SemeAd 2025
XXVIII Seminários em Administração

10, 11, 12, 13 e 14 de novembro de 2025
ISSN 2177-3866

Relatório de Impacto à Proteção de Dados Pessoais: análise da aplicabilidade do framework proposto pelo Programa de Privacidade e Segurança da Informação ao contexto da UFMG

JOSE GUILHERME MAGALHÃES E SILVA
UNIVERSIDADE FEDERAL DE MINAS GERAIS (UFMG)

TEREZINHA VITORIA DE SILVA
UNIVERSIDADE FEDERAL DE MINAS GERAIS

OCTÁVIO VALENTE CAMPOS
UNIVERSIDADE FEDERAL DE MINAS GERAIS (UFMG)

Relatório de Impacto à Proteção de Dados Pessoais: análise da aplicabilidade do framework proposto pelo Programa de Privacidade e Segurança da Informação ao contexto da UFMG

1 INTRODUÇÃO

Publicada em 2018, a Lei Geral de Proteção de Dados - LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio de disposições sobre o tratamento de dados pessoais por pessoas naturais e jurídicas. Atualmente, organizações públicas e privadas ainda buscam se adequar plenamente à referida lei e aos demais normativos emitidos pelas autoridades competentes. De acordo com o Acórdão nº 1.372/2025/TCU-Plenário, como resultado de um trabalho realizado com 387 organizações do Poder Executivo Federal, 97,16% das entidades questionadas já adotam, no mínimo, medidas preparatórias com vistas a se adequar a LGPD. Nesse contexto, a Universidade Federal de Minas Gerais (UFMG) tem realizado medidas para obter a plena conformidade.

O presente artigo aplicado emprega o modelo teórico de avaliação de impacto à proteção de dados pessoais fornecido pelo Programa de Privacidade e Segurança da Informação (PPSI) para revelar conhecimentos a respeito das medidas para adequação à LGPD no âmbito da UFMG, testando a aplicabilidade do modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) a essa Universidade.

Para tanto, o *paper* é dividido da seguinte forma: (i) Introdução (ii) Contexto Investigado, incluindo informações sobre a legislação e os conceitos essenciais sobre a estrutura organizacional da UFMG; (iii) Diagnóstico da Situação-Problema identificada na Universidade, mais precisamente no que tange à existência das ferramentas de proteção previstas na LGPD, aos processos e serviços com tratamento de dados pessoais e aos desafios enfrentados; (vi) Intervenção Proposta, destacando os mecanismos adotados para promover a conformidade da organização aos critérios aplicáveis; (v) Resultados Obtidos a partir da aplicação dos mecanismos pela equipe responsável; (v) Contribuição Tecnológica-Social do trabalho realizado.

2 CONTEXTO INVESTIGADO: A UFMG SOB A ÉGIDE DA LGPD

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), prevê normas gerais, a serem observadas pela União, Estados, Distrito Federal e Municípios. O texto apresenta, dentre outros tópicos, conceitos fundamentais, princípios e requisitos a serem observados em atividades de tratamento de dados pessoais, hipóteses que permitem o tratamento, responsabilidades e penalidades, além de criar a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

A lei representa a superação do paradigma então vigente, marcado pela existência de múltiplas normas legais de natureza setorial e versando isoladamente sobre temas como mercado financeiro, imóveis e proteção ao consumidor. Cria-se um cenário de segurança jurídica e de normas práticas padronizadas, visando à promoção da proteção igualitária, dentro e fora do país, de dados pessoais de pessoas naturais que estejam no Brasil (CELIDONIO, NEVES e DONÁ, 2020). Para Sales Sarlet e Linden Ruaro (2021), a LGPD reflete o reconhecimento da vinculação dos dados à pessoa humana, sendo uma forma de integralização das medidas legais que garantem a proteção desta. A pessoa humana assume o protagonismo nas escolhas sobre controle e compartilhamento de seus dados, podendo participar ativamente do processo de delimitação ou expansão do uso (SALES SARLET e LINDEN RUARO, 2021).

Nos termos do art. 5º, I, da LGPD, considera-se dado pessoal a "informação relacionada à pessoa natural identificada ou identificável". O inciso X do referido artigo dispõe que configura tratamento as mais diversas operações com dados pessoais, como, por exemplo, a coleta, utilização, transmissão, armazenamento, eliminação, etc. Toda atividade de tratamento deve estar lastreada em pelo menos uma hipótese prevista no art. 7º da lei (exemplo: tratamento pela administração pública, para fins de execução de políticas públicas).

Para evitar que os dados pessoais sejam objeto de tratamento irregular, vazamento ou outros possíveis incidentes, a referida lei e demais normativos publicados posteriormente por entidades como a ANPD preveem uma série de responsabilidades por partes de agentes de tratamento. Nesse sentido, o art. 38 da referida lei dispõe que:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente à suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Instruções específicas sobre as medidas de implantação do referido relatório de impacto se encontram dispostas no Programa de Privacidade e Segurança da Informação –

PPSI, instituído por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023. O programa consiste em um conjunto de controles nas áreas de privacidade e segurança da informação, voltados aos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

O PPSI apresenta um *framework* que visa fomentar a privacidade, a proteção de dados pessoais e a segurança da informação. Dentre os controles previstos, se encontra o Controle 30: Avaliação de Impacto, Monitoramento e Auditoria. No guia do *framework*, disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos – MGI, sugere-se a elaboração do RIPD, descrito como a documentação do controlador que descreve os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A Universidade Federal de Minas Gerais (UFMG) realiza as mais diversas ações de tratamento de dados pessoais, de diferentes grupos sociais. Assim, a Universidade ocupa o papel de controladora, por se tratar de pessoa jurídica, de direito público, competente por decisões referentes ao tratamento de dados pessoais. Enquanto controladora, a organização deve adotar as providências exigidas pela LGPD e demais normativos aplicáveis, inclusive no que tange ao RIPD.

No atendimento desses deveres, destaca-se o papel do encarregado, assim denominada a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Na UFMG, conforme dispõe a Portaria nº 6.917, de 24 de agosto de 2022, a função de encarregada é ocupada pela titular da Diretoria de Governança Informacional (DGI), unidade que concentra também as atividades de Ouvidoria, Serviço de Comunicação ao Cidadão (SIC) e abertura de dados no âmbito dessa Universidade.

As entidades públicas estão sujeitas a eventos que podem prejudicar o cumprimento de seus objetivos. A relação entre a probabilidade de ocorrência desses eventos e os impactos em caso de ocorrência é definida pela legislação como “risco”. Para minimizar os riscos na realização de suas atividades surgem os controles internos da gestão, tais como os procedimentos, protocolos, rotinas, etc. Além disso, compete às organizações adotarem o gerenciamento de riscos, um processo sistemático de identificação, avaliação, administração e controle de potenciais eventos. Nesse contexto, a auditoria interna consiste em atividades de

avaliação ou consultoria, voltados a adicionar valor e melhorar as operações de uma organização, principalmente por meio da avaliação e melhoria da eficácia dos processos de gerenciamento de riscos e dos controles internos (CGU, 2016). No âmbito da UFMG, as atividades de auditoria interna são realizadas pela Auditoria-Geral, órgão de assessoramento vinculado ao Conselho Universitário.

Ao longo do ano de 2023, a Auditoria-Geral da UFMG realizou trabalho para avaliar junto à DGI os controles relacionados à transparência ativa (Plano de Dados Abertos – PDA) e passiva (Serviço de Informação ao Cidadão – SIC), ouvidoria, classificação da informação e Lei Geral de Proteção de Dados. Concluído o referido trabalho de avaliação, foram emitidos o Relatório de Auditoria nº 2/2023 AG/UFMG[1] e a Nota Técnica nº 3/2023/AUDITORIA-UFMG[2]. Na ocasião, a Diretora de Governança Informacional, na condição de encarregada de proteção de dados pessoais na UFMG[3], informou interesse em obter o apoio do servidor designado pela Auditoria-Geral para fins de elaboração dos documentos Inventário de Dados Pessoais (IDP) e Relatório de Impacto de Proteção de Dados Pessoais (RIPD), procedimentos exigidos pela Lei Geral de Proteção de Dados Pessoais[4]. Isto posto, tem-se o início do trabalho de consultoria descrito a seguir, formalizado por meio da assinatura de Termo de Compromisso entre a DGI e a Auditoria-Geral. Os tópicos a seguir - diagnóstico da situação problema, intervenção proposta, resultados obtidos e contribuição tecnológica-social - são baseados nas atividades realizadas no decorrer desse serviço consultivo.

3 DIAGNÓSTICO DA SITUAÇÃO PROBLEMA

Com fulcro em sites e documentos institucionais, diálogo com a Encarregada e dados empíricos, foi possível identificar, descrever e analisar os problemas enfrentados pela UFMG no contexto de implementação do RIPD e demandas correlatas.

A UFMG é uma instituição federal de ensino superior, cuja missão é pautada no tripé ensino, pesquisa e extensão. Além dos processos e serviços relacionados à oferta de 14.287 (quatorze mil duzentos e oitenta e sete) vagas em cursos de graduação e pós-graduação, ainda há inúmeras atividades relacionadas aos dois hospitais universitários, farmácia universitária, hospital veterinário, restaurantes universitários, etc. A comunidade acadêmica é formada por 3.287 (três mil duzentos e oitenta e sete) servidores docentes, 4.039 (quatro mil e trinta e nove) servidores técnicos-administrativos e 48.487 (quarenta e oito mil quatrocentos e oitenta e sete) estudantes. Além disso, o cuidado com a proteção de dados na Universidade deve

considerar os dois milhões de atendimentos médicos realizados no Hospital das Clínicas até 2024[5].

Apesar da amplitude e extensão das atividades de tratamento de dados pessoais na UFMG, a organização ainda possui um longo caminho a trilhar para obter a plena conformidade à LGPD. Nesse contexto, o Tribunal de Contas da União (TCU) realizou, entre novembro de 2020 e maio de 2021, auditoria para elaborar um diagnóstico acerca dos controles implantados pelas organizações públicas federais para adequação à lei. Por ocasião da referida auditoria, 382 (trezentas e oitenta e duas) organizações públicas federais, incluindo a UFMG, foram avaliadas por meio de método de autoavaliação de controles (do inglês *Control Self-Assessment – CSA*), o qual consistiu no preenchimento de questionário pelos gestores. Esse trabalho culminou na publicação do Acórdão n.º 1.384/2022 – TCU –Plenário, além da emissão de relatórios de *feedback* destinados a cada organização avaliada. A UFMG obteve o valor 0,23 para o indicador de adequação, o que corresponde ao nível "Inicial", se encontrando abaixo da média (0,35) entre as organizações avaliadas.

A Auditoria-Geral da UFMG, no âmbito da elaboração do Plano Anual de Atividades de Auditoria Interna (PAINT) 2023, ao avaliar o tema "Lei Geral de Proteção de Dados Pessoais, Dados abertos e Sigilosos e Ouvidoria", classificou o risco (produto da multiplicação Probabilidade x Impacto) como crítico. Posteriormente ao trabalho de Auditoria, foi emitida a Nota Técnica 3/2023, na qual a unidade de auditoria interna governamental destaca, dentre outros pontos de atenção, a ausência dos seguintes controles internos voltados à proteção de dados pessoais: (i) Inventário de Dados Pessoais ou instrumento similar (documento essencial para a posterior elaboração do RIPD); (ii) Programa de Governança em Privacidade; (iii) programa de conscientização e treinamento de pessoas envolvidas no tratamento de dados pessoais, de forma a garantir que o pessoal entenda suas responsabilidades e procedimentos.

Os documentos institucionais indicam, ainda, a fragilidade do sistema de gestão de riscos na UFMG. O gerenciamento de riscos relacionados ao tratamento de dados pessoais deve ocorrer em consonância com a Política de Gestão de Riscos da instituição, conforme previsto na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016. *In casu*, a UFMG possui publicada sua Política de Gestão de Riscos, conforme Portaria nº 1.519, de 06 de março de 2020. Entretanto, ainda não foi institucionalizada na Universidade uma metodologia de Gestão de Riscos.

Diante das evidências obtidas, o diagnóstico obtido é de que a UFMG é uma organização responsável por um amplo rol de atividades de tratamento de dados pessoais, mas ainda em um estágio inicial de implementação das determinações da LGPD. O processo de conformidade pode ser prejudicado pela ausência de políticas primordiais e de uma cultura de difusão do conhecimento sobre práticas de privacidade. Especificamente no que tange à elaboração do RIPD, surgem os desafios relacionados à ausência de um inventário prévio das atividades de tratamento e de uma metodologia institucionalizada de gestão de riscos. Para enfrentar a situação-problema exposta, foram aplicadas as intervenções descritas a seguir.

4 INTERVENÇÃO PROPOSTA: METODOLOGIA DE ELABORAÇÃO DO RIPD

O trabalho realizado teve como objetivo identificar e propor uma estrutura de RIPD compatível com as necessidades da UFMG. Considerando os problemas destacados anteriormente, como a ausência de um inventário prévio dos processos, tendo em vista, ainda, o contexto marcado por um grande e diverso rol de processos e serviços realizados pela instituição, surgem objetivos secundários: (i) desenvolver uma metodologia replicável para a elaboração de RIPDs; (ii) construir os Inventários de Dados Pessoais (IDP) para posterior preenchimento dos RIPDs.

Para o atingimento dos objetivos, foram empregadas diferentes ferramentas metodológicas, conforme detalhado no Quadro 1:

Quadro 1 - Resumo da metodologia por objetivo

Objetivo	**Metodologia**
Inventário de Dados Pessoais dos processos escolhidos para projeto-piloto	Análise documental (fonte: fluxos de processos já mapeados) Reunião de facilitação junto aos donos de produtos Preenchimento do *template* pelos responsáveis pelos produtos e revisão e compilação pela Aud-Geral e DGI
Relatório de Impacto à Proteção dos processos escolhidos para projeto-piloto	Análise documental (fonte: IDPs) Avaliação do nível de risco (probabilidade x impacto) por meio de matriz de riscos Identificação dos controles implementados aplicáveis a cada risco por meio de consulta à ferramenta de acompanhamento do PPSI
Desenvolver uma metodologia aplicável ao projeto-piloto e replicável na posterior ampliação do trabalho	Modelagem do processo, conforme metodologia BPMN (*Business Process Modeling Notation*) utilizando o software Bizagi

Fonte: elaborado pelo(a)s autore(a)s (2025).

5 RESULTADOS OBTIDOS

5.1 Inventário de Dados Pessoais - IDP

Dispõe o art. 37 da LGPD que "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse". O PPSI, no âmbito do Controle 19 (Inventário e Mapeamento), prevê o IDP como ferramenta para atendimento da norma. Nesse sentido, o inventário deve abordar, no mínimo, os seguintes tópicos: agentes de tratamento (Controlador e Operador); encarregado; finalidade e hipótese do tratamento; compartilhamento dados pessoais; transferência internacional; propósitos para o tratamento; uma descrição das categorias dos dados pessoais e dos titulares de dados pessoais tratados pela instituição (por exemplo, crianças); o tempo de retenção dos dados pessoais; uma descrição geral das medidas de segurança técnica e organizacional (MGI, 2024).

Cabe destacar que a elaboração do IDP, originalmente, não constava, entre os objetivos do serviço de consultoria em questão. Contudo, no âmbito do PPSI, recomenda-se a elaboração do Inventário como etapa preliminar à produção do RIPD (MGI, 2023). Uma vez identificada a necessidade de elaboração do IDP, o primeiro desafio enfrentado é a extensa quantidade e a diversidade de processos e serviços que envolvem o tratamento de dados pessoais no âmbito da UFMG. Diante dessa situação, identificou-se a necessidade de implementar um projeto-piloto, composto por processos considerados prioritários com base nos critérios de relevância e volume de dados pessoais tratados. Assim, foram selecionados os seguintes processos para fins de mapeamento: (i) Sistema de Seleção Unificada (SISU); Processo Seletivo do Colégio Técnico (COLTEC); Processo Seletivo do Centro Pedagógico (CP); Vestibular "Habilidades"; Processo Seletivo do Teatro Universitário (TU); Admissão de servidores docentes; Admissão de servidores técnico-administrativos e; Acompanhamento Pedagógico.

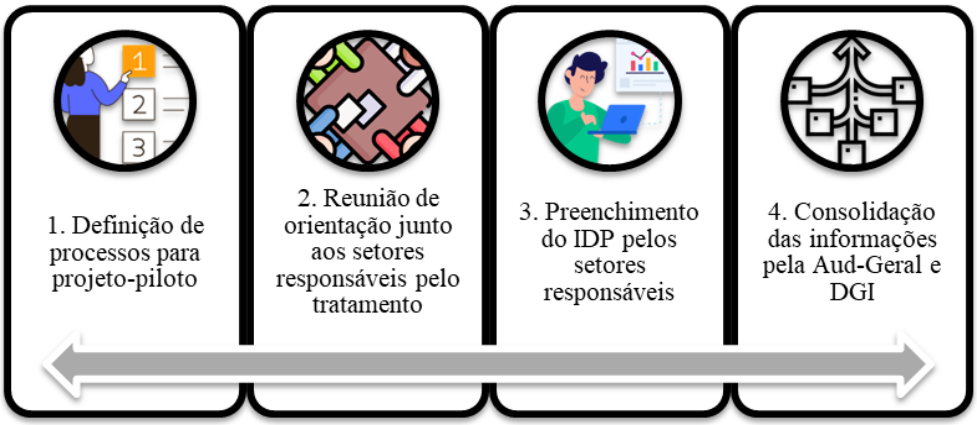
Para fins de elaboração do IDP, optou-se pela utilização de modelo e guia de preenchimento disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI). O *template* apresenta uma planilha, em formato compatível com programas de edição como o Excel, formado pelos seguintes tópicos: (i) Identificação dos serviços / processo de negócio de tratamento de dados pessoais; (ii) Agentes de tratamento e encarregado; (iii) Fases do Ciclo de Vida do Tratamento Dados Pessoais; (iv) Descrição do Fluxo do tratamento dos

dados pessoais; (v) Escopo e Natureza dos Dados Pessoais; (vi) Finalidade do Tratamento de Dados Pessoais; (vii) Categoria de Dados Pessoais; (viii) Categorias de Dados Pessoais Sensíveis; (ix) Frequência e totalização das categorias de dados pessoais tratados; (x) Categorias dos titulares de dados pessoais; (xi) Dados pessoais compartilhados; (xii) Tipo de Controle de Privacidade e Segurança da Informação; (xiii) Transferência Internacional de Dados Pessoais; (xiv) Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio.

A utilização do modelo mencionado é indicada por se tratar de uma ferramenta disponibilizada por autoridade ligada diretamente ao desenvolvimento e a implementação do PPSI e, principalmente, por abranger as mais diversas categorias de dados pessoais e dados pessoais sensíveis, de forma a abarcar processos e serviços com as mais diversas finalidades.

O preenchimento dos inventários de cada processo/serviço foi realizado pelas unidades gestoras, aqui identificadas como donos do produto. Optou-se por manter o protagonismo das equipes envolvidas diretamente com a execução das demandas, por considerar que se esse(a)s servidore(a)s detêm maior conhecimento e expertise sobre as peculiaridades de cada rotina. A figura 1 descreve a metodologia construída, enquanto o quadro 2 trata dos setores consultados.

Figura 1 - Processo de elaboração de Inventário de Dados Pessoais - IDP



Fonte: Elaborado pelo(s) autore(s) (2025).

O preenchimento do *template* revelou-se, contudo, desafiador, uma vez que abrange categorias de dados aplicáveis ou não ao contexto da UFMG. Conforme destacado anteriormente por Lugati e Almeida (2020), um problema recorrente no Brasil é que as organizações, em geral, tem priorizado a adoção de soluções pontuais e imediatistas em segurança da informação e privacidade, visando apenas evitar as sanções da ANPD, enquanto

negligenciam a importância da criação de uma cultura sustentável de proteção de dados. Durante as atividades realizadas para elaboração dos IDPs observou-se no âmbito da UFMG, que, apesar do engajamento individual dos servidores responsáveis pela gestão e execução das rotinas, a Universidade ainda carece de uma política sistemática voltada ao fomento e à disseminação de conhecimentos sobre proteção de dados. Nesse contexto, as reuniões de facilitação conduzidas pela Auditoria-Geral e pela DGI, assim como os contatos posteriores realizados por e-mail ou em encontros complementares, mostraram-se fundamentais para os esclarecimentos de dúvidas, a apresentação do *template* e a disseminação de conhecimentos essenciais sobre a LGPD. Apesar dos desafios, a aplicabilidade dos *templates* ao contexto da UFMG foi validada pela equipe designada, por meio da execução do projeto-piloto, que resultou na elaboração de oito inventários de dados pessoais.

Quadro 2 - Processos inventariados[6]

Processo	**Responsáveis**	**Motivo da inclusão em projeto-piloto**
Sistema de Seleção Unificada (SISU)	Departamento de Registro e Controle Acadêmico (DRCA)	- Elevado número de dados pessoais tratados; - Elevado número de titulares; - Tratamento de dados pessoais de crianças e adolescentes
Processo Seletivo do Colégio Técnico (COLTEC)	Comissão Permanente de Vestibular (COPEVE)	- Elevado número de dados pessoais tratados; - Elevado número de titulares; - Tratamento de dados pessoais de crianças e adolescentes
Processo Seletivo do Centro Pedagógico (CP)		
Vestibular “Habilidades”		
Processo Seletivo do Teatro Universitário (TU)		
Admissão de servidores docentes	Pró-Reitoria de Recursos Humanos (PRORH)	- Elevado número de dados pessoais tratados; - Elevado número de titulares;
Admissão de servidores técnico-administrativos		
Acompanhamento Pedagógico	Núcleo de Acessibilidade e Inclusão (NAI)	- Tratamento de dados pessoais sensíveis e de crianças e adolescentes

Fonte: Elaborado pelo(s) autore(s) (2025).

5.2 Relatório de Impacto à Proteção de Dados Pessoais - RIPD

A elaboração do RIPD tem por finalidade atender às disposições dos artigos 4º, § 3º, 32 e 38 da LGPD. Trata-se, ainda, de um instrumento fundamental para a implementação do Controle 30 (Avaliação de Impacto, Monitoramento e Auditoria), conforme previsto no Guia do Framework de Privacidade e Segurança da Informação. O RIPD tem como objetivo registrar e documentar as medidas adotadas para a mitigação dos riscos identificados no tratamento de dados pessoais.

No caso concreto, os RIPDs dos processos selecionados para projeto-piloto foram elaborados pelos membros designados pela Auditoria-Geral e DGI, utilizando o *template* disponibilizado pelo PPSI. A maior parte dos tópicos do relatório é preenchido a partir das informações previamente incluídas no Inventário de Dados Pessoais, tais como a identificação dos agentes de tratamento e do encarregado, a descrição do tratamento (natureza, escopo, contexto e finalidade), necessidade e proporcionalidade.

A principal dificuldade enfrentada pela equipe durante o preenchimento do documento foi a ausência de metodologia de gestão de riscos na UFMG. Diante disso, os riscos e controles aplicáveis foram avaliados pela equipe designada, com fulcro na Norma ISO/IEC 29134:2017, nas orientações do MGI e no art. 5º, XVII da LGPD. Na oportunidade, a equipe designada avaliou quatorze riscos referentes ao tratamento de dados pessoais, previstos na Norma ISO/IEC 29134:2017. Esse procedimento tem inicio com a avaliação de probabilidade e impacto, a qual foi realizada por meio da aplicação de notas escalares, conforme quadro a seguir:

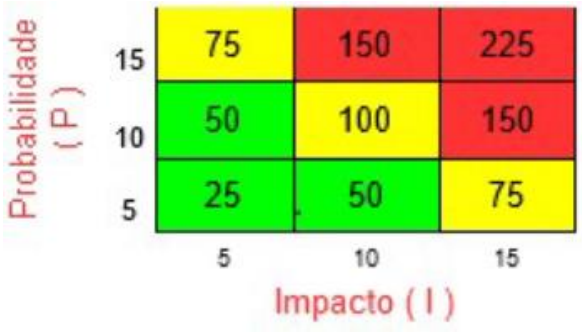
Quadro 3 - Classificação da Probabilidade (P) e Impacto (I)

Classificação	**Valor**
Baixo	5
Moderado	10
Alto	15

Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (2023).

Em seguida, para o cômputo do Nível de Risco adotou-se a expressão aritmética: PxI. A figura a seguir apresenta o Resultado da Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco. O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz. O enquadramento do risco em cada cor indica seu nível de risco: verde (25-50), é entendido como baixo; amarelo (75-100), representa risco moderado; vermelho (150-225), indica risco alto.

Figura 2 - Enquanto do nível de risco (PxI)



Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (2023).

Por fim, a equipe designada apurou os controles já implementados pela UFMG aplicáveis à cada risco. A fonte de informação para identificação dos controles foi a ferramenta preenchida pela Diretoria de Tecnologia da Informação da UFMG referente ao Ciclo 3 do PPSI. A partir da identificação das medidas e salvaguardas adotadas, apurou-se o nível de risco bem como seu valor residual.

No que tange à quantidade de RIPDs a serem elaborados, o MGI sugere que cada instituição avalie seus processos internos de trabalho, de forma a definir se elaborará um único documento para todas as operações de tratamento de dados pessoais ou um RIPD para cada projeto, sistema ou serviço (ANPD, 2023). Durante a realização do projeto-piloto, verificou-se que os controles de Privacidade e Segurança da Informação indicados pela DTI foram os mesmos em todos os diversos IDPs elaborados. Lado outro, verificou-se que os dados pessoais tratados variam de acordo com os processos selecionados. Nesse sentido, percebe-se que cada agente de tratamento identificado na UFMG concentra a gestão de serviços com finalidades correlatas. Por exemplo, a Pró Reitoria de Recursos Humanos - PRORH é responsável pela admissão de técnicos e docentes, processo em que ocorre intensa coleta de dados pessoais desse grupo. Posteriormente, tais dados, já coletados, podem ser objeto de tratamento em outros processos geridos pela PRORH, como a exoneração ou a concessão de benefícios. Ressalta-se, ainda, o fato de que, após envio de questionários junto aos órgãos superiores da UFMG, identificou-se que um pequeno grupo de unidades/órgãos é responsável pela gestão de grande parte dos processos que envolvem tratamento de dados pessoais de alto risco, conforme destacado no tópico a seguir. Dessa forma, avaliando o contexto institucional, a Auditoria-Geral e a DGI optaram pela elaboração de um RIPD para cada unidade/órgão responsável pela gestão de processos que envolvem tratamento de dados pessoais de alto risco.

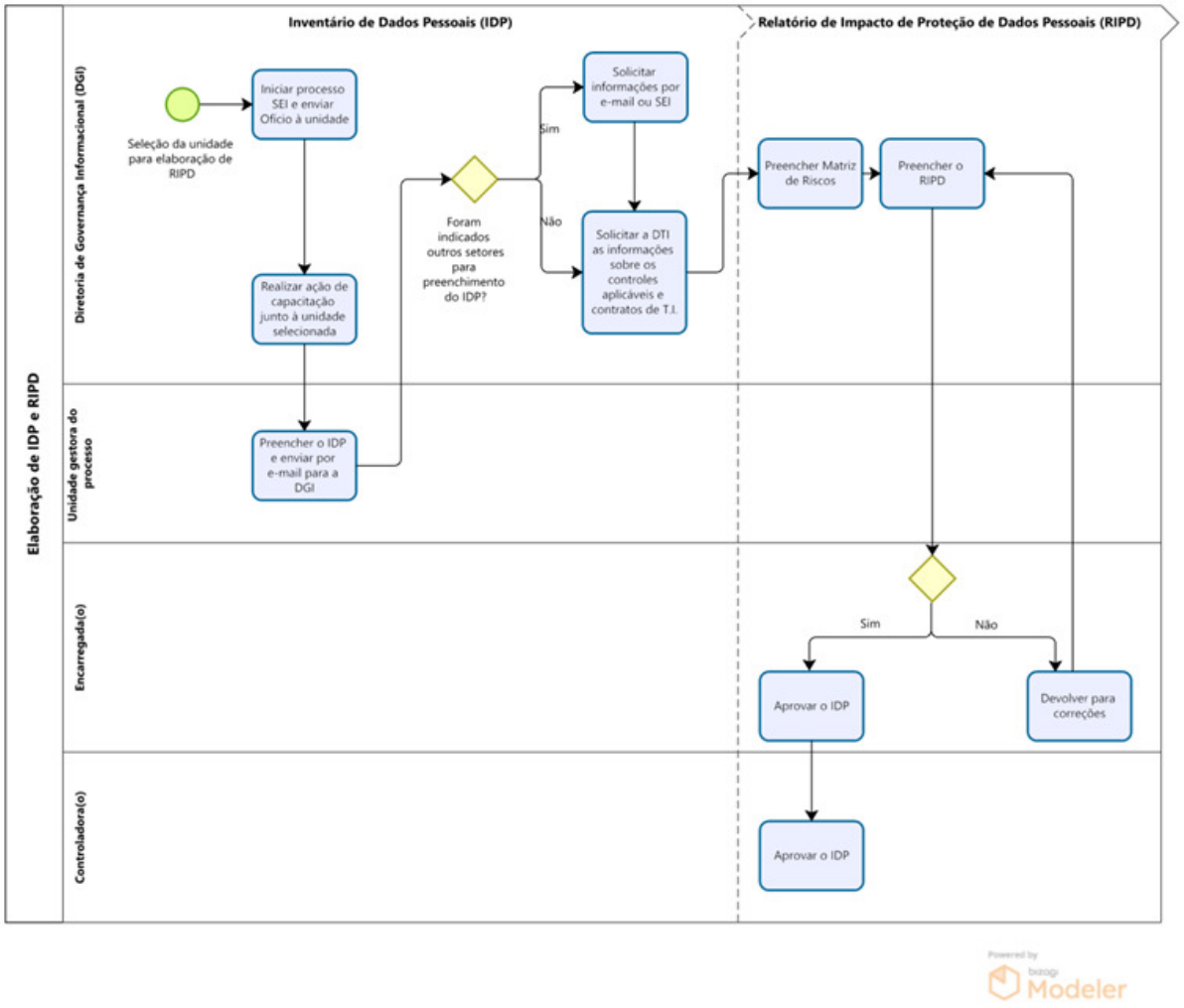
Assim, no âmbito do projeto piloto, foram elaborados quatro RIPDs, divididos por unidade responsável pela gestão de processos inventariados, que podem abranger um ou mais processos/serviços: (i) DRCA: processo de admissão via SISU; (ii) COPEVE: Processos Seletivos do COLTEC, CP, Teatro Universitário e Vestibular "Habilidades", (iii) PRORH: Nomeação e posse de servidores docentes e técnicos-administrativos; (iv) NAI: Acompanhamento Pedagógico[7].

5.3 Fluxo para a elaboração de IDPs e RIPDs

A complexidade inerente ao preenchimento dos IDPs é acentuada pela presença das seguintes limitações no âmbito da UFMG: (i) Ausência de bases de dados catalogadas pela Universidade no Catálogo de Bases de Dados do Governo Federal; (ii) Ausência de capacitação prévia sobre tratamento e proteção de dados pessoais. Ademais, a experiência com a elaboração dos IDPs eleitos para compor o projeto-piloto permitem identificar as seguintes oportunidades: (i) Os servidores lotados nos setores responsáveis pelos processos são os sujeitos mais indicados para fins de preenchimento do IDP, uma vez que detêm expertise na operação das demandas, desde que realizado um encontro de facilitação prévio; (ii) o *template* e o guia fornecidos pelo MGI fornecem orientações importantes para o preenchimento do documento; (iii) o(a)s servidores da Aud-Geral e DGI possuem a expertise necessária para consolidar e efetuar a análise crítica das informações inseridas pelas unidades gestoras no IDP e para avaliar riscos e controles no âmbito do RIPD.

Diante da complexidade da demanda e do elevado número de processos que tratam de dados pessoais, considerando ainda as oportunidades identificadas, a Auditoria-Geral disponibilizou à DGI um fluxo para a elaboração de IDPs e RIPDs de forma descentralizada, com participação ativa dos gestores de cada processo, sendo realizado um encontro prévio de capacitação, no formato de reunião ou oficina, priorizando processos que envolvam tratamento de alto risco. O referido fluxo é apresentado a seguir.

Figura 3 - Fluxo de trabalho desenvolvido pela Auditoria-Geral



Fonte: Elaborado pelo(s) autore(s) (2025).

6 CONTRIBUIÇÃO TECNOLÓGICA-SOCIAL

Ao longo do presente trabalho, foram apresentados os mecanismos adotados para intervir sobre uma situação-problema diagnosticada em um processo de adequação da organização às diretrizes da LGPD. A partir do modelo de conformidade proposto no âmbito do PPSI, foram aplicadas ferramentas de gestão de riscos, mapeamento de processo e diálogo com gestores para desenvolver controles internos voltados à proteção de dados pessoais na Universidade. Os objetivos definidos foram alcançados, com a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, Inventários de Dados Pessoais e de um fluxo replicável no âmbito da UFMG.

Os resultados do trabalho representam a implementação pela UFMG de dois importantes controles (19 e 30) previstos no PPSI. A institucionalização dos controles internos contribui para a mitigação de riscos como incidentes de vazamento e tratamento não lastreado em hipótese legal. Caso haja vazamento, os instrumentos contribuem para a rápida detecção de causas e pontos de fragilidade. Sob o viés social, as medidas de adequação à LGPD colaboram para a proteção de direitos fundamentais de liberdade e de privacidade e para o livre desenvolvimento da personalidade da pessoa natural.

Por fim, destaca-se que a plena efetivação dos benefícios oriundos das ações realizadas depende da expansão do trabalho pela gestão. Além disso, é preciso adotar medidas para difundir o conhecimento e a cultura de Privacidade e Segurança da Informação.

---

[1] O relatório foi fruto de auditoria que avaliou as ações realizadas pela Universidade Federal de Minas Gerais para fins de atendimento à legislação referente à gestão da informação, acesso à informação e controle social, mais precisamente no que tange à: publicação de Plano de Dados Abertos (PDA), abertura de conjuntos de dados para acesso ao público, classificação de informações, Serviço de Informação ao Cidadão (SIC) e Ouvidoria.

[2] A Nota Técnica, também fruto do trabalho de auditoria supracitado, apresenta a análise e encaminhamentos desta Auditoria Interna com fundamento nos resultados dos trabalhos de auditoria realizados sobre as medidas para atendimento às determinações da LGPD no âmbito da UFMG.

[3] De acordo com o art. 5º, VIII, da LGPD, encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

[4] De acordo com o art. 37 da LGPD: "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse." Para fins de atendimento da referida exigência, o instrumento sugerido pelo Governo Federal é o Inventário de Dados Pessoais (IDP), conforme Controle 19 (Inventário e Mapeamento) do Guia do Framework de Privacidade e Segurança da Informação, previsto no art. 7º da Portaria SGD/MGI n.º 852/2023.

[5] Fonte: Escritório de Governança de Dados Institucionais – EGDI. Consulta realizada em: 27.06.2025. Disponível em: < https://www.ufmg.br/egdi/>.

[6] Por serem documentos referentes à Segurança da Informação e Privacidade no âmbito da UFMG, os IDPs e RIPDs não poderão ser compartilhados em anexo ao presente artigo.

[7] Os RIPDs foram assinados pelos autores e pela encarregada, apresentados ao Grupo de Trabalho sobre LGPD e, até a presente data, se encontram em fase de assinatura pelo representante da controladora.

REFERÊNCIAS

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira: um estudo de caso. **Brazilian Journal of Business**, [S. l.], v. 2, n. 4, p. 3626–3648, 2020. Disponível em:

https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/18382. Acesso em: 30 jun. 2025.

CONTROLADORIA-GERAL DA UNIÃO (CGU). Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. **Diário Oficial da União**: seção 1, Brasília, DF, n. 96, p. 57, 20 maio 2016. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view. Acesso em: 30 jun. 2025.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito**, [S. l.], v. 14, n. 01, p. 01–20, 2022. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 30 jun. 2025.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). **Guia de Elaboração de Inventário de Dados Pessoais**: Programa de Privacidade e Segurança da Informação (PPSI). Versão 2.0. Brasília, DF: MGI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 30 jun. 2025.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). **Guia do Framework de Privacidade e Segurança da Informação**: Programa de Privacidade e Segurança da Informação (PPSI). Versão 1.1.4. Brasília, DF: MGI, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 30 jun. 2025.

SALES SARLET, G. B.; LINDEN RUARO, R. A Proteção de Dados Sensíveis no Sistema Normativo Brasileiro sob o Enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, [S. l.], v. 26, n. 2, p. 81–106, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 30 jun. 2025.

UNIVERSIDADE FEDERAL DE MINAS GERAIS (UFMG). Portaria nº 9.998, de 1º de novembro de 2023. Aprova as políticas para condução de serviços consultivos pela Auditoria-

Geral da Universidade Federal de Minas Gerais (UFMG). **Boletim Informativo da UFMG**, Belo Horizonte, n. 2197, 1 nov. 2023. Disponível em: https://www.ufmg.br/auditoria/wp-content/uploads/2023/12/PORTARIA-N%C2%BA-9998-DE-01-DE-NOVEMBRO-DE-2023.pdf. Acesso em: 30 jun. 2025.