de tratamento e o encarregado [Agência Nacional de Proteção de Dados, 2021b]. *Princípio de design:* Reconhecimento em vez de memorização [Nielsen, 1994] — os usuários devem ser apresentados às informações relevantes de forma explícita.

B Matriz das notas individuais dos avaliadores

A Tabela 9 reproduz as 234 notas atribuídas pelos três avaliadores, identificados pelos códigos A, B e C, a cada indicador e município. A partir dela é possível recalcular a consolidação pela mediana (Tabela 3), o Índice de Conformidade, os esquemas alternativos da Tabela 5 e os coeficientes de concordância da Seção 4.6. As inspeções foram realizadas entre 9 e 29 de maio de 2026: pelo avaliador A entre 24 e 25 de maio, pela avaliadora B entre 9 e 24 de maio e pelo avaliador C entre 24 e 29 de maio.

Tabela 9. Notas individuais por indicador e município, no formato A/B/C.

Ind.	Cuiabá	Várzea G.	Rondon.	Sinop	Sorriso	Tangará
1	2/1/2	2/1/1	2/1/2	2/2/2	2/2/2	2/2/2
2	2/1/2	0/1/2	2/1/2	1/1/2	2/2/2	2/2/2
3	0/0/0	2/1/0	2/1/2	2/2/2	2/2/0	2/2/0
4	1/0/0	2/0/0	1/1/2	1/2/2	1/1/0	2/1/0
5	0/1/0	2/0/1	1/1/2	2/1/2	0/0/0	1/1/0
6	0/0/0	0/2/0	0/1/1	2/2/1	0/0/1	2/2/1
7	2/1/2	2/1/2	2/1/2	2/2/2	2/2/2	2/2/2
8	0/0/0	0/0/0	0/0/1	1/1/2	1/0/0	0/0/0
9	0/0/0	1/0/1	1/1/2	0/1/1	2/1/1	1/1/1
10A	1/0/2	1/1/1	1/1/2	1/1/2	1/1/2	1/1/2
10B	1/1/2	1/1/1	1/1/2	2/1/2	1/1/1	1/1/1
11	0/0/0	0/0/1	2/0/2	1/2/2	0/1/1	0/0/1
12	0/0/0	2/0/1	1/1/2	1/2/2	1/0/1	1/1/1
Total	9/5/10	15/8/11	16/11/24	18/20/24	15/13/13	17/16/13