INSTITUTO EDUCAMINAS EAD LTDA

Yasmin Floriano Fernandes

ENTRE A CONFORMIDADE FORMAL E A CAPACIDADE REAL DE RESPOSTA: A SUFICIÊNCIA DO PLANO DE INCIDENTES DA PREFEITURA DE REALEZA (PR) SOB A LGPD

Bady Bassitt/SP

2026

INSTITUTO EDUCAMINAS EAD LTDA

Yasmin Floriano Fernandes

ENTRE A CONFORMIDADE FORMAL E A CAPACIDADE REAL DE RESPOSTA: A SUFICIÊNCIA DO PLANO DE INCIDENTES DA PREFEITURA DE REALEZA (PR) SOB A LGPD

Artigo Científico apresentado ao INSTITUTO EDUCAMINAS EaD LTDA, como parte das exigências para a obtenção do título de Pós-graduação em MBA Executivo em Gerenciamento de Crises.

Bady Bassitt/SP

2026

ENTRE A CONFORMIDADE FORMAL E A CAPACIDADE REAL DE RESPOSTA: A SUFICIÊNCIA DO PLANO DE INCIDENTES DA PREFEITURA DE REALEZA (PR) SOB A LGPD

Yasmin Floriano Fernandes

RESUMO

O presente artigo analisa a suficiência de instrumentos formais de governança em proteção de dados pessoais para demonstrar capacidade efetiva de resposta a incidentes em municípios de pequeno porte. O estudo parte do problema de saber se a publicação de políticas, a designação de encarregado e a existência de plano de resposta bastam, por si sós, para comprovar conformidade material com a Lei Geral de Proteção de Dados Pessoais e preparo para crises envolvendo dados pessoais. A pesquisa adota revisão bibliográfica, com análise documental acessória de materiais públicos disponibilizados pela Prefeitura Municipal de Realeza, Paraná, escolhidos como recorte ilustrativo por envolver município de pequeno porte e possuir documentos de governança acessíveis em portal institucional. A análise reconhece que a formalização reduz improvisação, cria linguagem comum, organiza etapas de triagem, contenção, comunicação, recuperação e aprendizagem, além de representar medida proporcional à realidade administrativa local. Contudo, sustenta que a suficiência depende de evidências de execução, como matriz de responsabilidades, registro do marco de ciência, observância do prazo regulatório, testes de continuidade, orientação aos operadores, exercícios simulados e ações corretivas verificáveis. Conclui-se que a conformidade municipal deve ser compreendida como processo progressivo e verificável: o plano é condição necessária e juridicamente relevante, mas somente se torna suficiente quando acompanhado de provas periódicas de funcionamento, decisão tempestiva, proteção aos titulares e manutenção de serviços essenciais.

Palavras-chave: Lei Geral de Proteção de Dados. Administração pública municipal. Incidente de segurança. Gerenciamento de crises. Conformidade.

1 INTRODUÇÃO

A adequação da Administração Pública à Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, costuma ser demonstrada por medidas visíveis, como política de privacidade, canal para titulares, designação do encarregado e plano de resposta a incidentes. Esses instrumentos são relevantes, pois indicam que o órgão público reconhece a proteção de dados como dever

institucional. Entretanto, a existência de documentos não elimina, por si só, a pergunta mais sensível em gerenciamento de crises: o ente público possui capacidade real de decidir, conter danos, comunicar adequadamente, preservar evidências e manter serviços essenciais quando o incidente efetivamente ocorre?

O debate é especialmente importante para municípios de pequeno porte. Prefeituras com equipes reduzidas acumulam funções, dependem de sistemas contratados, compartilham estruturas entre secretarias e nem sempre dispõem de unidade permanente de segurança da informação. Ao mesmo tempo, tratam dados pessoais e sensíveis em áreas como saúde, assistência social, educação, tributos, recursos humanos e fiscalização. A limitação de recursos justifica modelos proporcionais, mas não afasta a condição do município como controlador nem reduz o direito fundamental à proteção de dados pessoais, incorporado expressamente ao art. 5º da Constituição pela Emenda Constitucional nº 115/2022 (BRASIL, 1988; BRASIL, 2022a).

O presente artigo examina essa tensão a partir da seguinte pergunta de pesquisa: em que medida planos e documentos públicos de governança em proteção de dados são suficientes para demonstrar capacidade material de prevenir e administrar crises envolvendo dados pessoais em municípios de pequeno porte? Como recorte documental ilustrativo, utilizam-se documentos públicos da Prefeitura Municipal de Realeza, no Paraná, município com 19.247 habitantes no Censo 2022 (IBGE, 2023), incluindo página institucional de privacidade, portaria de designação de encarregado, política de proteção de dados, política de privacidade e plano de resposta a incidentes (REALEZA, 2024; 2025a; 2025b; 2025c; 2026).

A hipótese adotada é intermediária. A formalização é condição necessária e possui valor jurídico e administrativo, pois reduz a improvisação, define linguagem comum e cria base mínima de coordenação. Todavia, a suficiência não pode ser presumida apenas pela existência do documento. Ela depende de evidências de que as pessoas envolvidas conhecem o fluxo, possuem autoridade decisória, registram o momento da ciência, observam prazos regulatórios, comunicam titulares quando necessário, acionam operadores, restauram serviços e corrigem causas. Essa formulação será denominada conformidade progressiva verificável.

O objetivo geral consiste em analisar a suficiência de instrumentos formais de governança em LGPD como evidência de capacidade de resposta a incidentes em municípios de pequeno porte. Como objetivos específicos, pretende-se: examinar o valor jurídico da formalização; confrontar o plano de incidentes com deveres legais e regulatórios; distinguir papéis do controlador, do

encarregado, das áreas técnicas e dos operadores; e apresentar critérios mínimos auditáveis para gerenciamento de crises envolvendo dados pessoais.

2 METODOLOGIA

A pesquisa utiliza método de revisão bibliográfica, com abordagem qualitativa, descritiva e exploratória. A revisão bibliográfica fundamenta a análise em legislação, doutrina especializada, orientações da Autoridade Nacional de Proteção de Dados e literatura de gestão de riscos e crises. Como complemento, emprega-se análise documental acessória de documentos públicos, sem realização de pesquisa de campo, entrevistas, auditoria técnica, teste de sistemas ou atribuição de irregularidade a agentes públicos.

O corpus documental utilizado como recorte ilustrativo é composto por documentos disponibilizados publicamente pela Prefeitura Municipal de Realeza: Plano de Respostas a Incidentes, Política de Proteção de Dados Pessoais, Política de Privacidade, Portaria nº 7.841/2024 e página institucional de privacidade e proteção de dados. A ausência de determinada informação em documento público é tratada apenas como ausência de evidência pública, e não como prova de inexistência interna. Essa cautela é indispensável para evitar que inferências sejam convertidas em fatos.

A análise observa quatro eixos: existência de governança e definição de papéis; ciclo do incidente, desde detecção até aprendizagem; aderência a normas, especialmente LGPD, Resolução CD/ANPD nº 15/2024 e Resolução CD/ANPD nº 18/2024; e presença de evidências de operacionalização, como matriz de decisão, prazo de comunicação, contatos de contingência, objetivos de recuperação, registro de exercícios e indicadores. O estudo, portanto, avalia o que os documentos demonstram e quais evidências seriam necessárias para comprovar funcionamento efetivo.

3 FORMALIZAÇÃO COMO RESPOSTA PROPORCIONAL E JURIDICAMENTE RELEVANTE

A primeira perspectiva reconhece que a crise não pode ser administrada a partir de improvisação integral. Incidentes com dados pessoais exigem decisões simultâneas sobre tecnologia, continuidade do serviço, direitos dos titulares, deveres regulatórios, comunicação institucional e preservação de evidências. Sem etapas previamente definidas, cada área tende a responder a

partir de sua própria lógica: tecnologia busca restabelecer sistemas; jurídico reduz exposição; comunicação organiza mensagens; e a área finalística tenta preservar a prestação do serviço.

A LGPD estabelece princípios de segurança, prevenção e responsabilização e prestação de contas, além de impor a adoção de medidas técnicas e administrativas aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Também determina a comunicação de incidentes que possam acarretar risco ou dano relevante e estimula regras de boas práticas e governança (BRASIL, 2018). Não há, contudo, formato único de plano ou exigência de estrutura idêntica para todos os controladores, o que permite adequação proporcional aos riscos e à realidade administrativa.

Nesse sentido, documentos de governança têm valor concreto. Um plano escrito, aprovado, conhecido pelas áreas e associado a registros internos cria referência comum para treinamento, auditoria, orientação e aprendizagem. A simplicidade estrutural não significa, por si só, ineficácia. Em pequenas prefeituras, listas de contatos, formulário único, substituições definidas, exercício de mesa e checklists podem produzir resultados mais úteis do que sistemas sofisticados sem responsabilização clara.

O conjunto público de Realeza indica que a proteção de dados foi tratada além de uma declaração genérica. A página institucional identifica encarregada titular e substituta e indica canal de contato; a Política de Proteção de Dados apresenta diretrizes de ciclo de vida, responsabilidades e segurança; a Política de Privacidade informa o titular sobre práticas de tratamento; e o Plano de Respostas a Incidentes prevê etapas de identificação, triagem, contenção, preservação de evidências, recuperação, comunicação e lições aprendidas (REALEZA, 2024; 2025a; 2025b; 2025c; 2026).

Esse arranjo demonstra diligência inicial. A publicação de documentos e canal de contato amplia a transparência e permite que cidadãos, titulares de dados e órgãos de controle identifiquem compromissos assumidos pelo município. A publicidade não substitui segurança, mas reduz opacidade e cria base para cobrança institucional. Por isso, negar valor à formalização seria equivocado. Políticas e planos integram a arquitetura mínima de controle e representam etapa necessária de maturidade administrativa.

4 LIMITES DA DOCUMENTAÇÃO COMO PROVA DE CAPACIDADE MATERIAL

A perspectiva oposta parte do princípio da responsabilização e prestação de contas. A LGPD exige demonstração de medidas eficazes e capazes de comprovar observância às normas, não apenas intenção documental (BRASIL, 2018). A diferença entre existir e funcionar é decisiva. Um procedimento pode conter etapas corretas e ainda fracassar se a autoridade decisória não estiver definida, se os contatos estiverem desatualizados, se o operador não informar o controlador, se o backup não restaurar ou se o prazo regulatório for percebido tarde demais.

Em gerenciamento de crises, planos são representações antecipadas de um ambiente que se altera sob pressão. Pearson e Clair (1998) e Boin et al. (2016) destacam que crises envolvem ameaça, incerteza, urgência, construção de sentido, coordenação e comunicação. Nenhuma dessas capacidades pode ser integralmente inferida do texto. A prontidão surge quando pessoas, autoridade, recursos, comunicação e informação são testados em conjunto. Por isso, a documentação é indício de governança, mas não prova completa de resposta.

No plano analisado, há uma ressalva expressiva: o próprio documento informa tratar-se de proposta a ser customizada pela Prefeitura Municipal de Realeza de acordo com as peculiaridades de cada área e sob supervisão do encarregado e do comitê gestor (REALEZA, 2025a). A advertência pode ser interpretada positivamente, como abertura ao aperfeiçoamento, mas também impede concluir, apenas pelo texto, que a customização já ocorreu em todos os sistemas, secretarias e serviços críticos.

Outro ponto relevante é o prazo de comunicação. A Resolução CD/ANPD nº 15/2024 e as orientações oficiais da ANPD determinam que, havendo risco ou dano relevante, a comunicação à ANPD e aos titulares deve ocorrer no prazo de três dias úteis, ressalvada legislação específica (ANPD, 2024a). Além disso, quando as informações não estiverem completas, admite-se comunicação preliminar e posterior complementação. Assim, o plano operacional deve registrar o momento da ciência, o marco inicial do prazo, a decisão de comunicar ou não comunicar e a possibilidade de complementação.

A decisão também não pode ser atribuída de modo difuso. A Resolução CD/ANPD nº 18/2024 organiza a atuação do encarregado como canal de comunicação e orientação, sem transferir a responsabilidade do controlador. O encarregado pode orientar, articular e receber comunicações, mas não substitui a alta administração, a área técnica, os operadores, o jurídico ou a comunicação institucional. Sem matriz de responsabilidades, há risco de se esperar do encarregado decisão para a qual ele não possui autoridade ou meios.

Há, ainda, riscos de classificação inadequada. Incidentes com poucos registros podem ser graves quando envolvem crianças, pacientes, pessoas em situação de vulnerabilidade, dados de saúde, assistência social, denunciantes ou informações capazes de gerar fraude ou discriminação. A própria ANPD considera relevantes incidentes que possam causar danos materiais ou morais, envolver dados sensíveis ou alcançar grupos vulneráveis. Assim, critérios quantitativos devem ser acompanhados de gatilhos qualitativos centrados no titular.

Por fim, a capacidade material depende de evidências de continuidade e aprendizagem. Não basta prever recuperação progressiva; é necessário saber quais serviços são prioritários, qual tempo de indisponibilidade é tolerável, como preservar logs, como acionar fornecedores, como restaurar cópias e como registrar ações corretivas. Um plano nunca testado comprova intenção; um plano testado, medido e corrigido comprova capacidade em grau superior.

5 CONFORMIDADE PROGRESSIVA VERIFICÁVEL

O confronto entre as duas perspectivas permite rejeitar conclusões extremas. A primeira seria afirmar que um plano sem prova pública de exercícios é inútil. Essa conclusão ignora que procedimentos, papéis e conceitos são componentes reais de prevenção. A segunda seria declarar que a publicação do conjunto documental basta para comprovar adequação plena. Essa posição ignora que a suficiência depende de execução, treinamento, decisão e resultado.

A solução proposta é distinguir três níveis de evidência. A evidência normativa demonstra que existem regras, papéis e compromissos aprovados. A evidência operacional demonstra que as pessoas conseguem executar o fluxo em exercícios controlados ou em situações reais. A evidência de resultado demonstra que falhas foram corrigidas, prazos melhoraram, serviços foram recuperados e danos foram reduzidos. Esses níveis não se substituem: a norma sem operação pode ser simbólica; a operação sem aprendizagem pode repetir vulnerabilidades.

Aplicada ao recorte analisado, essa distinção conduz a uma conclusão intermediária. O município possui evidência normativa relevante, porque o conjunto público contempla política, canal, encarregado e plano. Todavia, o corpus público não oferece elementos suficientes para afirmar, de forma completa, os níveis operacional e de resultado. A conclusão mais segura é que existe base de governança a ser validada, e não conformidade plena presumida ou ausência total de conformidade.

A proporcionalidade também precisa ser corretamente compreendida. Ela não reduz o direito protegido; ajusta os meios. Um município de pequeno porte não precisa reproduzir estruturas de grandes órgãos, mas precisa saber quem decide, quem executa, quem comunica, onde registra, como contém, quanto tempo o serviço pode parar, quando aciona o operador e como presta contas. A complexidade pode diminuir; as funções essenciais permanecem.

A conformidade progressiva verificável reúne esses elementos. Ela é progressiva porque admite maturidade construída por etapas, priorizando riscos mais relevantes. É verificável porque cada etapa deve produzir prova de funcionamento. Não basta declarar que equipes serão treinadas; registra-se quem participou. Não basta prever backup; testa-se a restauração. Não basta dizer que haverá comunicação; mede-se o tempo entre ciência, decisão e protocolo. O progresso deixa de ser promessa e passa a ser demonstrável.

6 CRITÉRIOS MÍNIMOS PARA GERENCIAMENTO DE CRISES COM DADOS PESSOAIS

Para que um plano municipal de incidentes deixe de ser mera referência e se converta em capacidade demonstrável, propõe-se a adoção de seis critérios mínimos auditáveis: regra local aplicável, comando, relógio regulatório, continuidade, operadores e aprendizagem. O objetivo não é substituir programa completo de privacidade, inventário de dados ou política de segurança, mas estabelecer núcleo essencial de resposta para municípios de pequeno porte.

A regra local aplicável exige plano aprovado, versionado, datado, ajustado à Resolução CD/ANPD nº 15/2024 e vinculado à realidade das secretarias e sistemas municipais. O documento deve indicar responsáveis pela revisão, critérios de ativação e encerramento, canais de entrada e existência de anexos restritos, quando necessário. A cada alteração normativa, tecnológica ou contratual relevante, deve haver revisão ou decisão fundamentada de manutenção.

O comando demanda matriz simples de responsabilidades, distinguindo quem decide, quem executa, quem orienta e quem deve ser informado. A alta administração ou autoridade delegada decide sobre recursos, paralisação de serviços e comunicação institucional; a área técnica executa contenção e recuperação; a área finalística avalia impacto no serviço; o jurídico interpreta obrigações; a comunicação organiza mensagens; o operador coopera; e o encarregado orienta e mantém canal com titulares e ANPD.

O relógio regulatório exige registro do momento da ciência. Todo relato deve receber identificador, data, hora, descrição inicial, pessoas envolvidas, categoria de dados, medidas adotadas e decisão fundamentada sobre comunicação. Se houver risco ou dano relevante, o município deve trabalhar com o prazo de três dias úteis e preparar comunicação preliminar quando ainda não possuir todas as informações. O prazo não pode depender da conclusão da perícia.

A continuidade deve ser planejada com preservação de evidências. Cada serviço crítico precisa indicar tempo tolerável de indisponibilidade, informação necessária à retomada, procedimento manual seguro e critérios de retorno. A restauração deve ser validada tecnicamente e pela área usuária. A velocidade da recuperação não pode destruir registros indispensáveis para avaliação do incidente e prestação de contas.

Quanto aos operadores, contratos e renovações devem prever alerta imediato, preservação de logs, cooperação com avaliação de risco, comunicação de suboperadores e apoio após o incidente. O prazo interno do operador deve ser menor que o prazo regulatório do controlador. Cláusulas sem canal funcional e sem teste periódico geram segurança apenas formal.

A aprendizagem fecha o ciclo. Após incidente ou exercício, relatório deve registrar causa, decisões, tempos, dificuldades, medidas adotadas e ações corretivas. Cada ação deve ter responsável e prazo. A maturidade aumenta quando a prefeitura demonstra que uma falha identificada produziu correção verificável. Em municípios pequenos, exercícios de mesa semestrais e teste anual de restauração podem ser suficientes para iniciar ciclo consistente de melhoria.

6.1 HIPÓTESES OBJETIVAS DE VALIDAÇÃO

A capacidade de resposta pode ser testada sem exposição de titulares e sem simular ocorrência real atribuída a agente público específico. Uma prefeitura pode utilizar exercícios de mesa, com informações progressivas, nos quais os participantes precisam registrar decisões, justificar a avaliação de risco e indicar providências. O objetivo não é punir erros do exercício, mas verificar se o plano é compreendido, se o decisor é identificado, se o prazo regulatório é percebido e se a documentação produzida permitiria prestação de contas.

A primeira hipótese útil envolve publicação indevida, em portal oficial, de anexo contendo dados pessoais e informação de saúde. O teste deve verificar retirada controlada do arquivo,

preservação da versão publicada, análise de indexação por mecanismos de busca, identificação dos titulares, avaliação do risco, comunicação interna e revisão do fluxo de transparência. O resultado esperado não se limita à retirada do documento, pois a maturidade aparece quando a organização preserva evidências, avalia disseminação e impede nova publicação.

A segunda hipótese envolve credencial institucional comprometida, especialmente em área sensível como assistência social, saúde ou educação. O exercício deve verificar revogação de sessões, troca de credencial, autenticação multifator, análise de regras de encaminhamento, identificação de arquivos acessíveis, continuidade do atendimento e possibilidade de fraude. Nessa situação, a quantidade de registros acessados não deve ser o único critério; a vulnerabilidade dos titulares e o potencial de uso malicioso também orientam a gravidade.

A terceira hipótese envolve indisponibilidade de sistema crítico, causada por código malicioso ou falha de fornecedor, sem certeza inicial sobre extração de dados. O teste separa disponibilidade de confidencialidade. A prefeitura precisa manter serviço prioritário, isolar ativos, preservar logs, acionar operador, restaurar cópia validada e avaliar indícios de exfiltração. A ausência de confirmação inicial não elimina o relógio regulatório: registra-se a incerteza e atualiza-se a análise conforme surgem evidências.

Cada exercício deve possuir critérios mínimos de êxito: tempo de acionamento, identificação do decisor, completude do registro, preservação de evidência, qualidade da avaliação de risco, continuidade do serviço e conclusão das ações corretivas. Um simulado que apenas declara sucesso, sem medir desempenho, produz pouca aprendizagem. Ao contrário, uma falha identificada e corrigida demonstra maturidade superior, porque revela que o plano foi utilizado como instrumento de melhoria institucional.

A frequência pode ser proporcional. Um exercício de mesa semestral, somado a um teste anual de restauração, já cria ciclo mínimo de aprendizagem para estrutura municipal pequena. Incidentes reais, troca de fornecedor, alteração relevante de sistema ou mudança de equipe devem gerar validação adicional. O controle interno pode acompanhar evidências sem assumir a coordenação operacional, preservando independência para avaliar a execução.

7 DISCUSSÃO

Os achados confirmam a hipótese inicial. Documentos de Realeza são relevantes e apresentam elementos materiais de resposta, razão pela qual não devem ser reduzidos a formalidade vazia.

Ao mesmo tempo, eles não bastam para comprovar, sozinhos, capacidade real, pois a suficiência depende de customização, treinamento, exercício, indicadores e evidências de continuidade. A conformidade progressiva verificável descreve com maior precisão esse estágio: há base normativa cuja força probatória cresce quando convertida em execução testada.

A contribuição teórica está em separar conformidade de completude. A Administração Pública não precisa esperar programa perfeito para agir, mas também não pode confundir início com conclusão. A proteção de dados é processo contínuo de governança, coerente com a responsabilidade organizacional discutida por Doneda (2021), Mendes e Bioni (2021), Wimmer (2021) e Carvalho (2023). O critério decisivo não é a quantidade de documentos, mas a relação entre risco, medida e evidência de eficácia.

Na perspectiva do MBA em Gerenciamento de Crises, incidente de dados não é apenas problema jurídico ou tecnológico. Ele pode interromper serviço, afetar confiança pública, exigir comunicação urgente e expor pessoas a fraude, discriminação ou constrangimento. A resposta precisa lidar com informação incompleta e pressão temporal. Por isso, comunicação adequada, preservação de evidências, autoridade decisória e continuidade do serviço são elementos centrais da crise, e não providências acessórias.

A comunicação aos titulares merece destaque. Ela permite que a pessoa atingida adote medidas de proteção e reduz assimetria informacional. Mensagens defensivas, genéricas ou tardias tendem a aprofundar a crise. Coombs (2019) sustenta que instruções úteis e reconhecimento adequado dos afetados integram a resposta. Assim, a comunicação humanizada não significa discurso emocional, mas linguagem clara, precisa e útil para o titular.

A limitação do estudo decorre de seu caráter bibliográfico-documental. Não foram realizadas entrevistas, simulações, testes técnicos ou análise de contratos. Portanto, não se afirma que o município descumpre a LGPD, tampouco que possui plena prontidão. A conclusão limita-se ao que os documentos públicos permitem demonstrar: existe formalização relevante, mas a suficiência material exige evidências adicionais de funcionamento.

8 CONCLUSÃO

O artigo analisou se planos e documentos públicos de governança em proteção de dados pessoais são suficientes para demonstrar capacidade material de prevenção e administração de crises em municípios de pequeno porte. A resposta é negativa quando suficiência significa prova completa

de prontidão, mas positiva em sentido inicial: tais documentos demonstram formalização relevante e oferecem base para construção de capacidade institucional.

A formalização possui valor jurídico e organizacional. Políticas, canal de contato, encarregado e plano de resposta reduzem improvisação, organizam linguagem comum e estruturam etapas de detecção, triagem, criticidade, contenção, preservação de evidências, recuperação, comunicação e aprendizagem. Para municípios com recursos limitados, instrumentos concisos podem representar solução proporcional, desde que relacionados aos riscos locais.

Entretanto, a existência do documento não comprova execução. A suficiência material exige autoridade decisória definida, prazo regulatório expresso, registro do momento da ciência, matriz de responsabilidades, comunicação clara, acionamento de operadores, continuidade de serviços, testes de restauração, exercícios simulados e ações corretivas acompanhadas. Sem essas evidências, o plano comprova intenção institucional, mas não demonstra plenamente capacidade de resposta.

Conclui-se que a conformidade municipal com a LGPD deve ser compreendida como processo progressivo e verificável. Progressivo, porque admite amadurecimento por etapas compatíveis com a realidade local. Verificável, porque cada etapa precisa produzir prova de funcionamento. A prevenção de crises envolvendo dados pessoais depende menos da extensão dos manuais e mais da capacidade demonstrável de transformar regras em decisões tempestivas, proteção aos titulares, continuidade do serviço público e aprendizagem institucional.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Comunicação de incidente de segurança. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 12 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). 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. Brasília, DF: ANPD, 2022a. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 12 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. 2. ed. Brasília, DF: ANPD, 2022b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 12 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Guia orientativo: tratamento de dados pessoais pelo Poder Público. 2. ed. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 12 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: seção 1, Brasília, DF, 26 abr. 2024, p. 114-115. 2024a. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 12 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). 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: seção 1, Brasília, DF, 17 jul. 2024, p. 42. 2024b. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 12 ago. 2026.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

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 Técnicos da CGU, v. 1, p. 8-19, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 12 ago. 2026.

BOIN, Arjen; HART, Paul; STERN, Eric; SUNDELIUS, Bengt. The politics of crisis management: public leadership under pressure. 2. ed. Cambridge: Cambridge University Press, 2016. DOI: 10.1017/9781316339756.

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: 12 ago. 2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Texto compilado. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 12 ago. 2026.

BRASIL. Tribunal de Contas da União. Acórdão nº 1.384/2022 - Plenário. Auditoria: diagnóstico do grau de implementação da LGPD na Administração Pública Federal. Brasília, DF: TCU, 2022b. Disponível em: https://pesquisa.apps.tcu.gov.br/resultado/todas-bases/1384%252F2022%2520-%2520Plen%25C3%25A1rio. Acesso em: 12 ago. 2026.

CARVALHO, Lucas Borges de. O poder público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. Revista de Direito Administrativo, Belo Horizonte, v. 282, n. 2, p. 133-162, maio/ago. 2023. Disponível em: https://periodicos.fgv.br/rda/article/view/89347. Acesso em: 12 ago. 2026.

COOMBS, W. Timothy. Ongoing crisis communication: planning, managing, and responding. 5. ed. Thousand Oaks: SAGE, 2019.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Realeza (PR): cidades e estados. Rio de Janeiro: IBGE, 2023. Disponível em: https://www.ibge.gov.br/cidades-e-estados/pr/realeza.html. Acesso em: 12 ago. 2026.

MENDES, Laura Schertel; BIONI, Bruno Ricardo (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

PEARSON, Christine M.; CLAIR, Judith A. Reframing crisis management. Academy of Management Review, v. 23, n. 1, p. 59-76, 1998. DOI: 10.5465/AMR.1998.192960.

REALEZA (Município). Portaria nº 7.841, de 1º de novembro de 2024. Designa a encarregada pelo tratamento de dados pessoais da Prefeitura Municipal de Realeza. Diário Oficial dos Municípios do Paraná, edição 3146, 4 nov. 2024. Disponível em: https://www.realeza.pr.gov.br/docs/dados/PORTARIA%20N7841.pdf. Acesso em: 12 ago. 2026.

REALEZA (Município). Plano de Respostas a Incidentes. Realeza, PR: Prefeitura Municipal, 2025a. Documento datado de 14 fev. 2025. Disponível em: https://www.realeza.pr.gov.br/docs/Plano_Resposta_Incidentes.pdf. Acesso em: 12 ago. 2026.

REALEZA (Município). Política de Proteção de Dados Pessoais da Prefeitura Municipal de Realeza. Realeza, PR: Prefeitura Municipal, 2025b. Disponível em: https://realeza.pr.gov.br/docs/dados/POLITICA_DE_PROTECAO_DADOS_REALEZA.pdf. Acesso em: 12 ago. 2026.

REALEZA (Município). Política de Privacidade. Realeza, PR: Prefeitura Municipal, 2025c. Disponível em: https://realeza.pr.gov.br/docs/dados/5-POLITICA_DE_PRIVACIDADE.pdf. Acesso em: 12 ago. 2026.

REALEZA (Município). Privacidade e proteção de dados. Realeza, PR: Prefeitura Municipal, 2026. Disponível em: https://www.realeza.pr.gov.br/privacidade-e-protecao-de-dados. Acesso em: 12 ago. 2026.

REASON, James. Managing the risks of organizational accidents. Aldershot: Ashgate, 1997.

WEICK, Karl E.; SUTCLIFFE, Kathleen M. Managing the unexpected: sustained performance in a complex world. 3. ed. San Francisco: Jossey-Bass, 2015.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, Laura Schertel; BIONI, Bruno Ricardo (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 282-299.