

ABORDAGENS TEÓRICAS E PRÁTICAS EM PESQUISA

COORDENADORES

Patricia Bieging

Raul Inácio Busarello

ISBN 978-85-7221-552-7

2026

Lilian Gonçalves dos Santos

CULTURA DE SEGURANÇA, ASSINATURA ELETRÔNICA E CONTROLES INTERNOS:

DESAFIOS DA INTEGRIDADE DOCUMENTAL
E DA CONFORMIDADE NA ADMINISTRAÇÃO PÚBLICA

DOI: 10.31560/pimentacultural/978-85-7221-552-7.8

RESUMO

A transformação digital mundial impõe à Administração Pública a necessidade de ampliar a utilização de documentos eletrônicos, assinaturas digitais e sistemas informatizados, trazendo benefícios para a eficiência administrativa, mas também desafios relacionados à integridade documental, à segurança da informação e à conformidade regulatória. Este estudo tem como objetivo analisar como os controles internos, a gestão de riscos, a cibersegurança e a cultura organizacional contribuem para a redução de vulnerabilidades e para o fortalecimento da segurança jurídica nos processos administrativos. A pesquisa caracteriza-se como aplicada, de abordagem qualitativa, com objetivos descritivos e exploratórios, desenvolvida por meio de pesquisa bibliográfica e documental, fundamentada em legislação, referenciais técnicos e literatura especializada. Conforme pesquisas na literatura, as falhas na autenticidade documental e no uso inadequado de assinaturas eletrônicas geram retrabalho, atrasos na tramitação processual e aumento dos riscos administrativos. Evidenciou-se, ainda, que a adoção de controles internos, mecanismos de validação de assinaturas eletrônicas, gestão de riscos e programas de capacitação contínua fortalece a conformidade administrativa, reduz vulnerabilidades operacionais e aumenta a confiabilidade dos processos. Conclui-se que a efetividade da transformação digital depende da integração entre tecnologia, governança e desenvolvimento de uma cultura organizacional voltada à prevenção de riscos e à melhoria contínua da gestão pública.

Palavras-chave: Conformidade. Retrabalho. Cibersegurança. Digital. Riscos.

INTRODUÇÃO

A transformação digital na Administração Pública brasileira tem se consolidado como um vetor fundamental para a promoção da eficiência, da transparência e da desburocratização dos serviços prestados à sociedade. O esforço institucional para migrar processos físicos para o ecossistema digital visa, primordialmente, atender ao Princípio da Eficiência, previsto no artigo 37 da Constituição Federal de 1988 (Brasil, 1988, art. 37). Contudo, a transição para o ambiente digital impõe desafios complexos no que tange à garantia da segurança jurídica, à integridade dos atos administrativos e à observância das normas regulatórias.

No contexto das organizações públicas dotadas de poder administrativo e de regulação, a celeridade processual depende diretamente da exatidão dos atos praticados pelos requerentes. A conformidade documental não se limita ao preenchimento de requisitos formais; hoje, abrange de forma indissociável a proteção de dados sensíveis e a verificação inequívoca da identidade dos envolvidos. Quando há desconhecimento por parte dos usuários — sejam eles internos ou externos — acerca das normas de segurança da informação, surgem vulnerabilidades críticas que comprometem a integridade de todo o fluxo de trabalho institucional.

Na esfera pública, o poder de polícia administrativa representa a prerrogativa que o Estado possui de limitar, disciplinar ou regular o exercício de direitos, atividades ou o uso de bens por parte dos cidadãos, em benefício do interesse público, manifestando-se frequentemente na concessão de licenças, alvarás e autorizações. Nesse cenário, o principal gargalo identificado na tramitação de processos administrativos digitais reside na falta de autenticidade

documental e na inadequação às diretrizes da Lei Geral de Proteção de Dados (LGPD). Falhas na tramitação de documentos e assinaturas, decorrentes da ausência de uma cultura digital integrada, geram recorrentes pendências administrativas. Esse retrabalho sistemático estende os prazos de análise e de aprovação e, conseqüentemente, adia a emissão da documentação solicitada, resultando em períodos que podem ultrapassar 30 dias de morosidade.

Longe de configurar um entrave burocrático da instituição, a triagem rigorosa constitui um mecanismo de salvaguarda indispensável para mitigar fraudes e garantir a segurança jurídica do processo. Trata-se do princípio da Eficiência que garante a estabilidade das leis e dos atos administrativos, assegurando que o procedimento seja robusto e imune a fraudes, protegendo simultaneamente o cidadão administrado e o Estado.

Diante desse cenário, este artigo propõe uma abordagem educativa e preventiva, analisando de que forma a disseminação de conceitos de cibersegurança e auditoria pode mitigar riscos nos trâmites públicos. O objetivo geral é demonstrar que a segurança da informação e a conformidade (*compliance*) não representam obstáculos à eficiência e à eficácia, mas sim os pilares que viabilizam a verdadeira eficiência administrativa. Com o intuito de viabilizar essa celeridade, questiona-se: de que forma a integridade documental e os controles internos podem contribuir para a mitigação de riscos administrativos?

O presente estudo caracteriza-se como uma pesquisa de natureza aplicada, com abordagem qualitativa e objetivo descritivo-exploratório, voltada à análise da importância da integridade documental, da cibersegurança e dos controles internos na administração pública contemporânea.

A abordagem qualitativa foi adotada por possibilitar interpretação mais aprofundada dos fenômenos relacionados à segurança da informação, à conformidade administrativa e à gestão documental no setor público.

Quanto aos objetivos, a pesquisa possui caráter descritivo, por apresentar conceitos relacionados à autenticidade documental, cibersegurança, governança e controles internos, além do caráter exploratório, uma vez que busca ampliar a compreensão sobre os desafios enfrentados pela administração pública, diante da transformação digital e do aumento das exigências relacionadas à segurança da informação.

Os procedimentos metodológicos adotados basearam-se em pesquisa bibliográfica e documental. Já a pesquisa documental concentrou-se na análise de dispositivos legais e normativos que regulamentam o uso de assinaturas eletrônicas, proteção de dados pessoais e controles administrativos no contexto brasileiro.

Entre os principais referenciais normativos analisados destacam-se a Medida Provisória nº 2.200-2/2001 (Brasil, 2001), responsável pela criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a Lei nº 14.063/2020 (Brasil, 2020), que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 (Brasil, 2018)), que estabelece diretrizes relacionadas à proteção e ao tratamento de dados pessoais.

A análise dos conteúdos foi realizada de forma interpretativa, buscando identificar relações entre transformação digital, segurança documental, conformidade administrativa e eficiência dos processos públicos, à luz do referencial teórico e normativo selecionado.

DISCUSSÃO TEÓRICA

FUNDAMENTAÇÃO TEÓRICA: O PILAR DA AUDITORIA E O PROCESSO CULTURAL DE CONFORMIDADE (*COMPLIANCE*) NO SETOR PÚBLICO

O termo *compliance*, originado do verbo em inglês *to comply* (agir de acordo com uma regra, pedido ou comando), possui suas raízes no ambiente corporativo privado, historicamente associado à necessidade de mitigar riscos operacionais e evitar sanções legais. Contudo, esse conceito, no âmbito da Administração Pública, é frequentemente denominado integridade ou conformidade pública e ganhou contornos fundamentais nas últimas décadas. No setor público, a cultura de conformidade não visa o lucro ou a proteção de mercado, mas sim a garantia de que o interesse coletivo e a legalidade estrita guiem integralmente cada ato administrativo.

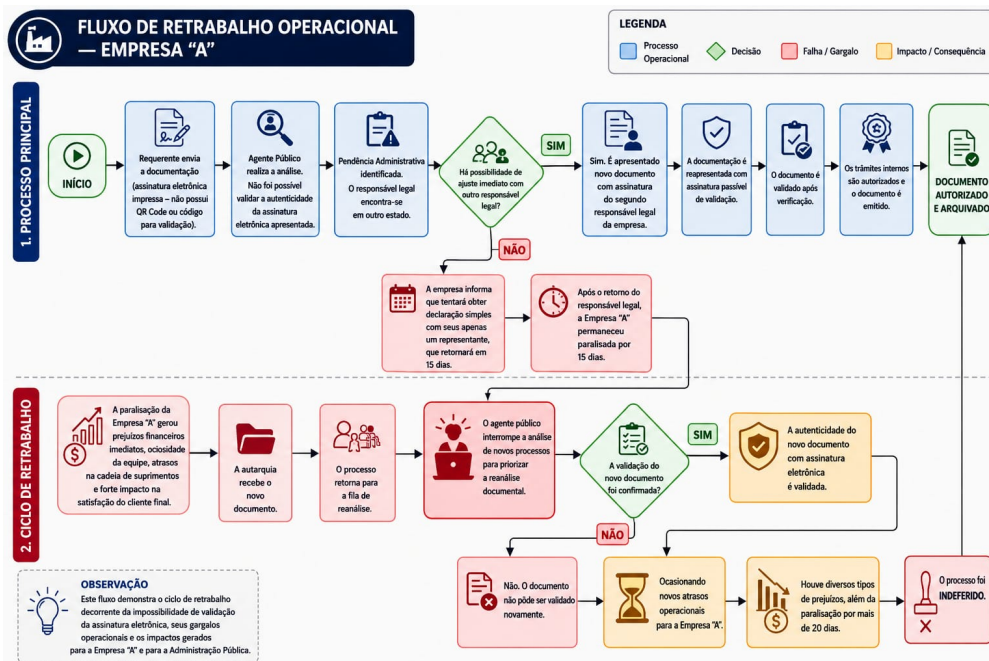
A conformidade na esfera pública traduz-se no alinhamento contínuo das atividades da instituição com as leis, decretos, portarias, normas e regulamentos que regem a sua atuação. No âmbito de órgãos de controle interno e fiscalizadores, onde o cumprimento de requisitos documentais rígidos é obrigatório por lei, a auditoria interna atua como uma ferramenta de proteção estratégica. Ela assegura que os processos de autorização e licenciamento não sejam maculados por fraudes, falsificações ou desvios procedimentais. Assim, a conformidade documental deixa de ser um mero formalismo e passa a ser entendida como um pilar de sustentação da integridade institucional. Quando o cidadão submete uma solicitação e o agente público a analisa, ambos estão operando dentro de um ecossistema normativo que visa salvaguardar a sociedade e preservar o interesse comum.

GESTÃO DE RISCOS ADMINISTRATIVOS E O IMPACTO DO RETRABALHO

O risco é um elemento inerente a qualquer atividade organizacional. No contexto administrativo público, a gestão de riscos envolve identificar, avaliar e mitigar eventos que possam comprometer a eficiência ou a legalidade dos processos. Um dos riscos mais frequentes e de alto impacto operacional na triagem de documentos é a desconformidade de assinaturas e a recepção de dados inadequados. Quando um requerimento é submetido com falhas graves de autenticidade, o processo não pode prosseguir; a consequência direta é a abertura de uma pendência administrativa e a notificação do usuário para a emissão de um novo documento, o que dá início a outra análise.

Esse ciclo gera o fenômeno do retrabalho. Na engenharia de processos, o retrabalho é considerado um dos maiores desperdícios de recursos, pois exige que o agente público analise várias vezes o mesmo objeto, aumentando o tempo médio de atendimento e criando gargalos temporais que atrasam a prestação do serviço. Segundo a Teoria das Filas, aplicável ao estudo dos pontos de estrangulamento e dos tempos de espera na administração, a maior parte dos problemas operacionais situa-se precisamente nesses gargalos de fluxo. Conforme aponta Chiavenato (2004), essa teoria dedica-se a analisar os atrasos verificados em determinados pontos de serviço devido a descompassos na capacidade de processamento. Esse ciclo é sintetizado na Figura 1.

Figura 1 – Fluxograma comparativo do impacto do retrabalho na análise documental pública



Fonte: elaborado pela autora (2026), com base em Chiavenato (2004).

Nota: O fluxo destaca o atraso gerado pela abertura de pendências administrativas, que pode estender o prazo de resolução em até 20 dias.

Portanto, a exigência de conformidade rigorosa no protocolo de entrada do processo não reflete uma escolha burocrática, mas uma estratégia proativa de gestão de risco. A entrada de um documento inválido fragiliza o ato administrativo, pode suscitar questionamentos jurídicos futuros e gerar um custo consideravelmente maior para o Estado e para o cidadão. Sobre o papel da eficiência nas organizações, Chiavenato (2004, p. 155) esclarece:

A eficiência preocupa-se com os meios, com os métodos e procedimentos mais indicados que precisam ser devidamente planejados e organizados a fim de assegurar a otimização da utilização dos recursos disponíveis. A eficiência não se preocupa com os fins, mas simplesmente com os meios. O alcance dos objetivos visados não entra na esfera de competência da eficiência; é um assunto ligado à eficácia.

No contexto analisado, o retrabalho decorrente de inconsistências documentais compromete diretamente a eficiência administrativa ao exigir reprocessamentos, correções e novas tramitações, impactando negativamente o desempenho do fluxo de assinatura eletrônica. Diante disso, a busca pela celeridade no processamento das demandas administrativas não pode ocorrer em detrimento da segurança jurídica e da legalidade. Existe uma tensão natural entre o desejo do usuário de obter uma licença imediata e o dever do Estado de auditar minuciosamente as informações prestadas. Em serviços que envolvem produtos regulados ou autorizações especiais, a celeridade sem critérios técnicos pode resultar na concessão indevida de direitos, gerando riscos graves à sociedade.

A verdadeira eficiência, sob a ótica da auditoria moderna, reside em educar os requerentes para que os processos sejam protocolados e admitidos. Ao eliminar os erros na origem por meio da educação digital, a velocidade processual é maximizada sem desconsiderar a segurança jurídica. Como aponta a evolução do pensamento administrativo compilada por Chiavenato (2004, p. 153), a abordagem moderna considera os meios na busca da eficiência, mas sem perder de vista os fins e os resultados para o alcance da eficácia.

ANÁLISE DE DADOS

O PILAR DA CIBERSEGURANÇA E DA LEGISLAÇÃO NA INTEGRIDADE DOCUMENTAL PÚBLICA

A transformação digital na administração pública trouxe avanços significativos para a tramitação de documentos, otimização de processos e ampliação da eficiência administrativa. Entretanto, o aumento da dependência de sistemas eletrônicos ampliou os riscos relacionados à segurança da informação, à autenticidade documental e à proteção de dados institucionais e pessoais. Nesse cenário, a cibersegurança passa a ocupar posição estratégica dentro dos órgãos públicos, deixando de ser uma questão tecnológica para tornar-se uma ferramenta essencial da governança e da conformidade administrativa.

Tabela 1 – Síntese comparativa dos principais indicadores de incidentes cibernéticos na Administração Pública

Indicador	CTIR Gov (2026)	Hackmageddon (2026)
Total de incidentes registrados	2.539 notificações de incidentes cibernéticos	1.748 ataques cibernéticos divulgados mundialmente
Administração Pública	Um dos setores mais impactados pelas notificações e alertas de segurança	Entre os setores mais visados por ataques direcionados
Software vulnerável	Exploração de vulnerabilidades em sistemas e aplicações entre as principais causas dos incidentes	Exploração de vulnerabilidades conhecidas como um dos principais vetores de ataque
Mês de maior incidência	Março	Outubro

Fonte: adaptado de CTIR Gov (2026) e Hackmageddon (2026); adaptação da autora (2026).

Os indicadores apresentados na Tabela 1 demonstram que a Administração Pública permanece exposta a incidentes cibernéticos,

capazes de comprometer a disponibilidade, a confidencialidade e a integridade das informações institucionais. Nesse contexto, a adoção de mecanismos que assegurem a autenticidade documental torna-se elemento indispensável para a mitigação desses riscos. Entre tais mecanismos, destacam-se as assinaturas eletrônicas baseadas na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que garantem rastreabilidade, autoria e integridade dos documentos digitais nos processos administrativos.

A utilização de assinaturas eletrônicas, plataformas digitais e sistemas integrados de gestão documental exige mecanismos capazes de assegurar a integridade, autenticidade e rastreabilidade das informações. A ausência de controles adequados pode resultar em fraudes documentais, vazamento de dados, adulterações e comprometimento da confiabilidade dos processos administrativos. Dessa forma, os controles internos associados à segurança digital tornam-se instrumentos indispensáveis para a mitigação de riscos institucionais.

No contexto brasileiro, a modernização administrativa foi acompanhada pela criação de dispositivos legais voltados à regulamentação do ambiente digital. Entre eles, destaca-se a Lei nº 14.063/2020 (Brasil, 2020), responsável por disciplinar o uso de assinaturas eletrônicas em interações com entes públicos, estabelecendo níveis de confiabilidade e mecanismos de validação documental. A legislação contribuiu para ampliar a segurança jurídica das transações eletrônicas e fortalecer a legitimidade dos documentos digitais.

Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018 (Brasil, 2018), reforçou a necessidade de proteção das informações tratadas pelos órgãos públicos. A legislação estabeleceu princípios relacionados à segurança, transparência e responsabilização no tratamento de dados pessoais, exigindo das instituições públicas maior rigor.

Outro aspecto relevante refere-se à necessidade de desenvolvimento de uma cultura organizacional voltada à segurança da informação. Embora ferramentas tecnológicas sejam fundamentais, a atuação humana continua sendo um dos principais fatores associados às falhas de segurança. Procedimentos inadequados, compartilhamento indevido de acessos, ausência de verificação documental e desconhecimento das normas internas podem comprometer a integridade dos processos administrativos.

Nesse sentido, a conscientização dos servidores e a implementação de práticas educativas tornam-se medidas importantes para o fortalecimento da conformidade institucional. A promoção de capacitação, treinamentos, atualização contínua e disseminação de boas práticas contribuem para reduzir vulnerabilidades operacionais e aumentar a confiabilidade dos sistemas administrativos.

Portanto, a integração entre cibersegurança, legislação e controles internos representa um dos pilares para a preservação da integridade documental na administração pública. Mais do que garantir proteção tecnológica, trata-se de assegurar transparência, confiabilidade e legitimidade aos processos administrativos.

Sob a perspectiva da Teoria Geral dos Sistemas, a Administração Pública pode ser compreendida como um sistema aberto, que recebe entradas, processa informações e gera respostas ao ambiente externo. Conforme ensina Chiavenato (2004), as organizações operam sob dois processos opostos e complementares: a homeostasia, que garante a tendência do sistema em permanecer em equilíbrio mantendo seu *status quo* interno; e a adaptabilidade, que representa a mudança estrutural necessária para ajustar-se aos novos padrões exigidos pelo ambiente. No processo de digitalização, a falta de adaptabilidade normativa e cultural gera disfunções e fragilidades.

O marco da cibersegurança estruturada no Brasil ganhou impulso, notadamente a partir de diagnósticos realizados pelo Tribunal de Contas da União (TCU) em sua “Lista de Alto Risco da Administração Pública Federal”, que evidenciou vulnerabilidades relativas à segurança cibernética no setor público. Em resposta a esse panorama, o Decreto Presidencial nº 11.856 instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança (CNCiber), visando proteger o ciberespaço nacional e articular respostas a incidentes governamentais. Gráficos e estatísticas mapeados por centros de resposta a incidentes cibernéticos (como o CTIR Gov) revelam um cenário de ataques mensais, ressaltando a urgência de ferramentas de mitigação robustas.

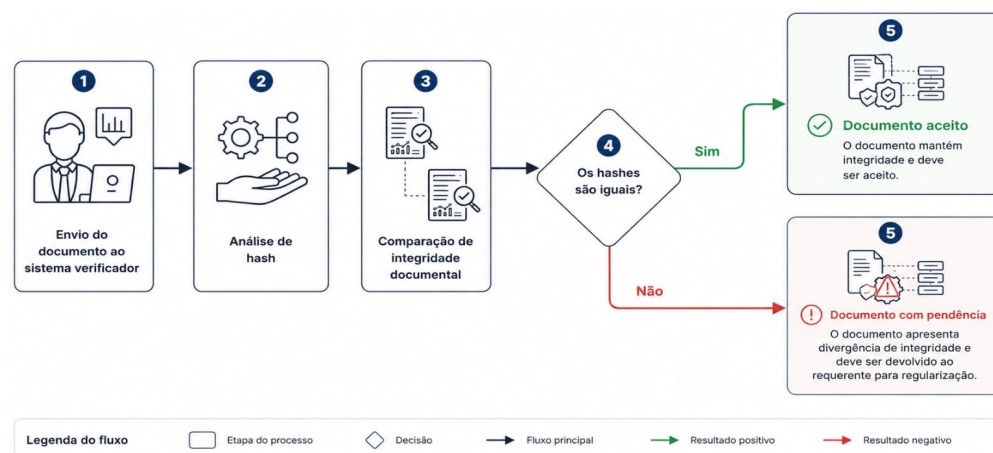
INFRAESTRUTURA DE CHAVES PÚBLICAS E CATEGORIAS DE ASSINATURAS

Para estruturar e viabilizar a segurança nessas operações digitais, o ordenamento brasileiro baseia-se na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). No gerenciamento eletrônico de documentos, as assinaturas são subdivididas em 3 (três) categorias legais, conforme o nível de complexidade e segurança exigido:

1. **Simples:** permite a identificação básica do signatário por meio de cruzamento de dados elementares (como endereço de IP e e-mail), sendo indicada para interações de baixo risco;
2. **Avançada:** associa-se de modo unívoco ao signatário, utilizando chaves criptográficas ou biometria, garantindo validade jurídica para a maior parte dos atos e contratos administrativos; e
3. **Qualificada:** possui o nível máximo de segurança e presunção de legalidade, é gerada obrigatoriamente a partir de um certificado digital emitido pela ICP-Brasil e tem equivalência legal à assinatura manuscrita com firma reconhecida em cartório (Brasil, 2020).

O ciclo de vida de uma assinatura qualificada compreende as etapas de criação (cifração com a chave privada do signatário), verificação (validação por meio da chave pública contida no certificado digital), armazenamento (preservação em mídias atualizadas) e revalidação (por meio de novas assinaturas ou carimbos do tempo para combater a expiração de algoritmos). O fluxo de validação da integridade do documento assinado eletronicamente é apresentado na Figura 2.

Figura 2 – Fluxo de validação da integridade de documento assinado eletronicamente



Fonte: elaborado pela autora (2026), com base no Instituto Nacional de Tecnologia da Informação (2026a).

O processo criptográfico opera por meio de funções de hash criptográfico, que funcionam como uma “impressão digital” matemática de tamanho fixo para qualquer volume de dados. Na criação, o *hash* do documento é cifrado com a chave privada do signatário. Na validação, realizada em serviços como o portal oficial validar.iti.gov.br, o sistema decifra a assinatura com a chave pública e recalcula o *hash*. Se os valores forem idênticos, a integridade e a autoria do documento eletrônico restam comprovadas.

É importante destacar que, conforme as diretrizes do Governo Digital (2026), a impressão física de um documento assinado eletronicamente não preserva a validade jurídica da assinatura digital, uma vez que os metadados criptográficos e os certificados não são passíveis de validação em suporte de papel. A desatenção a esse fator pelos requerentes constitui uma das principais causas de rejeição e geração de pendências administrativas nos órgãos fiscalizadores.

No contexto das organizações, a segurança cibernética consolida-se como um conjunto de ferramentas, políticas, salvaguardas e práticas de gerenciamento de riscos destinadas a proteger o ecossistema digital. A ausência desse conhecimento técnico e de controles internos adequados resulta na paralisação dos fluxos administrativos, trazendo prejuízos tanto para o Estado quanto para os administrados.

CONTROLES INTERNOS E MITIGAÇÃO DE RISCOS NA GESTÃO DOCUMENTAL PÚBLICA

Os controles internos desempenham papel essencial na manutenção da integridade documental e na prevenção de falhas administrativas dentro das organizações públicas. Sua função está relacionada à criação de mecanismos capazes de assegurar maior confiabilidade aos processos, reduzir vulnerabilidades operacionais e fortalecer a conformidade institucional diante das exigências legais e administrativas.

Na administração pública, os controles internos não se limitam à fiscalização financeira ou contábil, abrangendo também procedimentos relacionados à tramitação documental, validação de informações, autenticação de registros eletrônicos e monitoramento das atividades executadas pelos agentes públicos. Dessa forma, tais mecanismos contribuem para a redução de inconsistências, fraudes

documentais e erros operacionais que possam comprometer a eficiência do processo.

A crescente digitalização dos serviços públicos ampliou a necessidade de controles mais estruturados e integrados aos sistemas eletrônicos utilizados pelas instituições. Nesse cenário, práticas como segregação de funções, controle de acessos, rastreabilidade das ações realizadas em plataformas digitais, auditorias internas e monitoramento contínuo passaram a representar ferramentas de mitigação de riscos institucionais.

A ausência de controles eficientes pode favorecer a ocorrência de falhas na submissão de documentos, utilização indevida de credenciais institucionais, compartilhamento inadequado de informações e comprometimento da autenticidade documental. Tais situações geram impactos administrativos relevantes, incluindo retrabalho, atrasos processuais, insegurança jurídica e prejuízos à credibilidade institucional perante os cidadãos e órgãos fiscalizadores.

Além dos aspectos tecnológicos, a efetividade dos controles internos depende diretamente da atuação humana e da cultura organizacional existente na instituição. A falta de capacitação dos servidores, o desconhecimento sobre procedimentos de segurança e a baixa conscientização quanto à importância da conformidade documental podem enfraquecer os mecanismos de controle.

Nesse contexto, a gestão de riscos assume função estratégica ao permitir a identificação de vulnerabilidades capazes de afetar a integridade dos processos administrativos. A adoção de medidas preventivas, associada ao fortalecimento da cultura de segurança e conformidade, possibilita maior proteção às informações institucionais e contribui para a construção de ambientes administrativos mais seguros, transparentes e eficientes.

Portanto, os controles internos devem ser compreendidos como instrumentos para a governança pública contemporânea, especialmente diante dos desafios impostos pela transformação digital e pelo aumento da circulação de documentos eletrônicos nos processos administrativos. Conforme orienta o referencial técnico do Tribunal de Contas da União (2018):

Art. 6º Além dos controles internos da gestão, os órgãos e entidades do Poder Executivo federal podem estabelecer instâncias de segunda linha (ou camada) de defesa, para supervisão e monitoramento desses controles internos. Assim, comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance, por exemplo, podem se constituir em instâncias de supervisão de controles internos.

O Quadro 1 relaciona riscos documentais, consequências administrativas, controles internos e benefícios esperados.

Quadro 1 – Relação entre riscos documentais, controles internos e benefícios para a Administração Pública

Risco Documental	Consequência Administrativa	Controle Interno Aplicado	Benefício Gerado
Assinatura inválida	Pendência administrativa	Validação eletrônica	Redução de retrabalho
Documento incompleto	Retrabalho processual	Checklist documental	Maior eficiência operacional
Dados divergentes	Atraso processual	Conferência cadastral	Maior segurança jurídica
Falha de autenticação	Fraude documental	Certificado ICP-Brasil	Preservação da integridade documental

Fonte: Elaborado pela autora (2026), com base em Idalberto Chiavenato (2003), nas diretrizes do Tribunal de Contas da União (2018) e na legislação sobre assinaturas eletrônicas.

O Quadro 2 sintetiza as linhas de defesa aplicadas à gestão documental.

Quadro 2 – Linhas de defesa aplicadas à gestão documental

SEGREGAÇÃO DE DEVERES: LINHAS DE DEFESA	
Visão geral do modelo organizacional	
1ª Linha: Gestão e Controles Operacionais	2ª Linha: Supervisão e Integridade (Comitês)
Execução e Fluxo de Processos — Controles embutidos nas atividades diárias	Supervisão Independente — Verificação da eficácia dos controles
Gerenciamento de Riscos — Gestão operacional integrada	Avaliação de Riscos — Avaliação de riscos
Conformidade Operacional — Garantia de conformidade na execução	Relatórios e Conselhos — Estrutura de reporte e governança
—	Comitê — Órgão de apoio e supervisão

Fonte: elaborado pela autora (2026), com base nos parâmetros do Referencial Técnico de Controle Interno do TCU (2018).

Nota: Destaca a segregação entre os controles operacionais da gestão (1ª linha) e a supervisão dos comitês de integridade (2ª linha).

CULTURA ORGANIZACIONAL, CONSCIENTIZAÇÃO E CONFORMIDADE ADMINISTRATIVA

A efetividade das políticas de segurança da informação e dos controles internos está relacionada à cultura organizacional presente nas instituições públicas. Embora recursos tecnológicos e instrumentos normativos sejam indispensáveis para a proteção documental, a atuação humana continua sendo um dos fatores na prevenção de falhas, inconformidades e vulnerabilidades nos processos administrativos.

A cultura organizacional pode ser compreendida como o conjunto de valores, práticas, comportamentos e padrões adotados por uma instituição ao longo de suas atividades. No contexto da administração pública, uma cultura voltada à segurança e à conformidade contribui para fortalecer a responsabilidade funcional,

estimular boas práticas administrativas e reduzir condutas que possam comprometer a autenticidade documental e a confiabilidade das informações institucionais.

A ausência de conscientização dos agentes públicos representa um dos principais desafios relacionados à segurança documental. Em muitos casos, falhas operacionais decorrem não apenas de limitações tecnológicas, mas também da falta de treinamento, do desconhecimento dos procedimentos institucionais e da utilização inadequada de sistemas eletrônicos. Situações como compartilhamento indevido de credenciais, submissão incorreta de documentos, armazenamento inadequado de informações e descumprimento de protocolos internos podem gerar impactos à administração pública.

Nesse cenário, programas de capacitação contínua tornam-se necessários para fortalecer a cultura de segurança organizacional. A realização de treinamentos periódicos, campanhas educativas e orientações voltadas à proteção da informação contribui para ampliar o nível de conscientização dos servidores e reduzir riscos relacionados ao fator humano nos processos administrativos.

Além da conscientização, a conformidade administrativa assume papel estratégico na consolidação de práticas institucionais mais seguras e transparentes. O conceito de conformidade está associado ao cumprimento de normas legais, regulamentos internos e procedimentos internos, garantindo que as atividades administrativas sejam executadas de forma ética, padronizada e alinhada aos princípios da administração pública.

A adoção de práticas de conformidade fortalece a governança institucional ao assegurar a confiabilidade dos fluxos documentais, ampliar a rastreabilidade das operações realizadas e aumentar a confiabilidade aos atos administrativos. Dessa maneira, a integração entre cultura organizacional, segurança da informação e conformidade administrativa possibilita a construção de ambientes

institucionais mais resilientes diante dos desafios impostos pela transformação digital.

Como sistemas abertos, as organizações possuem a capacidade intrínseca de enfrentar e superar perturbações provocadas pelo meio externo sem que se comprometa seu potencial de auto-organização. Essa capacidade de absorção é definida na teoria administrativa como resiliência. Conforme salienta Chiavenato (2004, p. 481), a resiliência determina o grau de defesa ou de vulnerabilidade de um sistema frente às pressões externas. Instituições com elevada resiliência em seus modelos tradicionais e burocráticos podem apresentar forte resistência cultural ao avanço da inovação, tornando imperiosa a sensibilização contínua dos agentes para que a transição digital ocorra de forma segura e colaborativa.

IMPACTOS DAS FALHAS DOCUMENTAIS NOS PROCESSOS ADMINISTRATIVOS

A integridade documental representa elemento essencial para o funcionamento adequado da administração pública, especialmente em um cenário marcado pela evolução da digitalização dos serviços prestados à sociedade e pela utilização intensiva de sistemas eletrônicos nos fluxos administrativos. Nesse contexto, falhas relacionadas à autenticidade, validação ou submissão inadequada de documentos podem gerar impactos na eficiência operacional, na segurança institucional e na confiabilidade dos processos públicos.

Os processos administrativos dependem da veracidade e consistência das informações apresentadas pelo solicitante para que decisões sejam tomadas de maneira segura e conforme os princípios legais da administração pública. Quando documentos apresentam inconsistências, ausência de autenticidade comprovada ou irregularidades em sua tramitação, ocorre o comprometimento da

confiabilidade processual, favorecendo retrabalho, atrasos operacionais e aumento da burocracia administrativa.

As falhas documentais geram impactos sobre a eficiência administrativa, destacando-se a necessidade de reanálise dos procedimentos, a interrupção dos fluxos de trabalho, a devolução de processos para correção e a ampliação do tempo requerido para a conclusão das demandas institucionais. Essas situações também podem comprometer a prestação de serviços públicos à sociedade.

Além dos prejuízos operacionais, falhas na integridade documental também podem gerar consequências jurídicas e institucionais. A utilização inadequada de assinaturas eletrônicas, o envio de documentos sem validação apropriada ou a fragilidade nos mecanismos de controle interno podem resultar em questionamentos administrativos, responsabilizações funcionais e vulnerabilidades durante auditorias e processos de fiscalização.

No âmbito da governança pública, a ocorrência frequente de inconsistências documentais tende a reduzir a credibilidade institucional e enfraquecer a confiança da sociedade nos processos administrativos. A transparência e a confiabilidade das informações públicas constituem pilares da legitimidade institucional, o que torna indispensável a adoção de práticas destinadas à proteção da autenticidade documental e à mitigação dos riscos cibernéticos decorrentes da manipulação inadequada de documentos eletrônicos.

A ausência de políticas eficientes de segurança da informação pode favorecer acessos indevidos, alterações não autorizadas, vazamento de dados e utilização fraudulenta de credenciais institucionais. Tais vulnerabilidades ampliam a exposição da administração pública a incidentes de segurança capazes de comprometer tanto a continuidade operacional quanto a proteção das informações institucionais.

O estudo desses mecanismos de controle e retroação encontra forte fundamentação na Cibernética, ciência interdisciplinar voltada aos sistemas de processamento de informações e regulação. Citando a perspectiva sistêmica clássica, Chiavenato (2004, p. 416-417) aponta que a Cibernética se configura como uma teoria dos sistemas de controle baseada na comunicação e na transferência de dados entre o sistema e o meio, operando por meio de mecanismos de retroação (*feedback*) para ajustar o funcionamento do todo em relação às demandas externas. Na gestão documental digital, o fluxo de validação serve como esse canal de retroação para corrigir desconformidades antes que afetem o ato final.

Diante desse cenário, torna-se evidente que a prevenção de falhas documentais depende da integração entre tecnologia, controles internos, capacitação dos agentes públicos e fortalecimento da cultura organizacional voltada à conformidade e à segurança da informação. A adoção de medidas preventivas contribui não apenas para a redução de riscos administrativos, mas também para o aprimoramento da governança pública e da eficiência institucional.

Portanto, garantir a autenticidade e a integridade dos documentos públicos ultrapassa a dimensão operacional, configurando-se como requisito essencial à segurança jurídica, à confiabilidade administrativa e à efetividade dos processos públicos.

CONSIDERAÇÕES FINAIS

A transformação digital promovida na administração pública proporcionou avanços na tramitação de processos, no acesso às informações e na modernização dos serviços institucionais. A adoção de documentos eletrônicos, assinaturas digitais e sistemas integrados contribuiu para maior agilidade administrativa, redução

de custos operacionais e aumento da eficiência na gestão pública. Entretanto, esse novo cenário também trouxe desafios relacionados à segurança da informação, autenticidade documental e conformidade administrativa.

Ao longo deste estudo, verificou-se que a integridade documental representa um elemento fundamental para a confiabilidade dos processos administrativos e para a preservação da segurança jurídica nas atividades desempenhadas pela administração pública. A autenticidade dos documentos não depende exclusivamente de recursos tecnológicos, mas também da existência de controles internos eficientes, políticas institucionais adequadas e conscientização dos agentes públicos quanto à relevância da proteção das informações institucionais.

Observou-se, ainda, que a cibersegurança passou a ocupar posição estratégica dentro da governança pública contemporânea, especialmente diante do aumento da circulação de documentos eletrônicos e da ampliação dos riscos cibernéticos. Nesse contexto, mecanismos como assinaturas eletrônicas, controle de acessos, rastreabilidade das operações e gestão de riscos tornam-se essenciais para a mitigação de vulnerabilidades e consolidação da conformidade organizacional.

Além dos aspectos tecnológicos, o estudo evidenciou que a cultura organizacional exerce influência na efetividade das práticas de segurança da informação e de conformidade administrativa. Verificou-se que a ausência de capacitação contínua, o desconhecimento dos procedimentos institucionais e a insuficiente conscientização dos servidores comprometem a integridade documental, aumentam a vulnerabilidade dos processos administrativos e favorecem a ocorrência de falhas operacionais.

Dessa forma, conclui-se que a proteção da autenticidade documental deve ser compreendida como responsabilidade

compartilhada entre tecnologia, gestão institucional e atuação humana. O fortalecimento dos controles internos, aliado ao investimento em capacitação e cultura de segurança, contribui para a construção de ambientes administrativos mais seguros, transparentes e eficientes.

Por fim, destaca-se que o desenvolvimento de práticas voltadas à conformidade e à integridade documental tende a fortalecer a governança pública e aprimorar a confiabilidade dos processos administrativos, tornando-se um fator para a contínua evolução responsável da administração pública contemporânea.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 27 dez. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm. Acesso em: 19 jul. 2026.

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

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. **Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos**. Brasília, DF: Presidência da República, 2020.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. **Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil**. Brasília, DF: Presidência da República, 2001.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 35. ed. São Paulo: Atlas, 2021.

CENTRO DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (CTIR GOV). **CTIR Gov em números**. Brasília, DF: CTIR Gov, 2026. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros>. Acesso em: 12 jun. 2026.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**: uma visão abrangente da moderna administração das organizações. 7. ed. rev. e atual. Rio de Janeiro: Elsevier, 2003.

CHIAVENATO, Idalberto. **Teoria Geral da Administração**. 7. ed. São Paulo: Campus, 2004.

GOVERNO DIGITAL. **Assinatura eletrônica**. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/assinatura-eletronica>. Acesso em: 13 jun. 2026.

HACKMAGEDDON. **Mega Invasões em 2026**. [S. l.]: Hackmageddon, Disponível em: <https://www.hackmageddon.com/category/security/cyber-attacks-statistics/>. Acesso em: 13 jun. 2026.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Validador de Assinaturas Eletrônicas**: cartilha de uso. Brasília, DF: ITI, 2026a. Disponível em: <https://validar.iti.gov.br/>. Acesso em: 8 jun. 2026.

TRIBUNAL DE CONTAS DA UNIÃO. **Lista de alto risco da Administração Pública federal**. 2. ed. Brasília: TCU, 2024. Disponível em: <https://sites.tcu.gov.br/listadealtorisco/index.html>. Acesso em: 19 jul. 2026.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial básico de gestão de riscos**. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018.

Lilian Gonçalves dos Santos

Bacharela em Administração, possui conhecimentos em Gestão de Projetos e Gestão de *compliance* e é pós-graduanda em Auditoria Empresarial. Atua na Administração Pública com experiência em gestão documental, auditoria, controles internos e *compliance*.

E-mail: lilian.goncalves88@gmail.com.