Casi 17ª Edição
Congresso de Administração, Sociedade e Inovação

Artigo completo
De 03 a 05 de dezembro de 2025

Governança de Dados e Proteção de Dados: Análise das Seções de Ensino da UFMG.

Isla Marinho Parreiras[1], Samara Martins Araújo Mendes[2], Luís Fernando Silva Andrade[3], Cledinaldo Aparecido Dias[4].

Resumo: A crescente digitalização dos processos acadêmicos trouxe desafios significativos para a proteção de dados pessoais em instituições públicas de ensino superior. Nesse cenário, a Lei Geral de Proteção de Dados Pessoais (LGPD) surge como marco regulatório essencial, exigindo adequações institucionais e revisão das práticas de tratamento de informações. Este estudo tem como objetivo avaliar a conformidade das atividades realizadas pelas Seções de Ensino de sete unidades acadêmicas da Universidade Federal de Minas Gerais (UFMG) em relação aos princípios da LGPD. Para tanto, foi conduzido um estudo de caso de abordagem qualitativa, que combinou análise documental com entrevistas semiestruturadas aplicadas a servidores responsáveis pela gestão acadêmica. Os resultados indicam conformidade parcial: princípios como Finalidade e Adequação foram respeitados, mas fragilidades importantes foram constatadas em Transparência, Segurança e Responsabilização, especialmente pela ausência de diretrizes institucionais claras, pela falta de padronização de processos e pela carência de capacitação formal. Conclui-se que o fortalecimento da governança de dados e a implementação de protocolos uniformes podem ampliar a proteção das informações e assegurar maior alinhamento à legislação, promovendo confiança e segurança no ambiente acadêmico.

Palavras-Chave: governança de dados; lei geral de proteção de gados; LGPD; universidade; proteção de dados pessoais.

[1] Mestranda em Administração Pública (PROFIAP) – Universidade Federal de Minas Gerais (UFMG). E-mail: isla.parreiras@gmail.com
[2] Mestranda em Administração Pública (PROFIAP) – Universidade Federal de Minas Gerais (UFMG). E-mail: samara.martins@gmail.com
[3] Universidade Federal de Minas Gerais (UFMG). ORCID: https://orcid.org/0000-0001-9963-2048. E-mail: andradelfs@gmail.com
[4]Universidade Estadual de Montes Claros (UNIMONTES); Universidade Federal de Minas Gerais (UFMG). ORCID: https://orcid.org/0000-0002-7707-9664. E-mail: cledinaldo.dias@unimontes.br

1. Introdução

As transformações da vida social diante do avanço tecnológico e da digitalização de dados mostram que, como apresentado por Doneda (2021), na chamada Sociedade da Informação, a circulação de informações pessoais se intensifica, tornando a privacidade um valor essencial e, ao mesmo tempo, vulnerável. A noção de pessoa, mediada por registros, bancos de dados e sistemas de informação, transita entre acessos, oportunidades e formas de reconhecimento social. Nesse interim, o indivíduo não é visto apenas como sujeito físico, mas também como conjunto de dados processados e compartilhados.

Os riscos advindos dessa realidade demandam um desdobramento jurídico que possa garantir a autonomia, a dignidade e os direitos fundamentais do cidadão. A privacidade, antes entendida como direito à intimidade, precisa ser redefinida em face da coleta massiva de informações, assumindo uma dimensão coletiva e dinâmica (Doneda, 2021).

A promulgação da Lei Nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), cuja finalidade é dispor sobre o tratamento de dados pessoais, em suportes físicos e digitais (Brasil, 2018), trouxe à tona a preocupação com a coleta massiva, o processamento e uso indiscriminado de informações pessoais por organizações públicas e privadas. Como atesta Reis et al. (2024), a lei emergiu em resposta ao crescimento exponencial na coleta e compartilhamento de informações na era digital, onde os riscos de violações à privacidade se tornaram mais evidentes.

Se antes a Constituição Federal já assegurava que "[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas" (Brasil, 1988, cap. I, art. 5°, inc. X), a publicação da lei reforçou a necessidade de que entidades públicas e privadas adotarem medidas voltadas à proteção da privacidade e à promoção de práticas éticas no uso de dados. A LGPD visa estabelecer princípios fundamentais que orientem a coleta e o tratamento de dados, priorizando transparência, finalidade e necessidade, ao mesmo tempo em que busca equilibrar o avanço tecnológico com a garantia de direitos fundamentais (Reis et al., 2024).

Entretanto, a aplicação da lei representa um desafio significativo para as instituições públicas demandando um sistema de governança que garanta os objetivos propostos pela legislação. Como afirma Vouri (2024), uma política de governança de dados define instrumentos e procedimentos voltados para solucionar, de forma eficaz, questões ligadas ao uso de dados, levando em conta as demandas dos diferentes atores envolvidos.

No setor educacional, com a digitalização dos processos (Brasil, 2022) e a coleta de dados sensíveis sobre alunos, professores e servidores, as instituições enfrentam a tarefa de equilibrar o uso eficiente das informações com a proteção dos direitos fundamentais de privacidade e a garantia de transparência.

Nesse contexto, a questão norteadora do presente estudo é: como a proteção de dados vem sendo implementada em uma Universidade pública? Para tanto, definiu-se como objetivo avaliar a conformidade das atividades realizadas pelas seções de ensino de sete unidades

acadêmicas da Universidade Federal de Minas Gerais (UFMG) em relação aos princípios da LGPD.

Institucionalmente, em conjunto, as sete seções de ensino selecionadas comportam 45 dos 91 cursos de graduação ofertados pela universidade (UFMG, 2021). Essas seções são responsáveis por registros da vida acadêmica dos estudantes, abrangendo atividades como lançamento de trancamentos de matrícula, aproveitamentos de estudos e atividades complementares, além da emissão de documentos acadêmicos e administrativos, como atestados, históricos escolares e diplomas. Esses setores também gerenciam processos de transferência, inscrição para colação de grau e matrículas em disciplinas isoladas, bem como a guarda e conservação de dados e documentos acadêmicos (UFMG, 2015, 2022). Tais responsabilidades tornam essas unidades fundamentais na gestão das informações dos estudantes, exigindo atenção rigorosa aos princípios estabelecidos pela LGPD.

Os registros lotados nesses setores inscrevem uma ampla variedade de dados pessoais e sensíveis de estudantes, incluindo informações de identificação, dados de contato, documentos oficiais, histórico escolar prévio, declaração étnico-racial, renda, estado de saúde (quando atestados médicos são anexados ao sistema), situações particulares de Pessoas com Deficiência (PCD), frequências em sala de aula, atividades extracurriculares, entre outras informações de cunho estritamente pessoal. Esses dados, por sua natureza, estão diretamente relacionados a elementos conceituais tratados na LGPD, que estabelece critérios rigorosos para o tratamento e a proteção de informações pessoais de indivíduos identificáveis.

Considerando o escopo das informações acessadas pelas Seções de Ensino, cuja divulgação não autorizada pode configurar violação à privacidade e ao sigilo de dados pessoais (Brasil, 2018), este estudo tende a trazer reflexões quanto a obrigatoriedade de as Universidades públicas atenderem os princípios da LGPD, sem contrariar o fluxo das informações necessárias para o seu funcionamento. A levantar essas reflexões a análise desperta para a adoção de boas práticas de gestão das informações pessoais, expõe as fragilidades e lacunas institucionais, além de propor medidas que assegurem maior alinhamento com a legislação, contribuindo para uma governança de dados mais segura, ética e legal no contexto acadêmico.

2. Governança de dados e a LGPD: reflexões necessárias.

Segundo o Data Governance Institute (2014), a governança de dados é o exercício da tomada de decisões e autoridade baseadas em dados. Pode ser compreendida como um sistema que estabelece direitos e responsabilidades nos processos relacionados a informações, no qual modelos e frameworks estabelecem os papéis e ações que podem ser executados com elas.

A proteção de dados pessoais vem sendo reconhecida como um direito fundamental autônomo, distinto, relacionado à privacidade e à intimidade dos sujeitos (Brasil, 2022). Sá e Vital (2024) destacam que, os dados pessoais, bem como as informações que deles se extraem, tornaram-se recursos econômicos essenciais na sociedade contemporânea, frequentemente comparados ao petróleo em termos de seu impacto econômico e estratégico. O tratamento de dados pode ser

então compreendido como uma atividade de risco, já que, ao permitir vigilância, monitoramento e classificação de indivíduo, reorganiza relações de poder (Doneda, 2021).

O Supremo Tribunal Federal (STF), em julgamento da Ação Direta de Inconstitucionalidade (ADI) 6387, reforçou essa compreensão ao reconhecer a proteção de dados como direito fundamental implícito (Brasil, STF, 2020), posição consolidada pela Emenda Constitucional nº 115/2022, que incluiu formalmente a proteção de dados pessoais no rol de direitos fundamentais.

Com a evolução das tecnologias de informação e comunicação o volume de informações pessoais e empresariais que circulam pelas redes tem crescido exponencialmente, o que reflete uma nova dinâmica no mercado global (Agune; Carlos, 2005). De acordo com Reis et al. (2024), a era digital trouxe consigo uma explosão na coleta, processamento e compartilhamento de dados, fenômeno associado ao uso de *big data* e inteligência artificial, o que amplia os riscos relacionados à privacidade.

Segundo Dahl (2001), o capitalismo de mercado pode tanto favorecer quanto prejudicar a democracia. Embora coordene e controle decisões econômicas por meio de sua lógica competitiva e de direitos de propriedade, o autor argumenta que sua eficácia democrática não é autossuficiente. A dependência de legislações, políticas públicas e ações governamentais para regular a competitividade e evitar monopólios demonstra que, sem intervenção, o sistema de mercado pode gerar danos sociais significativos. Nesses casos, a exigência por ações governamentais torna-se inevitável, sublinhando que a democracia não pode progredir sem a devida regulamentação do capitalismo.

Para Agune e Carlos (2005), com a revolução tecnológica, sobretudo, o paradigma da sociedade do conhecimento e a globalização, o Estado precisou se reinventar migrando para um Estado mais horizontal, colaborativo, flexível e inovador, adotando uma estrutura que estivesse em sintonia com as demandas e características dessa nova era.

Diante desse cenário, Viana (2016) destaca que os modelos tradicionais de governo eletrônico se tornaram insuficientes, dando lugar ao governo digital, que vai além da simples automação e passa a valorizar a cocriação com cidadãos e empresas, sinalizando uma nova era de políticas públicas baseadas em tecnologia avançada. Essa transição de governo eletrônico para governo digital, vai além da digitalização: adota princípios como governo aberto, digital por padrão, abertura de dados e segurança digital, envolvendo cidadãos como co-construtores de serviços, fortalecendo, consequentemente, a confiança nas relações (OCDE, 2016; Viana, 2021).

O governo aberto introduz inovações importantes ao priorizar a eficiência, a transparência, o controle social e, sobretudo, a participação cidadã como pilares centrais da gestão pública. Essa abordagem representa uma mudança de valores, deslocando o foco da administração para o cidadão como protagonista do processo (Viana, 2021).

No Brasil, a Lei de Acesso à Informação (LAI), Lei nº 12.527/2011**,** marcou um avanço no fortalecimento da transparência pública, *accountability*, participação social e conformidade das

informações e dados tratados na esfera pública (Angélico, 2012). A LAI foi promulgada em 2011 com o objetivo de assegurar o acesso à informação dos órgãos do governo aos cidadãos (Brasil, 2011).

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, em vigor desde 2020, ampliou esse quadro normativo ao estabelecer bases legais para o tratamento de dados pessoais e criar a Autoridade Nacional de Proteção de Dados (ANPD), responsável por orientar, fiscalizar e aplicar sanções. A LGPD aplica-se tanto ao setor privado quanto ao público, abrangendo qualquer operação que seja realizada ou coletada no Brasil, ou tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território nacional (Brasil, 2018).

Além dos requisitos para tratamento de dados, a lei determina que as instituições observem a boa fé e o cumprimento de dez princípios norteadores, apresentados na Tabela 1 (Brasil, 2018). Esses princípios não apenas estabelecem limites jurídicos, mas também impõem padrões de governança pública, aproximando a gestão de dados da lógica de prestação de contas e de garantia de direitos.

Tabela 1. Princípios LGPD.

Princípios	**Descrição**
Finalidade	Propósitos legítimos, específicos, explícitos e informados ao titular.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular
Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades;
Livre Acesso	Garantia de acesso gratuito e integralidade dos dados.
Qualidade dos Dados	Garantia de dados exatos, atualizados e relevantes.
Transparência	Garantia de informações claras e facilmente acessíveis.
Segurança	Medidas técnicas e administrativas aptas a proteger os dados pessoais
Prevenção	Medidas para prevenir a ocorrência de danos
Não Discriminação	Impossibilidade de tratamento para fins discriminatórios ilícitos ou abusivos;
Responsabilização e prestação de contas	Demonstração medidas eficazes e capazes de comprovar a proteção de dados pessoais

Fonte: adaptado de Brasil (2018).

No caso das Instituições de Ensino Superior (IES), os desafios são complexos devido à pluralidade de titulares de dados — candidatos, alunos, responsáveis, professores, egressos e pacientes em hospitais-escola — e à natureza sensível de muitos dos dados que são tratados. A literatura aponta que as IES adotem modelos de categorização de titulares, com regimes diferenciados de proteção segundo o vínculo institucional, facilitando a definição de bases legais, prazos de retenção e mecanismos de anonimização (Reis et al., 2024).

Para suprimir as deficiências apresentadas no contexto da evolução tecnológica e digital, versos a necessidade da privacidade que deve ser garantida a todo cidadão, a governança de dados

apresenta-se como um instrumento potencial para assegurar a "melhoria na valoração e produção dos dados, monitoração de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de compliance, associadas a eles" (Barbieri, 2019, p. 36).

Nesse sentido, os dados deixam de ser considerados apenas elementos técnicos ou tecnológicos e passam a assumir o papel de ativos organizacionais estratégicos, inseridos em processos de transformação digital e monetização. A análise da governança deve, portanto, contemplar todo o ciclo de vida dos dados, sua origem, armazenamento, compartilhamento e adequação às normas legais, especialmente à Lei Geral de Proteção de Dados (LGPD). A integração entre qualidade, metadados, ciclo de vida e gestão de riscos fortalece a governança e contribui para um ambiente de maior confiança no uso dos dados.

Na perspectiva de Rêgo (2013), a governança de dados é também um exercício de autoridade, que deve ser conduzido a partir da alta administração e se estender a todas as áreas da organização. Ela estabelece papéis e responsabilidades, define processos e cria mecanismos de controle para assegurar que os dados sejam tratados de forma coerente com os objetivos institucionais. Além de garantir eficiência operacional, a governança de dados fortalece a conformidade legal e promove maior alinhamento estratégico com a missão da instituição.

3. Método de pesquisa

Esta pesquisa é um estudo de caso sobre as Seções de Ensino de sete unidades da Universidade Federal de Minas Gerais (UFMG), em Belo Horizonte. Esses setores constituem unidades administrativas que apoiam a graduação, atuando na guarda e conservação de registros acadêmicos, na emissão de documentos oficiais e no atendimento a estudantes e ao público externo (UFMG, 2025b; 2025d). Também são responsáveis por procedimentos de matrícula, atualizações cadastrais e organização de colações de grau (UFMG, 2025c; 2025e).

Iniciou-se o trabalho a partir de uma pesquisa documental para identificar as legislações e resoluções pertinentes, no âmbito federal e nas políticas internas da UFMG, especialmente a Política de Proteção de Dados Pessoais, a Política de Acesso à Informação e à Política de Segurança da Informação da UFMG, buscando situar o objeto investigado dentro do seu quadro institucional e normativo (Creswell; 2007).

Na sequência, foram definidas como unidades de análise sete Seções de Ensino previamente selecionadas com base em critérios de relevância acadêmica e disponibilidade para participação do estudo. Foram priorizadas as unidades que concentram maior número de cursos de graduação, uma vez que apresentam maior complexidade organizacional, volume expressivo de dados acadêmicos e diversidade de processos administrativos relacionados ao tratamento de informações pessoais.

Outro aspecto considerado foi a estrutura administrativa das unidades. Em alguns casos, as funções de colegiado e de seção de ensino estavam integradas em um mesmo setor, o que poderia dificultar a delimitação das atividades de cada instância. Nessas situações, buscou-se selecionar, preferencialmente, seções que apresentavam maior autonomia funcional em relação

aos colegiados de curso, com servidores especificamente lotados e dedicados às atividades da seção de ensino. Também foram observados aspectos de viabilidade prática, como a possibilidade de estabelecer contato com os responsáveis pelos setores e a anuência dos participantes em colaborar com a pesquisa.

Para coleta de dados primários, utilizou-se da entrevista semiestruturada, realizadas com um servidor de cada seção de ensino analisada, tendo como instrumento um roteiro contendo perguntas principais e questões contextuais que permitiram aprofundar as observações sobre a aplicação da LGPD (Manzini, 2004).

Todas as entrevistas foram transcritas integralmente e, juntamente com os dados secundários coletados, submetidas à análise temática indutiva, conforme proposto por Braun e Clarke (2006). Optou-se por essa abordagem para que os temas emergissem diretamente das falas dos servidores, sem imposição de categorias prévias, garantindo maior fidelidade às percepções sobre a aplicação da LGPD.

O processo seguiu seis etapas: (1) familiarização com os dados, por meio de leitura exaustiva das transcrições e documentos institucionais; (2) geração de códigos iniciais, destacando trechos relevantes relacionados às práticas de gestão de dados; (3) busca por temas, agrupando os códigos em padrões mais amplos de significado; (4) revisão dos temas, verificando a coerência interna e a distinção entre eles; (5) definição e nomeação dos temas, assegurando clareza e representatividade; e (6) produção do relatório, integrando os temas identificados à discussão e relacionando-os com os princípios da LGPD e com a literatura especializada.
Esse processo resultou na sistematização de onze temas principais: documentos pessoais mantidos, formas de guarda, acesso a documentos, tramitação de documentos, disponibilização para alunos, solicitações de acesso de informação por terceiros, nível de conhecimento da LGPD, mudanças após a LGPD, benefícios percebidos, dificuldades enfrentadas e orientações formais da UFMG.

Um quadro síntese das respostas dadas por sete servidores entrevistados foi utilizado para analisar e interpretar da atuação dos servidores perante a LGPD, o que torna essa uma abordagem qualitativa, já que permite uma análise e entendimento cuidadoso do objeto pesquisado (Creswell, 2007). Por fim, por meio de uma análise comparativa, foi realizada uma análise de conformidade entre o resultado das entrevistas e os princípios da LGPD.

4. Resultados e Discussão.

Os resultados obtidos revelam que, desde 2018 a UFMG vem envidando esforços para adequação à LGPD. Suas ações se voltam para o mapeamento de processos, o desenvolvimento de ferramentas e sistemas, a adequação dos serviços e a disponibilização das informações obtidas e geradas (UFMG, 2025a). Registros internos demonstram que em 2021, a Reitoria instituiu um grupo de trabalho específico para a LGPD, atualizado pela portaria nº 6918, de 24 de agosto de 2022.

Concomitantemente, a Auditoria-Geral da universidade passou a prestar consultoria à Diretoria de Governança Informacional (DGI), a fim de apoiar a gestão da proteção de dados pessoais. Esse trabalho teve início após a emissão da Nota Técnica nº 3/2023/AUDITORIA-UFMG, que apresentou medidas necessárias ao cumprimento das determinações da Lei Geral de Proteção de Dados (UFMG, 2023). Na avaliação realizada, foi revelado que a universidade apresentava um nível de adequação abaixo da média entre as organizações avaliadas, encontrando-se ainda em um nível inicial de conformidade (UFMG, 2023).

Entre as principais fragilidades identificadas naquele momento estavam: a ausência de um programa conscientização e treinamento de profissionais envolvidos no tratamento de dados pessoais; a inexistência de um programa de governança em privacidade; a falta de ferramentas para registrar as operações de tratamento de dados realizadas por sistemas, produtos, processos ou serviço; e a falta do monitoramento preventivo de acidentes (UFMG, 2023). De acordo com o auditor responsável pelo trabalho, algumas das medidas recomendadas já estão em fase de implementação, prevendo-se, entre outras iniciativas, a criação de dois instrumentos fundamentais: o Inventário de Dados Pessoais (IDP) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Como não foram encontrados registros específicos sobre o tratamento de dados sensíveis dos estudantes nos setores acadêmicos, foi realizado contato com a DGI, dirigida pela encarregada da LGPD na UFMG. Em resposta, foi informado que a universidade possui a Política de Segurança da Informação (POSIN), elaborada pela Diretoria de Tecnologia da Informação (DTI) em 2022, que estabelece diretrizes gerais de segurança alinhadas às normativas vigentes. Além disso, a também foi informado a previsão de envio, a partir de 2025, de orientações periódicas às unidades acadêmicas e à administração central sobre procedimentos relacionados à proteção de dados.

Como percebido nas entrevistas, essas iniciativas, embora relevantes, ainda são incipientes e não chegam de maneira uniforme às seções de ensino, que permanecem sem protocolos padronizados para o tratamento de dados. Tal cenário evidencia tanto os avanços institucionais quanto os desafios persistentes para a plena adequação da UFMG à LGPD.

4.1 Seções de Ensino e LGPD: refletindo as convergências e divergências.

A LGPD estabelece que o tratamento de dados só pode ocorrer em condições específicas, como consentimento do titular, cumprimento de obrigação legal ou regulatória e execução de políticas públicas, pela Administração Pública (Brasil, 2018). No caso das Seções de Ensino da UFMG, o enquadramento recai principalmente nas duas últimas hipóteses, uma vez que o processamento de informações é necessário para matrícula, registro acadêmico e emissão de documentos oficiais, não havendo exigência de consentimento expresso (Brasil, 2018).

Os dados tratados nesses setores incluem dados pessoais (CPF, RG e histórico escolar) e sensíveis (ex.: laudos médicos, declarações de pessoas com deficiência e informações socioeconômicas), nos termos do art. 5º da LGPD (Brasil, 2018). Esse caráter sensível demanda maior rigor no tratamento, especialmente quanto à guarda, descarte e controle de acesso.

Parte dessas informações é inserida no Sistema Acadêmico de Graduação (SIGA) pelo Departamento de Registro e Controle Acadêmico (DRCA), responsável por alimentar a base institucional no momento da matrícula. Em parceria com esse departamento, a DTI também já desenvolveu uma Política de Privacidade e mapeou os principais fluxos de dados (UFMG, 2025a).

As entrevistas semiestruturadas permitiram identificar onze categorias de análise, que integram ações de mapear as práticas de gestão, armazenamento, acesso e compartilhamento de dados. Esses achados estão sintetizados na Tabela 2.

Tabela 2. Categorização sistemática das entrevistas

Categoria	**Achados principais**
Documentos pessoais mantidos	Documentos básicos (RG, CPF, históricos) e documentos sensíveis (laudos médicos, declarações PCD, certidões). Em alguns setores há acúmulo de documentos sem critérios claros de descarte.
Forma de guarda	Predomínio de arquivos físicos, com progressiva migração para digitais (Sistema de Gestão Acadêmica - SIGA, Sistema Eletrônico de Informações - SEI, servidores locais). Falta padronização: alguns setores ainda utilizam armários e caixas-box; outros desenvolveram plataformas próprias digitais.
Acesso a documentos	Em geral, restrito a servidores da seção. Há variação nos protocolos de controle de acesso, alguns mais robustos (autenticação no SIGA) e outros frágeis (armazenamento local sem padronização).
Tramitação de documentos	Uso misto de SEI, SIGA, e-mail e, em três setores, plataformas próprias. A ausência de padronização gera desigualdade de procedimentos e riscos à segurança.
Disponibilização para alunos	Envio majoritariamente via SEI ou e-mail. Em alguns setores há conferência de identidade do solicitante, enquanto outros adotam verificações simplificadas, por meio de nome, matrícula, e-mail.
Solicitações de acesso de informação por terceiros	Regra geral: acesso negado sem autorização formal do aluno.
Nível de conhecimento da LGPD	Uniformemente baixo: servidores afirmam conhecer a lei, mas sem capacitação técnica ou protocolos formais oferecidos pela UFMG.
Mudanças após a LGPD	Impacto reduzido: poucos setores relataram adequações relevantes (anonimização em atas, criação de plataforma de diplomas). A maioria afirmou "nenhuma mudança" significativa.
Benefícios percebidos	Poucos setores identificaram ganhos concretos; quando citados, restringem-se a maior proteção de dados e anonimização em atas.
Dificuldades enfrentadas	Destacam-se: ausência de diretrizes claras da instituição, falta de padronização de processos, carência de armazenamento seguro, digitalização incompleta e desinformação sobre protocolos.

Categoria	Achados principais
Orientações formais da UFMG	Nenhum setor relatou receber instruções consistentes. A percepção geral é de ausência de comunicação institucional sobre procedimentos relacionados à LGPD.

Fonte: elaborada pelas autoras (2025).

Segundo as entrevistas, um grande número de documentos da vida acadêmica do aluno é mantido, desde sua entrada até a saída da universidade, incluindo dados de identificação, comprovantes de conclusão do ensino médio, comprovante de endereços, passaportes de intercambistas e dados sensíveis, como laudos médicos e informações sobre deficiência, entre outros.

O arquivamento desses documentos revela uma forma híbrida e não padronizada. Todas as seções utilizam uma combinação de arquivos físicos e digitais. O armazenamento físico varia desde pastas e caixas-box até armários de aço. Já o digital ocorre nos sistemas institucionais SIGA e SEI, mas também em servidores locais das unidades, plataformas próprias, em um caso, e arquivos digitais não estruturados. Uma seção relatou o uso do *Google Forms* para coleta de dados, ferramenta externa não homologada pela universidade (UFMG, 2022).

O acesso aos documentos, físicos e digitais, é geralmente restrito aos servidores lotados na própria seção ou, em alguns casos, ao colegiado do curso. No entanto, os protocolos para tramitação e disponibilização de informações aos alunos são inconsistentes entre as unidades. A circulação de documentos ocorre por múltiplos canais: papel, e-mail institucional, SEI, SIGA e, em três seções, por meio de plataformas locais desenvolvidas internamente.

A verificação de identidade para o envio de documentos aos alunos também é um ponto de alternância. Enquanto algumas seções adotam métodos mais robustos, como a exigência de login institucional combinado com anexo de documento, outras realizam verificações simplificadas, como a simples conferência do e-mail do aluno no sistema SIGA, ou não possuem um protocolo estabelecido.

Em relação a solicitações de terceiros, há um consenso positivo: a regra geral é não fornecer informações sem autorização expressa do aluno, frequentemente exigindo uma procuração formal.

Um dos achados mais consistentes e críticos da pesquisa é o baixo nível de conhecimento técnico sobre a LGPD entre os servidores entrevistados. As respostas variaram de "muito baixo" a "prático, sem técnico", com todos os setores confirmando a ausência de treinamento formal sobre o tema.

Consequentemente, a maioria das seções relatou que a promulgação da LGPD gerou pouca ou nenhuma mudança em suas rotinas de trabalho. As alterações mencionadas foram pontuais, como a anonimização de dados pessoais em atas ou o reforço de práticas de sigilo já existentes.

De forma unânime, todas as sete seções afirmaram não ter recebido orientações formais da UFMG sobre como aplicar a LGPD em seus processos. As dificuldades mais citadas pelos servidores refletem essa lacuna institucional: falta de diretrizes claras, ausência de padronização nos procedimentos, carência de um sistema de armazenamento digital seguro e centralizado, e a desinformação geral sobre protocolos de proteção de dados.

A análise dos resultados, à luz dos princípios da LGPD, revela uma conformidade parcial e heterogênea nas Seções de Ensino da UFMG. Esse resultado não é isolado: como apontam Filgueiras, Lui e Veloso (2025), a governança de dados no setor público brasileiro caracteriza-se pela fragmentação e pela ausência de padrões comuns, o que dificulta a consolidação de práticas institucionais de proteção. A Tabela 3 sintetiza a avaliação de conformidade, servindo como guia para a presente discussão.

Tabela 3. Comparação das práticas dos setores com os princípios da LGPD.

Princípio (LGPD)	**O que prevê a lei**	**Evidências nas entrevistas**	**Conformidade observada**
Finalidade	Uso de dados para propósitos legítimos, específicos e informados ao titular	Dados coletados apenas para fins acadêmicos.	Alto – práticas alinhadas, embora falte registro formal do propósito.
Adequação	Tratamento compatível com a finalidade informada	Uso compatível com a finalidade (processos acadêmicos e administrativos).	Alto – coerência entre coleta e uso.
Necessidade	Limitação da coleta ao mínimo necessário	Alguns setores armazenam dados além do indispensável; falta tabela de temporalidade e critérios de descarte.	Média – risco de excesso de dados.
Livre Acesso	Garantia de acesso do titular aos próprios dados	Alunos acessam dados mediante solicitação formal (e-mail, SEI, plataforma própria); ausência de mecanismos de transparência ativa.	Médio – acesso restrito e pouco automatizado.
Qualidade dos Dados	Dados exatos, atualizados e relevantes	Conferência por matrícula, CPF ou documento de identidade no SIGA; ausência de rotina de atualização sistemática.	Médio – checagens casuais, sem processo estruturado.
Transparência	Informações claras sobre coleta e tratamento	Falta de comunicação clara, relatórios públicos e protocolos formais de divulgação.	Baixo – ponto mais crítico.
Segurança	Medidas técnicas e administrativas de proteção	Uso de logins institucionais (SIGA, minhaUFMG) em alguns setores; mas também uso de ferramentas externas (*Google Forms*).	Médio/baixo – boas práticas em alguns setores, fragilidades em outros.

Prevenção	Adoção de medidas para evitar danos	Ações apenas reativas; inexistência de protocolos preventivos de segurança	Baixo
Não Discriminação	Proibição de uso abusivo ou discriminatório	Dados usados estritamente para fins acadêmicos, sem relatos de usos abusivos.	Alto
Responsabilização e prestação de contas	Demonstração de conformidade com a LGPD	Não há auditorias internas sistemáticas nem relatórios de impacto; dependência da Reitoria/DRCA.	Baixo

Fonte: elaborado pelas autoras.

Os princípios de finalidade, adequação e não discriminação apresentaram alto nível de conformidade. Todos os setores coletam e utilizam os dados estritamente para propósitos acadêmicos legítimos, como matrícula, registros da vida acadêmica e emissão de documentos, não havendo indícios de uso para fins discriminatórios ou incompatíveis com os princípios de finalidade e adequação que a lei solicita (Brasil, 2018). Essa constatação converge com o que defende Doneda (2021), ao enfatizar que a legitimidade do tratamento é central para assegurar a confiança dos titulares e para consolidar a proteção de dados como direito fundamental. Reis et al. (2024) alertam que, em ambientes educacionais, é recorrente a ausência de parâmetros claros para a definição da finalidade dos dados coletados, o que evidencia a necessidade de maior precisão normativa e prática no alinhamento entre coleta e uso da informação.

O princípio da necessidade, entretanto, mostrou-se fragilizado em algumas unidades, que relataram a manutenção de documentos “além do estritamente indispensável”, sem critérios claros de triagem ou descarte repassado por instâncias superiores. Essa prática contradiz a diretriz de coleta mínima prevista pela LGPD (Brasil, 2018) e amplia a exposição a riscos de segurança, já que o acumulo de dados aumenta a superfície de risco a incidentes de segurança. Conforme Vuori (2024), políticas de ciclo de vida dos dados e monitoramento de riscos são critérios centrais da governança; a ausência desses mecanismos pode ser entendida como sinal de baixa maturidade nesse campo.

Dois pontos críticos da análise são os princípios do livre acesso e da transparência. O acesso dos alunos aos seus próprios dados ocorre de forma majoritariamente reativa, dependendo de uma solicitação formal, sem a existência de mecanismos de transparência ativa que permitam a consulta autônoma e simplificada (exceto, apenas, no caso do comprovante de matrícula e do histórico escolar).

Quanto a transparência, nenhum setor informou práticas consistentes de transparência ativa, como a publicação de relatórios que permitam o público interessado acompanhar a prática de tratamento de dados. Esse cenário dialoga com Reis et al. (2024), que ressaltam a ausência de parâmetros claros e de práticas estruturadas de governança como um dos principais entraves à efetividade da LGPD em instituições de ensino. Doneda (2021) também diz que a transparência no tratamento de dados não se limita ao fornecimento de informações, mas envolve garantir

clareza, inteligibilidade e acompanhamento contínuo por parte dos titulares, constituindo elemento central para a efetivação do direito fundamental à proteção de dados.

Apenas um setor afirmou dispor de protocolos divulgados sobre o tratamento de dados em sua plataforma própria de diploma. A ausência unânime de políticas formais sobre tratamento e de comunicação aos titulares e a percepção de "desinformação" relatada pelos próprios servidores demonstram uma falha grave na garantia de clareza e previsibilidade exigida pela lei (Brasil, 2018).

Em relação à qualidade dos dados, constatou-se que a atualização ocorre apenas de forma pontual, vinculada a demandas específicas do estudante ou de processos administrativos acadêmicos. Tal fato reforça as discussões de Vouri (2024) que enfatiza que para o que o princípio da qualidade do dado seja cumprido se faz necessário a definição de procedimentos de verificação contínua relacionados à exatidão, clareza, relevância e atualização dos dados.

A falta de diretrizes, a comunicação inadequada e a dependência de consultas a órgãos superiores para resolver demandas atípicas das seções também comprometem a transparência e a eficiência, impactando o princípio da responsabilidade. Como apontam Almeida e Soares (2022), as instituições devem estar alinhadas e prontas para atender às demandas de tratamento e armazenamento de dados, pois o cenário digital atual não dispões de outro caminho senão o de estarmos todos preparados para interagir com essas regulamentações.

No que tange à segurança, práticas ambivalentes que refletem a falta de padronização foram observadas. Por um lado, há pontos positivos, como o uso de autenticação robusta em plataformas locais e protocolos claros para atendimentos de terceiros, que incluem autorizações formais e instrumento de mandato, que também são uma rotina positiva quanto ao respeito ao sigilo da informação pessoal, como define a LAI (Brasil, 2011).

Por outro, apesar de Somoza et al (2022) defenderem que as estruturas públicas precisariam revisar suas estruturas e processos de TI, foram identificadas vulnerabilidades, como o uso de ferramentas externas não homologadas (*Google Forms*), o armazenamento de dados em servidores locais sem a devida infraestrutura e protocolos de segurança inconsistentes para verificação de identidade. Tais práticas violam diretamente POSIN da universidade, que orienta o uso exclusivo de recursos providos ou homologados pela instituição (UFMG, 2022). Essa diretriz vale também no caso de armazenamento e de preservação da informação, que devem ser realizados exclusivamente em infraestrutura da UFMG ou em nuvem, desde que aprovada e homologada pela instituição (UFMG, 2022).

De forma associada, o princípio da prevenção revelou-se praticamente ausente: os setores atuam de maneira reativa, sem protocolos específicos para mitigar riscos ou evitar incidentes de segurança antes que ocorram. Isso evidencia o quadro descrito por Filgueiras, Lui e Veloso (2025) e Somoza et al. (2024), para os quais a governança de dados no setor público ainda se mostra fragmentada, dependente de soluções reativas e pouco integrada às diretrizes estratégicas institucionais. Também reforça o alerta de Reis et al. (2024), de que a falta de

estratégias preventivas e de integração entre os diferentes agentes e sistemas educacionais amplia os riscos de não conformidade com a LGPD.

Por fim, os princípios de Responsabilização e a Prestação de Contas mostraram-se dimensões deficitários. A inexistência de auditorias internas nessas seções, relatórios de impacto ou registros formais que comprovem a conformidade com a LGPD demonstra que a responsabilidade não é exercida de forma proativa nos setores, que permanecem dependentes de orientações pontuais da Reitoria ou do DRCA. Vouri (2024) ressalta os mecanismos de registro e auditoria são fundamentais para assegurar a *accountability*, pilar da governança de dados; assim, sua ausência pode revelar fragilidades na demonstração de conformidade com a LGPD

4.2 Desafios Estruturais e a Necessidade de uma Governança Centralizada

Os achados reforçam que os desafios de conformidade não se restringem a práticas locais, mas revelam problemas estruturais de gestão. Reis et al. (2024) argumentam que mapear os obstáculos no contexto educacional é essencial para obter uma visão abrangente dos aspectos envolvidos na aplicação da lei, como o déficit na capacitação dos servidores, a ausência de armazenamento seguro, a falta de padronização nos processos e a carência de integração tecnológica.

A limitação de treinamentos compromete a capacidade dos servidores de implementar a LGPD de forma eficaz, enquanto a inexistência de soluções institucionais padronizadas para o armazenamento digital gera vulnerabilidades. A gestão descentralizada, por sua vez, resulta em práticas divergentes, aumentando os riscos de não conformidade. Por fim, plataformas locais, desenvolvidas por três seções de ensino, demandam maior integração e suporte institucional para assegurar a segurança e a continuidade dos processos.

Essas fragilidades corroboram com a análise de Filgueiras, Lui e Veloso (2025), segundo a qual as inovações trazidas pela LGPD criaram um contexto em que organizações públicas são desafiadas a redesenhar suas políticas de dados e processos organizacionais, para incorporar a proteção de dados como dimensão central da governança institucional.

Para lidar com essas dificuldades, algumas propostas podem ser adotadas, como: (1) proporcionar treinamentos regulares e obrigatórios sobre a LGPD para todos os servidores, com conteúdo acessíveis, nos programas de educação continuada da UFMG; (2)promover o desenvolvimento de uma plataforma institucional para armazenamento digital e gestão de dados sensíveis, integrando SIGA e outras ferramentas utilizadas; (3) criar diretrizes claras e padronizadas para a identificação de solicitantes e o processamento, envio e guarda de dados, aplicáveis a todos os setores; e (4) implementar processos internos sistemáticos de auditoria e acompanhamento, para verificar a conformidade e ajustar práticas onde necessário.

A análise evidencia, assim que, embora existam boas práticas isoladas, há oportunidades para avanços significativos na implementação da governança de dados nos setores de ensino da UFMG, promovendo maior segurança, eficiência e adequação com a legislação.

5. Considerações Finais

O estudo demonstra que a UFMG já criou regulamentações internas relacionadas à Política de Segurança da Informação, como a POSIN e a Comissão de Gestão da Informação, mas que ainda enfrenta desafios para consolidar a implementação da LGPD, conforme a própria auditoria interna da Universidade demostrou em sua nota técnica, em 2023. A ausência de uniformidade nos sistemas tecnológicos e a falta de orientação formal aos servidores que lidam com informações e dados dos alunos nas Seções de Ensino geram disparidades significativas entre as unidades. Enquanto algumas possuem infraestrutura e processos mais avançados e seguros, outras enfrentam limitações no tratamento e na salvaguarda dos dados.

Essas lacunas, contudo, representam oportunidades para avanços na governança de dados na Universidade. Além de implementar treinamentos formais e obrigatórios para os servidores que trabalham com essa demanda, é necessário desenvolver protocolos claros para lidar com incidentes relacionados a dados e estabelecer canais dedicados para reportar irregularidades ou dúvidas. Tais iniciativas devem promover o entendimento amplo da norma, padronizar o tratamento dos dados e garantir a conformidade com a legislação.

Ademais, identificou-se a necessidade de desenvolver um sistema integrado, para armazenamento digital, promovendo a centralização e padronização das demandas elencadas relacionadas à LGPD. O armazenamento em nuvem e o uso servidores homologados pela UFMG, garantiria a segurança, a disponibilidade e a governança de dados, além de apoiar a atuação da encarregada de dados sob supervisão da Diretoria de Tecnologia da Informação.

Estabelecer diretrizes claras e divulgá-las amplamente à comunidade acadêmica e externa, padronizando os fluxos de atendimento e promovendo maior transparência e segurança nas requisições de dados pessoais sensíveis também se mostrou necessário. Tal iniciativa contribuiria para aumentar a transparência e padronizar os fluxos de atendimento, garantindo maior segurança e conformidade.

Por fim, a auditoria interna conduzida pela Auditoria-Geral da UFMG desempenha um papel essencial na verificação da conformidade dos processos e no ajustamento das práticas relacionadas à LGPD. Essa medida não apenas garante a melhoria contínua, mas também fortalece a confiança da comunidade acadêmica e externa no tratamento dos dados realizados pela Universidade.

Todavia, este trabalho apresenta-se como um ponto de partida para as discussões sobre governança de dados na UFMG e abre caminhos para novas pesquisas. Estudos futuros podem aprofundar a análise dos papéis de controlador, operador e encarregado de dados, bem como acompanhar os avanços no alinhamento à legislação e na consolidação da governança de dados na instituição. Espera-se que tais práticas possam servir de referência para outras organizações do setor público.

Referências

AGUNE, R.; CARLOS, J. Governo eletrônico e novos processos de trabalho. In: LEVY, E.; DRAGO, P. (Orgs.). **Gestão pública no Brasil contemporâneo.** São Paulo: Fundap, 2005. Disponível em: https://governancaegestao.wordpress.com/wp-content/uploads/2008/04/governo_eletronico_roberto_agune.pdf. Acesso em: 28 ago. 2025.

ALMEIDA, S. do C. D. de; SOARES, T. A.. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital**. Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26–45, jul. 2022. Disponível em: https://doi.org/10.1590/1981-5344/25905. Acesso em: 16 jan. 2025.

ANGÉLICO, Fabiano. **Lei de acesso à informação pública e seus possíveis desdobramentos à accountability democrática no Brasil**. São Paulo, 2012. Dissertação (Administração Pública e Governo.) - FUNDAÇÃO GETÚLIO VARGAS. Disponível em: https://hdl.handle.net/10438/9905. Acesso em: 20 jan. 2025.

BARBIERI, Carlos. Governança de Dados: Práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019.
BRASIL. Constituição 1998. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 4 jan. 2025.

BRASIL. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 6 set. 2025.

BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 jan. 2025.

BRASIL. **Lei nº 14.129**, de 29 de março de 2021. Governo digital. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em 22 jan. 2025.

BRASIL. **Lei n. 12.527**, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 12 jan. 2025.

BRASIL. Ministério da Educação. **Portaria n. 360, de 18 de maio de 2022**. Diário Oficial da União: Seção 01, 19 de maio de 2022, p. 40. Disponível

em: https://www.in.gov.br/en/web/dou/-/portaria-n-360-de-18-de-maio-de-2022-401082263. Acesso em: 11 jan. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387/DF**. Relator: Ministra Rosa Weber. Julgamento em 07 maio 2020. Plenário. Brasília, DF. Disponível em: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdfAcesso em: 28 ago. 2025.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology**. Qualitative Research in Psychology**, v. 3, n. 2, p. 77–101, 2006. Disponível em: https://doi.org/10.1191/1478088706qp063oa . Acesso em: 06 set. 2024

CRESWELL, John W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 2. ed. Porto Alegre: Artmed, 2007.

DAHL, Robert A. Por que o capitalismo de mercado favorece a democracia. In: DAHL, Robert A. **Sobre a democracia**. Brasília: EdUnB, 2001. p. 183 – 190.

DATA GOVERNANCE INSTITUTE. The DGI Data Governance Framework. Prepared by Gwen Thomas. **Data Governance Institute**, 2014. Disponível em: https://neweditions.net/sites/default/files/sites/default/files/ACLDataCouncil/Data%20Governance%20Institute%202014%20Data%20Governance%20Framework.pdf. Acesso em: 3set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da autoridade e da regulação.** 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

FILGUEIRAS, F.; LUI, L.; VELOSO, M. T. T.. A Gramática Institucional da Proteção de Dados e da Privacidade no Brasil. **Dados**, v. 68, n. 1, p. e20220169, mar. 2025. Disponível em: https://doi.org/10.1590/dados.2025.68.1.346. Acesso em: 16 jan. 2025.

MANZINI, Eduardo José. Entrevista semi-estruturada: análise de objetivos e de roteiros. **Seminário internacional sobre pesquisa e estudos qualitativos**, Bauru, v.2, 2004. Disponível em: https://wp.ufpel.edu.br/consagro/files/2012/03/MANZINI-Jos%C3%A9-Eduardo-Entevista-semi-estruturada-An%C3%A1lise-de-objetivos-e-de-roteiros.pdf. Acesso em: 04 jan.2020.

OECD. **Digital government strategies for transforming public services in the welfare areas**. Paris: OECD Publishing, 2016. (OECD Digital Government Studies). Disponível em: https://doi.org/10.1787/0d2eff45-en. Acesso em: 28 ago. 2025

RÊGO, Bergson Lopes. **Gestão e Governança de Dados: promovendo dados como ativos de valor nas empresas.** Brasport. Rio de Janeiro - RJ. 2013.

REIS, S. R. F. et al. Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. **Revista de Gestão e Secretariado**, [s. l.], v. 15, n. 3, p. e3292, 2024. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/3292. Acesso em: 25 jan. 2025.

SÁ, E.; VITAL, L. P.. Mapeamento do fluxo de informações pessoais no cadastro eleitoral do TRE-SC sob a ótica da LGPD. **Em Questão**, v. 30, p. e–133709, 2024.

SOMOZA, Laura Sofia Narvaez et al. Avaliação de conformidade da Lei Geral de Proteção de Dados Pessoais nas instituições federais de educação do Paraná através do uso de dados abertos. **Revista Gestão do Conhecimento e Tecnologia da Informação**. v. 6, n. 1, p. 40-50, 28 nov. 2024. Disponível em: https://doi.org/10.31501/rgcti.v6i1.13875. Acesso em: 16 jan. 2025.

UFMG. Auditoria Geral. **Nota Técnica n° 3, de 06 de dezembro de 2023**. Análise e encaminhamentos desta Auditoria Interna com fundamento nos resultados dos trabalhos de auditoria realizados sobre as medidas para atendimento às determinações da Lei Geral de Proteção de Dados no âmbito da Universidade Federal de Minas Gerais (UFMG). Processo SEI: 23072.221483/2023-31.

UFMG. Diretoria de Avaliação Institucional. **UFMG em Números**. 2021. Disponível em: https://www.ufmg.br/dai/noticia/ufmg-em-numeros/. Acesso em: 19 jan. 2025.

UFMG. Diretoria de Tecnologia da Informação. **Política de Segurança da Informação (POSIN-UFMG),** 26 set. 2022. Disponível em: https://www.ufmg.br/dti/wp-content/uploads/2022/11/posin.pdf. Acesso em: 30 mai. 2025.

UFMG. Reitoria. **Portaria n° 1844, de 10 de março de 2021**. Disponível em: https://ufmg.br/storage/4/6/3/1/46314485cc4277ef1f1b5d0a788e5e47_16155540375792_116533740.pdf. Acesso em: 20 jan. 2025.

UFMG. Reitoria. **Portaria n° 6918, de 24 de agosto de 2022.** Disponível em: https://ufmg.br/storage/4/6/3/1/46314485cc4277ef1f1b5d0a788e5e47_16155540375792_116533740.pdf. Acesso em: 20 jan. 2025.

UFMG. Proteção de Dados Pessoais. **DTI - Diretoria de Tecnologia da Informação.** 2025. Disponível em: https://www.ufmg.br/dti/pagina-inicial/protecao-de-dados-pessoais/. Acesso em: 13 mai. 2025.

UFMG. Trabalho de consultoria em LGPD é iniciado junto à Diretoria de Governança Informacional (DGI). **Auditoria Geral da UFMG**. 2023. Disponível em: https://www.ufmg.br/auditoria/noticia/trabalho-de-consultoria-em-lgpd-e-iniciado-junto-a-diretoria-de-governanca-informacional-dgi/. Acesso em: 20 jan. 2025.

UFMG. Seção de Ensino**. Escola de Arquitetura**. Belo Horizonte: UFMG, 2025. Disponível em: https://www.arq.ufmg.br/ea/ensino/secao-de-ensino/. Acesso em: 6 set. 2025.

UFMG. Seção de Ensino. **Faculdade de Direito.** Belo Horizonte: UFMG, 2025. Disponível em: https://colgrad.direito.ufmg.br/?page_id=13. Acesso em: 6 set. 2025.

UFMG. Seção de Ensino. **Faculdade de Educação.** Belo Horizonte: UFMG, 2025. Disponível em: https://www.fae.ufmg.br/graduacao-pedagogia/secao-de-ensino/. Acesso em: 6 set. 2025.

UFMG. Seção de Ensino. **Escola de Educação Física, Fisioterapia e Terapia Ocupacional.** Belo Horizonte: UFMG. 2025. Disponível em: http://www.eeffto.ufmg.br/eeffto/institucional/exibe/6/secao_de_ensino/. Acesso em: 6 set. 2025.

UFMG. Seção de Ensino. **Instituto de Ciências Biológicas**. 2015. Disponível em: https://www.icb.ufmg.br/institucional/administracao-central/secoes-administrativas/secao-de-ensino#:~:text=A%20se%C3%A7%C3%A3o%20de%20Ensino%20do,20%20cursos%20atendidos%20pelo%20Instituto. Acesso em: 5 jan. 2025

UFMG. Seção de Ensino**. Instituto de Ciências Exatas.** 2022. Disponível em https://www.icex.ufmg.br/icex_novo/atendimento-secao-de-ensino/. Acesso em: 5 jan. 2025.

VIANA, Ana Cristina Aguilar. Transformação digital na administração pública: do governo eletrônico ao governo digital. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, v. 8, n. 1, p. 115–136, jan./jun. 2021. Disponível em: https://www.redalyc.org/journal/6559/655969720005/. Acesso em: 28 ago. 2025.

VUORI, Natália Brezolin. Compartilhamento de dados pessoais no poder público. Dissertação (Mestrado em Governança e Desenvolvimento) – Escola Nacional de Administração Pública, Brasília, 2024. 97 f. Disponível em: https://repositorio.enap.gov.br/handle/1/8341. Acesso em: 4 set. 2025.