Priorização de processos e ativos críticos à privacidade e à proteção de dados pessoais no contexto do PPSI 2.0

Raquel Chamone Barbosa
Virgínia de Melo Dantas Trinks

Resumo

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) impõe desafios significativos aos órgãos públicos, demandando a estruturação de práticas e mecanismos voltados à proteção de dados pessoais. Nesse contexto, o Programa de Privacidade e Segurança da Informação (PPSI 2.0) surge como iniciativa para apoiar a adequação institucional, adotando uma abordagem baseada em riscos e orientando a identificação e priorização dos processos e ativos mais relevantes para a proteção da privacidade. Entretanto, observa-se a ausência de métodos específicos voltados à priorização desses processos e ativos críticos sob a ótica da privacidade e da proteção de dados pessoais. Este trabalho propõe um modelo estruturado para a identificação e priorização desses elementos, por meio da adaptação da metodologia Análise das Joias da Coroa, tradicionalmente aplicada à segurança da informação. A pesquisa possui abordagem qualitativa, natureza aplicada e caráter exploratório-descritivo, fundamentando-se em revisão bibliográfica e análise de normas e frameworks, incluindo LGPD, PPSI 2.0, ISO/IEC 27701, GDPR e Resolução CD/ANPD nº 2/2022. Com base nesses referenciais, definem-se critérios de criticidade relacionados ao volume de tratamento, perfil dos titulares, natureza dos dados, uso de tecnologias emergentes, decisões automatizadas, grau de vigilância e impacto potencial sobre os direitos dos titulares. A aplicabilidade do modelo é demonstrada por meio de estudo de caso realizado na Agência Nacional de Aviação Civil (Anac). Os resultados indicam que a proposta contribui para orientar a priorização de ações e a alocação eficiente de recursos, fortalecendo a implementação de práticas de conformidade em privacidade e proteção de dados pessoais no setor público.

Palavras-chave: LGPD; gestão de riscos; privacidade; PPSI; Joias da Coroa.

1. Introdução

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), constitui o marco regulatório brasileiro sobre o tratamento de dados pessoais, tanto em meios físicos quanto digitais. Sua promulgação ocorreu em um cenário de transformação digital, caracterizado pelo crescimento do volume de dados e pela consolidação da economia da informação, em que a interconexão crescente entre sistemas e a coleta massiva de dados tornaram o indivíduo mais vulnerável e exigiram uma resposta normativa que estabelecesse limites, responsabilidades e sanções para o uso dessas informações (D'Oliveira; Cunha, 2024).

Sob essa premissa, a LGPD tem por objetivo resguardar os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade da pessoa natural, além de estabelecer normas claras para o tratamento de dados pessoais e instituir mecanismos de responsabilização e prestação de contas para as organizações que realizam esse tratamento (Brasil, 2018).

A efetiva implementação da LGPD, entretanto, não se concretiza sem desafios significativos. A conformidade com seus princípios e requisitos exige transformações organizacionais e envolve a estruturação de uma governança interna, o redesenho de processos, a capacitação contínua de colaboradores e a classificação rigorosa das informações. Inclui, ainda, a definição de critérios objetivos para retenção, preservação e descarte de dados, além da organização de atividades voltadas ao atendimento das exigências de órgãos fiscalizadores e da garantia dos direitos dos titulares (Souza, 2022).

Especificamente no setor público, esses desafios aumentam devido ao grande volume de dados sob custódia dos órgãos governamentais, à utilização de sistemas legados desatualizados e à complexidade administrativa que caracteriza suas estruturas (Souto; Motta, 2024).

Com o propósito de apoiar os órgãos e entidades da Administração Pública Federal na superação desses desafios, a Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) instituiu o Programa de Privacidade e Segurança da Informação (PPSI), por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023, posteriormente atualizado para a versão 2.0 pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. O programa caracteriza-se como um conjunto de projetos e processos voltados à adequação nas áreas de privacidade e segurança da informação, fundamentado nos valores de soberania, maturidade, resiliência, efetividade, colaboração e inteligência (Brasil, 2025).

Entre seus principais direcionadores, o PPSI 2.0 atribui à alta administração a responsabilidade pela gestão da privacidade e da segurança da informação, incluindo os riscos relacionados ao tratamento de dados pessoais. Essa diretriz é reforçada pela medida 0.17 do framework do programa, que estabelece a necessidade de implantação e manutenção de um processo formal e documentado de gestão de riscos associado às operações de tratamento de dados pessoais (Brasil, 2025). Além disso, o programa prevê a realização de diagnósticos de maturidade e a integração da gestão de riscos em privacidade e segurança da informação aos processos corporativos já existentes (Brasil, 2025).

Ao posicionar a gestão de riscos como um dos pilares para a efetividade das ações de privacidade e segurança da informação, o PPSI reforça uma abordagem amplamente reconhecida na literatura e nos modelos contemporâneos de governança. Nesse contexto, a gestão de riscos consiste em um conjunto de atividades coordenadas destinadas à identificação, análise, avaliação, tratamento e monitoramento de riscos, com o propósito de assegurar um nível razoável de confiança no alcance dos objetivos organizacionais (TCU, 2018). A adoção dessa abordagem assume papel central na construção de uma cultura organizacional orientada à conformidade e à governança corporativa, conforme destaca o COSO (2017), que enfatiza a integração entre gestão de riscos e desempenho estratégico.

A relevância da gestão de riscos para a implementação da LGPD é evidenciada pela própria legislação. Conforme observam Garbaccio e Kischelewski (2024), o termo "risco" é mencionado onze vezes ao longo da lei, refletindo a adoção de uma abordagem baseada em risco, amplamente incorporada por frameworks e modelos de governança da privacidade e proteção de dados pessoais.

A gestão de riscos envolve a determinação do valor de ativos de informação, a identificação das ameaças e vulnerabilidades existentes, a análise dos controles implementados e de seus respectivos efeitos sobre os riscos identificados. Adicionalmente, envolve a avaliação das possíveis consequências associadas a cada risco, o que possibilita sua priorização e classificação de acordo com os critérios de avaliação previamente definidos (Alves, 2021).

No campo da segurança da informação, diversas metodologias têm sido desenvolvidas com o objetivo de operacionalizar a priorização baseada em riscos. Entre elas, destaca-se a Análise das Joias da Coroa, método voltado à identificação de ativos críticos de tecnologia da informação a partir da missão organizacional (MITRE, 2021). Nessa mesma linha, Silva et al. (2025) identificaram critérios relevantes para a classificação de ativos críticos e, com base nessa priorização, estruturaram um modelo hierárquico que organiza os critérios e subcritérios de forma sistemática, permitindo sua aplicação na gestão de riscos e segurança cibernética.

Importa destacar que a definição dos processos e ativos críticos constitui etapa anterior à gestão de riscos, pois estabelece a base para a priorização do que será efetivamente analisado, bem como para a identificação e avaliação dos impactos potenciais. Conforme Silva et al. (2025), a relação de ativos e sua respectiva classificação constitui insumo para a avaliação de riscos, orientando a identificação de vulnerabilidades e ameaças.

Embora amplamente consolidada no âmbito da segurança da informação, essa lógica de priorização ainda encontra aplicação incipiente quando considerada sob o enfoque da privacidade e da proteção de dados pessoais. Considerando a realidade do setor público, em que limitações de recursos

humanos e orçamentários exigem a alocação eficiente de esforços (TCU, 2020), priorizar os processos e ativos a serem protegidos torna-se uma necessidade prática de gestão.

Diante dessa lacuna, o presente trabalho propõe um modelo estruturado para a priorização de processos e ativos críticos, aplicável à realidade de órgãos e entidades públicas, com a finalidade de subsidiar a gestão de riscos à privacidade e à proteção de dados pessoais prevista no PPSI 2.0.

Como objetivos específicos, propõe-se: (i) analisar as similaridades e complementaridades entre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a *Privacy Impact Assessment* (PIA) e a metodologia Análise das Joias da Coroa; (ii) avaliar a aplicabilidade dessa metodologia ao contexto da privacidade e do Programa de Privacidade e Segurança da Informação (PPSI); e (iii) validar o modelo proposto por meio de um estudo de caso aplicado à Agência Nacional de Aviação Civil (Anac).

Para tanto, este trabalho está estruturado da seguinte forma: a Seção 2 discute o referencial teórico, contemplando produções acadêmicas, normas técnicas, guias institucionais e marcos regulatórios relacionados à abordagem baseada em riscos, proteção de dados pessoais e privacidade, incluindo análise da metodologia Análises das Joias da Coroa; a Seção 3 descreve a metodologia adotada; a Seção 4 detalha o modelo proposto e sua aplicação por meio de estudo de caso; e a Seção 5 analisa os resultados obtidos; e a Seção 6 apresenta as conclusões e sugestões para pesquisas futuras.

2. Referencial teórico

2.1. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto no Art. 5º, inciso XVII, da LGPD, consiste em um documento que descreve os processos de tratamento de dados que possam gerar riscos às liberdades e aos direitos fundamentais, bem como os mecanismos adotados para a mitigação desses riscos (BRASIL, 2018).

O RIPD integra-se à gestão de riscos de privacidade, funcionando como um instrumento estruturado para identificar, avaliar e mitigar impactos do tratamento de dados pessoais. Ao promover a conformidade com a LGPD e as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD), o RIPD fortalece a governança de dados, protege os direitos dos titulares e promove maior transparência nas relações entre controladores e titulares. Além disso, sua implementação favorece a adoção de práticas responsáveis e em conformidade com a legislação, garantindo que os impactos do tratamento de dados sejam adequadamente monitorados e tratados (Silva, 2025).

Segundo Silva (2025), o RIPD é uma ferramenta fundamental para garantir a conformidade com a LGPD. Entretanto, sua implementação ainda enfrenta desafios, incluindo a ausência de critérios objetivos e padronizados para sua elaboração, a insuficiente capacitação técnica das equipes envolvidas e a prevalência de abordagens reativas, muitas vezes motivadas unicamente por exigências regulatórias ou pelas sanções impostas pela ANPD. Tais limitações evidenciam a necessidade de aprimoramentos metodológicos e investimentos em qualificação para assegurar que o RIPD cumpra plenamente seu papel de proteger os dados pessoais.

Reconhecendo a importância desse instrumento para a governança da privacidade, a Secretaria de Governo Digital (SGD) publicou, em 2020, o Guia de Boas Práticas da Lei Geral de Proteção de Dados Pessoais (LGPD). Nesse documento, o RIPD é apresentado como um importante mecanismo de verificação e demonstração da conformidade das atividades de tratamento de dados pessoais realizadas pelas instituições, servindo de subsídio tanto para a análise dos riscos quanto para o registro e a documentação das medidas adotadas. Adicionalmente, a Seção 2.5 do guia apresenta orientações destinadas a apoiar órgãos e entidades públicas na elaboração do relatório, contribuindo para sua padronização e aplicação prática.

2.2. Privacy Impact Assessment (PIA)

O *Privacy Impact Assessment* (PIA) é uma metodologia estruturada voltada à identificação, análise e mitigação de potenciais impactos negativos à privacidade decorrentes de projetos, políticas, programas, serviços, produtos ou outras iniciativas. O processo envolve a participação das partes interessadas e a definição de ações corretivas necessárias para evitar ou reduzir tais impactos. Assim, o

PIA deve ser compreendido como parte integrante da gestão de riscos da organização, e não apenas como um procedimento de conformidade (Wright, 2012).

A ISO/IEC 27701 estabelece que os riscos à privacidade devem ser avaliados por meio de uma PIA, considerando a natureza, o contexto e a finalidade do tratamento de dados pessoais. Essa avaliação deve abranger critérios que indiquem maior potencial de risco aos titulares, como a realização de decisões automatizadas que produzam efeitos legais ou significativos, o tratamento em larga escala de categorias especiais de dados pessoais, incluindo informações relativas à saúde, origem étnica ou racial e opinião política, ou o monitoramento sistemático de áreas acessíveis ao público em larga escala. Tais elementos orientam a identificação de cenários de alto impacto e servem de base para definir controles de mitigação proporcionais à sensibilidade e à exposição do tratamento.

De forma similar, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) estabelece que o *Data Protection Impact Assessment* (DPIA) é obrigatório sempre que o tratamento envolver a avaliação sistemática e abrangente de aspectos pessoais, incluindo decisões automatizadas com efeitos legais ou significativos; tratamento em larga escala de categorias especiais de dados, como dados genéticos e origem racial/étnica ou dados relativos à condenações penais; ou monitoramento sistemático em larga escala de locais públicos (União Europeia, 2016).

2.3. Identificação e priorização de ativos críticos: o conceito de Joias da Coroa da segurança da informação

No âmbito da segurança da informação e da gestão de riscos, o conceito de Joias da Coroa refere-se aos dados e sistemas mais sensíveis ou críticos que, se comprometidos, podem gerar danos significativos à organização e aos titulares dos dados. Conforme define a MITRE (2021), esses ativos são elementos essenciais cuja proteção deve ser priorizada para garantir a continuidade operacional e a resiliência institucional.

No que se refere à gestão de riscos em segurança da informação, a identificação de ativos é reconhecida como etapa essencial e determinante para a avaliação eficaz dos riscos organizacionais, pois apenas com um inventário abrangente e detalhado pode-se avaliar corretamente ameaças, vulnerabilidades e impactos potenciais. O estudo de Shedden et al. (2016) destaca que as metodologias tradicionais de avaliação de riscos frequentemente são limitadas por uma visão restrita dos ativos, e propõe uma abordagem mais ampla que considera ativos formais e informais, oferecendo maior granularidade e cobertura no processo de identificação de ativos e destacando a importância de reconhecer ativos críticos de conhecimento e práticas de negócio que geralmente são negligenciados nas avaliações convencionais. Essa perspectiva reforça que a identificação e classificação adequada dos ativos é condição prévia para a posterior priorização baseada nos riscos efetivos que esses ativos representam para a organização.

De acordo com Parkkinen (2023), a proteção eficaz dos ativos de informação pressupõe o seu pleno conhecimento. Assim, o primeiro passo consiste em reconhecer e localizar as chamadas Joias da Coroa, ou seja, os ativos mais sensíveis e críticos para a organização. Em última análise, a priorização da proteção deve ser proporcional ao valor, sensibilidade e criticidade que cada ativo possui para a missão e os objetivos estratégicos da entidade, reforçando a premissa de que a segurança deve ser aplicada de forma direcionada e inteligente.

Faria (2022) propõe um ciclo de vida para a estratégia de cibersegurança, no qual a etapa de identificação de recursos, requisitos e regulamentações desempenha papel fundamental. Nessa fase, recomenda-se priorizar os ativos e sistemas mais críticos ou estratégicos antes de avançar para os de menor relevância, permitindo alocação mais eficiente de esforços e recursos. O autor observa ainda que, ao chegar a essa etapa, é comum constatar que o escopo inicial definido é excessivamente amplo, o que pode comprometer a eficácia das etapas subsequentes da gestão de riscos.

Essa abordagem proativa, centrada na identificação de ativos, constitui uma etapa preliminar essencial ao processo de gestão de riscos. Segundo Silva et al. (2025), esse reconhecimento estruturado dos recursos críticos orienta os esforços de segurança da informação, pois permite priorizar os ativos conforme seu grau de criticidade no contexto organizacional. A listagem e categorização resultantes servem como insumo fundamental para a avaliação de riscos subsequente, estabelecendo uma base

consistente para a identificação de vulnerabilidades e ameaças. No entanto, o processo de identificação e classificação desses ativos não é trivial; como apontado por Forbes (2018), ele se constitui em uma tarefa complexa que demanda investimento significativo de tempo, esforço e coordenação entre as diversas áreas da organização.

Em consonância com essa necessidade, a identificação e proteção de processos e ativos críticos constituem etapas centrais na gestão de riscos e na continuidade de negócios, sendo amplamente preconizadas pelas principais normas internacionais. A ISO/IEC 27001:2022, por exemplo, em seus controles 5.29 e 5.30 (Gestão da Continuidade da Segurança da Informação), estabelece a necessidade de integrar a segurança da informação aos planos de continuidade organizacional, visando garantir a manutenção e a rápida restauração de operações essenciais diante de interrupções ou incidentes.

Nesse sentido, torna-se mandatório identificar processos críticos, mapear ativos e implementar planos de resposta estruturados, com testes periódicos para assegurar a resiliência operacional. Em complemento, a ISO/IEC 27005:2022 orienta que a identificação de processos e ativos deve abranger não apenas recursos tecnológicos, mas também os processos de negócio que sustentam os objetivos estratégicos, permitindo uma avaliação abrangente de impactos e vulnerabilidades.

2.4. Metodologia Análise das Joias da Coroa

A metodologia Análise das Joias da Coroa é um processo estruturado e repetível, originalmente desenvolvido para priorizar a segurança de ativos de informação com base em sua criticidade para a missão e continuidade operacional da organização (MITRE, 2021).

De acordo com Silva et al. (2025), os critérios mais relevantes para a classificação das Joias da Coroa da segurança da informação envolvem múltiplas dimensões que refletem tanto a importância estratégica quanto os riscos associados à sua indisponibilidade ou comprometimento. Os autores destacam cinco critérios principais: Missão da Organização, que diz respeito à relevância do ativo para a continuidade operacional e o cumprimento da missão institucional; Imagem e Reputação, que avalia o impacto na confiança pública e nas parcerias estratégicas; Volume de Usuários Afetados, que considera a quantidade e a criticidade dos usuários impactados; Impacto Financeiro, relacionado aos custos diretos, perdas indiretas e eventuais penalidades; e Impacto Legal/Regulatório, que aborda a conformidade com legislações aplicáveis.

Silva et al. (2025) em seu estudo *International Perspectives on Critical Infrastructure: Evaluation Criteria and Definitions*, realizaram uma análise abrangente das definições e dos critérios empregados na seleção de infraestruturas críticas em diferentes países. O estudo identificou que cinco critérios se destacam nesse processo: impacto sobre as pessoas, impacto social, impacto econômico, impacto geográfico e impacto por interdependência. Outros critérios, como impacto ambiental e duração dos efeitos, foram observados com menor frequência. Os resultados evidenciam que os critérios relacionados a impactos humanos e sociais apresentam maior relevância e recorrência entre as nações analisadas, refletindo uma tendência global de priorização de aspectos sociais e de bem-estar na definição de infraestruturas críticas.

2.5. Identificação e priorização de ativos críticos de privacidade e proteção de dados pessoais

A identificação dos ativos críticos também assume um papel estratégico para a privacidade e proteção de dados pessoais. A ISO/IEC 27701:2019 (ABNT, 2019) e o *NIST Privacy Framework* (2020) estabelecem que o mapeamento de processos e ativos que tratam informações pessoais é essencial para a avaliação e mitigação dos riscos à privacidade. Em conformidade com essas diretrizes que orientam a integração da privacidade à gestão de riscos corporativos, a análise de criticidade permite que a organização direcione seus recursos de forma eficiente, implementando controles de segurança proporcionais aos riscos identificados. Tal priorização evita a dispersão de esforços, assegurando que as medidas de proteção incidam sobre os elementos mais relevantes para a confidencialidade, integridade e disponibilidade das informações pessoais, reforçando assim a governança e a resiliência institucional (MITRE, 2021; ABNT, 2019; NIST, 2020).

Sob a perspectiva da Lei Geral de Proteção de Dados Pessoais (LGPD), a definição das Joias da Coroa permite alocar e priorizar recursos e controles de segurança conforme o grau de criticidade e o impacto potencial de incidentes. Dessa forma, a organização asseguraria que as medidas de mitigação sejam proporcionais aos riscos associados à violação de dados, não apenas fortalecendo a governança da informação, mas também promovendo a conformidade regulatória e a proteção efetiva dos direitos dos titulares de dados.

3. Metodologia

A presente pesquisa tem abordagem qualitativa, de natureza aplicada, com caráter exploratório e descritivo.

Como primeira etapa metodológica, realiza-se uma revisão bibliográfica, incluindo a análise da própria LGPD, PPSI, materiais da ANPD, normas e frameworks pertinentes, como as famílias ISO/IEC 27000 e 27701, e produções acadêmicas, com vistas a construir um referencial teórico-analítico que fundamente a proposição do modelo.

Em seguida, à luz dos referenciais teóricos, normativos e institucionais apresentados, são definidos critérios voltados à priorização de processos e ativos críticos sob a ótica da privacidade e da proteção de dados pessoais, visando subsidiar a implementação proporcional, progressiva e orientada a riscos das medidas previstas na LGPD e no PPSI 2.0.

A principal inovação do modelo proposto reside na adaptação estruturada da metodologia Análise das Joias da Coroa ao campo da privacidade e da proteção de dados pessoais, incorporando critérios normativos de alto risco previstos na LGPD e na Resolução CD/ANPD nº 2/2022.

3.1. Definição dos critérios de criticidade

A definição dos critérios de criticidade tem como finalidade estabelecer parâmetros objetivos para avaliar o impacto potencial de incidentes, falhas ou violações que afetem o tratamento de dados pessoais e os direitos dos titulares. Essa etapa permite identificar os ativos e atividades mais sensíveis à privacidade dos titulares de dados e ao cumprimento das obrigações legais e regulatórias.

A definição dos critérios para a identificação e hierarquização dos processos e ativos críticos ocorre a partir da análise comparativa de referenciais normativos e técnicos, especialmente a Resolução CD/ANPD nº 2/2022 e a ISO/IEC 27701, complementados por diretrizes do GDPR. São selecionados os critérios com maior recorrência e aderência ao conceito de alto risco à privacidade e à proteção de dados pessoais, priorizando aqueles diretamente relacionados ao potencial de impacto sobre os direitos e liberdades dos titulares. Adicionalmente, são desconsiderados critérios estritamente técnicos de segurança da informação que não apresentam relação direta com a dimensão da privacidade.

Nesse sentido, recomenda-se adotar os seguintes critérios: tratamento em larga escala, categoria de titulares afetados, sensibilidade dos dados, natureza da ferramenta e monitoramento/vigilância de locais públicos em larga escala. Essa abordagem permite à organização estabelecer uma base estruturada para priorizar ações de mitigação de riscos e direcionar recursos de forma proporcional e eficiente.

Tabela 1: Critérios para avaliação da criticidade de processos e ativos

Critério	Base normativa	Descrição
Volume e escala do tratamento	Critério de alto risco da Resolução CD/ANPD nº 2/2022	Quantidade de titulares cujos dados seriam comprometidos
Perfil dos titulares	Critério de alto risco da Resolução CD/ANPD nº 2/2022	Tratamento de dados de categorias vulneráveis: crianças, adolescentes ou idosos
Natureza dos dados tratados	Critério de alto risco da Resolução CD/ANPD nº 2/2022, critério para avaliação de impacto à privacidade da ISO/IEC 27701	Volume e tipos de dados sensíveis tratados
Uso de tecnologias emergentes e Inteligência Artificial	Critério de alto risco da Resolução CD/ANPD nº 2/2022	Utilização de Inteligência Artificial - IA ou outras tecnologias emergentes
Automação e tomada de decisão	Critério de alto risco da Resolução CD/ANPD nº 2/2022, critério para	Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas

	avaliação de impacto à privacidade da ISO/IEC 27701	destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular Para a ISO/IEC: decisões automatizadas e que produzem efeitos legais ou impactos significativos sobre os titulares
Grau de vigilância ou exposição	Critério de alto risco da Resolução CD/ANPD nº 2/2022, critério para avaliação de impacto à privacidade da ISO/IEC 27701	Monitoramento ou vigilância sistemática de áreas acessíveis ao público, em larga escala
Impacto potencial aos direitos dos titulares	Critério de alto risco da Resolução CD/ANPD nº 2/2022, critério para avaliação de impacto à privacidade da ISO/IEC 27701	Tratamento de dados pessoais que possa afetar significativamente os interesses e direitos fundamentais dos titulares A ISO/IEC 27701 também orienta que a organização considere: ● a natureza, o escopo, o contexto e as finalidades do tratamento; ● se há potencial impacto relevante sobre direitos e liberdades dos titulares

3.2. Mapeamento dos processos que tratam dados pessoais e suas características

Esta etapa consiste em elencar todos os processos da organização que envolvem tratamento de dados pessoais, destacando para cada processo as seguintes informações:

- A quantidade de titulares e o volume de dados tratados.
- A natureza dos dados tratados (comuns ou sensíveis);
- Tratamento de dados pessoais de grupos vulneráveis (crianças, adolescentes, idosos);
- Uso de tecnologias emergentes e Inteligência Artificial;
- A existência de decisões automatizadas;
- Grau de vigilância e exposição; e
- Possíveis impactos sobre os direitos dos titulares.

3.3. Identificação dos ativos

Para cada processo mapeado, são identificados os ativos essenciais à execução segura e contínua das atividades, incluindo dados, softwares, hardwares, sistemas, infraestrutura e pessoas.

A interrupção ou comprometimento de qualquer um desses elementos pode representar falha operacional e risco direto à privacidade dos titulares.

3.4. Reconhecimento dos Ativos Críticos (As Joias da Coroa)

Nesta etapa, identifica-se o subconjunto de processos e ativos, ou Joias da Coroa da Privacidade cujo comprometimento causaria a falha da função essencial do sistema ou colocaria em risco a missão de privacidade da organização.

Para avaliar a criticidade dos ativos, propõe-se a análise das dimensões previamente definidas na etapa inicial, utilizando uma escala de quatro níveis de criticidade: Baixa, Moderada, Alta e Crítica, conforme apresentado na tabela a seguir.

Tabela 2: Escala de impacto dos ativos sobre a privacidade

Pontuação	Descrição do Impacto
0 (inexistente)	O critério não se aplica ao ativo ou processo, ou não há impacto identificável à privacidade.
1 (Baixo)	Impacto insignificante ou facilmente contido.
2 (Moderado)	Impacto limitado, com efeito reversível.
3 (Alto)	Impacto relevante e de recuperação difícil.
4 (Crítico)	Impacto severo, com danos permanentes ou sistêmicos.

Fonte: Elaboração própria (2026).

A soma dos critérios avaliados determina o nível de criticidade geral do ativo ou processo:

Tabela 3: Níveis de criticidade dos ativos

Faixa de Pontuação	Classificação
até 10 pontos	Baixa
11 – 15 pontos	Moderada
16 – 20 pontos	Alta
acima de 20	Crítica

Fonte: Elaboração própria (2026).

4. Proposta de Modelo para Priorização de Processos e Ativos Críticos

Considerando a lacuna identificada na literatura quanto à aplicação de métodos estruturados de priorização no âmbito da privacidade, esta seção apresenta uma adaptação da metodologia Análise das Joias da Coroa ao contexto da LGPD e do PPSI 2.0. A proposta tem por finalidade subsidiar a identificação e a priorização de processos e ativos críticos para a gestão de riscos à privacidade e à proteção de dados pessoais e demonstrar sua aplicabilidade por meio de estudo de caso na Anac.

4.1. Fundamentação da Adaptação da metodologia Análise das Joias da Coroa da privacidade

Esta seção apresenta os fundamentos que embasam a adaptação da metodologia Análise das Joias da Coroa ao contexto da privacidade. Originalmente desenvolvida para identificar e priorizar os ativos mais críticos de uma organização sob a perspectiva da segurança da informação, a metodologia é reinterpretada neste trabalho para apoiar a identificação dos processos e ativos de tratamento de dados que apresentam maior potencial de impacto aos direitos e liberdades dos titulares.

Para tanto, são analisadas as relações entre a metodologia das Joias da Coroa e os principais instrumentos de avaliação de riscos à privacidade, o RIPD e a PIA. Em seguida, são discutidos os critérios normativos e conceituais que podem subsidiar a identificação de processos críticos para a privacidade, bem como a aderência dessa abordagem aos direcionamentos do PPSI, especialmente no que se refere ao fortalecimento da gestão de riscos.

4.1.1. Comparativo entre RIPD, PIA e Joias da Coroa

O RIPD é o instrumento previsto na LGPD para avaliar e demonstrar os riscos envolvidos no tratamento de dados pessoais, especialmente quando há alto risco aos titulares. De forma similar, o PIA é uma metodologia mais ampla e internacionalmente difundida para análise prévia de impactos à privacidade, com abordagem estruturada de identificação, mitigação e monitoramento de riscos. Embora apresentem diferenças quanto ao ambiente regulatório, ao grau de formalização e aos requisitos documentais, ambos possuem como objetivo central apoiar a gestão dos riscos à privacidade e subsidiar a tomada de decisão pelos agentes de tratamento.

Por sua vez, a metodologia Análise das Joias da Coroa possui uma finalidade distinta, porém complementar. Em vez de se concentrar na avaliação detalhada dos riscos de uma operação específica, busca identificar e priorizar os ativos ou processos considerados mais críticos para a organização. Essa

priorização permite direcionar recursos, esforços de governança e mecanismos de proteção para os elementos cuja materialização de riscos pode produzir os impactos mais significativos.

Dessa forma, as metodologias desempenham papéis complementares no processo de gestão de riscos. Enquanto a Análise das Joias da Coroa auxilia na identificação e priorização dos processos e ativos que demandam maior atenção institucional, o RIPD e o PIA fornecem mecanismos estruturados para a avaliação detalhada, o tratamento e o monitoramento dos riscos associados a essas atividades. Nesse contexto, a identificação das Joias da Coroa pode subsidiar a decisão sobre quais processos ou operações de tratamento devem ser submetidos à elaboração de RIPDs ou PIAs, permitindo que a organização concentre seus esforços de avaliação nos tratamentos com maior potencial de impacto à privacidade. Em conjunto, esses instrumentos contribuem para uma abordagem baseada em riscos, fortalecendo a governança em privacidade.

4.1.2. Metodologia Análise das Joias da Coroa para a privacidade

A metodologia Análise das Joias da Coroa, adaptada à privacidade, transcende o foco tradicional em ativos puramente tecnológicos para centrar-se nos processos de negócio que tratam dados pessoais.

Segundo Wairimu et al. (2024), a principal diferença entre a avaliação de riscos de privacidade e a avaliação de riscos de segurança está no foco prioritário: enquanto a avaliação de riscos de privacidade considera, em primeiro plano, o potencial de danos aos titulares dos dados, na avaliação de riscos de segurança esse aspecto assume um papel secundário. Dessa forma, ao transpor a lógica de Joias da Coroa para o ecossistema de privacidade, a análise de criticidade deve abranger não apenas os impactos técnicos e organizacionais, mas, prioritariamente, o potencial de dano aos direitos e liberdades fundamentais dos titulares, deslocando o eixo da proteção do ativo para a proteção do indivíduo.

Segundo Menke (2022), embora o GDPR não defina expressamente o que caracteriza "alto risco", o Conselho Europeu de Proteção de Dados (*European Data Protection Board* – EDPB) elaborou parâmetros a serem considerados na identificação de operações de tratamento que possam representar riscos elevados, os quais podem, inclusive, subsidiar a elaboração das listas das autoridades de controle. Conforme as diretrizes do EDPB, são indicativos de alto risco atividades de tratamento que envolvem, entre outros aspectos, avaliação e pontuação de titulares (incluindo perfis e previsões sobre aspectos como saúde, preferências ou comportamento), decisões automatizadas com efeitos legais, monitoramento sistemático, tratamento de dados sensíveis, processamento em larga escala, combinação de conjuntos de dados de diferentes origens, tratamento de dados de titulares vulneráveis, operações que impeçam o exercício de direitos pelos titulares, e o uso inovador de tecnologias ou soluções organizacionais que possam impactar significativamente direitos fundamentais. Estes parâmetros não apenas orientam a necessidade de realizar avaliações de impacto à proteção de dados (DPIAs), mas também podem ser utilizados como critérios auxiliares para a identificação e priorização de processos e ativos críticos para a privacidade, dado que tais operações possuem maior potencial de causar prejuízos aos direitos dos titulares.

A Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, estabelece que são considerados de alto risco as operações que atendam cumulativamente a pelo menos um critério geral e um critério específico. Entre os critérios gerais, incluem-se o tratamento de dados pessoais em larga escala e aquele que possa afetar significativamente os interesses e direitos fundamentais dos titulares. Já os critérios específicos abrangem o uso de tecnologias emergentes ou inovadoras, a vigilância ou monitoramento de áreas acessíveis ao público, a tomada de decisões baseadas exclusivamente em tratamento automatizado de dados pessoais, e a utilização de dados pessoais sensíveis ou de crianças, adolescentes e idosos.

Complementarmente, a ANPD publicou o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, com o objetivo de auxiliar órgãos e entidades públicas na adequação à LGPD, fornecendo orientações sobre as bases legais aplicáveis, os princípios que regem o tratamento de dados pessoais e os aspectos relacionados ao compartilhamento e à divulgação de informações no setor público. Embora não trate especificamente da identificação de tratamentos de alto risco, o documento fornece diretrizes relevantes para a compreensão dos riscos inerentes às operações de tratamento realizadas por órgãos e entidades públicas (ANPD, 2023).

Assim, entende-se que as Joias da Coroa da Privacidade ou, em outras palavras, processos e ativos críticos sob a ótica da privacidade estão diretamente relacionados ao seu potencial de gerar riscos significativos aos indivíduos e à coletividade, refletindo o grau de impacto que o tratamento de dados pode ocasionar à privacidade, à autodeterminação informativa e à confiança social. Para sua identificação e priorização, podem ser utilizados os critérios de tratamento de alto risco previstos na Resolução CD/ANPD nº 2/2022 e os parâmetros estabelecidos pelo GDPR e pela ISO/IEC 27701 para a realização de avaliações de impacto à proteção de dados (PIA/DPIA). Essa abordagem reforça a centralidade do titular e promove a priorização dos ativos críticos com base não apenas na continuidade operacional, mas também na salvaguarda dos direitos fundamentais à privacidade e à proteção de dados pessoais.

4.1.3. As Joias da Coroa no âmbito do PPSI

O Framework do PPSI 2.0 estabelece que a gestão de riscos associada às operações de tratamento de dados pessoais deve contemplar, necessariamente, a definição, a aplicação e a avaliação de medidas de segurança técnicas e administrativas aptas a proteger as informações pessoais (BRASIL, 2025).

Nesse contexto normativo e, considerando o referencial teórico apresentado ao longo deste trabalho, a identificação dos processos e ativos críticos, as Joias da Coroa da Privacidade, fortalece a gestão de riscos e contribui para a efetividade das medidas previstas no PPSI, ao possibilitar a concentração dos esforços institucionais naqueles elementos que concentram os riscos mais relevantes.

Adicionalmente, a definição dessas Joias da Coroa mostra-se relevante em cenários institucionais caracterizados por restrições orçamentárias e limitações de pessoal, nos quais se torna inviável a implementação simultânea e abrangente de todas as medidas de privacidade e segurança da informação previstas nos frameworks de referência.

4.2. Modelo Proposto

Com base no referencial teórico apresentado e nas etapas metodológicas descritas na Seção 3, propõe-se um modelo estruturado para a identificação e priorização de processos e ativos críticos sob a ótica da privacidade e da proteção de dados pessoais, conforme apresentado na Figura 1:

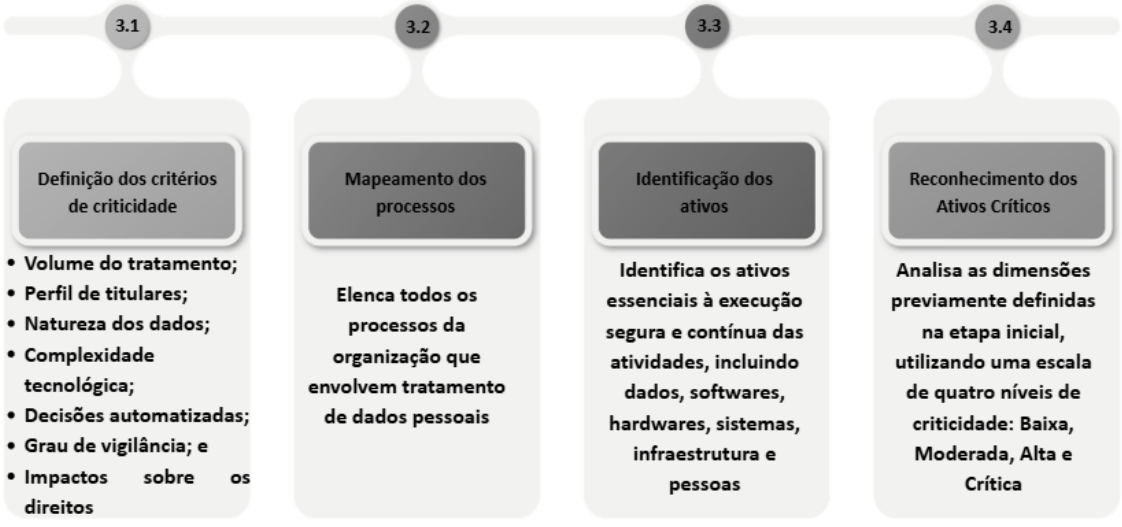

Figura 1 – Metodologia para identificação dos ativos críticos para privacidade
Fonte: Elaboração própria (2026).

O modelo proposto fundamenta-se em critérios relacionados às características do tratamento de dados pessoais e aos potenciais riscos à privacidade dos titulares. Para cada critério, foi estabelecida uma escala de avaliação variando de 1 (baixo) a 4 (crítico), permitindo mensurar o nível de criticidade dos processos e ativos analisados. A Tabela 4 apresenta os critérios e as respectivas faixas de pontuação utilizadas na avaliação.

Tabela 4 – Critérios para avaliação da criticidade de processos e ativos

Critério	Impacto 0 (inexistente)	Impacto 1 (Baixo)	Impacto 2 (Moderado)	Impacto 3 (Alto)	Impacto 4 (Crítico)
1 - Volume e Escala de tratamento	O critério não se aplica ao ativo ou processo	Até 1.000 titulares	De 1.001 a 10.000 titulares	De 10.001 a 50.000 titulares	Acima de 50.000 titulares
2 - Natureza dos dados tratados	O critério não se aplica ao ativo ou processo	Apenas dados cadastrais básicos (nome, e-mail, telefone, endereço)	Dados pessoais comuns associados a informações profissionais, financeiras ou de localização	Dados cuja exposição possa gerar discriminação, fraude ou danos relevantes ao titular	Dados pessoais sensíveis (saúde, biometria, origem racial, convicções religiosas, filiação sindical etc.)
3- Tratamento de dados de grupos vulneráveis	O critério não se aplica ao ativo ou processo	Tratamento eventual ou indireto envolvendo grupos vulneráveis, sem foco específico	Envolve idosos	Envolve adolescentes	Envolve crianças ou múltiplos grupos vulneráveis simultaneamente
4 - Uso de tecnologias emergentes e Inteligência Artificial	O critério não se aplica ao ativo ou processo	Utiliza sistemas convencionais sem IA ou tecnologias emergentes	Utiliza automações simples ou ferramentas analíticas de baixo impacto	Utiliza IA ou tecnologias emergentes como suporte à tomada de decisão	Utiliza IA ou tecnologias emergentes capazes de produzir impactos significativos sobre direitos ou interesses dos titulares
5 - Decisões automatizadas	O critério não se aplica ao ativo ou processo	Automatizações meramente operacionais, sem produção de decisões sobre titulares	Automatizações sem efeitos relevantes ao titular	Decisões automatizadas sujeitas à revisão humana	Decisões automatizadas com efeitos legais ou impactos significativos sobre os titulares
6 - Grau de vigilância ou exposição	O critério não se aplica ao ativo ou processo	Monitoramento limitado para fins operacionais ou de segurança, com baixa capacidade de identificação dos titulares	Monitoramento pontual e restrito a ambientes controlados	Monitoramento sistemático de grupos ou ambientes específicos	Vigilância ou monitoramento sistemático em larga escala de áreas acessíveis ao público
7 - Impacto potencial sobre os direitos dos titulares	O critério não se aplica ao ativo ou processo	Impacto insignificante ou facilmente reversível	Impacto limitado e reversível	Impacto relevante, com recuperação difícil ou custos significativos ao titular	Impacto severo, permanente ou sistêmico sobre direitos e liberdades fundamentais

Fonte: Elaboração própria (2026).

A partir da aplicação desses critérios, cada processo ou ativo recebe uma pontuação correspondente ao seu nível de exposição aos riscos de privacidade. A soma das pontuações possibilita sua classificação em diferentes níveis de criticidade, subsidiando a priorização de ações de gestão de riscos, a elaboração de RIPD e a implementação de controles de proteção de dados pessoais.

4.3. Estudo de caso: aplicação do modelo em uma Agência Reguladora:

Com o intuito de demonstrar a aplicabilidade prática do modelo proposto, apresenta-se um estudo de caso referente à sua implementação no âmbito da Agência Nacional de Aviação Civil (Anac).

Inicialmente, realiza-se o mapeamento dos processos institucionais que envolvem o tratamento de dados pessoais, bem como dos respectivos ativos de informação a eles associados. A partir desse levantamento, são selecionados cinco processos para análise no escopo deste trabalho: pessoal da aviação civil, habilitação AVSEC, cadastro de usuários externos no protocolo eletrônico, cadastro no portal de capacitação e autorização provisória para balões.

A seleção desses processos tem como finalidade assegurar a representatividade e a abrangência do estudo, contemplando atividades tanto das áreas finalísticas quanto das áreas meio, sob a responsabilidade de diferentes unidades organizacionais e suportadas por distintos sistemas de informação. Essa diversidade possibilita avaliar a aplicação do modelo em cenários organizacionais e tecnológicos heterogêneos, característicos de uma agência reguladora de abrangência nacional.

Na sequência, os processos selecionados são avaliados à luz dos critérios definidos na metodologia apresentada no item 3.1, considerando-se o volume e a sensibilidade dos dados pessoais tratados, a presença de titulares em situação de vulnerabilidade, a existência de decisões automatizadas, o uso de tecnologias inovadoras, o potencial impacto sobre os direitos dos titulares e o grau de vigilância ou exposição envolvido.

Por fim, para viabilizar a priorização dos processos e dos ativos identificados, aplica-se uma matriz de pontuação estruturada a partir dos critérios do modelo, empregando-se uma escala de impacto que varia de 0 (não se aplica) a 4 (crítico), conforme apresentado na Tabela 4. A consolidação das pontuações permite comparar o grau de criticidade dos processos analisados e identificar aqueles que demandam maior atenção sob a perspectiva da privacidade. Os resultados são apresentados na Tabela 5.

Tabela 5: Avaliação da criticidade dos processos selecionados

Processo	Critério 1	Critério 2	Critério 3	Critério 4	Critério 5	Critério 6	Critério 7	Total
Pessoal da Aviação Civil	> 50 mil (4)	Dados de saúde (4)	Adolescentes e idosos (4)	Sistemas convencionais (1)	Não se aplica (0)	Não se aplica (0)	Limitado e reversível (2)	15
Habilitação AVSEC	> 50 mil (4)	Dados profissionais e foto (3)	Idosos - (2)	Sistemas convencionais (1)	Não se aplica (0)	Não se aplica (0)	Limitado e reversível (1)	11
Cadastro de usuário externo no protocolo eletrônico	> 50 mil (4)	Apenas dados cadastrais (1)	Adolescentes e idosos (4)	Sistemas convencionais (1)	Não se aplica (0)	Não se aplica (0)	Limitado e reversível (2)	12
Cadastro de usuário externo no portal de capacitação	> 50 mil (4)	Dados profissionais (2)	Idosos (2)	Sistemas convencionais (1)	Não se aplica (0)	Não se aplica (0)	Insignificante (1)	10
Autorização provisória para balões	< 1 mil (1)	Apenas dados cadastrais (1)	Idosos (2)	Sistemas convencionais (1)	Não se aplica (0)	Não se aplica (0)	Insignificante (1)	6

Fonte: Elaboração própria (2026).

No que tange à expedição de licenças de pessoal da aviação civil, de acordo com dados disponíveis em painel institucional – habilitações válidas (Power BI), verifica-se a existência de mais de 116 mil licenças válidas e mais de 55 mil pessoas ativas, o que corresponde ao volume de titulares. Ressalta-se que um mesmo titular pode possuir mais de uma licença ativa.

A aplicação do modelo ao referido processo resultou na seguinte pontuação: volume e escala do tratamento, com mais de cinquenta mil titulares com licenças (4); tratamento de dados de categorias vulneráveis, incluindo adolescentes e idosos (4); natureza dos dados tratados, abrangendo informações relativas à saúde (4); uso de sistemas convencionais, sem inteligência artificial (1); decisão automatizada (0), uma vez que o tratamento não envolve classificações ou encaminhamentos automatizados; grau de vigilância ou exposição (0); e impacto potencial sobre os direitos e interesses dos titulares (2), considerando que eventual incidente envolvendo informações relacionadas à saúde pode gerar prejuízos relevantes aos indivíduos, embora com potencial de reversão e mitigação por meio de medidas adequadas de proteção e resposta. Ao todo, o processo alcançou 15 pontos, sendo classificado como de criticidade moderada.

No que se refere ao processo de habilitação AVSEC, conforme dados disponíveis em painel institucional - habilitados AVSEC (Power BI), observa-se a existência de aproximadamente 102 mil pessoas habilitadas. Dentre os titulares, encontram-se indivíduos com mais de sessenta anos. Ademais, embora a Instrução Suplementar (IS) nº 110.11-001, Revisão A, exija a realização periódica de avaliações psicofísicas para fins de habilitação, os dados clínicos decorrentes desses exames são tratados pelas instituições credenciadas responsáveis pela avaliação, não sendo compartilhados com a Anac. O processo também não contempla a utilização de tecnologias emergentes ou inteligência artificial, decisões automatizadas ou atividades de vigilância. Considerando o elevado volume de titulares, a presença de informações pessoais de idosos e a natureza das informações envolvidas, a aplicação do modelo resultou em 11 pontos, classificando o processo em nível de criticidade inferior ao observado para a expedição de licenças de pessoal da aviação civil.

O processo de cadastro no protocolo eletrônico, por sua vez, não envolve o tratamento de dados pessoais sensíveis, tampouco a utilização de tecnologias emergentes, decisões automatizadas ou atividades de vigilância. Entretanto, apresenta volume expressivo de titulares cadastrados, superior a cinquenta mil registros, e contempla o tratamento de informações de adolescentes e idosos. Ademais, o sistema não prevê a eliminação do cadastro, mas apenas a inativação, aspecto que pode demandar atenção sob a perspectiva da retenção e do ciclo de vida dos dados. Em razão desses fatores, o processo obteve 12 pontos na avaliação de criticidade.

Já o processo de cadastro no Portal de Capacitação, conforme as informações constantes do formulário de cadastro de usuário externo e do Aviso de Privacidade, disponibilizados no portal institucional da Anac, envolve a coleta de dados cadastrais e profissionais dos usuários. Entretanto, o

processo não contempla o tratamento de dados pessoais sensíveis nem de dados de crianças e adolescentes. Adicionalmente, o processo não utiliza tecnologias emergentes, decisões automatizadas ou atividades de monitoramento e vigilância associadas ao tratamento de dados pessoais. Considerando essas características, especialmente a natureza dos dados tratados e o reduzido potencial de impacto aos titulares, o processo apresentou baixa criticidade. Embora o volume de titulares seja superior a 50 mil pessoas, a ausência de outros fatores de risco manteve sua classificação em patamar reduzido de criticidade, totalizando 10 pontos na avaliação realizada.

Por fim, o processo de autorização provisória para balões não contempla o tratamento de dados pessoais sensíveis nem de informações relativas a crianças ou adolescentes. Ademais, conforme informações disponibilizadas no painel institucional - aeronaves balões (Power BI), esse processo abrange um número reduzido de titulares, inferior a mil registros. O processo também não envolve o uso de tecnologias emergentes ou inteligência artificial, a adoção de decisões automatizadas com efeitos sobre os titulares, tampouco atividades de vigilância ou monitoramento. Além disso, eventual incidente tende a gerar impactos limitados aos titulares, uma vez que as informações coletadas possuem baixa sensibilidade e são utilizadas exclusivamente para fins de identificação e instrução do procedimento administrativo. Em razão da baixa sensibilidade dos dados tratados, do reduzido volume de titulares envolvidos e do limitado potencial de impacto sobre os direitos e liberdades dos titulares, o processo apresentou baixa criticidade, totalizando 6 pontos na avaliação proposta.

Aplicando-se a escala de criticidade definida na Tabela 3 às pontuações obtidas, os processos avaliados são classificados conforme apresentado a seguir.

Tabela 6: Resultado da avaliação da criticidade dos processos selecionados

Processo	Total	Criticidade
Pessoal da Aviação Civil	15	Moderada
Habilitação AVSEC	11	Moderada
Cadastro de usuário externo no protocolo eletrônico	12	Moderada
Cadastro de usuário externo no portal de capacitação	10	Baixa
Autorização provisória para balões	6	Baixa

Fonte: Elaboração própria (2026).

Dessa forma, a aplicação da metodologia de priorização aos processos que envolvem tratamento de dados pessoais possibilita a elaboração de um ranking de criticidade, permitindo identificar aqueles que apresentam maior potencial de risco à privacidade. Como resultado, torna-se possível direcionar de forma objetiva os esforços institucionais para a elaboração prioritária de RIPDs, o fortalecimento de controles técnicos e administrativos relacionados aos ativos de informação utilizados, a revisão de instrumentos contratuais firmados e a implementação de mecanismos específicos de monitoramento, tratamento e resposta a incidentes de segurança. Essa abordagem apoia a alocação mais eficiente dos recursos de governança em privacidade e para o atendimento ao princípio da responsabilização e prestação de contas previsto na LGPD.

5. Discussão e análise de dados

A identificação sistemática dos processos e ativos críticos para a privacidade e proteção de dados pessoais configura-se como elemento estruturante da gestão de riscos, na medida em que permite direcionar esforços institucionais, otimizar a alocação de recursos escassos e definir controles proporcionais ao nível de impacto potencial sobre os direitos e liberdades fundamentais dos titulares. Nesse sentido, o modelo proposto contribui para operacionalizar, no setor público, a abordagem baseada em risco preconizada pela LGPD, pelo GDPR, pela ISO/IEC 27701 e pelo próprio PPSI 2.0.

Do ponto de vista teórico, a adaptação da metodologia Análise das Joias da Coroa amplia sua aplicação tradicional, centrada na segurança da informação, ao incorporar critérios relacionados à privacidade, como sensibilidade dos dados, categorias de titulares, escala do tratamento e impacto potencial aos direitos dos titulares. Essa transposição reforça a convergência entre os campos da segurança da informação e da privacidade, ao mesmo tempo em que preserva a centralidade do titular como elemento orientador da gestão de riscos.

Sob a perspectiva institucional, o modelo oferece um instrumento capaz de apoiar a alta administração na definição de prioridades, na justificativa técnica para alocação de recursos e na estruturação de ciclos progressivos de implementação da governança em privacidade e proteção de dados pessoais. Ao permitir a diferenciação objetiva entre processos e ativos de maior e menor criticidade, o modelo favorece a adoção de estratégias graduais de conformidade, especialmente em cenários marcados por restrições orçamentárias, limitações de pessoal e heterogeneidade de maturidade organizacional.

Os resultados obtidos no estudo de caso da Anac demonstram a aplicabilidade prática da metodologia proposta. A utilização dos critérios definidos permitiu distinguir processos que demandam maior atenção institucional daqueles que, embora relevantes, apresentam menor potencial de impacto à privacidade. Essa diferenciação fornece subsídios objetivos para a priorização de ações de governança, a realização de avaliações de impacto e o fortalecimento de controles técnicos e administrativos.

Os resultados também demonstram a influência de determinadas características do tratamento na classificação de criticidade. Conforme apresentado na Tabela 5, a ausência, nos processos analisados, de decisões automatizadas, do uso de tecnologias emergentes e de atividades de vigilância ou monitoramento sistemático contribuiu para que nenhum processo fosse classificado na faixa mais elevada de criticidade. Esse resultado sugere que a adoção dessas práticas deve ser acompanhada de uma avaliação criteriosa dos riscos envolvidos, uma vez que tendem a elevar o potencial de impacto aos titulares e, consequentemente, demandar investimentos adicionais em governança, controles de segurança e medidas de mitigação.

Adicionalmente, a priorização realizada sugere que o processo de expedição de licenças de pessoal da aviação civil reúne características que indicam maior pertinência para a elaboração de RIPD, em razão do nível de criticidade apurado. Os processos de cadastro no protocolo eletrônico e habilitação AVSEC, embora tenham apresentado criticidade inferior, também podem ser considerados em análises complementares de risco. Por sua vez, os processos de cadastro no portal de capacitação e autorização provisória para balões apresentaram níveis reduzidos de criticidade, não sinalizando, a princípio, necessidade prioritária de elaboração de RIPD, sem prejuízo de reavaliações futuras decorrentes de alterações na forma de tratamento ou nos riscos associados.

Cumpre destacar que a escala de criticidade proposta na Tabela 4 foi concebida e aplicada considerando a realidade institucional da Anac, especialmente o volume de titulares envolvidos nos processos analisados, a natureza dos dados tratados e o contexto regulatório em que a Agência está inserida. Nesse cenário, o tratamento de dados de dezenas ou centenas de milhares de titulares pode representar um fator relevante para a classificação da criticidade dos processos.

Todavia, os parâmetros adotados não devem ser interpretados como universais. Em organizações com volume significativamente superior de operações de tratamento, um universo de 50 mil titulares, por exemplo, pode não representar um nível elevado de criticidade quando comparado ao conjunto de dados habitualmente tratado pela instituição. Dessa forma, recomenda-se que a escala seja calibrada de acordo com o contexto organizacional em que será aplicada, considerando fatores como o porte da organização, a quantidade de titulares e a natureza dos tratamentos realizados.

6. Considerações finais

Este estudo parte do reconhecimento da centralidade da gestão de riscos para a governança em privacidade e proteção de dados pessoais para a implementação da LGPD no setor público, bem como da lacuna metodológica relacionada à identificação e priorização de processos e ativos críticos sob a ótica da privacidade. Como contribuição, propõe-se a adaptação da metodologia Análise das Joias da Coroa, originalmente aplicada à segurança da informação, para o contexto da privacidade.

O modelo oferece critérios operacionais para a determinação das chamadas Joias da Coroa da Privacidade, permitindo direcionar esforços institucionais aos pontos de maior impacto potencial sobre os direitos dos titulares. Espera-se que essa abordagem contribua para a efetividade dos programas de governança em privacidade, ao viabilizar uma implementação progressiva, proporcional e baseada em riscos das medidas previstas no PPSI 2.0 e demais instrumentos de conformidade.

Cumpre ressaltar que o modelo proposto apresenta limitações. A atribuição de pontuações ainda envolve julgamento especializado, o que indica a necessidade de capacitação técnica e de mecanismos de governança que assegurem consistência e transparência no processo decisório. Ademais, a proposta adota pesos equivalentes para os critérios por simplicidade operacional, podendo trabalhos futuros empregar ponderações diferenciadas.

Apesar dessas limitações, o modelo oferece uma estrutura sistematizada para a identificação e priorização de processos e ativos críticos para a privacidade, contribuindo para suprir uma lacuna na aplicação do PPSI 2.0 e para o fortalecimento da governança de dados no setor público.

Como perspectivas para trabalhos futuros, sugere-se a aplicação empírica do modelo a todos os processos da Anac, de modo a validar seus critérios, avaliar sua viabilidade operacional e aperfeiçoar seus instrumentos. Recomenda-se, ainda, o desenvolvimento de artefatos de apoio que possibilitem mensurar o grau de criticidade dos ativos considerando a privacidade e investigar a integração do modelo com a elaboração de RIPDs e com frameworks institucionais de gestão de riscos. Esses desdobramentos podem contribuir para o refinamento da abordagem proposta e para o fortalecimento da governança em privacidade no setor público.

Referências

ALVES, GUILHERME BARBOSA. **Uma proposta de processo de gerenciamento de riscos baseado na LGPD**. 2021. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Escola Politécnica, Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO/IEC 27701:2019* — **Segurança da informação, privacidade e gestão da proteção de dados pessoais — Requisitos e diretrizes.** Rio de Janeiro: ABNT, 2019.

BELTRÃO, R. **O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos.** Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 6 fev. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Painel Institucional - habilitações válidas.** Disponível em: https://app.powerbi.com/view?r=eyJrIjoiZTVlNjA1NmYtYjQxNC00MGIyLTk3YWItNmM1MDFiMzgwNzY3IiwidCI6ImI1NzQ4ZjZlLWI0YTQtNGIyYi1hYjJhLWVmOTUyMjM2ODM2NiIsImMiOjR9&pageName=ReportSection. Acesso em: 1 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Painel Institucional - habilitados AVSEC.** Disponível em: https://app.powerbi.com/view?r=eyJrIjoiYmMxZmIxZjUtMTQ4Ny00OGI4LWI2YzAtZGM3NmY5Z

TFhZTViIiwidCI6ImI1NzQ4ZjZlLWI0YTQtNGIyYi1hYjJhLWVmOTUyMjM2ODM2NiIsImMiOjR9. Acesso em: 1 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Instrução suplementar – IS 110.11-001 Revisão A.** Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/iac-e-is/is/is-110-11-001/@@display-file/arquivo_norma/IS110.11-001A.pdf. Acesso em: 1 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Painel Institucional – aeronaves balões.** Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/dados-abertos/areas-de-atuacao/aeronaves-1/registro-aeronautico-brasileiro/painel-aeronaves-baloes. Acesso em 1 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (Anac). **Portal de Capacitação: cadastro de usuário externo**. Disponível em: https://capacitacao.anac.gov.br/login/signup.php. Acesso em: 5 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (Anac). **Aviso de Privacidade Específico – Portal de Capacitação da Anac**. Disponível em: https://capacitacao.anac.gov.br/mod/page/view.php?id=91040. Acesso em: 9 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (Anac). **Protocolo Eletrônico: cadastro de usuário externo**. Disponível em: https://sei.anac.gov.br/sei/controlador_externo.php?acao=usuario_externo_avisar_cadastro&id_orgao_acesso_externo=0. Acesso em: 5 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (Anac). **Aviso de Privacidade Específico – SEI Anac**. Disponível em: https://www.gov.br/anac/pt-br/sistemas/protocolo-eletronico-sei/aviso-de-privacidade-sei-anac. Acesso em: 9 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (Anac). **Autorização Provisória de Balão cadastrado no Aerodesporto**. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/operadores-de-balao/autorizacao-provisoria-de-baloes/autorizacao-provisoria-operacional-de-baloes-do-aerodesporto. Acesso em: 5 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo: tratamento de dados pessoais pelo Poder Público.** Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 5 jun. 2026.

BRASIL. AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Diário Oficial da União: seção 1, Brasília, DF, 28 jan. 2022.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. SECRETARIA DE GOVERNO DIGITAL. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.** Diário Oficial da União: seção 1, Brasília, DF, 28 out. 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 2 nov. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. SECRETARIA DE GOVERNO DIGITAL. **Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf/view. Acesso em: 4 jun. 2026.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. SECRETARIA DE GOVERNO DIGITAL. **Guia do Framework de Privacidade e Segurança da Informação – PPSI 2.0.** Disponível em https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf. Brasília, 2025. Acesso em: 4 jun. 2026.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise Risk Management — Integrating with Strategy and Performance.** New York: AICPA, 2017.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS (CCGD). **Guia de Boas Práticas da Lei Geral de Proteção de Dados Pessoais.** Brasília, 2020.

D'OLIVEIRA, N. P. C.; CUNHA, F. J. A. P. **Brazilian General Data Protection Law (LGPD): the relationship between information policy and information regime.** Revista Digital de Biblioteconomia e Ciência da Informação, v. 22, e024015, 2024.

ESESP – ESCOLA DE SERVIÇO PÚBLICO DO ESPÍRITO SANTO. **Proteção de dados, privacidade e LGPD para servidores públicos.** Vitória, 2025. Disponível em: https://esesp.es.gov.br. Acesso em: 6 fev. 2026.

FARIA, Nelson Correia. **Estratégia de cibersegurança.** 2022. Dissertação (Mestrado em Engenharia Informática) – Universidade do Minho, Portugal, 2022.

FORBES. **Protecting the Crown Jewels.** Forbes Tech Council, 13 ago. 2018. Disponível em: https://www.forbes.com. Acesso em: 6 nov. 2025.

GARBACCIO, G. L.; KISCHELEWSKI, F. L. N. **Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability.** Revista Brasileira de Estudos Políticos, n. 128, 2024.

MENKE, F. **Lei geral de proteção de dados: subsídios teóricos à aplicação prática.** Brasília: Foco, 2022.

MITRE. **Crown Jewels Analysis (CJA).** Bedford, MA: MITRE Corporation, 2021. Disponível em: https://www.mitre.org. Acesso em: 2 nov. 2025.

NAKAMURA, E.; FORMIGONI FILHO, J. R.; IDE, M. C. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados pessoais.** In: WORKSHOP DE REGULAÇÃO, AVALIAÇÃO DA CONFORMIDADE E CERTIFICAÇÃO DE SEGURANÇA, 5., 2019, São Paulo. Anais [...]. Porto Alegre: SBC, 2019. p. 11–16.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST Privacy Framework: a tool for improving privacy through enterprise risk management.** Gaithersburg, MD, 2020. Disponível em: https://www.nist.gov.

PARKKINEN, Henrik. **Safeguarding the Crown Jewels – Information Classification.** 2023. Disponível em: https://henrikparkkinen.com. Acesso em: 6 fev. 2026.

PELOSO PIURCOSKY, F. et al. **A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos.** Suma de Negocios, v. 10, n. 23, p. 89–99, 2019.

SHEDDEN, P. et al. **Asset identification in information security risk assessment: a business practice approach.** Communications of the Association for Information Systems, v. 39, n. 1, p. 297–320, 2016.

SILVA, E. G. et al. **Tomada de decisão em segurança cibernética: modelo para identificação de joias da coroa.** RISTI, n. E77, p. 61–75, 2025.

SILVA, E. G. et al. **International perspectives on critical infrastructure: evaluation criteria and definitions.** International Journal of Critical Infrastructure Protection, v. 49, 2025.

SOUTO, J. E.; MOTTA, G. H. M. B. **LGPD e infraestrutura de TI: proposta de modelo de conformidade para o setor público.** Revista Foco, v. 17, n. 12, 2024.

SOUZA, Carolina Vilela. **Compliance digital: privacidade e proteção de dados à luz da Lei Geral de Proteção de Dados e os desafios de implementação.** 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2022.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial básico de gestão de riscos.** Brasília, 2018.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública.** Brasília, 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Jornal Oficial da União Europeia, Bruxelas, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 4 jun. 2026.

WRIGHT, D. **The state of the art in privacy impact assessment.** Computer Law & Security Review, v. 28, n. 1, p. 54–61, 2012.