

GESTÃO DO CONHECIMENTO NA PERÍCIA ADMINISTRATIVA DE INCÊNDIOS E EXPLOSÕES: PRÁTICAS DE COMPLIANCE NO COMPARTILHAMENTO DE DADOS

*Manoel Maurício Ramos Neto*¹

<https://orcid.org/0009-0004-3858-7422>

*Murilo Pedro Demarchi*²

<https://orcid.org/0000-0003-1941-6340>

RESUMO

Este artigo analisa as diretrizes jurídicas e operacionais aplicáveis à gestão do conhecimento (GC) dos dados produzidos no âmbito da perícia administrativa de incêndios e explosões (PAIE), atividade técnico-científica exercida pelos Corpos de Bombeiros Militares (CBMs) com relevância para a retroalimentação do ciclo operacional e formulação de políticas públicas baseadas em evidências. Utilizando metodologia qualitativa, de cunho teórico-descritivo, a pesquisa fundamenta-se em revisão normativa, doutrinária e institucional, com foco na Lei de Acesso à Informação (LAI) e na Lei Geral de Proteção de Dados Pessoais (LGPD). A partir dessa análise, propõe-se um modelo de governança da informação estruturado em quatro eixos: (i) transparência ativa, mediante a divulgação proativa de dados anonimizados e estatísticas públicas; (ii) transparência passiva, com fornecimento de informações mediante solicitação, respeitados os limites legais; (iii) níveis diferenciados de acesso, conforme o perfil e finalidade do requerente; e (iv) critérios para o fornecimento de dados a terceiros, com base na legalidade, necessidade, anonimização e proteção do interesse público. Conclui-se que a harmonização entre transparência e proteção de dados é viável e necessária, desde que observadas boas práticas de *compliance* informacional, contribuindo para a legitimidade, eficiência e segurança jurídica na atuação dos CBMs.

Palavras-chave: Perícia administrativa de incêndios; Gestão do conhecimento; Lei Geral de Proteção de Dados (LGPD); Lei de Acesso à Informação (LAI).

¹CBMRS, Oficial do Corpo de Bombeiros Militar do Rio Grande do Sul – manuelmm.ramosneto@gmail.com

²CBMSC, Oficial do Corpo de Bombeiros Militar de Santa Catarina.

KNOWLEDGE MANAGEMENT IN ADMINISTRATIVE FIRE AND EXPLOSION INVESTIGATIONS: COMPLIANCE PRACTICES IN DATA SHARING

ABSTRACT

This article examines the legal and operational guidelines applicable to knowledge management (KM) of data produced within the scope of administrative fire and explosion investigations (PAIE), a technical-scientific activity carried out by the Military Fire Departments (CBMs) with relevance to the feedback of the operational cycle and the formulation of evidence-based public policies. Using a qualitative, theoretical-descriptive methodology, the research is based on normative, doctrinal, and institutional analysis, focusing on the Access to Information Law (LAI) and the General Data Protection Law (LGPD). From this analysis, a governance model is proposed, structured around four pillars: (i) active transparency, through the proactive disclosure of anonymized data and public statistics; (ii) passive transparency, with the provision of information upon request, within legal limits; (iii) differentiated levels of access, based on the requester's profile and purpose; and (iv) criteria for data sharing with third parties, based on legality, necessity, anonymization, and the protection of the public interest. The study concludes that harmonizing transparency and data protection is both feasible and necessary, provided that good practices of informational compliance are observed, contributing to legitimacy, efficiency, and legal certainty in the actions of CBMs.

Keywords: Administrative fire investigation; Knowledge management; General Data Protection Law (LGPD); Access to Information Law (LAI).

Artigo Recebido em 13/05/2025

Aceito em 20/09/2025

Publicado em 25/03/2026

1. INTRODUÇÃO

A perícia administrativa de incêndios e explosões (PAIE) desempenha papel estratégico no âmbito dos Corpos de Bombeiros Militares (CBMs), não apenas como atividade técnico-operacional, mas também como fonte primária de dados para a retroalimentação do ciclo operacional e para a formulação de políticas públicas baseadas em evidências. No entanto, a utilização adequada dos dados produzidos nesse contexto exige o alinhamento a princípios e normas que regem a administração pública, a gestão do conhecimento (GC) e a proteção de informações sensíveis, de modo a garantir a conformidade com o regime jurídico-administrativo e a efetividade dos direitos fundamentais.

O objeto de estudo deste artigo consiste na análise jurídica das diretrizes aplicáveis à governança de dados e da informação no âmbito da PAIE, considerando a função precípua da perícia na melhoria contínua da prestação do serviço público de segurança contra incêndio, bem como a necessidade de harmonização entre a transparência pública e a proteção de dados pessoais. A GC, nesse cenário, configura-se como instrumento essencial para estruturar o tratamento, a circulação e o aproveitamento estratégico das informações produzidas, respeitando os limites e fundamentos legais.

O objetivo do trabalho é identificar e apontar as principais normas jurídicas pertinentes, em especial a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), e, com base nelas, propor um modelo simplificado de diretrizes que possa orientar a GC dos dados e informações da PAIE, de forma a compatibilizar transparência, proteção de dados e promoção da eficiência administrativa. Pretende-se demonstrar que, mediante a adoção de boas práticas de *compliance* informacional e observância criteriosa dos princípios legais, é possível fortalecer a governança pública sem comprometer os direitos fundamentais.

A metodologia utilizada foi a pesquisa qualitativa, de caráter teórico-descritivo, baseada em análise normativa e doutrinária, com revisão de literatura especializada sobre direito administrativo, proteção de dados pessoais, acesso à informação e gestão do conhecimento no setor público. Foram examinados dispositivos legais aplicáveis, entendimentos doutrinários e práticas institucionais voltadas à proteção e ao aproveitamento estratégico da informação pública.

2. A PAIE COMO FONTE ESTRATÉGICA DE DADOS E SUA RELAÇÃO COM A GC

A PAIE desempenha função central na retroalimentação do ciclo operacional de bombeiro, integrando-se às fases normativa, preventiva e ativa (Camargo, 2019). Mais do que mero instrumento técnico de análise de eventos passados, a PAIE constitui uma fonte estratégica de dados que, quando devidamente sistematizada, pode orientar políticas públicas, aperfeiçoar protocolos operacionais e fortalecer a eficiência institucional (Oliveira; Silva, 2023).

O ciclo operacional de bombeiro depende da coleta e da análise criteriosa de informações para evoluir de forma contínua. As conclusões extraídas das perícias, ao registrarem as circunstâncias, causas e consequências dos incêndios e explosões, oferecem subsídios empíricos fundamentais para a revisão de normas, o desenvolvimento de campanhas preventivas, a modernização de equipamentos e o aprimoramento das estratégias de combate. Dessa maneira, a PAIE não apenas cumpre a função administrativa de apuração de fatos, mas também promove a transformação dos dados obtidos em conhecimento institucional valioso para a gestão pública baseada em inteligência (Feliciano, Pelozzi, 2024).

Nesse cenário, a GC apresenta-se como elemento indispensável para viabilizar a conversão dos vestígios técnicos recolhidos nas perícias em conhecimento aplicável e disseminável. Caracteriza-se tanto como processo quanto como produto e possibilita a identificação, criação, retenção, transferência (compartilhamento) e aplicação do conhecimento, efetivado por meio da relação entre pessoas e agentes não humanos para a geração de valor (SBGC, 2024; UFSC, 2025).

A literatura especializada destaca que a GC no setor público visa melhorar a tomada de decisões, aumentar a participação cidadã e fomentar a competitividade intelectual da sociedade. Tais melhorias, por sua vez, dependem de um ambiente organizacional, conhecido como *ba*, que busca valorizar o conhecimento, a inovação e a aprendizagem contínua, sendo considerado um espaço de confiança onde os indivíduos estejam dispostos a aprender, a inovar e a compartilhar seus conhecimentos (SBGC, 2024).

A aplicação da GC na atividade de PAIE exige processos estruturados de captura, organização, análise, compartilhamento e reuso das informações, assegurando que o conhecimento tácito produzido pelos peritos seja formalizado em padrões, relatórios, estatísticas e bases de dados acessíveis (Wiig, 2002).

Modelos teóricos como a pirâmide DIKW (Dados, Informação, Conhecimento e Sabedoria) ilustram essa transformação progressiva dos dados brutos em inteligência estratégica, demonstrando a importância da interpretação crítica e da contextualização dos resultados periciais (Felicidade *et al.*, 2021). Assim, os dados coletados deixam de ser elementos isolados e passam a compor um arcabouço de conhecimento organizacional capaz de apoiar decisões preventivas e corretivas.

Ferramentas como sistemas informatizados de gestão pericial, plataformas de *Business Intelligence* (BI), *dashboards* analíticos e bancos de dados interoperáveis constituem instrumentos fundamentais para

operacionalizar a GC no contexto da PAIE. Esses recursos permitem integrar informações, detectar padrões de risco, gerar relatórios de produtividade e subsidiar análises preditivas que otimizam a alocação de recursos e a priorização de políticas públicas (Alvarenga *et al.*, 2020; Ahbabi *et al.*, 2019).

No que concerne aos impactos, a literatura demonstra que a GC exerce influência positiva direta sobre o desempenho operacional, a qualidade dos serviços e a capacidade inovadora das organizações públicas (Ahbabi *et al.*, 2019). Em especial, os processos de criação, captura, compartilhamento e aplicação do conhecimento são apontados como essenciais para o aprimoramento contínuo desses órgãos. Além disso, a GC pode mediar a relação entre o compromisso organizacional e o desempenho dos trabalhadores do conhecimento (Razzaq *et al.*, 2018).

Ademais, a implementação de uma cultura organizacional orientada ao compartilhamento e à análise crítica das informações é apontada como um dos fatores críticos de sucesso para a GC no setor público (Pee; Kankanhalli, 2016). No âmbito dos CBMs, essa cultura pode ser fomentada por meio de capacitações, padronização de formulários periciais, criação de perfis de acesso seguros e incentivo à retroalimentação contínua do ciclo operacional.

Assim, a PAIE, articulada com práticas robustas de GC, revela-se um vetor essencial para a modernização da gestão pública no campo da segurança contra incêndios, consolidando o conhecimento produzido em ações concretas de proteção da vida, do patrimônio e do meio ambiente.

3. COMPLIANCE NO SETOR PÚBLICO E NAS CORPORAÇÕES DE BOMBEIRO MILITAR

O conceito de *compliance*, embora historicamente associado ao setor privado, tem sido progressivamente absorvido pela administração pública como mecanismo de promoção da conformidade normativa, da ética e da responsabilidade institucional. No setor público, *compliance* significa assegurar

que os atos administrativos observem os parâmetros legais e regulamentares vigentes, promovendo também práticas de integridade, transparência e eficiência. Essa internalização responde a contextos crescentes de exigência por controle, fiscalização e prestação de contas, conforme apontam autores como Szewczak (2024) e Wiatrak (2021), que destacam a relevância de diretrizes anticorrupção e canais de denúncia (*whistleblowing*) como componentes essenciais.

No Brasil, o avanço da legislação, especialmente a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados, reforça esse movimento de incorporação normativa e administrativa. A conformidade, nesse cenário, ultrapassa a simples obediência a leis, assumindo uma função estratégica no fortalecimento da governança pública e na valorização da *accountability* (Santos *et al.*, 2024).

A implementação de sistemas de *compliance* no setor público, contudo, não se restringe à adesão normativa; ela pressupõe transformações institucionais que exigem marcos legais e regulatórios específicos para garantir sua efetividade (Szewczak, 2024). Trata-se de um processo que demanda a criação de estruturas de governança voltadas à integridade, com definição de protocolos internos, responsabilidades e mecanismos de controle.

No contexto das Corporações Bombeiro Militar, por exemplo, o *compliance* adquire um caráter particularmente estratégico, ao alinhar ações operacionais e administrativas aos marcos normativos internos e externos. A atuação dessas corporações deve observar não apenas os regulamentos técnicos e os códigos de conduta, mas também as exigências legais que incidem sobre o serviço público como um todo. Ao adotar práticas de conformidade, essas instituições fortalecem sua legitimidade, ampliam a eficiência das suas atividades e promovem uma cultura organizacional voltada à integridade pública. Nesse sentido, a adoção de instrumentos normativos e tecnológicos, em consonância com os princípios constitucionais da

Administração Pública, é condição indispensável para o sucesso de qualquer política de integridade institucional.

4. REGIME JURÍDICO ADMINISTRATIVO E A EFICIÊNCIA OPERACIONAL

O regime jurídico administrativo brasileiro é fundamentado por princípios explícitos no caput do artigo 37 da Constituição Federal, os quais orientam toda a atuação da Administração Pública. Legalidade, impessoalidade, moralidade, publicidade e eficiência constituem não apenas enunciados normativos, mas diretrizes operacionais para a boa governança pública (Galdino; Puel, 2017). No âmbito dos Corpos de Bombeiros Militares, esses princípios assumem papel estruturante, sobretudo no que se refere à qualificação das atividades operacionais e técnico-periciais.

Nesse viés, o uso estratégico de dados produzidos nas perícias de incêndio deve estar em consonância com o princípio da legalidade, sendo realizado dentro dos limites normativos e respeitando os marcos legais vigentes (Filho; Monteiro, 2024). O modelo de retroalimentação institucional, ao articular dados periciais com a formulação de políticas internas, representa uma aplicação concreta desse regime jurídico, promovendo uma atuação mais racional, legítima e integrada à missão pública da corporação.

A impessoalidade, enquanto fundamento da Administração Pública, assegura que decisões e processos internos sejam orientados por critérios objetivos, desvinculados de preferências individuais ou interesses particulares (Filho; Monteiro, 2024). Quando aplicada ao contexto dos Corpos de Bombeiros, essa diretriz evita que os dados oriundos de perícias sejam utilizados de forma seletiva ou distorcida. Já o princípio da moralidade exige que a conduta administrativa esteja pautada por padrões éticos e por um senso de justiça material, garantindo a correção institucional (Filho; Monteiro, 2024).

Com efeito, a atuação técnica, quando orientada por essas premissas, contribui para uma cultura organizacional de integridade, fortalecendo a confiança da sociedade nas instituições. Assim, ao transformar os dados periciais em insumos para decisões operacionais e normativas, os Corpos de Bombeiros reafirma seu compromisso com o interesse público e com uma gestão pública orientada por valores republicanos estatuídos na Constituição de 1988.

A publicidade, enquanto princípio constitucional, impõe à administração o dever de tornar transparentes seus atos, decisões e fundamentos, permitindo o controle social e promovendo a *accountability* institucional (Neto *et al.*, 2007). No contexto da perícia de incêndios, isso se traduz na possibilidade de divulgar informações consolidadas e anonimizadas que contribuam para a prevenção de riscos e a padronização de condutas. Essa prática reforça o princípio da eficiência, uma vez que permite o uso qualificado do conhecimento acumulado para a melhoria dos serviços públicos (Filho; Monteiro, 2024).

Com fulcro nos princípios acima aludidos, a proposta de um modelo jurídico de retroalimentação institucional, ancorado na governança de dados e na intersetorialidade entre os setores técnico-operacionais, representa uma forma de concretizar essas normas constitucionais de maneira pragmática. A transparência nesse processo não apenas legitima a atuação administrativa, mas favorece a construção de políticas públicas baseadas em evidências.

Ocorre que, apesar da centralidade desses princípios, a Administração Pública brasileira ainda enfrenta obstáculos para sua plena efetivação. A persistência de práticas patrimonialistas e a fragilidade dos mecanismos de *accountability* comprometem a aplicação uniforme desses valores no cotidiano institucional (Galdino; Puel, 2017).

Isto posto, nos Corpos de Bombeiros Militares, superar tais desafios requer a institucionalização de processos que garantam a racionalização das decisões, a qualificação da produção pericial e o uso estratégico da

informação. A retroalimentação operacional baseada em dados é uma resposta contemporânea a essas exigências, permitindo que a estrutura militar estadual atue de forma proativa, transparente e eficiente. Ao alinhar sua prática ao regime jurídico administrativo, o Corpo de Bombeiros fortalece sua legitimidade institucional e aprimora sua capacidade de gerar valor público, não apenas no atendimento de ocorrências, mas também na prevenção e planejamento de longo prazo.

5. LAI E LGPD COMO FUNDAMENTOS PARA A GC NA PAIE

A GC aplicada à PAIE deve observar rigorosamente as diretrizes estabelecidas pela LAI e pela LGPD. Ambas as normas, embora orientadas por finalidades distintas. A primeira é voltada à transparência e ao controle social e a segunda à proteção da privacidade, sendo que ambas atuam de forma complementar para disciplinar o fluxo informacional no âmbito da Administração Pública (Bioni *et al.*, 2022).

A LAI estabelece o direito de acesso à informação como vetor de fortalecimento democrático, determinando que as informações de interesse público sejam disponibilizadas de maneira proativa (transparência ativa) e que os cidadãos possam solicitar dados não previamente divulgados (transparência passiva), conforme dispõe seu art. 8º (Bioni *et al.*, 2022). No contexto da PAIE, a LAI orienta que relatórios estatísticos, dados agregados sobre incêndios, bens salvados e prejuízos estimados, campanhas educativas, bem como orientações técnicas de interesse geral, sejam acessíveis à sociedade, observadas as limitações relacionadas à segurança da informação e à proteção da intimidade, da vida privada, da honra e da imagem das pessoas (art. 31 da LAI).

Já a LGPD impõe balizas para o tratamento de dados pessoais, inclusive no setor público, exigindo que qualquer atividade envolvendo dados sensíveis, tais como informações sobre vítimas, responsáveis por imóveis ou testemunhas constantes nos laudos periciais, seja pautada pelos princípios da finalidade, necessidade, adequação, minimização e segurança (arts. 6º e 7º da LGPD). A anonimização, prevista no art. 5º, inciso XI, e no art. 12 da LGPD, surge como técnica essencial para compatibilizar o acesso à informação pública com a preservação da privacidade dos indivíduos (Bioni *et al.*, 2022).

No âmbito da GC aplicada à PAIE, a LAI e a LGPD oferecem o conjunto normativo que fundamenta práticas como: (i) classificação da informação por grau de sensibilidade; (ii) definição de perfis diferenciados de acesso; (iii) adoção de técnicas de anonimização para divulgação segura; e (iv) utilização de protocolos de segurança da informação. A análise dos pedidos de acesso deve ser orientada pela ponderação entre o interesse público na transparência e a proteção dos dados pessoais, utilizando critérios de proporcionalidade e finalidade, como indicam Bioni *et al.* (2022) e Fortini *et al.* (2021).

Ademais, a harmonização interpretativa entre LAI e LGPD, conforme propõem Limberger (2022) e a jurisprudência do Supremo Tribunal Federal, exige que os órgãos públicos, como os CBM, construam políticas de governança da informação que assegurem a máxima transparência possível sem comprometer os direitos fundamentais dos titulares de dados (Bioni *et al.*, 2022). Dessa forma, a GC da PAIE deve ser estruturada de maneira a potencializar a retroalimentação do ciclo operacional de bombeiro, promovendo a eficiência da gestão pública baseada em evidências, mas sempre em consonância com os parâmetros legais de proteção de dados e de acesso à informação.

6. TÉCNICAS DE GOVERNANÇA DA INFORMAÇÃO APLICÁVEIS À PAIE

A GC na PAIE deve voltar-se para a adoção de técnicas de governança da informação que respeitem simultaneamente as diretrizes da LAI e da LGPD. A articulação dessas técnicas é fundamental para que a retroalimentação do ciclo operacional de bombeiro ocorra de maneira ética, segura e juridicamente adequada.

Entre as práticas recomendadas destaca-se a classificação das informações por grau de sensibilidade, permitindo distinguir dados de acesso público irrestrito daqueles que exigem restrições por envolverem dados pessoais sensíveis, conforme preveem a LGPD (art. 5º, II) e a LAI (art. 31).

A anonimização de dados representa outra técnica essencial para viabilizar a divulgação de informações sem comprometer a privacidade dos envolvidos (LGPD, art. 12). Relatórios estatísticos, mapas de incidência de incêndios e análises de bens salvados podem ser elaborados a partir de dados anonimizados, promovendo a transparência sem exposição de indivíduos.

O controle de acessos é igualmente imprescindível. Deve-se estruturar perfis diferenciados de acesso para (i) público geral, (ii) instituições públicas externas, (iii) usuários internos da corporação e (iv) partes interessadas específicas. Cada perfil deve ter acesso apenas às informações compatíveis com sua finalidade, necessidade e competência, conforme recomendam Bioni *et al.* (2022) e Fortini *et al.* (2021).

Outra prática recomendada é a adoção de termos de responsabilidade para terceiros que solicitam dados mais sensíveis, como seguradoras, advogados ou vizinhos de imóveis sinistrados. Essa medida visa garantir a rastreabilidade, o compromisso com o uso adequado das informações e a proteção da privacidade dos titulares, conforme sugerem as boas práticas de governança indicadas pela Autoridade Nacional de Proteção de Dados (ANPD, 2023).

A implementação de protocolos de segurança da informação e procedimentos de descarte seguro de dados ao final do seu ciclo de vida são medidas necessárias para mitigar riscos de vazamentos, acessos indevidos e perdas de integridade, em consonância com o art. 46 da LGPD (ANPD, 2024).

Especificamente quanto à LAI, no âmbito da transparência ativa, é recomendada a publicação periódica de dados agregados e anonimizados (Bioni *et al.*, 2022), tais como: (i) relatórios de produtividade pericial; (ii) estatísticas de causas de incêndios; (iii) prejuízos e bens salvados; (iv) análises técnicas preventivas; (v) campanhas educativas em mídias digitais; e (vi) relatórios de custos e desempenho institucional para órgãos de controle externo.

Já na transparência passiva, o atendimento às solicitações de informações deve ser orientado pelos critérios da necessidade, da pertinência e da finalidade, sempre ponderando o interesse público com a proteção de dados pessoais, e aplicando técnicas como a restrição de dados excessivos ou a anonimização prévia, nos termos da LAI e da LGPD (Bioni *et al.*, 2022).

Tais técnicas, devidamente integradas em uma política de gestão do conhecimento da PAIE, não apenas asseguram o cumprimento das normas de transparência e proteção de dados, mas também consolidam a governança pública baseada em evidências, fortalecendo o ciclo operacional de bombeiro e a confiança social nas instituições.

7. COMPARTILHAMENTO DE DADOS PESSOAIS NA PAIE

O compartilhamento de dados pessoais pelos CBMs no contexto da PAIE deve observar rigorosamente os parâmetros definidos na LGPD e nas orientações expedidas pela ANPD (2023), segundo a qual, o uso compartilhado de dados pessoais, de acordo com a norma supracitada, compreende a comunicação, difusão, transferência ou interconexão de dados pessoais entre

órgãos e entidades públicas ou entre estes e privados, com autorização específica, para finalidades legítimas e delimitadas (BRASIL, 2018). No caso da PAIE, isso se aplica, por exemplo, ao envio de relatórios estatísticos anonimizados para órgãos de controle externo, universidades ou outras corporações públicas de segurança.

Para que o compartilhamento de dados pessoais na PAIE esteja em conformidade com a LGPD e as orientações da ANPD (2023), é necessário que cada etapa do processo observe critérios jurídicos e administrativos específicos, organizados em seis requisitos principais. Em primeiro lugar, exige-se a (i) formalização e registro do compartilhamento, na medida em que deve ser instaurado um processo administrativo formal, no qual sejam documentadas a motivação, a necessidade e a adequação do compartilhamento ao interesse público, conforme exige o regime jurídico da administração pública, ou seja, não pode haver trocas informais de dados.

Em seguida, deve haver a (ii) definição clara do objeto e da finalidade. Os dados a serem compartilhados precisam estar vinculados diretamente à finalidade pública previamente estabelecida, sendo vedado o compartilhamento genérico, indiscriminado ou desvinculado do interesse público. A finalidade deve ser específica, legítima e compatível com a função pública desempenhada (ANPD, 2023).

O terceiro requisito é a (iii) indicação expressa da base legal que autoriza o compartilhamento, como, por exemplo, a execução de políticas públicas, o cumprimento de obrigação legal ou a proteção da vida e da incolumidade física do titular ou de terceiros (BRASIL, 2018, art. 7º, incisos II, III e VII). A ausência de base legal válida pode invalidar todo o tratamento de dados (ANPD, 2023).

O quarto critério refere-se à (iv) delimitação do prazo de tratamento e do destino dos dados. Deve-se estabelecer de forma clara quanto tempo os dados serão utilizados e o que será feito com eles após o encerramento da finalidade

— se serão eliminados, anonimizados ou arquivados nos termos da legislação aplicável. Além disso, deve-se assegurar a (v) garantia de transparência e preservação dos direitos dos titulares. O titular dos dados tem o direito de ser informado, de maneira adequada e acessível, sobre o compartilhamento de seus dados pessoais e, sempre que possível, deve ter assegurado o exercício de seus direitos previstos na LGPD (ANPD, 2023).

Por fim, é imprescindível a (vi) adoção de medidas de segurança proporcionais aos riscos envolvidos no tratamento e compartilhamento dos dados. Isso inclui, por exemplo, o uso de sistemas seguros, o controle de acesso restrito, a assinatura de termos de responsabilidade e a aplicação de boas práticas de proteção da informação, conforme recomendam a LGPD e a ANPD (ANPD, 2023).

Importante destacar que o compartilhamento de dados sensíveis ou identificáveis deve ser evitado sempre que possível, preferindo-se o uso de técnicas como anonimização ou pseudonimização. Além disso, nos casos em que o compartilhamento envolva terceiros privados, como seguradoras ou advogados, devem ser respeitados os limites impostos pelos artigos 26 e 27 da LGPD, vedando-se a utilização dos dados para finalidades distintas daquelas autorizadas e exigindo-se, quando necessário, a celebração de instrumentos específicos, como termo de responsabilidade (ANPD, 2023).

8. MODELO PROPOSTO: PRINCIPAIS DIRETRIZES PARA A GC NA PAIE

A partir da análise normativa e doutrinária realizada, propõe-se um modelo de diretrizes para a GC no âmbito da PAIE, que harmonize a função estratégica da informação para a retroalimentação do ciclo operacional de bombeiro com as obrigações de transparência e proteção de dados estabelecidas pela LAI e LGPD.

O modelo estrutura-se a partir de quatro eixos fundamentais. O primeiro refere-se à transparência ativa, no âmbito da qual, os CBMs devem divulgar espontaneamente informações de interesse coletivo, conforme previsto no art. 8º da LAI. A difusão deve priorizar dados anonimizados e agregados, tais como: Relatórios estatísticos de ocorrência de incêndios por tipologia; Mapas de calor indicando áreas de maior incidência; Relatórios de produtividade e custos, destinados também aos órgãos de controle externo; Análises técnicas de causas recorrentes de incêndios; Dados de prejuízos e bens salvados; Relatórios sobre o desempenho operacional (tempo-resposta médio, taxa de sucesso nas operações); Campanhas educativas de prevenção veiculadas em mídias digitais.

Essas informações devem ser previamente tratadas mediante técnicas de anonimização, classificação por sensibilidade, aplicação de protocolos de segurança da informação, controle de acessos e procedimentos de descarte seguro, em conformidade com as boas práticas de GC recomendadas pela ANPD e a doutrina especializada (Fortini *et al.*, 2021; ANPD, 2023).

O segundo eixo é o da transparência passiva, o qual se refere ao fornecimento de informações mediante solicitação do cidadão, desde que respeitados os limites legais, via serviço de informações ao cidadão (LAI, art. 9º) na forma prevista pela legislação federal e respectivas leis estaduais. De acordo com a LAI (art. 31), devem ser preservadas informações que comprometam a segurança da sociedade ou do Estado e a vida privada, intimidade, honra ou imagem das pessoas. Exemplos de informações protegidas incluem: identificações pessoais de vítimas ou testemunhas; dados médicos; fotografias de áreas privadas internas de imóveis sinistrados; dados financeiros sensíveis, informações detalhadas sobre vulnerabilidades prediais.

Vale pontuar, por oportuno, que o atendimento a pedidos de acesso deve observar os princípios da necessidade, adequação, proporcionalidade e finalidade, realizando a anonimização dos dados pessoais sempre que

possível. Nesse sentido, torna-se necessário observar o terceiro eixo, que diz respeito à estruturação de níveis de acesso, a partir do qual se propõe a adoção de uma matriz, organizada em quatro categorias: (i) Público geral: acesso a dados agregados e anonimizados de interesse coletivo; (ii) Instituições públicas externas: acesso a dados técnicos mais detalhados, mediante termo de responsabilidade e avaliação de finalidade legítima; (iii) Usuários internos dos CBMs: acesso integral às informações no exercício de suas funções, com perfis individualizados e monitoramento de acessos; e, por fim, (iv) Partes interessadas específicas (vítimas, proprietários, seguradoras, órgãos judiciais): acesso condicionado à demonstração de interesse legítimo ou direito juridicamente protegido, preferencialmente com anonimização dos dados de terceiros e assinatura de termos de responsabilidade.

No primeiro nível, dirigido ao público geral, devem ser disponibilizados dados agregados e anonimizados, como estatísticas de incêndios, análises de tendência, mapas de calor de incidência de sinistros e dados estimativos de prejuízos e bens salvados. A disponibilização ativa dessas informações atende ao princípio da publicidade e ao dever de transparência ativa previsto na LAI, além de contribuir para a difusão da cultura prevencionista e para o fortalecimento do controle social (Limberger, 2022).

O segundo nível contempla as instituições públicas externas, tais como órgãos de controle, Poder Judiciário, Ministério Público, Defensoria Pública e instituições de pesquisa. Conforme a LGPD (art. 7º, III), o compartilhamento de dados com tais entes é legítimo desde que vinculado à execução de políticas públicas ou ao cumprimento de obrigações legais, sendo exigida a demonstração da finalidade específica e a assinatura de termos de responsabilidade para garantir a preservação dos direitos dos titulares e a segurança da informação (ANPD, 2023).

No terceiro nível encontram-se os usuários internos dos CBMs, como peritos, gestores de estatística, setores de inteligência, planejamento e

corregedoria. A esses agentes admite-se o acesso integral aos dados coletados na PAIE, incluindo dados pessoais sensíveis, limitado ao exercício regular de suas funções públicas (LGPD, art. 7º, II e III). Em atenção ao princípio da *accountability*, recomenda-se a adoção de perfis individualizados de acesso, com autenticação forte, monitoramento contínuo e trilhas de auditoria, conforme boas práticas de governança da informação (Bioni *et al.*, 2022).

Por fim, o quarto nível refere-se às partes interessadas específicas, como vítimas de incêndios, proprietários de imóveis sinistrados, seguradoras e órgãos judiciais ou administrativos que comprovem interesse legítimo ou direito juridicamente protegido. O acesso deverá ser condicionado a requerimento formal, fundamentado na demonstração da finalidade e da pertinência, além de, sempre que possível, ser precedido da anonimização de dados de terceiros, conforme a técnica prevista no art. 5º, XI, da LGPD (Sombra, 2020). Ademais, deve-se exigir a assinatura de termos de responsabilidade para reforçar o compromisso com o uso adequado das informações e prevenir usos indevidos.

Assim, a adoção dessa matriz de acesso dialoga diretamente com a necessidade de uma GC, em especial o compartilhamento de conhecimento, orientada pelos princípios da proporcionalidade, da segurança da informação e da supremacia do interesse público (Limberger, 2022), alinhando a retroalimentação da PAIE às exigências normativas de proteção de dados e de transparência na administração pública. Com base nessa estrutura de níveis de acesso, têm-se o quarto eixo, que se refere aos critérios para fornecimento de dados a terceiros interessados. Com efeito, o fornecimento de dados a terceiros interessados na PAIE deve observar, cumulativamente, princípios previstos na legislação em comento.

Dentre os princípios aludidos, tem-se: (i) Finalidade legítima e específica: comprovação do vínculo entre o pedido e o interesse jurídico ou

público; (ii) Necessidade e adequação: limitação do fornecimento apenas às informações estritamente necessárias ao atendimento da finalidade declarada; (iii) Aplicação da anonimização: sempre que possível, antes da entrega de documentos, para proteger dados pessoais de terceiros; e, finalmente, (iv) Proteção do interesse público e proporcionalidade: avaliação da efetividade e do risco da divulgação, fundamentando motivadamente as decisões de deferimento ou indeferimento.

O princípio da finalidade legítima e específica implica que o requerente deve demonstrar claramente a relação entre o pedido de acesso e um interesse jurídico protegido ou um interesse público relevante, afastando solicitações genéricas ou desvinculadas de uma finalidade concreta. Tal exigência encontra respaldo tanto na LGPD (art. 6º, inciso I) quanto na LAI (art. 7º, § 2º), que reforçam a necessidade de vinculação entre a coleta ou o compartilhamento de dados e objetivos previamente definidos (De Barcellos, 2015).

O princípio da necessidade e adequação orientam que o fornecimento de dados deve ser estritamente limitado às informações necessárias ao atendimento da finalidade declarada. A LAI e a LGPD compartilham essa preocupação em seus textos normativos, exigindo que o tratamento de dados não seja excessivo em relação à necessidade informada (Bioni *et al.*, 2022). No contexto da PAIE, essa limitação garante que apenas os dados pertinentes ao objetivo legítimo sejam compartilhados, resguardando informações pessoais ou sensíveis não essenciais.

Outro critério fundamental é a aplicação da anonimização, porquanto, a LGPD, em seu art. 5º, inciso XI, e art. 12, prioriza essa técnica para proteção de dados pessoais quando não houver necessidade de identificação dos titulares. Logo, na hipótese de fornecimento de laudos ou documentos periciais para terceiros, recomenda-se que sejam anonimizados dados pessoais sensíveis de vítimas, testemunhas e outros terceiros, sempre que possível,

assegurando a proteção da intimidade, honra e imagem, conforme também orienta a doutrina especializada (Sombra, 2020).

Por fim, Fortini *et al.* (2021) destaca-se a necessidade de avaliação da proteção do interesse público e da proporcionalidade na decisão de deferimento ou indeferimento de pedidos de acesso. A Administração Pública, ao analisar cada solicitação, deve ponderar entre o direito à informação e o direito à proteção de dados pessoais, justificando motivadamente sua decisão. Os autores aludidos concordam com Limberger (2022) no sentido de que essa análise deve levar em conta o potencial impacto da divulgação sobre os direitos dos titulares e a relevância da informação para a promoção do interesse público, promovendo a compatibilização entre a LGPD e a LAI, como tem sido defendido pela doutrina e pela jurisprudência.

Outrossim, a jurisprudência STF, em casos como o ARE 652777, reconheceu que o princípio da publicidade administrativa impõe a necessidade de divulgação de informações sobre a remuneração de servidores públicos, mas também reforçou a necessidade de proteger dados que possam atingir a intimidade e a vida privada dos indivíduos. Assim, mesmo quando o dado é de interesse público, é preciso avaliar a pertinência da divulgação, especialmente para dados pessoais sensíveis (Limberger, 2022).

De maneira semelhante, nas ações ADI 6387 e ADPF 690, o STF validou a proteção constitucional dos dados pessoais e reafirmou que a transparência pública deve observar limites proporcionais e razoáveis para evitar a exposição indevida de dados sensíveis. A Corte estabeleceu que a informação pública deve ser divulgada preferencialmente de forma agregada, estatística ou anonimizada sempre que possível, em consonância com a LGPD e com a LAI.

No contexto da PAIE, essas decisões reforçam que: publicação de relatórios estatísticos, mapas de risco e dados operacionais é legítima e importante para a sociedade; a divulgação de dados pessoais de vítimas,

proprietários ou responsáveis técnicos deve ser precedida de rigorosa avaliação quanto à necessidade, adequação e proporcionalidade; pedidos de acesso feitos por terceiros interessados devem ser analisados caso a caso, aplicando-se os critérios de finalidade, necessidade e proteção do interesse público, conforme preconizado pela jurisprudência e pelos princípios extraídos da LGPD e da LAI (Limberger, 2022).

Diante do exposto, essa proposta de modelo simplificado, esquematizado no quadro a seguir, visa orientar a atuação dos CBMs na gestão estratégica da informação pericial, compatibilizando a retroalimentação do ciclo operacional de bombeiro, a efetividade das políticas públicas de segurança contra incêndios e a observância rigorosa dos princípios da administração pública, da LAI e da LGPD.

Quadro 1 – Principais Diretrizes para a GC na PAIE

Eixo	Definição	Principais Elementos	Observações
1 – Transparência Ativa	Divulgação espontânea de informações de interesse coletivo.	- Relatórios estatísticos - Mapas de calor - Relatórios de produtividade e custos - Análises técnicas - Dados de prejuízos e bens salvados - Indicadores operacionais - Campanhas educativas	Informações devem ser anonimizadas, classificadas e protegidas por protocolos de segurança.
2 – Transparência Passiva	Atendimento a solicitações individuais de acesso à informação.	- Proteção de dados pessoais sensíveis - Aplicação de necessidade, adequação, proporcionalidade e finalidade	Dados de vítimas, testemunhas e informações sensíveis devem ser protegidos.

3 – Estruturação de Níveis de Acesso	Definição de perfis de acesso diferenciados conforme a natureza do usuário.	1. Público Geral (dados agregados) 2. Instituições Públicas (dados técnicos) 3. Usuários Internos CBMs (acesso integral com controle) 4. Partes Interessadas Específicas (acesso condicionado a interesse legítimo)	Implantação de controle de acesso, autenticação forte e trilhas de auditoria.
4 – Critérios para Fornecimento de Dados a Terceiros	Estabelecimento de critérios para liberação de informações sensíveis a terceiros.	- Finalidade legítima - Necessidade e adequação - Aplicação da anonimização - Proteção do interesse público	Análise fundamentada conforme LGPD, LAI e jurisprudência do STF.

Fonte: os autores (2025).

9. CONSIDERAÇÕES FINAIS

A PAIE, ao ser reconhecida como atividade estratégica para a retroalimentação do ciclo operacional de bombeiro, destaca-se também como relevante fonte de dados e informações para a gestão pública baseada em evidências. A construção de um modelo de GC voltado à PAIE, conforme demonstrado, exige a harmonização de diferentes marcos jurídicos, especialmente a LGPD e a LAI, de forma a assegurar tanto a transparência ativa e passiva quanto a proteção dos dados pessoais sensíveis.

No contexto da administração pública, a observância das boas práticas de governança da informação torna-se imperativa para os CBMs, cuja atuação deve ser orientada pelos princípios constitucionais e pela necessidade de gerir os dados periciais com segurança jurídica, eficiência e responsabilidade. A GC, quando corretamente estruturada, permite transformar os dados brutos da

PAIE em ativos estratégicos para a prevenção, o planejamento operacional e a formulação de políticas públicas mais eficazes.

As técnicas analisadas, como a anonimização, a classificação da informação, o controle de acesso, o descarte seguro e a adoção de termos de responsabilidade, constituem ferramentas indispensáveis para o tratamento adequado dos dados, reduzindo riscos e fortalecendo a confiabilidade institucional. A definição de níveis de acesso e o desenvolvimento de fluxos de análise e autorização de informações complementam essa arquitetura, respeitando a necessidade, a adequação e a finalidade dos compartilhamentos.

A convergência entre a LAI e a LGPD, conforme exposto, demonstra que a transparência pública e a proteção da privacidade não são objetivos antagônicos, mas complementares e interdependentes. A gestão dos dados da PAIE, realizada de maneira fundamentada, contribui para a legitimidade democrática da administração, a eficiência dos serviços de segurança contra incêndios e o fortalecimento do compromisso dos CBMs com a proteção da vida, do patrimônio e do meio ambiente.

Diante disso, o desenvolvimento de políticas internas claras de governança da informação no âmbito da PAIE revela-se essencial para assegurar o equilíbrio entre a publicidade das informações de interesse público e a preservação dos direitos fundamentais dos titulares de dados, promovendo, assim, a consolidação de uma cultura institucional orientada pela integridade, pela transparência e pela inovação.

REFERÊNCIAS

AHBABI, S.; SINGH, S.; BALASUBRAMANIAN, S.; GAUR, S. Employee perception of impact of knowledge management processes on public sector performance. *Journal of Knowledge Management*, v. 23, n. 2, p. 351-373, 2019. Disponível em: <https://doi.org/10.1108/JKM-08-2017-0348>. Acesso em: 02 abr. 2025.

ALVARENGA, A.; MATOS, F.; GODINA, R.; MATIAS, J. Digital transformation and knowledge management in the public sector. *Sustainability*, v. 12, n. 14, 2020. Disponível em: <https://doi.org/10.3390/su12145824>. Acesso em: 26 abr. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo: atuação do encarregado pelo tratamento de dados pessoais*. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf. Acesso em: 24 abr. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo para o tratamento de dados pessoais pelo poder público: versão 2.0*. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 23 abr. 2025.

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. *Cadernos da Pós-Graduação em Ouvidoria Pública*, v. 1, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 15 abr. 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 21 abr. 2025.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto na Constituição. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 abr. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais - LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 abr. 2025.

BRASIL. *Lei nº 14.751, de 12 de dezembro de 2023*. Institui a Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares dos Estados, do Distrito Federal e dos Territórios. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 13 dez. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14751.htm. Acesso em: 27 abr. 2025.

CAMARGO, Marcus Vinicius Braz de. *Perícia criminal de incêndio versus perícia de incêndio: conflito de competências?*. Monografia (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília (UnICEUB), Brasília, 2019. Orientadora: Míria Soares Eneias. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/13792>. Acesso em: 12 abr. 2025.

DE BARCELLOS, Ana Paula. Acesso à informação: os princípios da Lei nº 12.527/2011 (Access to Information: The Principles of the Law Nº 12.527/2011). *Revista Quaestio Iuris*, v. 8, p. 1741–1759, 2015. Disponível em: <https://doi.org/10.12957/RQI.2015.18818>. Acesso em: 11 abr. 2025.

FELICIANO, Antonio Marcos; PELOZZI, Tadeu Luiz Alonso. Inteligência na investigação de incêndio: o caso do Corpo de Bombeiros Militar de Santa Catarina (CBMSC). *Revista Flammae: Revista Científica do Corpo de Bombeiros Militar de Pernambuco*, v. 10, n. 31, jul./dez. 2024. Disponível em: <https://www.revistaflammae.com/c%C3%B3pia-vol-9-n%C3%BAmero-28>. Acesso em: 5 abr. 2025.

FELICIDADE, Christian Pereira; ARAÚJO, Wánderon Cássio Oliveira; POLEZA, Mariângela; VARVAKIS, Gregório. *Tópicos em Gestão do Conhecimento para Iniciantes*. Florianópolis: UFSC, 2021.

FORTINI, Cristiana; AMARAL, Greycielle; CAVA, Caio Mário Lana. LGPD x LAI: sintonia ou antagonismo? *APEMINAS*, 2021. Disponível em: <https://apeminas.org.br/publicacoes/artigos/artigo-lgpd-x-lai-sintonia-ou-antagonismo/>. Acesso em: 5 abr. 2025.

FILHO, P.; MONTEIRO, L. Principles of public administration: A brief comment in light of administrative reform. In: *SEVEN INTERNATIONAL MULTIDISCIPLINARY CONGRESS*, 7., 2024. Anais [...]. Disponível em: <https://doi.org/10.56238/sevenmulti2024-132>. Acesso em: 1 maio 2025.

GALDINO, M.; PUEL, J. A administração pública e o controle na Constituição da República Federativa do Brasil. *Universitas Fórum Democrático*, v. 8, p. 131-

144, 2017. Disponível em: <https://doi.org/10.19177/UFD.V8E152017131-144>. Acesso em: 2 maio 2025.

LIMBERGER, Thales. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI): um diálogo (im)possível? As influências do direito europeu. *Revista de Direito Administrativo*, v. 281, n. 1, p. 113–144, 2022. Disponível em: <https://doi.org/10.12660/rda.v281.2022.85654>. Acesso em: 8 abr. 2025.

NETO, O. A. P.; DA CRUZ, F.; ENSSLIN, S. R.; ENSSLIN, L. Publicidade e transparência das contas públicas: obrigatoriedade e abrangência desses princípios na administração pública brasileira. *Contabilidade Vista & Revista*, v. 18, n. 1, p. 75–94, 2007. Disponível em: <https://revistas.face.ufmg.br/index.php/contabilidadevistaerevista/article/view/320>. Acesso em: 8 maio 2025.

OLIVEIRA, Daniela Christina; SILVA, Thiago Henrique Costa. Ciclo operacional de segurança contra incêndio no Corpo de Bombeiros Militar do Estado de Goiás: a análise dos dados primários periciais como ferramenta para melhor gestão pública. *Revista de Direito Socioambiental – REDIS*, Goiás, v. 1, n. 2, p. 1–17, jan./jul. 2023. Disponível em: <https://www.revista.ueg.br/index.php/redis/article/view/13909>. Acesso em: 12 abr. 2025.

PEE, L.; KANKANHALLI, A. Interactions among factors influencing knowledge management in public-sector organizations: A resource-based view. *Government Information Quarterly*, v. 33, p. 188-199, 2016. Disponível em: <https://doi.org/10.1016/j.giq.2015.06.002>. Acesso em: 26 abr. 2025.

RAZZAQ, S. *et al.* Knowledge management, organizational commitment and knowledge-worker performance. *Business Process Management Journal*, v. 25, p. 923-947, 2018. Disponível em: <https://doi.org/10.1108/BPMJ-03-2018-0079>. Acesso em: 26 abr. 2025.

SANTOS, R.; AMARAL, M.; WILLERDING, I.; LAPOLLI, É. Compliance in the public sector from a systemic perspective: a bibliometric analysis. *Concilium*, [S.l.], v. 1, p. 1–22, 2024. Disponível em: <https://doi.org/10.53660/clm-3999-24r53>. Acesso em: 12 abr. 2025.

SOCIEDADE BRASILEIRA DE GESTÃO DO CONHECIMENTO (SBGC). *Modelo de Referência em Gestão do Conhecimento: Guia da Excelência em Gestão do Conhecimento*. 2. ed. São Paulo: SBGC, 2024. 82 p. Disponível em: <https://sbgc.org.br/>. Acesso em: 27 abr. 2025. ISBN 978-65-86604-09-2.

SOMBRA, T. The General Data Protection Law in Brazil: what comes next?. *Global Privacy Law Review*, [S.I.], 2020. Disponível em: <https://doi.org/10.54648/gplr2020083>. Acesso em: 12 abr. 2025.

SZEW CZAK, M. The legal conditions for implementing a compliance management system in public administration. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, [S.I.], v. 17, n. 1, p. 149–158, 2024. Disponível em: <https://doi.org/10.32084/tkp.9252>. Acesso em: 12 abr. 2025.

TAKEUCHI, Hirotaka; NONAKA, Ikujiro. *Gestão do conhecimento*. Tradução de Ana Thorell. Porto Alegre: Bookman, 2008. 319 p. ISBN 978-85-7780-191-6.

UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). *Programa de Pós-Graduação em Engenharia, Gestão e Mídia do Conhecimento – PPGE GC. Áreas de Concentração*. Disponível em: <https://ppgegc.paginas.ufsc.br/areas-de-concentracao/>. Acesso em: 27 abr. 2025.

WIATR AK, L. Compliance management in public administration bodies. *Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie*, [S.I.], v. 22, n. 1, p. 65–73, 2021. Disponível em: <https://doi.org/10.5604/01.3001.0015.0043>. Acesso em: 12 abr. 2025.

WIIG, Karl M. Knowledge management in public administration. *Journal of Knowledge Management*, v. 6, n. 3, p. 224–239, 2002. DOI: 10.1108/13673270210434331. Acesso em: 28 abr. 2025.