XI EDICIC Ibérico
FORMAÇÃO E INVESTIGAÇÃO EM CIÊNCIA DA INFORMAÇÃO
OPORTUNIDADES E DESAFIOS
10, 11 e 12 de novembro de 2025
POLITÉCNICO DO PORTO / ISCAP
PORTO - PORTUGAL

SIGILO E ÉTICA NA GESTÃO DE INFORMAÇÕES EM SAÚDE: A EXPERIÊNCIA DO NÚCLEO DE PERÍCIAS EM SAÚDE DO IF BAIANO

Marco Tulio Moreira de Souza, Instituto Federal Baiano, ORCID: https://orcid.org/0000-0003-1758-3639, Brasil, mtmsouza2@hotmail.com

José Carlos Sales dos Santos, Universidade Federal da Bahia, https://orcid.org/0000-0003-1758-3639 , Brasil, jsalles@ufba.br

Jaqueline Silva de Souza, Universidade Federal da Bahia , https://orcid.org/0000-0001-5743-780X , Brasil, jaquelinesou@gmail.com

Exo: Ética e Deontologia (inclusão, cidadania, direitos digitais e privacidade)

1 Introdução

O sigilo das informações de saúde constitui um dos pilares éticos fundamentais da prática profissional, especialmente no contexto das instituições públicas, onde o manejo de dados sensíveis de servidores envolve responsabilidades legais, morais, deontológicas e organizacionais. Informações relativas à condição física e mental de trabalhadores do serviço público são classificadas como dados sensíveis, cuja proteção é assegurada por marcos legais como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como por normas éticas, a exemplo do Código de Ética do Servidor Público Federal (Decreto nº 1.171/1994). No entanto, mais do que o cumprimento normativo, o tratamento dessas informações exige o fortalecimento de uma cultura institucional de confidencialidade, respeito à privacidade e compromisso com os direitos informacionais dos sujeitos (Batista, 2010).

A pandemia de COVID-19 deflagrou uma série de transformações nas práticas administrativas e tecnológicas das organizações públicas, exigindo respostas ágeis para assegurar a continuidade do funcionamento institucional em meio ao distanciamento físico. Esse contexto impôs desafios significativos à gestão de informações em saúde dos servidores, com a migração de processos físicos para plataformas digitais, ampliação do uso de sistemas remotos e reconfiguração de fluxos documentais envolvendo atestados, laudos e perícias médicas. A emergência sanitária evidenciou a tensão entre proteção de dados sensíveis e a necessidade de compartilhamento de informações entre órgãos públicos, sobretudo no uso secundário dos dados para controle e vigilância sanitária (Cristóvam, Bergamini & Hahn, 2021; Comitê Gestor da Internet no Brasil, 2021).

Este artigo se insere na interface entre a ética informacional, a gestão da informação em saúde e a cidadania informacional, articulando fundamentos da Ciência da Informação (CI) à experiência do Núcleo de Perícias em Saúde (NUPS) do Instituto Federal Baiano (IF Baiano), responsável pela tramitação e guarda de

dados sigilosos relacionados à saúde de servidores federais de diversos órgãos. A partir de 2020, o NUPS teve que reorganizar processos, adotar soluções tecnológicas e redefinir práticas de acesso e proteção às informações, afinando-se com as diretrizes da LGPD e os preceitos de governança informacional aplicáveis ao setor público. Nesse contexto, destaca-se a construção de um modelo de gestão orientado por princípios éticos e normativos, que se materializou na implantação de um prontuário eletrônico institucional e na criação de fluxos restritos de tramitação no Sistema Unificado de Administração Pública (SUAP), assegurando sigilo, rastreabilidade e controle de acesso aos documentos sensíveis.

A pesquisa adota uma abordagem qualitativa e reflexiva, ancorada na análise de conteúdo de Bardin (2011), para examinar registros administrativos, processos digitais e comunicações institucionais. Os resultados são organizados em três eixos analíticos — práticas informacionais, ética e proteção de dados — que revelam os avanços, desafios e sentidos atribuídos às transformações operadas. Como reforço metodológico e teórico, autores como Bardin (2011) e Belluzzo (2011) são mobilizados para discutir a informação como elemento estruturante da governança institucional.

Ao sistematizar essa experiência, o artigo contribui para o debate sobre cidadania informacional e proteção de dados no setor público, oferecendo subsídios para a formulação de políticas mais sensíveis à dignidade dos sujeitos e à realidade das instituições. As mudanças provocadas pelo contexto pandêmico evidenciaram lacunas históricas na infraestrutura e na capacitação dos servidores públicos para lidar com sistemas de informação sensíveis, ao mesmo tempo em que reforçaram a importância de princípios como responsabilidade, sigilo, confiabilidade e finalidade — pilares centrais da LGPD. Nesse cenário, as instituições públicas foram chamadas não apenas a cumprir a norma legal, mas a desenvolver competências institucionais voltadas à governança informacional ética e deontológica, com atenção à proteção dos sujeitos e à integridade dos sistemas. Isso implica alinhar procedimentos administrativos a princípios como o respeito à privacidade, à dignidade e ao sigilo profissional, conforme exigido tanto por marcos legais quanto pelos deveres morais e profissionais que regem o serviço público. O foco não está na produção de generalizações, mas na valorização de práticas concretas que colocam a ética e a deontologia informacional no centro das decisões administrativas e na mediação sensível dos fluxos informacionais em contextos de vulnerabilidade.

A experiência do NUPS/IF Baiano mostra que é possível construir soluções de baixo custo e alto impacto, baseadas em protocolos internos claros, diálogo intersetorial e uso criativo das plataformas já existentes na administração pública federal. A atuação do núcleo durante e após o período mais crítico da pandemia aponta para caminhos viáveis de inovação ética, nos quais a tecnologia é pensada como meio — e não fim — para garantir a confidencialidade e o respeito à dignidade informacional dos servidores públicos. Nesse sentido, o presente artigo oferece uma contribuição não apenas acadêmica, mas também prática, ao compartilhar uma experiência institucional que alia teoria e ação, articulando princípios da CI com os imperativos éticos e legais da gestão pública contemporânea.

2 Referencial Teórico

A ética, entendida em conjunto com a deontologia — isto é, o conjunto de deveres e normas que orientam condutas profissionais responsáveis (Jonas, 2006) —, bem como a proteção das informações sensíveis em saúde constituem pilares fundamentais para a construção da confiança, da cidadania informacional e da dignidade do sujeito no contexto do serviço público. A proteção da privacidade de dados sensíveis é discutida amplamente por autores como Castells (1999), que ressalta os desafios da sociedade em rede na manutenção da confidencialidade.

No campo da saúde, a Organização Mundial da Saúde (OMS) (2016) aponta a importância do sigilo como elemento essencial da confiança entre profissionais e usuários. No Brasil, a LGPD (Lei nº 13.709/2018) e o Código de Ética Médica (CFM, 2018) reforçam a obrigatoriedade da confidencialidade em todas as etapas de tratamento de dados pessoais.

A CI, enquanto campo interdisciplinar, dedica-se ao estudo dos processos de produção, organização, mediação, circulação, uso e preservação da informação em diferentes contextos sociais, científicos e institucionais. Segundo Le Coadic (1996), a CI busca compreender o ciclo informacional em sua totalidade, envolvendo os sujeitos, os suportes e os sistemas, sendo particularmente relevante quando se trata da gestão de informações sensíveis, como as relativas à saúde. Nesse sentido, a CI oferece ferramentas conceituais e metodológicas para analisar como o tratamento da informação afeta a vida dos sujeitos, especialmente em contextos de vulnerabilidade, como o adoecimento físico ou mental.

No âmbito da informação em saúde, a CI encontra um campo fértil para aplicação de seus conceitos centrais, pois lida diretamente com a circulação de dados sensíveis em ambientes institucionais. Como aponta Targino (2009), a informação em saúde deve ser tratada como um bem público, regulado por políticas específicas e alicerçado em princípios éticos e legais. Essa perspectiva dialoga com o conceito de cidadania informacional, proposto por Coutinho (2021), que defende o direito dos sujeitos à proteção de suas informações pessoais e ao controle sobre como esses dados são coletados, armazenados e utilizados por instituições públicas e privadas.

A ética, portanto, ocupa um lugar central na CI, especialmente em ambientes onde há assimetrias de poder entre os sujeitos que produzem, tratam e consomem dados. Capurro (2003) introduz a ideia de uma ética intercultural da informação, que reconhece os contextos socioculturais diversos nos quais as práticas informacionais ocorrem e propõe uma reflexão crítica sobre a responsabilidade dos agentes envolvidos na mediação informacional. Batista (2010), por sua vez, argumenta que a deontologia informacional deve ser entendida não apenas como um conjunto de normas técnicas, mas como uma prática reflexiva e ética que sustenta a confiança nas instituições e protege os sujeitos diante do tratamento de informações sensíveis.

A LGPD (Lei nº 13.709/2018) estabelece diretrizes fundamentais para o tratamento adequado de dados pessoais no Brasil, incluindo os dados sensíveis relacionados à saúde, que exigem proteção reforçada devido ao seu potencial de exposição e discriminação. Inspirada no General Data Protection Regulation (GDPR) da União Europeia (2016), a LGPD define princípios como a finalidade, necessidade, transparência e segurança, além de garantir direitos ao titular dos dados e impor obrigações às instituições públicas e privadas no trato dessas informações. No caso dos dados de saúde, a legislação prevê regras específicas para garantir o sigilo, o consentimento informado e a minimização do acesso, considerando que essas informações são frequentemente manipuladas por sistemas interinstitucionais, como no caso das perícias médicas no serviço público.

O serviço público federal brasileiro opera em um ambiente normativo complexo e cada vez mais exigente em termos de responsabilidade informacional. Por lidarem com volumes expressivos de dados sensíveis — relativos à saúde, à vida funcional, à identidade e à segurança dos cidadãos e servidores — as instituições públicas são obrigadas a adotar modelos de governança da informação que garantam não apenas eficiência administrativa, mas também segurança, transparência e respeito aos direitos fundamentais (Tarapanoff, 2001; Belluzzo, 2011).

A Constituição Federal de 1988, em seu artigo 5º, incisos X e XII, assegura a inviolabilidade da intimidade, da vida privada e das comunicações, estendendo essa proteção ao

tratamento de informações pessoais, inclusive em ambientes institucionais. No âmbito do serviço público, essa garantia ganha ainda mais relevância, uma vez que o Estado detém e manipula dados sensíveis de milhões de cidadãos e servidores. O princípio da legalidade administrativa, previsto no artigo 37 da mesma Constituição, reforça que todo tratamento de dados deve ser regido por normas específicas e fundamentado em interesse público, sem violar direitos individuais. Portanto, qualquer acesso, uso ou compartilhamento de informações, especialmente as relacionadas à saúde, exige respaldo legal e respeito ao sigilo.

A Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) regula o acesso a informações públicas, estabelecendo o dever da Administração Pública de garantir a transparência, mas também prevendo limites claros quanto ao acesso a dados classificados como sigilosos. O artigo 31 da LAI determina que informações pessoais relativas à intimidade, vida privada, honra e imagem devem ter seu acesso restrito por até cem anos, especialmente no caso de dados sensíveis como os de saúde. Já a Lei nº 8.112/1990, que rege o regime jurídico dos servidores públicos civis da União, estabelece em seu artigo 116, inciso IX, o dever do servidor de guardar sigilo sobre assuntos da repartição, inclusive após o desligamento do cargo. Tal obrigação reforça o caráter ético e jurídico do compromisso com a confidencialidade no trato da informação institucional.

No campo da saúde e das práticas profissionais, o Código de Ética Médica (Resolução CFM nº 2.217/2018) e o Código de Ética Profissional do Servidor Público (Decreto nº 1.171/1994) representam importantes instrumentos de deontologia. O primeiro, ao tratar das relações entre médicos, pacientes e instituições, determina em diversos artigos a obrigação de manter sigilo profissional sobre quaisquer dados obtidos no exercício da medicina, salvo por justa causa, dever legal ou autorização expressa do paciente. O segundo reafirma que o servidor deve manter discrição no manuseio de informações e agir com respeito à privacidade de colegas e usuários, além de proibir o uso da informação privilegiada para fins pessoais ou indevidos. Ambos os códigos se articulam com os princípios constitucionais da moralidade, da dignidade da pessoa humana e do interesse público.

A própria LGPD (Lei nº 13.709/2018), já mencionada, reforça e atualiza o tratamento ético e legal das informações no setor público, exigindo bases legais para coleta, tratamento e compartilhamento de dados, bem como a implementação de medidas técnicas e administrativas para proteger a privacidade dos titulares. Ela classifica dados de saúde como “dados sensíveis” e impõe regras mais rígidas para seu tratamento, sendo obrigatória a existência de protocolos de segurança, consentimento informado (exceto nos casos de cumprimento de obrigação legal ou execução de políticas públicas) e restrição de acesso apenas a pessoas autorizadas. O descumprimento dessas regras, conforme previsto na própria LGPD e na Lei nº 8.112/1990, pode acarretar responsabilizações disciplinares, civis e até penais, reforçando o compromisso do Estado com a proteção dos direitos informacionais dos cidadãos.

A governança da informação no setor público federal, especialmente em instituições como o Instituto Federal Baiano (IF Baiano), demanda um alinhamento efetivo entre a estrutura administrativa, os sistemas tecnológicos e os princípios éticos que regem o serviço público. Em contextos em que se lida com informações sensíveis — como dados de saúde, funcionais e pessoais de servidores —, torna-se fundamental adotar práticas responsáveis em todas as etapas do ciclo informacional: da coleta ao descarte. No IF Baiano, isso implica o fortalecimento de protocolos institucionais e a consolidação de uma cultura organizacional que valorize a confidencialidade, o cuidado e a integridade na gestão da informação. A proteção dos dados dos servidores, os sujeitos informcionais, portanto, não é apenas uma exigência normativa, mas uma condição para

a construção de relações institucionais pautadas na confiança, na legalidade e na dignidade (Oliveira & Freire, 2011; Ribeiro & Lima, 2021).

O IF Baiano é uma autarquia federal vinculada ao Ministério da Educação, com presença significativa em diversas regiões do interior da Bahia. Com a missão de promover educação pública, gratuita e de qualidade nos níveis médio, técnico e superior, a instituição tem se destacado pelo compromisso com o desenvolvimento regional e com a formação integral de seus estudantes. Conforme previsto no seu Plano de Desenvolvimento Institucional (PDI) 2021–2025, o IF Baiano tem priorizado a valorização das pessoas, com ações voltadas ao bem-estar biopsicossocial de servidores e discentes, à promoção da saúde mental e à construção de ambientes de trabalho pautados na ética, na escuta e no acolhimento. Essa diretriz estratégica revela um esforço institucional consistente para alinhar suas práticas administrativas aos princípios de cuidado, transparência e responsabilidade informacional no serviço público federal (IF Baiano, 2021).

O próprio PDI do IF Baiano 2021–2025 reconhece como um de seus compromissos estratégicos a necessidade de consolidar políticas institucionais voltadas ao bem-estar biopsicossocial dos servidores e estudantes, incluindo o aprimoramento da gestão das informações de saúde (IF Baiano, 2021). Entre suas diretrizes, o PDI destaca a importância da valorização das pessoas e do fortalecimento dos mecanismos de escuta, acolhimento e suporte psicossocial, o que demanda, necessariamente, uma governança da informação sensível pautada na ética, na segurança e no respeito aos direitos informacionais dos sujeitos envolvidos.

No âmbito da Diretoria de Gestão de Pessoas (DGP), a Coordenação de Atenção à Saúde e Qualidade de Vida (COASQ) é responsável por articular ações de promoção à saúde, acompanhamento de servidores adoecidos e suporte à gestão dos afastamentos por motivo de saúde física ou mental. A COASQ atua em consonância com diretrizes do Subsistema Integrado de Atenção à Saúde do Servidor (SIASS), e adota protocolos voltados à confidencialidade, como acesso restrito a sistemas, segmentação da informação e uso ético dos dados sensíveis.

Inserido na estrutura da COASQ, o Núcleo de Perícias em Saúde (NUPS) representa o setor técnico responsável pela organização e condução dos processos periciais que envolvem os servidores do IF Baiano e, por meio de cooperação técnica com outros órgãos, também atende servidores de inúmeros orgãos federais. O NUPS gerencia licenças para tratamento de saúde, perícias admissionais, readaptações, remoções por saúde, aposentadorias por invalidez, reavaliações funcionais, exames admissionais, dentre outros.

A atuação do NUPS exige não apenas conhecimento técnico-administrativo, mas também uma sólida formação ética-informacional. Conforme destaca Tarapanoff (2004), o tratamento da informação sensível no setor público deve estar fundado em valores como responsabilidade, justiça, equidade e empatia. A ética da informação concretiza-se nas decisões cotidianas dos profissionais que lidam com prontuários, laudos, pareceres e sistemas informatizados, sendo parte essencial da cidadania informacional.

O NUPS promove a mediação segura e eficaz entre servidores adoecidos, chefias, peritos e sistemas administrativos, assegurando que os fluxos informacionais estejam em conformidade com a legislação e os princípios éticos. Como ressaltam Freire e Prado (2012), essa mediação não é um mero canal técnico, mas um processo sociotécnico e ético que envolve escuta, empatia e responsabilidade institucional. A experiência do IF Baiano, por meio da COASQ e do NUPS, demonstra como a aplicação dos fundamentos da CI, aliados aos princípios éticos, ao sigilo profissional e à deontologia, pode fortalecer a governança informacional, garantir a proteção de dados sensíveis e promover a cidadania informacional no âmbito da administração pública.

3 Procedimentos Metodológicos

Trata-se de um estudo de natureza qualitativa, com abordagem descritiva, cujo método se baseia no relato de experiência institucional. Essa escolha metodológica visa documentar, refletir e sistematizar uma prática concreta ocorrida no âmbito do Núcleo de Perícias em Saúde (NUPS) do IF Baiano, entre os anos de 2020 e 2024. A produção dos dados foi realizada por meio de observação direta da rotina do setor, acompanhando de forma participativa os fluxos de trabalho, as dificuldades enfrentadas e as decisões administrativas adotadas ao longo do processo de adaptação tecnológica.

Durante esse acompanhamento, observou-se o uso cotidiano de sistemas como o SUAP (Sistema Unificado de Administração Pública), plataforma digital desenvolvida pelo Instituto Federal do Rio Grande do Norte (IFRN) e amplamente adotada por Institutos Federais, incluindo o IF Baiano. O SUAP integra funcionalidades administrativas, acadêmicas e de gestão de pessoas, funcionando como um ambiente institucional seguro para a tramitação de documentos oficiais, inclusive os de natureza sigilosa. Também foi identificado o uso de pastas digitais compartilhadas, acessíveis apenas pela equipe autorizada, como meio de armazenamento interno de documentos sensíveis, especialmente aqueles relacionados à saúde dos servidores.

A análise foi complementada por um levantamento documental envolvendo prontuários de saúde contendo atestados médicos, laudos periciais, relatórios assistenciais, receitas, exames e outros documentos clínico-administrativos. Foram examinados também processos individuais relacionados a licenças para tratamento de saúde, pedidos de remoção por motivo de saúde, solicitações de readaptação funcional e de concessão de horário especial. Além disso, foram considerados os registros de comunicações institucionais realizadas por e-mail entre os setores envolvidos, especialmente o NUPS, a COASQ e os servidores solicitantes. Essa variedade documental contribuiu para a triangulação das fontes, assegurando maior consistência na análise e favorecendo uma compreensão aprofundada das práticas informacionais e da gestão do sigilo no contexto institucional.

A interpretação dos dados considerou o impacto das medidas adotadas sobre três dimensões principais: eficiência administrativa, segurança da informação e conformidade ética e legal, com base nos referenciais da CI.

O estudo buscou compreender como a transição do suporte físico para o digital, impulsionada pela pandemia de COVID-19, afetou a proteção das informações sensíveis em saúde e exigiu novas práticas de mediação e governança informacional. A pandemia, ao restringir atividades presenciais, forçou a rápida digitalização dos fluxos de informação, desafiando os setores administrativos a implementarem soluções seguras e éticas para o tratamento de dados sensíveis, em conformidade com a LGPD.

A escolha pelo relato de experiência como estratégia metodológica se justifica pela necessidade de valorização dos saberes produzidos no interior das instituições públicas, especialmente aqueles que emergem da prática cotidiana e da resolução de problemas concretos. Como destaca André (1995), o relato de experiência é uma forma legítima de investigação, capaz de revelar saberes tácitos, decisões institucionais e aprendizados organizacionais que muitas vezes escapam aos métodos tradicionais de pesquisa.

A sistematização da experiência foi feita com base em um diário institucional de bordo mantido pelo autor durante sua atuação na chefia do NUPS, complementado por reuniões com colegas da área, revisão de normativas internas e análise crítica das legislações e comunicações oficiais. Tal abordagem permitiu não apenas reconstruir o percurso da transformação administrativa, mas também avaliar criticamente se os protocolos de sigilo aplicados na gestão das informações sensíveis estavam, de fato, alinhados às normas

deontológicas que regem o serviço público e a atuação em saúde.

A análise dos dados seguiu uma lógica de categorização temática, conforme proposto por Bardin (2011), que define a análise de conteúdo como um conjunto de técnicas sistemáticas e objetivas de descrição do conteúdo de mensagens, com vistas à interpretação de seus significados. No presente estudo, tal metodologia permitiu organizar o material empírico em três grandes eixos analíticos: práticas informacionais, ética e proteção de dados. Cada um desses eixos foi construído a partir da recorrência de temas identificados nos documentos institucionais, nos registros da experiência, nas interações entre os diversos setores envolvidos e na análise dos sistemas utilizados para a gestão informacional, como o SUAP e as pastas compartilhadas internas, que concentram dados sensíveis relacionados à saúde dos servidores.

O eixo das práticas informacionais compreendeu a análise dos fluxos de informação no interior da instituição, os modos de registro, circulação e arquivamento dos dados de saúde, bem como os canais de comunicação formal e informal estabelecidos entre o NUPS, a COASQ e os servidores atendidos e os demais setores administrativos. Nesse campo, buscou-se compreender como as práticas se ajustaram (ou não) às novas exigências tecnológicas e legais impostas pela LGPD, e como a cultura institucional influenciou o modo como essas práticas foram adotadas.

No eixo da ética, a análise recaiu sobre os dilemas enfrentados pelos profissionais envolvidos na gestão das informações de saúde, especialmente nos momentos em que se estabeleciam tensões entre o cumprimento de normas administrativas e o respeito à privacidade e à dignidade dos servidores adoecidos. Foram examinadas as decisões que demandaram julgamento ético, como o controle de acesso a sistemas, o compartilhamento restrito de informações com chefias, ou a mediação de conflitos relacionados à exposição indevida de dados sensíveis.

O eixo da proteção de dados permitiu identificar as medidas implementadas para garantir a segurança da informação, tais como a transição para formulários digitais com controle de permissões, o uso de sistemas com autenticação e o desenvolvimento de procedimentos para tramitação sigilosa de documentos. Essa dimensão também envolveu a análise das dificuldades enfrentadas, como a ausência de sistemas integrados, as limitações tecnológicas e a necessidade de capacitação dos servidores para lidar com ferramentas digitais alinhadas às exigências da LGPD.

Do ponto de vista metodológico, este estudo adota uma postura reflexiva e implicada, considerando a posição do pesquisador como sujeito participante da experiência institucional analisada. Tal posicionamento não compromete a objetividade da pesquisa; ao contrário, favorece uma análise crítica e engajada, que leva em conta os dilemas vivenciados na gestão de informações sensíveis. O foco do estudo não está na produção de generalizações estatísticas, mas na compreensão de processos, na identificação de boas práticas e na problematização de desafios enfrentados na busca pelo equilíbrio entre eficiência administrativa e respeito à privacidade dos servidores. Por tratar-se de uma análise de documentos administrativos e da descrição de processos institucionais, sem coleta de dados pessoais de terceiros nem aplicação de instrumentos com seres humanos, a pesquisa não demandou submissão ao Comitê de Ética em Pesquisa, conforme as diretrizes do Conselho Nacional de Saúde (CNS) para estudos institucionais de caráter não clínico.

A abordagem qualitativa adotada neste estudo permitiu revelar aspectos subjetivos e institucionais das decisões administrativas, como conflitos entre setores, silêncios organizacionais e ajustes informais que garantiram a continuidade do serviço em contextos desafiadores. Ao articular vivência prática e reflexão teórica, a metodologia

transcende a mera descrição burocrática e busca compreender os sentidos éticos, informacionais e institucionais envolvidos nas práticas de sigilo no serviço público. Com isso, pretende-se contribuir para o campo da CI e para a construção de políticas públicas mais sensíveis à proteção dos sujeitos informacionais.

4 Resultados Parciais ou Finais

A análise dos dados seguiu os princípios da análise de conteúdo propostos por Bardin (2011), que orienta a investigação qualitativa por meio de um processo sistemático de categorização temática. A escolha metodológica por esse modelo permitiu organizar a interpretação dos documentos institucionais e dos registros da experiência em três eixos analíticos principais: práticas informacionais, ética e proteção de dados. Esses eixos orientaram tanto a leitura crítica do material quanto a estruturação dos resultados obtidos.

No eixo das práticas informacionais, os dados revelaram uma transformação significativa nos fluxos de informação relacionados à saúde dos servidores. A implementação do prontuário eletrônico institucional e a criação de um fluxo digital específico no SUAP evidenciam a mudança da cultura documental baseada no papel para uma lógica de mediação tecnológica. As práticas passaram a ser orientadas por critérios de rastreabilidade, controle de acesso e padronização dos registros, permitindo não apenas maior segurança, mas também maior eficiência na tramitação dos processos sensíveis.

Nesse novo modelo, os documentos de saúde — como atestados médicos, relatórios clínicos e exames — são protocolados diretamente pelo servidor no SUAP, com o nível de acesso configurado como restrito e com a justificativa legal de informação pessoal, conforme a Lei de Acesso à Informação (Lei nº 12.527/2011) e a LGPD (Lei nº 13.709/2018). Após o envio, esses processos são direcionados exclusivamente ao setor RET-NUPS, onde passam a ser tratados apenas pela equipe técnica autorizada, com acesso limitado e sob o compromisso legal e deontológico de sigilo. A tramitação se encerra nesse ponto, sendo vedado o redirecionamento a outros setores, e as eventuais comunicações com os servidores são feitas exclusivamente por e-mail ou, em situações específicas, via WhatsApp institucional. Essa prática reforça o compromisso com a proteção dos dados sensíveis e a construção de uma governança informacional alinhada à ética, à legislação e à cidadania digital.

No eixo da ética, a análise permitiu identificar como a equipe da COASQ lida com dilemas recorrentes relacionados à exposição de dados sensíveis, à mediação entre chefias e servidores adoecidos, e à definição de limites institucionais para acesso à informação. A adoção de restrições formais no sistema SUAP, com definição de níveis de acesso e registro da hipótese legal “informação pessoal” nos processos de saúde, é um dos mecanismos que demonstram a incorporação prática de princípios da ética informacional, como o respeito à privacidade, à dignidade dos sujeitos e à não exposição indevida.

Uma das estratégias adotadas pela equipe do NUPS para garantir o sigilo das informações sensíveis foi a criação de uma pasta digital compartilhada e criptografada, hospedada em ambiente institucional seguro, destinada ao armazenamento dos prontuários de saúde dos servidores. Essa pasta reúne documentos altamente sensíveis — como atestados, laudos médicos, relatórios de saúde e comunicações periciais — e possui acesso controlado exclusivamente pela equipe autorizada do NUPS, sendo vedado o acesso por quaisquer outros setores da instituição. A existência dessa estrutura de armazenamento restrito reforça a cultura organizacional de proteção à privacidade e expressa, de forma concreta, o compromisso ético com o sigilo profissional e a confidencialidade dos dados de saúde.

Esse arranjo técnico-operacional, que inclui tanto as restrições no SUAP quanto o uso criterioso da pasta compartilhada, é resultado da construção de uma governança informacional baseada na confiança, no

cumprimento da legislação e na valorização da ética como princípio estruturante da atuação institucional no campo da saúde do servidor público.

Além disso, a equipe envolvida na gestão da saúde dos servidores realiza estudos sistemáticos da legislação aplicável — como a LGPD, o Código de Ética Médica, a Lei nº 8.112/1990, entre outras —, o que proporciona embasamento técnico e normativo às decisões tomadas no dia a dia. A atuação conjunta de peritos, equipe administrativa e profissionais da equipe multidisciplinar (como psicólogos e assistentes sociais) cria um ambiente de constante troca, que favorece decisões éticas, integradas e humanas.

Finalmente, o eixo da proteção de dados foi central para os resultados obtidos. A adoção de sistemas em nuvem com controle de permissões, a criação de registros auditáveis de acesso e a transição para plataformas compatíveis com a LGPD revelam um esforço institucional para atender às exigências legais sem comprometer a fluidez da gestão administrativa. A categorização dos documentos sensíveis e a limitação de sua visibilidade apenas a agentes autorizados demonstram a aplicação concreta dos dispositivos legais à realidade institucional do IF Baiano.

A articulação entre os eixos analíticos de Bardin e os resultados alcançados permitiu não apenas sistematizar os avanços administrativos, mas também compreender os sentidos atribuídos a essas mudanças pelos agentes envolvidos. Os achados mostram que a análise de conteúdo, quando aplicada em uma perspectiva crítica e situada, é capaz de iluminar tensões, aprendizagens e transformações organizacionais que transcendem a dimensão técnica e revelam o papel da informação como eixo estruturante da ética e da governança institucional. Como destaca Bardin (2011), o valor da análise está em sua capacidade de captar as significações latentes nos discursos.

Dentre os principais resultados obtidos com a experiência institucional conduzida pelo NUPS do IF Baiano, destaca-se a criação de um prontuário eletrônico institucional, desenvolvido com base em critérios de segurança, confidencialidade e rastreabilidade. Esse prontuário passou a ser armazenado em ambiente de nuvem institucional, com acesso rigorosamente restrito à equipe da COASQ. A digitalização dos documentos sensíveis, como atestados, laudos e pareceres médicos, permitiu a superação de práticas anteriormente baseadas em arquivos físicos, mais vulneráveis a extravios e acessos indevidos.

A implantação do prontuário eletrônico foi acompanhada da revisão dos fluxos administrativos internos, com a definição de novos protocolos para coleta, envio, armazenamento e exclusão de documentos. Todos os acessos aos prontuários passaram a ser registrados, reforçando a responsabilização dos usuários do sistema. Essa medida também facilitou o atendimento remoto de servidores lotados em diferentes campi, sem comprometer a integridade das informações, aspecto essencial diante das restrições impostas pela pandemia de COVID-19. Após o recebimento e análise dos documentos, os processos de saúde são finalizados ou arquivados diretamente no setor RET-NUPS, sem qualquer tramitação interna posterior. Essa decisão institucional visa restringir ao máximo a circulação de informações sensíveis e reforça o compromisso com o sigilo e a proteção dos dados pessoais.

Outro resultado relevante foi a criação de um fluxo específico de processos sensíveis dentro da plataforma SUAP. Por meio de customizações realizadas em parceria com a Diretoria de Tecnologia da Informação (DGTI), os processos relativos à saúde (como licenças, readaptações, remoções e aposentadorias por invalidez) passaram a ser classificados com grau de acesso restrito, visível apenas ao servidor interessado, à equipe técnica do NUPS e, quando necessário, a peritos autorizados.

Esse recurso eliminou um dos principais problemas identificados no diagnóstico inicial: o acesso não autorizado de setores administrativos a processos que continham dados médicos sigilosos. Antes da adoção dessa medida, documentos como atestados eram, por vezes, visíveis a servidores que não tinham qualquer vínculo com a área de saúde ou com o processo em questão, o que feria princípios legais e éticos fundamentais. Com a nova configuração, foi possível assegurar o princípio da minimização de dados, conforme previsto na LGPD.

Além dos ganhos em termos de segurança e conformidade legal, a iniciativa também promoveu mudanças culturais dentro da instituição, fortalecendo uma ética informacional mais sensível à proteção de dados pessoais. A delimitação clara de competências, o uso de ferramentas digitais seguras e a promoção de treinamentos internos contribuíram para ampliar a consciência dos servidores sobre a importância da confidencialidade no trato das informações em saúde.

O modelo adotado pelo NUPS também evidenciou a possibilidade de compatibilizar transparência institucional e sigilo, ao garantir que o servidor possa acompanhar seus próprios processos com clareza, sem que isso comprometa o sigilo dos dados perante terceiros. Tal equilíbrio é essencial para a construção de relações de confiança entre servidores e a administração pública, bem como para o fortalecimento da cidadania informacional.

A análise dos registros revelou contradições institucionais importantes, como a convivência entre práticas digitais e analógicas, a ausência de normativas claras e as adaptações informais adotadas para garantir a continuidade dos serviços. Tais elementos evidenciam os sentidos atribuídos à informação em saúde no IF Baiano e os limites entre a norma e a prática. Ao sistematizar erros, acertos e ajustes, a pesquisa contribui para a produção de aprendizados institucionais e oferece subsídios para o aprimoramento de políticas públicas informacionais mais aderentes à realidade do serviço público.

Os resultados alcançados apontam para a viabilidade da replicação dessa experiência em outras instituições públicas, especialmente aquelas que enfrentam desafios semelhantes no que diz respeito ao tratamento de informações em saúde. A experiência do IF Baiano demonstra que é possível alinhar práticas administrativas eficientes à proteção dos direitos fundamentais dos servidores, reforçando o papel da CI como campo estratégico para a governança ética da informação no setor público.

5 Considerações Parciais

A experiência do NUPS do IF Baiano revela que é possível conciliar inovação tecnológica com os princípios éticos, legais e informacionais que regem o tratamento de dados sensíveis no serviço público. A adoção de práticas baseadas na ética da informação, no respeito à privacidade dos servidores e na conformidade com a LGPD permitiu transformar rotinas administrativas e elevar o padrão institucional de segurança informacional, sem comprometer a eficiência da gestão.

Os resultados obtidos demonstram que soluções, como o prontuário eletrônico institucional, o controle de acesso a processos no SUAP e a rastreabilidade das ações administrativas não apenas protegem os sujeitos informacionais, mas também promovem uma nova cultura de responsabilidade na administração pública. Trata-se de um avanço que, embora impulsionado pelas exigências da pandemia, consolida uma mudança estrutural no modo como se compreende e se gerencia a informação em saúde no contexto institucional.

Como recomendações para pesquisas futuras, propõe-se a digitalização integral dos acervos físicos ainda existentes, com definição de protocolos claros de arquivamento. Além disso, é fundamental investir na capacitação continuada dos servidores, especialmente nas

áreas de ética, sigilo profissional e legislação informacional. A incorporação desses temas na formação institucional contribui para o desenvolvimento de uma cultura de vigilância ética e empatia no trato das informações sensíveis.

Outro aspecto relevante é a necessidade de consolidação de políticas institucionais de cidadania digital, alinhadas às diretrizes da CI, que garantam aos servidores a consciência de seus direitos como titulares de dados, bem como o acesso transparente aos canais de informação e aos mecanismos de controle sobre o tratamento de seus dados pessoais. No entanto, tais políticas só alcançarão efetividade plena se forem acompanhadas de um esforço mais amplo de fortalecimento da cultura organizacional voltada à proteção da privacidade, o que requer lideranças comprometidas, incentivos institucionais e participação ativa dos servidores. A construção de um ambiente informacional ético não pode ser imposta exclusivamente por normas, mas deve ser cultivada como um valor partilhado no cotidiano institucional, fortalecendo a noção de confiança mútua entre os sujeitos e as instituições públicas.

Os aprendizados gerados pela atuação do NUPS demonstram que a ética da informação no serviço público não se reduz ao cumprimento formal de normas legais. Trata-se de uma prática política e pedagógica que reafirma o valor da dignidade humana e a centralidade dos sujeitos na governança da informação. Promover a proteção dos dados em saúde é, acima de tudo, promover os direitos digitais, a cidadania informacional e a confiança nos serviços públicos em um cenário de crescente sensibilidade e complexidade das informações.

6 Referências

Batista, C. L. (2010). Informação pública: uma questão de acesso, de direito e de apropriação social. Revista da Escola de Comunicação, 10(1), 1–20.

Belluzzo, R. C. B. (2011). Gestão da informação e do conhecimento nas organizações contemporâneas. São Paulo: Saraiva.

Brasil. (1994). Decreto nº 1.171, de 22 de junho de 1994. Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal. Diário Oficial da União, Brasília, DF, 23 jun. 1994. http://www.planalto.gov.br/ccivil_03/decreto/D1171.htm

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Capurro, R. (2003). Ética intercultural da informação. Ciência da Informação, 32(3), 9–15.

Castells, M. (1999). A sociedade em rede (Vol. 1). São Paulo: Paz e Terra.

Comitê Gestor da Internet no Brasil (2021). Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia (Panorama Setorial da Internet, n. 4). Comitê Gestor da Internet no Brasil. https://cetic.br/pt/publicacao/limites-e-possibilidades-para-o-uso-secundario-de-dados-pessoais-no-poder-publico/

Conselho Federal de Medicina – CFM. (2018). Código de Ética Médica: Resolução CFM nº 2.217/2018. https://portal.cfm.org.br

Coutinho, D. (2021). Proteção de dados e cidadania digital: desafios da informação sensível no setor público. Brasília: IBICT.

Cristóvam, J. S. da S., Bergamini, J. C. L., & Hahn, T. M. (2021). Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). Interesse Público – IP, 23(129), 75–101.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, Brussels, 2016. Disponível em: https://eur-

lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 18 jul. 2025.

Freire, I. & Prado, D. G. (2012). Mediação da informação e ética: uma análise das práticas de atuação em bibliotecas universitárias. Perspectivas em Ciência da Informação, 17(3), 22–41. https://doi.org/10.1590/S1413-99362012000300003

Le Coadic, Y. F. (1996). A ciência da informação. Brasília: Briquet de Lemos.

Oliveira, E. F. T., & Freire, I. (2011). Governança da informação e cultura organizacional: contribuições da Ciência da Informação. Transinformação, 23(2), 139–148. https://doi.org/10.1590/S0103-37862011000200002

Organização Mundial da Saúde – OMS. (2016). Framework on integrated, people-centred health services. https://apps.who.int/iris/handle/10665/252698

Ribeiro, F. R., & Lima, G. A. S. (2021). Cultura informacional e proteção de dados no serviço público. Revista Informação & Sociedade, 31(2), 75–91. https://doi.org/10.22478/ufpb.1809-4783.2021v31n2.51091

Tarapanoff, K. (2001). Responsabilidade ética e informação. Ciência da Informação, 30(2), 23–29. https://doi.org/10.18225/CI.INF.V30I2.128.

Tarapanoff, K. (2004). Inteligência organizacional e competitiva: Informação e conhecimento nas organizações. Brasília: Editora Universidade de Brasília.

Targino, M. das G. (2009). Políticas públicas de informação em saúde: informação como bem público. Perspectivas em Ciência da Informação, 14(2), 18–36. https://doi.org/10.1590/S1413-99362009000200003.