RELATÓRIO ANALÍTICO

Pesquisa Nacional de *Proteção de Dados* 2025

Percepções, práticas e dificuldades reais vivenciadas por profissionais que atuam direta ou indiretamente com **Programas de *Governança de Proteção de Dados***.

Coordenação:
Mariana *Ruzzi*
Rogério *Coutinho*

Introdução

Sobre a #PNPD25

A **Pesquisa Nacional de Proteção de Dados (PNPD25)** foi desenvolvida com o propósito de **compreender os desafios enfrentados nos Programas de Proteção de Dados.**

Esta iniciativa captou **percepções, práticas e dificuldades reais vivenciadas por profissionais que atuam direta ou indiretamente na área de Privacidade e Segurança da Informação**, tanto no setor público quanto privado durante os meses de abril e maio de 2025.

O escopo da pesquisa abrangeu **diversos aspectos do ecossistema de Proteção de Dados**, como a distribuição geográfica dos profissionais, áreas de atuação, tipos de organizações, atividades mais demandadas na rotina, percepção sobre a atuação da ANPD e do Judiciário, uso de tecnologia para automação, importância dos comitês de proteção de dados e sinergia com governança de inteligência artificial. Além disso, foram abordados temas como a conscientização da sociedade sobre seus direitos e o nível de otimismo em relação à Proteção de Dados nos próximos anos.

A pesquisa foi realizada por **meio de um formulário digital, disseminado nacionalmente**. O questionário foi composto por perguntas objetivas (de múltipla escolha ou escala de percepção) e foi direcionado a profissionais de diferentes perfis – incluindo DPOs, gestores de TI, jurídicos, compliance, segurança da informação e consultorias especializadas. **O levantamento contou com 680 respondentes, o que oferece uma amostra significativa para análise das tendências e desafios enfrentados na prática.**

Introdução

Sobre a #PNPD25

Ao consolidar os dados, **o estudo não apenas fornece um panorama da realidade atual, mas também aponta caminhos para o fortalecimento da cultura de proteção de dados** identificando lacunas de capacitação, oportunidades de regionalização e fatores críticos para a efetividade dos programas de proteção de dados. **A pesquisa visa contribuir com o debate técnico, apoiar políticas públicas e orientar decisões estratégicas de organizações que buscam amadurecer sua governança em proteção de dados**.

Coordenação

Mariana Ruzzi
Advogada especialista em Privacidade e Proteção de Dados. Doutoranda em Direito pela UNESP. Tem pós-graduação em Direito Empresarial (Legale) e Direito Imobiliário (EPD). Possui certificações em Proteção de Dados pela Exin e IAPP (CDPO/CIPM). Palestrante, mentora e autora de livros. Pesquisadora no Legal Fronts Institute.

ruzzimariana@gmail.com

Rogério Coutinho
Engenheiro de Computação formado pela Universidade Federal de São Carlos (UFSCar). Sócio-fundador da Podium Tecnologia (Consultoria especializada em Governança de Segurança da Informação, Privacidade e Continuidade de Negócios) e da SimpleWay (Plataforma de Governança Cibernética, Privacidade e Inteligência Artificial).

rogerio.coutinho.silva@gmail.com

Design Editorial

Jéssica Camargo
Mestre em Gestão de Marketing e Especialista em Comunicação e Mídia. Analista de Marketing na SimpleWay (Plataforma de Governança de Segurança Cibernética, Privacidade e Inteligência Artificial).

j.jessicacamargo@gmail.com

Apoio

A Pesquisa Nacional de Proteção de Dados 2025 foi realizada com o apoio de:

Netuno Network

Fórum de Proteção de Dados do Interior Paulista

Podium

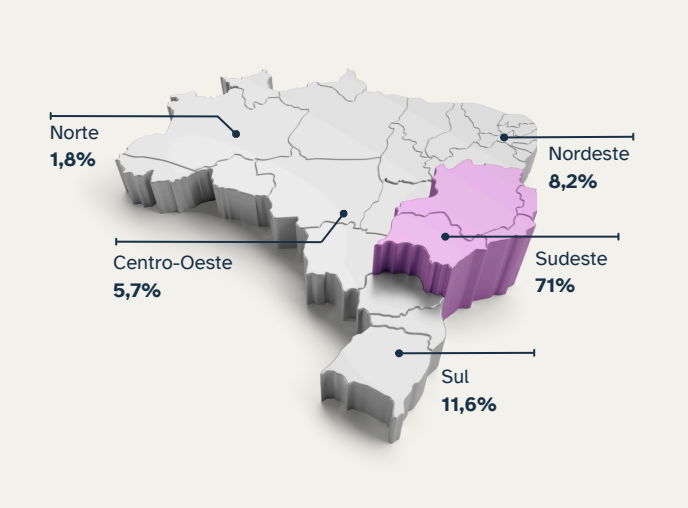
SimpleWay
CyberSecurity & Privacy & AI Governance and Management

Sumário

Consulte também a Apresentação Executiva deste Relatório Analítico.

1. Perfil profissional e formação

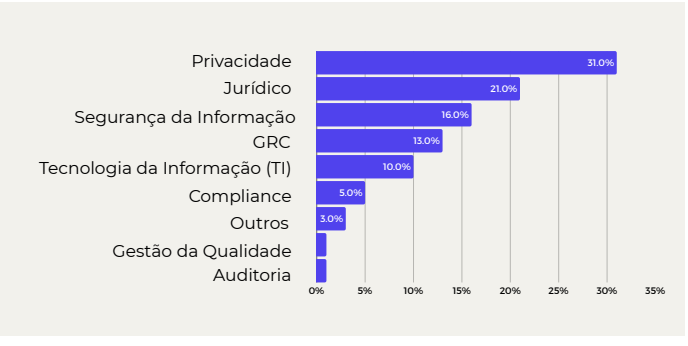
Região



A maior parte dos respondentes da PNPD25 está **concentrada na região Sudeste.** Essa distribuição acompanha a lógica de **concentração econômica e populacional do país,** especialmente em estados como São Paulo e Rio de Janeiro, refletindo onde estão as principais oportunidades de emprego, melhores remunerações e maior presença de empresas demandando profissionais de Privacidade e Proteção de dados.

> O cenário brasileiro para a área de proteção de dados vive uma **fase de crescimento acelerado.** A vigência da LGPD, aliada à complexidade crescente das operações corporativas, tem impulsionado a **valorização de especialistas no tema**. Isso se traduz não apenas em maior demanda, mas também em aumento da competitividade para atrair e reter profissionais qualificados.

Área de Atuação



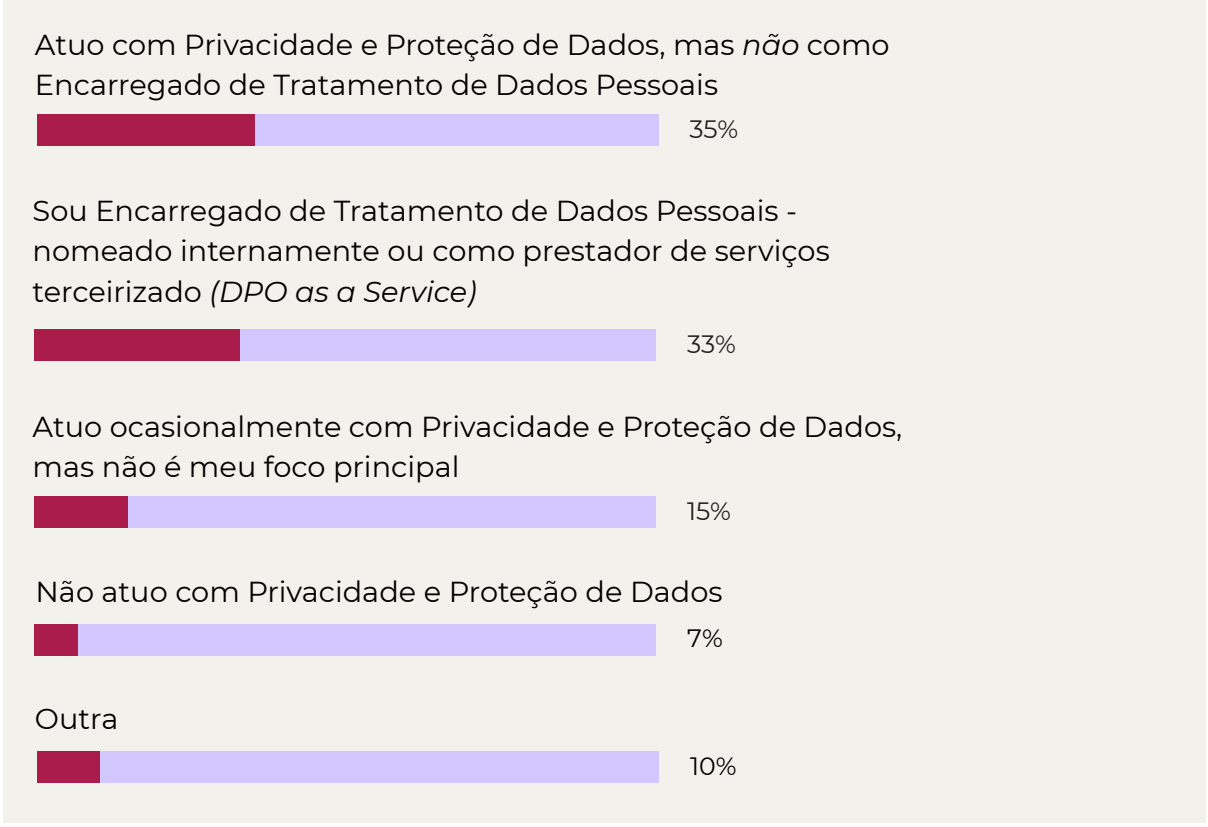
No perfil de atuação, predominam profissionais vinculados diretamente à área de Privacidade, seguidos por Jurídico e Segurança da Informação — o que reafirma o **caráter multidisciplinar da Governança de Proteção de Dados.**

> Esse movimento é reforçado por tendências de mercado: segundo o LinkedIn Notícias[1], a função de **Analista de Privacidade** figura entre as profissões com maior projeção de crescimento no Brasil em 2024, evidenciando o reconhecimento dessa carreira no cenário nacional.

1. LinkedIn Notícias

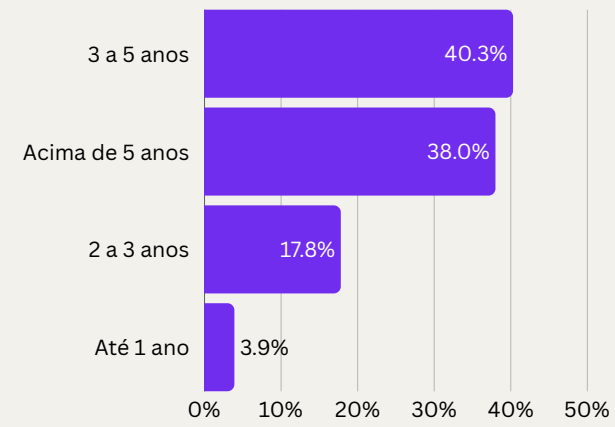
Outro aspecto relevante é **a valorização de profissionais com formações complementares e certificações técnicas — como CIPP/E, CIPM, CDPO, EXIN**, entre outras — que têm se tornado diferenciais importantes no mercado. A atuação em proteção de dados exige não apenas conhecimento legal e técnico, mas também **habilidades transversais, como gestão de riscos, comunicação e visão estratégica**. O perfil que combina essas competências se destaca em um cenário cada vez mais exigente e dinâmico.

Atuação



Chama a atenção o número significativo de profissionais que trabalham com privacidade sem exercer formalmente a função de **Encarregado pelo Tratamento de Dados Pessoais (DPO)** — foram 204 participantes nessa condição. Esse dado aponta para a **ampliação da cultura de proteção de dados dentro das organizações**, com responsabilidades sendo compartilhadas por diferentes áreas, mesmo fora das estruturas formais previstas pela LGPD.

Tempo de atuação



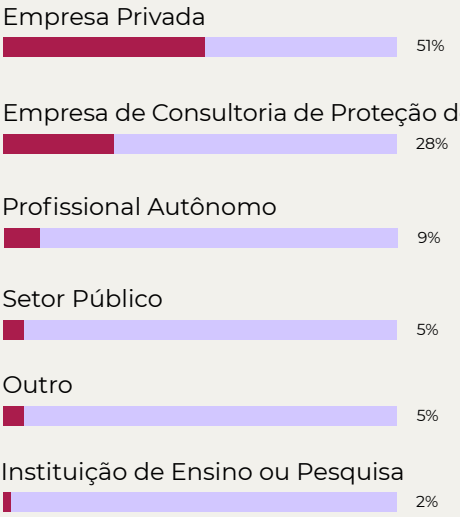
+78% tem mais de 3 anos de atuação.

Outro destaque relevante está no nível de experiência do público participante: cerca de **78% afirmam atuar há mais de três anos na área de privacidade e proteção de dados**. Esse perfil mais experiente sugere um avanço na profissionalização do setor, com parte dos respondentes já tendo vivenciado desde a fase inicial de adequação até os **desafios contínuos de manutenção e evolução da proteção de dados.**

No conjunto, os dados indicam que a conformidade com **a LGPD tem deixado de ser tratada como um projeto pontual e vem se consolidando como uma disciplina permanente** — mais integrada à rotina de empresas e consultorias.

2. Atividades prioritárias, temas críticos e principais desafios

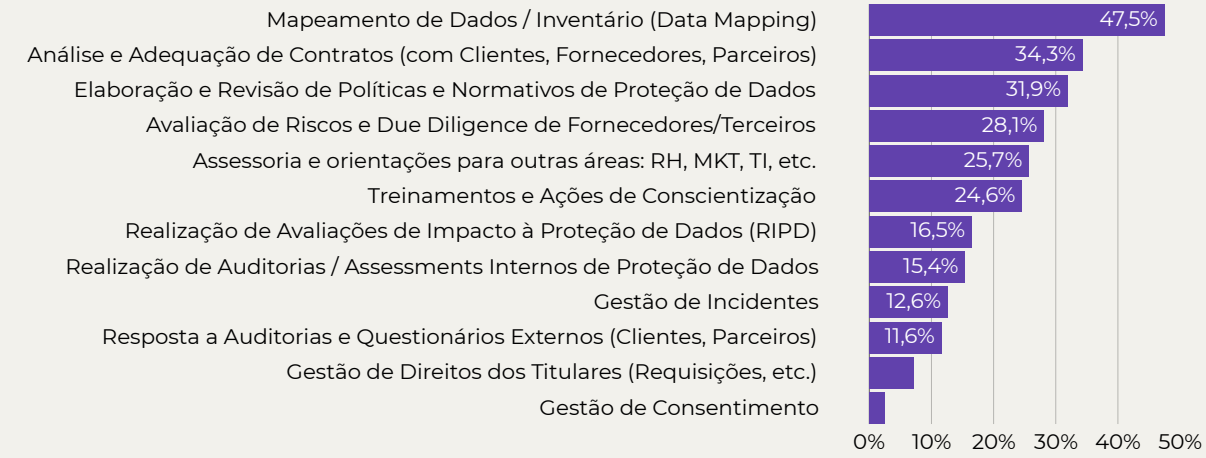
Setores ou tipo de organização



A maioria dos respondentes atua internamente em **empresas privadas,** seguida por um contingente expressivo de **profissionais vinculados a consultorias especializadas.** Esse cenário reforça o **papel estratégico** que a proteção de dados passou a ocupar no ambiente corporativo, ao mesmo tempo em que evidencia a **demanda contínua por suporte técnico e jurídico oferecido por terceiros** — especialmente em estruturas que ainda estão em fase de consolidação da Governança do tema.

Atividades que mais demandam tempo

Entre as atividades mais recorrentes na rotina dos profissionais de proteção de dados, destacam-se o **mapeamento de dados, a revisão e elaboração de políticas internas e a análise contratual à luz da LGPD**. Essas tarefas, além de demandarem tempo e atenção, são estruturantes para a Governança de Proteção de Dados e têm sido apontadas como pontos críticos tanto por especialistas quanto pela literatura especializada na área.



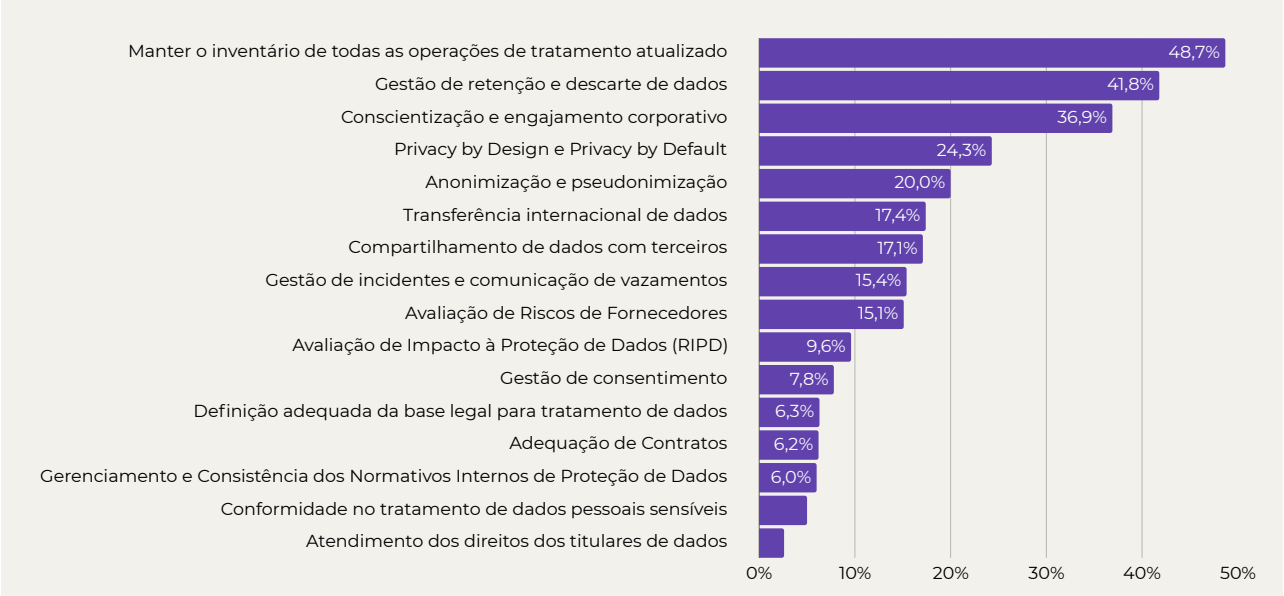
Nesta questão, os respondentes foram direcionados a selecionar até 3 opções.

O **Registro das Operações de Tratamento de Dados Pessoais (ROPA)**, por exemplo, é considerado um dos pilares da adequação à LGPD, mas o mapeamento, manutenção e evolução de forma contínua do inventário tem sido um enorme desafio. Muitas organizações ainda operam com **inventários incompletos, frequentemente atualizados manualmente, comprometendo a eficiência do processo e exige revisões constantes**. O esforço para manter o **ROPA** atualizado é agravado pela necessidade de integrar informações de diferentes áreas da empresa, o que reforça a importância de uma **governança bem estruturada.**

Já no que diz respeito à **revisão de contratos**, os profissionais jurídicos enfrentam uma carga significativa de trabalho. A adaptação de cláusulas contratuais que envolvem o tratamento de dados pessoais — especialmente em relações com terceiros, operadores e parceiros internacionais — exige atenção contínua. **A escassez de modelos padronizados e o desalinhamento entre as áreas jurídica e técnica tornam o processo mais lento e custoso**. Apesar da existência de cláusulas-padrão e acordos de compartilhamento recomendados, sua adoção ainda encontra resistência ou desconhecimento dentro de muitas organizações.

A recorrência dessas atividades evidencia um cenário marcado por **baixa padronização, excesso de tarefas manuais, pouca integração entre áreas e maturidade operacional limitada**. A expectativa, no entanto, é que esse cenário evolua com a adoção de ferramentas tecnológicas específicas para a proteção de dados, a implementação de práticas mais maduras de governança e o engajamento ativo da alta liderança. Esses fatores são decisivos para reduzir a sobrecarga operacional e consolidar programas de proteção de dados mais eficientes e sustentáveis.

Os temas mais desafiadores e/ou obscuros na implementação prática da Proteção de Dados



Nesta questão, os respondentes foram direcionados a selecionar até 3 opções que entendem como obstáculos para avançar com o tema de proteção de dados dentro das organizações.

Os desafios apontados pelos participantes da PNPD25 evidenciam os **temas mais obscuros e desafiadores** na estruturação de programas de Governança de Proteção de Dados. Para superá-los, torna-se indispensável **investir em tecnologia, capacitação contínua das equipes e na consolidação de uma cultura organizacional orientada à proteção de dados**.

Três temas se destacaram como **os mais desafiadores ou obscuros** na prática cotidiana:

- Manutenção do inventário de operações de tratamento (ROPA) – *331 menções*
- Gestão de retenção e descarte de dados pessoais – *284 menções*
- Conscientização e engajamento corporativo – *251 menções*

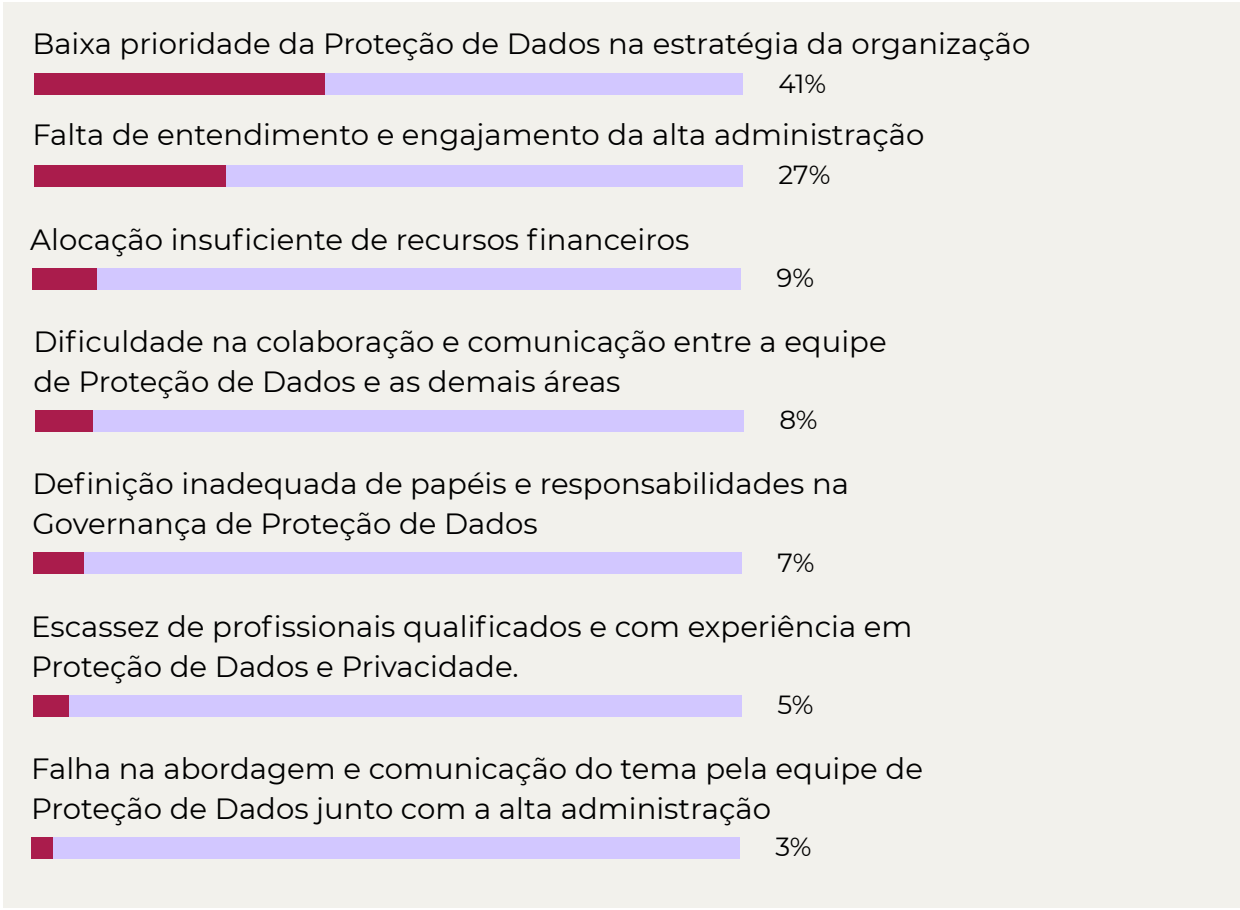
A manutenção do ROPA é vista como um dos principais pilares da conformidade, por permitir o mapeamento estruturado do ciclo de vida dos dados dentro da organização. No entanto, esse processo ainda esbarra em **obstáculos como a complexidade operacional — que envolve diversos sistemas, áreas e fornecedores — e a ausência de processos bem definidos.** Além disso, o **uso intensivo de planilhas manuais, sem ferramentas adequadas, compromete a atualização e consistência das informações**. Outro fator crítico é o baixo envolvimento das áreas operacionais, que muitas vezes não compreendem seu papel na alimentação e revisão do inventário. A consequência direta é um inventário desatualizado, que afeta negativamente a realização de avaliações de risco, o cumprimento de direitos dos titulares e a transparência exigida pela LGPD.

A gestão do ciclo de vida dos dados, especialmente no que se refere à retenção e descarte, também foi amplamente apontada como uma fragilidade. Pode-se inferir que entre os principais desafios estão o desconhecimento das bases legais e prazos aplicáveis, a ausência de políticas formais de retenção, o receio de excluir dados que possam ser úteis juridicamente no futuro e a dificuldade de operacionalizar a exclusão. Somam-se a isso **limitações técnicas — como sistemas legados ou dispersos — que dificultam o descarte seguro de dados. Essa retenção excessiva eleva os riscos em caso de incidentes de segurança e fere princípios fundamentais da LGPD,** como necessidade, minimização e segurança da informação.

No campo da cultura organizacional, o desafio está em sensibilizar as equipes para que compreendam que **a proteção de dados é uma responsabilidade coletiva**, e não restrita ao jurídico, **Segurança da Informação** ou ao DPO.

Esses três desafios — ROPA, retenção e descarte e cultura organizacional — estão interligados e indicam a necessidade de um salto de maturidade. Superá-los exige clareza de processos, automação, colaboração interdepartamental e engajamento da alta liderança da organização. A atuação conjunta entre Jurídico, Segurança da Informação, TI e áreas de negócio é o caminho para fortalecer a Governança de Proteção de Dados e garantir a estruturação do programa de governança do tema e consequentemente uma maior conformidade com a LGPD.

Os principais obstáculos no Programa de Proteção de Dados



Apesar dos avanços promovidos pela LGPD, **a proteção de dados ainda é, em muitas organizações, tratada como uma obrigação regulatória**, e não como um elemento estratégico ou diferencial competitivo. Essa visão limitada compromete o investimento adequado em iniciativas estruturantes de privacidade e segurança da informação, que acabam recebendo atenção apenas em momentos pontuais ou diante de pressões externas.

De forma recorrente, a **conformidade com a LGPD ainda é encarada como um projeto de adequação com início, meio e fim**, em vez de ser incorporada como um programa/processo contínuo dentro da governança corporativa. **Esse modelo reativo tende a fragilizar a sustentabilidade das ações implementadas**, dificultando a atualização de políticas, a manutenção de inventários e o acompanhamento de riscos em tempo real — fatores essenciais para uma postura preventiva.

Nesta questão, os respondentes foram direcionados a selecionar até 3 opções que entendem como obstáculos para avançar com o tema de proteção de dados dentro das organizações.

Um dos principais entraves para essa mudança de mentalidade é a baixa sensibilização da alta liderança. A compreensão limitada, por parte dos executivos, sobre os impactos legais, reputacionais e operacionais do uso indevido de dados pessoais reduz a prioridade do tema na agenda institucional. Uma **abordagem menos técnica e mais estratégica** pode impactar fortemente nessa compreensão, ganhando força, visibilidade e integração com áreas-chave, como Compliance, Tecnologia, Jurídico e RH.

É importante destacar que esses fatores são interdependentes**: quando a liderança não reconhece o valor estratégico da proteção de dados, dificilmente haverá engajamento genuíno ou alocação de recursos.** Por outro lado, sem ações estruturadas e resultados concretos, torna-se mais difícil demonstrar o retorno e a relevância do tema para o negócio. **Romper esse ciclo exige ações intencionais de sensibilização da liderança**, alinhamento com os objetivos organizacionais e adoção de indicadores que evidenciem os benefícios da Governança de Proteção de Dados.

3. Percepção sobre a ANPD

A percepção sobre a atuação da Autoridade Nacional de Proteção de Dados

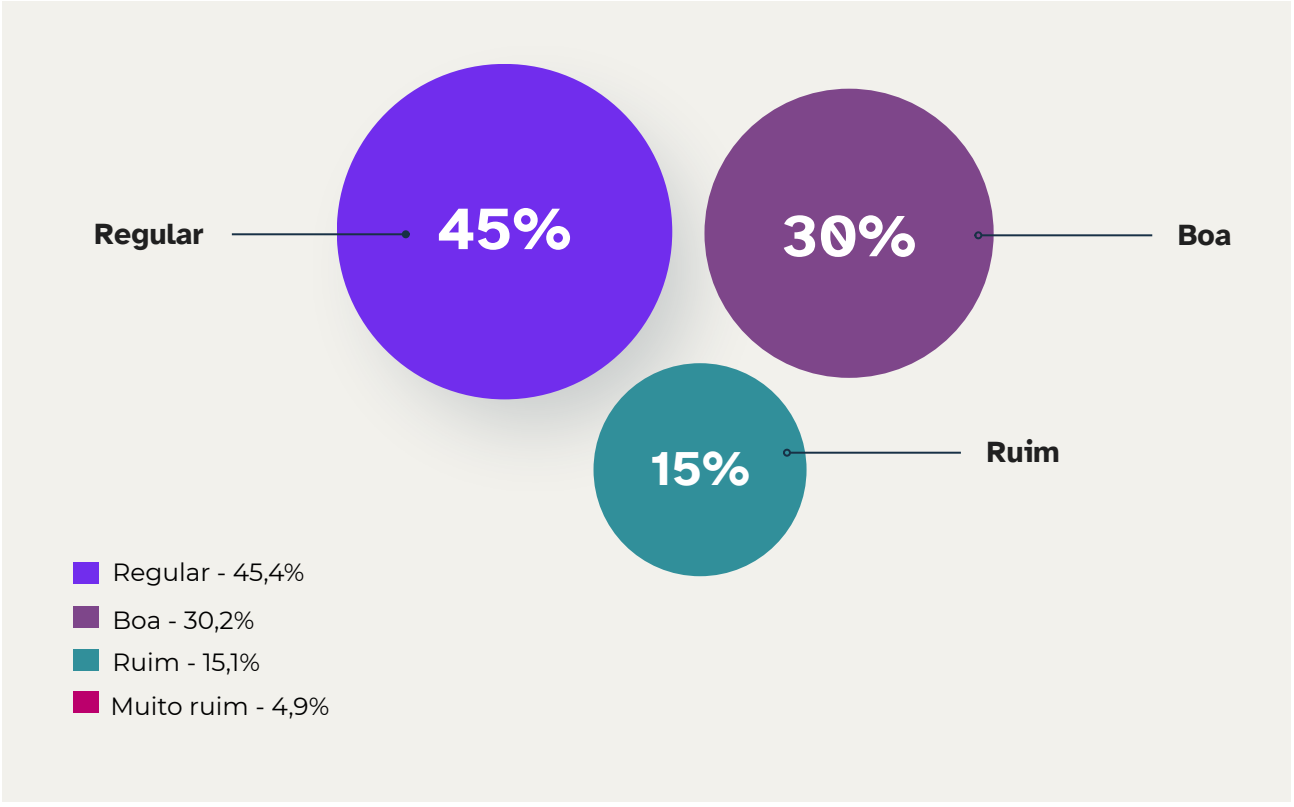
A PNPD25 indicou que 45% dos participantes avaliam a **atuação da Autoridade Nacional de Proteção de Dados (ANPD)** como "regular", enquanto 30% a classificam como "boa". Esse resultado reflete um **reconhecimento dos avanços institucionais** alcançados até o momento, mas também aponta que parte significativa dos profissionais da área ainda aguarda avanços em aspectos estratégicos e operacionais da Autoridade.

Embora a ANPD tenha desempenhado um papel relevante na consolidação da agenda de proteção de dados no Brasil, **pode-se sugerir algumas áreas que demandam evolução.** A primeira diz respeito à **capacidade operacional**, já que limitações de estrutura e de recursos humanos podem afetar a eficácia das ações de fiscalização e o atendimento ágil às demandas dos diversos setores regulados.

Outro ponto é a comunicação institucional. Infere-se que pode existir uma expectativa por mais clareza, agilidade e previsibilidade nas orientações emitidas pela ANPD, sobretudo no que diz respeito à interpretação da LGPD e à aplicação de sanções. Além disso, a **transparência nas decisões e processos regulatórios** ainda é percebida como uma área em desenvolvimento.

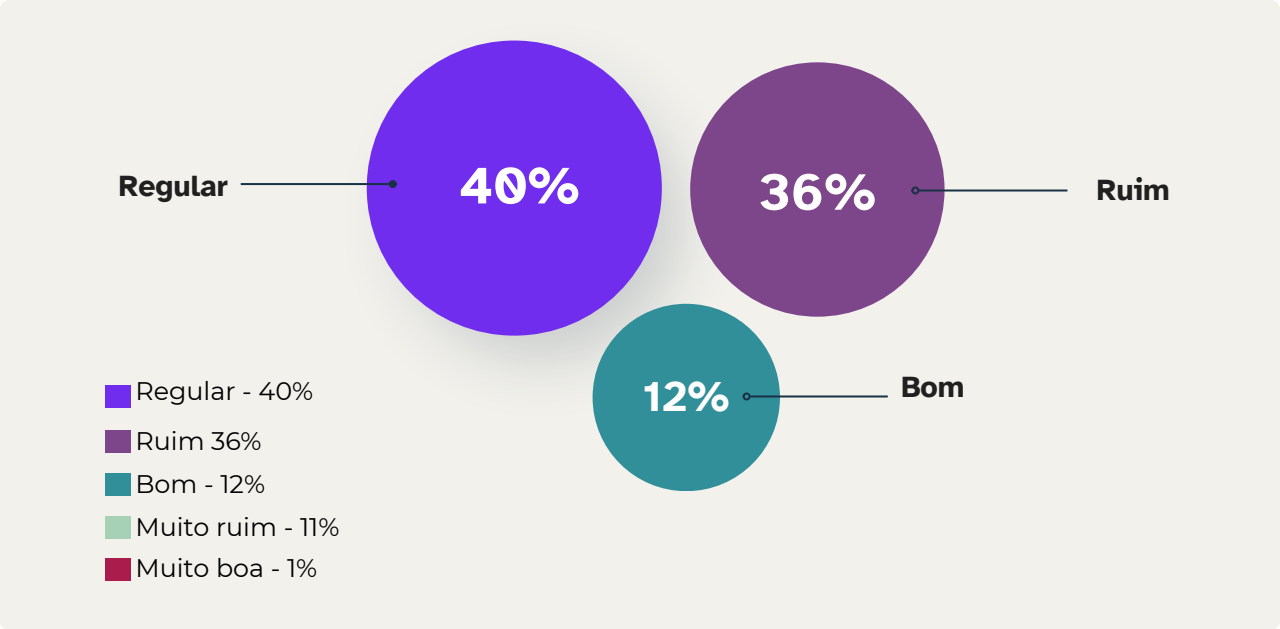
Por fim, destaca-se a importância de a ANPD **ampliar seu diálogo com a sociedade civil, empresas e entes públicos**, promovendo uma participação mais ampla e colaborativa na construção da cultura de proteção de dados no país. Embora a atuação da Autoridade seja reconhecida como essencial, a avaliação "regular" atribuída por boa parte dos profissionais demonstra que há espaço — e urgência — para **fortalecer sua estrutura, intensificar o engajamento com a sociedade e tornar sua comunicação mais acessível e eficaz**.

A percepção da atuação da ANPD



4. Percepção sobre a atuação do Judiciário

A percepção sobre a atuação e o preparo do Judiciário Brasileiro em relação a temas de Proteção de Dados



Desde que entrou em vigor em 2020, a LGPD vem ganhando espaço nas decisões judiciais brasileiras. De acordo com a quarta edição do Painel LGPD, elaborado pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) em parceria com o Jusbrasil e com apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD),[2] **o número de decisões que aplicam LGPD de forma substancial teve um significativo aumento desde a primeira edição do painel (1ª edição: 274; 2ª edição: 629; 3ª edição: 1234; 4ª edição: 1109).** Esse crescimento sinaliza uma **evolução na conscientização do Poder Judiciário** sobre a importância da proteção de dados e um avanço na incorporação da LGPD às práticas decisórias.

Apesar desse avanço quantitativo, persistem desafios significativos no plano qualitativo. Muitas decisões ainda tratam a LGPD de forma tangencial, sem aprofundar os conceitos fundamentais da legislação, como os princípios de finalidade, adequação, necessidade e responsabilização. **Em diversos casos, a LGPD é apenas mencionada como complemento a outras normas já consolidadas**, como o Marco Civil da Internet ou o Código de Defesa do Consumidor, sem uma análise específica de suas disposições e sem reconhecimento pleno de sua autonomia normativa.

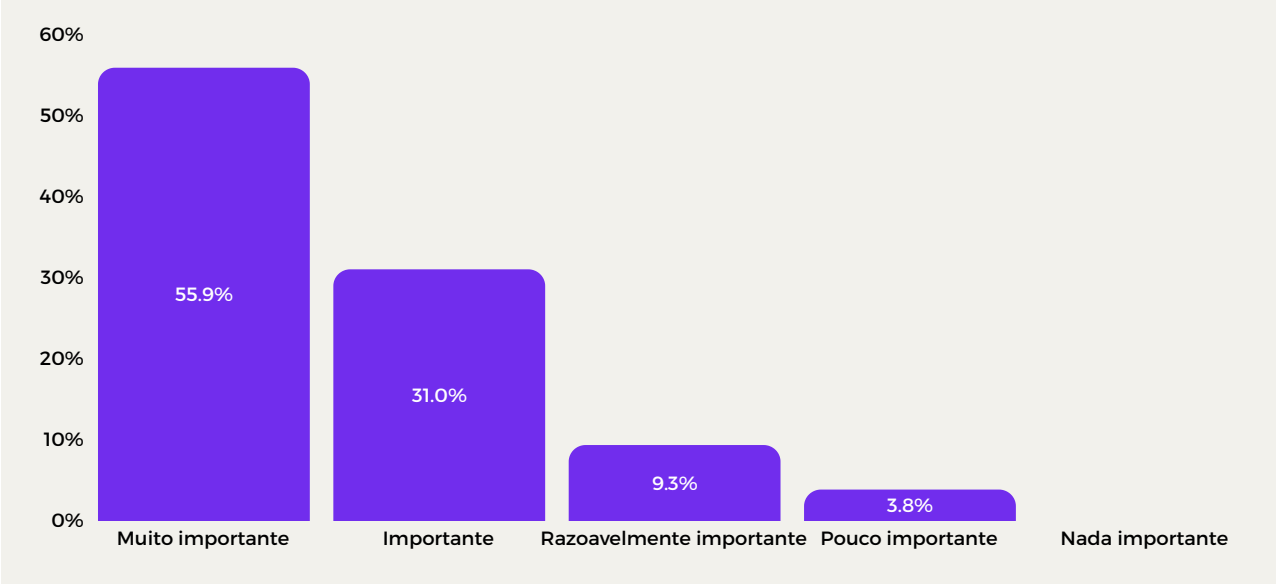
2. Painel LGPD JusBrasil (https://painel.jusbrasil.com.br/)

Essa realidade reforça a percepção, amplamente compartilhada entre especialistas e profissionais da área, de que **o Judiciário brasileiro ainda está em processo de amadurecimento na aplicação da LGPD**. Embora haja avanços consistentes, como o aumento no número de decisões e a atuação do Superior Tribunal de Justiça (STJ) na consolidação de entendimentos mais estruturados, **ainda há um longo caminho a ser percorrido** para que os princípios e direitos previstos na lei sejam interpretados com a profundidade e coerência que exigem.

Para fortalecer a efetividade da LGPD no contexto judicial, torna-se fundamental **investir na capacitação contínua dos magistrados e operadores do Direito**. Além disso, é necessária uma maior articulação entre o Judiciário e a ANPD, de forma que as decisões estejam alinhadas com as diretrizes técnicas e regulatórias da Autoridade. **A harmonização dessas esferas é um passo fundamental para garantir segurança jurídica, promover decisões mais consistentes e assegurar a proteção adequada dos dados pessoais no Brasil.**

5. Comitê de Proteção de Dados

A importância da estruturação e manutenção dos Comitês



Os Comitês de Proteção de Dados têm um papel estratégico dentro das organizações, especialmente na implementação e sustentação da conformidade com a Lei Geral de Proteção de Dados (LGPD). Como **instâncias de natureza multidisciplinar**, esses comitês reúnem representantes de diferentes áreas para atuar de forma coordenada em diversas frentes, desde a definição de políticas até o monitoramento de práticas internas relacionadas ao tratamento de dados pessoais. **Cabe a esse grupo liderar a elaboração e atualização de diretrizes internas,** assegurando o alinhamento com as exigências legais e regulatórias, além de acompanhar continuamente as atividades da organização para garantir uma governança madura. Entretanto, mesmo com sua importância amplamente reconhecida, a **estruturação e funcionamento efetivo dos comitês de proteção de dados ainda esbarram em diversos desafios.**

Para que esses comitês cumpram sua missão com efetividade, **é necessário que estejam formalmente reconhecidos dentro da estrutura de governança corporativa**, recebam apoio institucional e contem com membros devidamente capacitados. É fundamental que haja **clareza quanto às atribuições de cada participante, bem como um esforço contínuo de alinhamento entre áreas**, promovendo uma atuação articulada e estratégica. Com uma **base sólida de apoio e estrutura,** os comitês de proteção de dados contribuem significativamente para fortalecer a governança, garantir a conformidade com a LGPD e construir uma cultura organizacional comprometida com a ética e a proteção de dados pessoais.

O Encarregado pelo Tratamento de Dados Pessoais nos comitês

Na percepção da maioria dos respondentes da PNPD25, **o Encarregado pelo Tratamento de Dados Pessoais (DPO) deve exercer a liderança do Comitê de Proteção de Dados,** sendo o responsável por organizar as reuniões e conduzir as decisões estratégicas. Essa leitura, que obteve 414 menções, reflete uma expectativa de protagonismo por parte do encarregado de proteção de dados, o que está alinhado com a maturidade que essa função vem adquirindo nas organizações brasileiras. Esse reconhecimento enquanto líder do comitê reflete o **reconhecimento de seu papel técnico e ético** na estrutura organizacional.

O papel do DPO nos comitês

65%	Líder (lidera e organiza as reuniões e decisões)
25%	Membro participante comum (contribui nas discussões, mas sem papel de liderança)
10%	Apenas para pareceres, mas sem direito a voto (fornece pareceres, mas não participa ativamente das decisões

A LGPD, no artigo 41, define que **o encarregado deve atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD**, além de orientar colaboradores sobre práticas de proteção de dados e executar outras atividades determinadas pela organização. Embora a lei não estabeleça explicitamente o encarregado como líder de comitês, também não restringe esse papel, abrindo **espaço para que sua atuação seja definida conforme a estrutura e cultura da organização**.

Entretanto, essa centralização pode trazer riscos. **Em estruturas organizacionais menores, há o perigo de sobrecarga**, com o encarregado acumulando tarefas operacionais e estratégicas, o que compromete sua efetividade. Também é preciso considerar que, **em algumas empresas, o encarregado não possui autonomia funcional suficiente**, o que pode transformar sua posição no comitê em algo meramente simbólico. **Outro ponto crítico é o potencial conflito de interesses:** se o encarregado também estiver vinculado a áreas operacionais, como o jurídico ou o TI, sua independência pode ser comprometida. A própria ANPD já sinalizou a importância da independência funcional do encarregado, inclusive para que ele possa se opor a decisões internas, quando necessário.

Para que **o protagonismo do encarregado se traduza em impacto real**, é preciso garantir condições institucionais que preservem sua independência, distribuam responsabilidades de forma equilibrada e promovam uma governança sólida e compartilhada da proteção de dados.

6. Uso de plataformas

A utilização de plataformas que automatizam as atividades de Governança em Proteção de Dados

Essa visão reflete diretamente **o nível de complexidade organizacional para assegurar a proteção de seus dados.** A dependência que as empresas tem dos dados atualmente é intensa e qualquer incidente pode impactar imediatamente seus processos de negócio, clientes e parceiros. Além disso, a LGPD impõe às organizações uma série de obrigações recorrentes e integradas, como manter o ROPA, conduzir avaliações de impacto (DPIA), controlar e revisar contratos com terceiros.

Nesse contexto, sem o **apoio de ferramentas tecnológicas,** esses processos tornam-se operacionalmente difíceis e até inviáveis, especialmente em empresas que lidam com grandes volumes de dados ou com estruturas descentralizadas. **Outro fator relevante que se pode inferir é a redução de falhas associadas à gestão manual.** Planilhas dispersas, controles via e-mail e ausência de versionamento dificultam a rastreabilidade e aumentam o risco de erros, retrabalho ou inconsistência nas informações. **As plataformas especializadas oferecem recursos de padronização e centralização, facilitando a governança, o controle de revisões e a geração de relatórios de forma segura e auditável.**

Além disso, algumas soluções automatizam o **processo de avaliação de riscos de fornecedores**, que é um processo fundamental nas empresas, assim como permitem a criação de portais para os próprios titulares de dados acompanharem suas solicitações, o que melhora a experiência do usuário e **reduz o esforço operacional das equipes envolvidas.**

Apesar dessa percepção positiva, a adoção plena de plataformas ainda encontra barreiras importantes. A mais evidente é o custo: ferramentas robustas exigem investimento contínuo e nem sempre estão acessíveis a empresas de pequeno e médio porte. **Por outro lado, o mercado brasileiro já conta com algumas soluções acessíveis e práticas amenizando esse cenário**.

Além disso, muitas organizações em fase inicial de adequação ainda não percebem a complexidade operacional que virá nas etapas seguintes, o que leva à subestimação da necessidade de automação. Por fim, o desconhecimento sobre as opções disponíveis no mercado ou a falta de profissionais preparados para liderar a implementação dessas soluções também são entraves comuns.

De forma geral, o destaque dado às plataformas na PNPD25 aponta para uma **tendência de profissionalização e fortalecimento da governança digital.** As ferramentas tecnológicas ampliam a **capacidade de gestão** por profissionais de proteção de dados, aumentam a confiabilidade das operações e permitem que o programa de proteção de dados se sustente com eficiência no longo prazo. A maturidade em proteção de dados passa, cada vez mais, por uma combinação entre conhecimento técnico, processos bem definidos e uso inteligente da tecnologia.

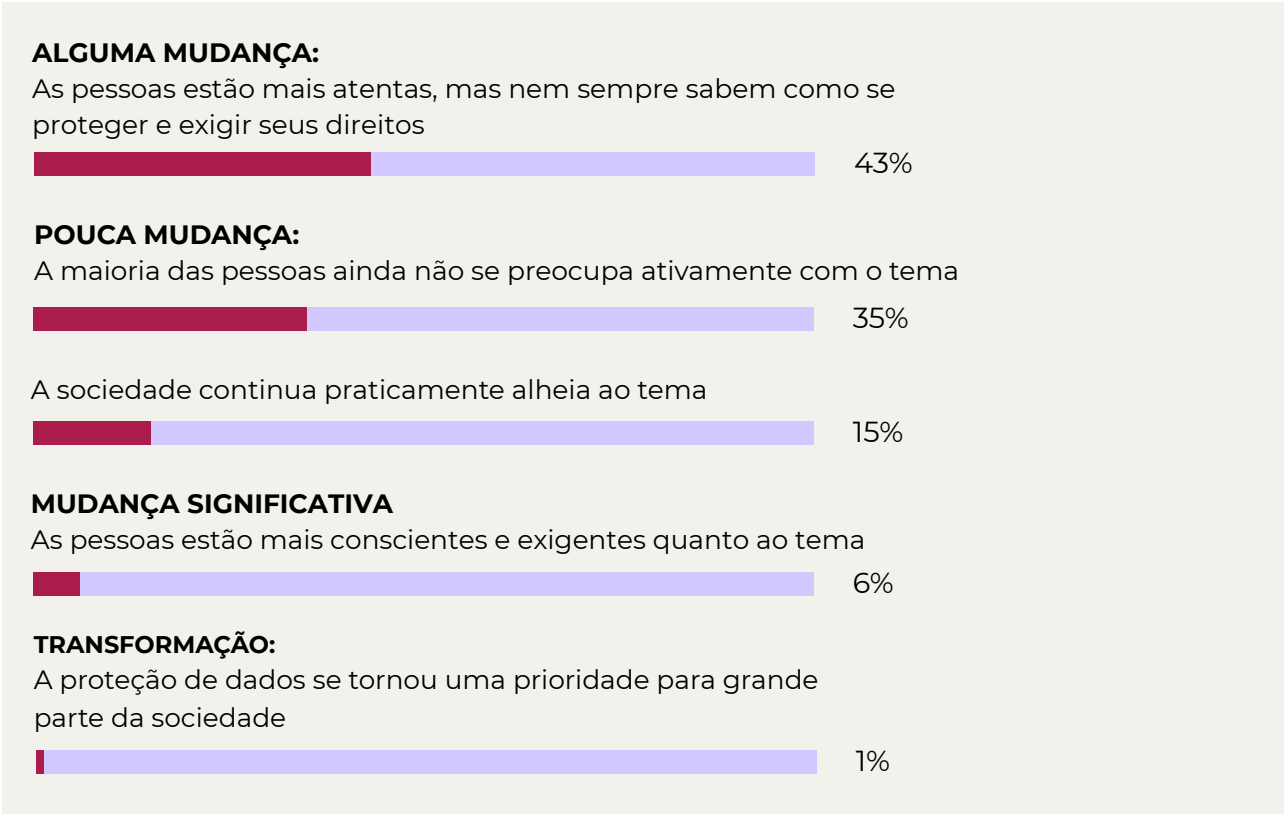
7. Percepção da sociedade brasileira sobre a Proteção de Dados Pessoais

De acordo com os dados da **PNPD25**, 43% dos respondentes acreditam que a população começa a compreender seus direitos em relação aos dados pessoais, embora ainda falte engajamento efetivo. Esse cenário revela um **avanço na sensibilização sobre o tema**, mas também escancara o desafio de transformar essa consciência inicial em ação prática e cidadania digital.

Nos últimos anos, especialmente em 2024, a **ANPD intensificou seus esforços para ampliar o conhecimento da sociedade sobre a LGPD**. Entre as iniciativas estão a **realização de eventos técnicos, a elaboração de materiais educativos e o lançamento de campanhas voltadas à formação** tanto dos titulares quanto dos agentes de tratamento.

Apesar desses avanços institucionais, **persistem barreiras significativas no entendimento e, sobretudo, na aplicação dos direitos previstos em lei.** Muitos indivíduos ainda desconhecem quais são esses direitos, tampouco sabem como exercê-los junto às organizações. Além disso, **é comum a percepção de que a responsabilidade pela proteção de dados recai exclusivamente sobre as empresas,** o que reduz o protagonismo do titular nesse processo.

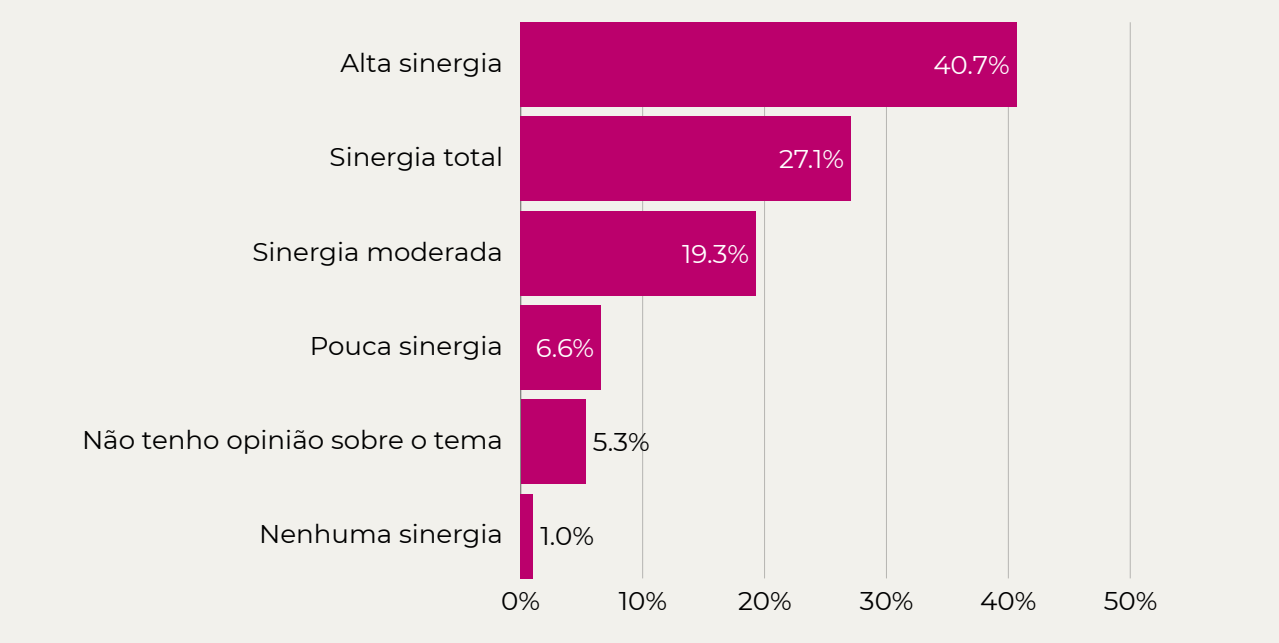
O impacto da LGPD na conscientização da sociedade



A LGPD teve um papel importante ao despertar o interesse da sociedade sobre privacidade, mas ainda falta converter esse alerta em ação. A proteção de dados segue sendo tratada como um tema técnico ou restrito ao jurídico, quando deveria ocupar um lugar central no cotidiano dos titulares. **O momento atual representa uma janela estratégica para consolidar uma cultura de proteção de dados no Brasil**, por meio da educação, do empoderamento dos titulares e do fortalecimento da responsabilidade das empresas no tratamento ético e transparente das informações pessoais.

8. Governança de Proteção de Dados X Governança de IA

O nível de sinergia entre a Governança de Inteligência Artificial (IA) e a Governança de Proteção de Dados



A convergência entre a governança de proteção de dados e a governança de Inteligência Artificial (IA) tem se tornado cada vez mais evidente no cenário corporativo e regulatório. À medida que as organizações avançam no uso de tecnologias baseadas em dados e algoritmos, cresce a necessidade de **integrar práticas que assegurem não apenas a conformidade legal, mas também a gestão de riscos, transparência e, acima de tudo, a ética na tomada de decisões automatizadas.** A possibilidade de conduzir ambas as governanças por uma mesma equipe está diretamente relacionada à maturidade organizacional, à complexidade dos sistemas de IA utilizados e à disponibilidade de recursos técnicos e humanos.

Há diversos pontos em comum entre essas duas áreas. Ambas compartilham **preocupações centrais com a qualidade e integridade dos dados,** reconhecendo que decisões — humanas ou automatizadas — dependem de informações confiáveis e bem estruturadas. Do ponto de vista regulatório, tanto a proteção de dados quanto a governança de IA exigem aderência a marcos legais como a LGPD no Brasil e o GDPR na Europa, que impõem obrigações relacionadas à finalidade, à minimização e à segurança dos dados.

Além disso, a transparência é um princípio-chave para as duas frentes: enquanto a proteção de dados requer clareza quanto ao uso das informações pessoais, a governança de IA demanda explicabilidade dos algoritmos e responsabilidade pelas decisões tomadas por sistemas automatizados. Outro elo importante é a segurança da informação, que constitui a base técnica para prevenir acessos não autorizados e **proteger tanto dados pessoais quanto modelos de IA contra vulnerabilidades e abusos.**

Para enfrentar esses desafios, algumas estratégias são recomendadas.

- **Investir na formação de equipes multidisciplinares** é essencial, combinando conhecimentos em direito, tecnologia, ética e gestão de riscos.

- **A criação de comitês internos com representantes de diferentes áreas** pode fortalecer o alinhamento entre as práticas de governança e facilitar a tomada de decisões baseadas em critérios técnicos e regulatórios.

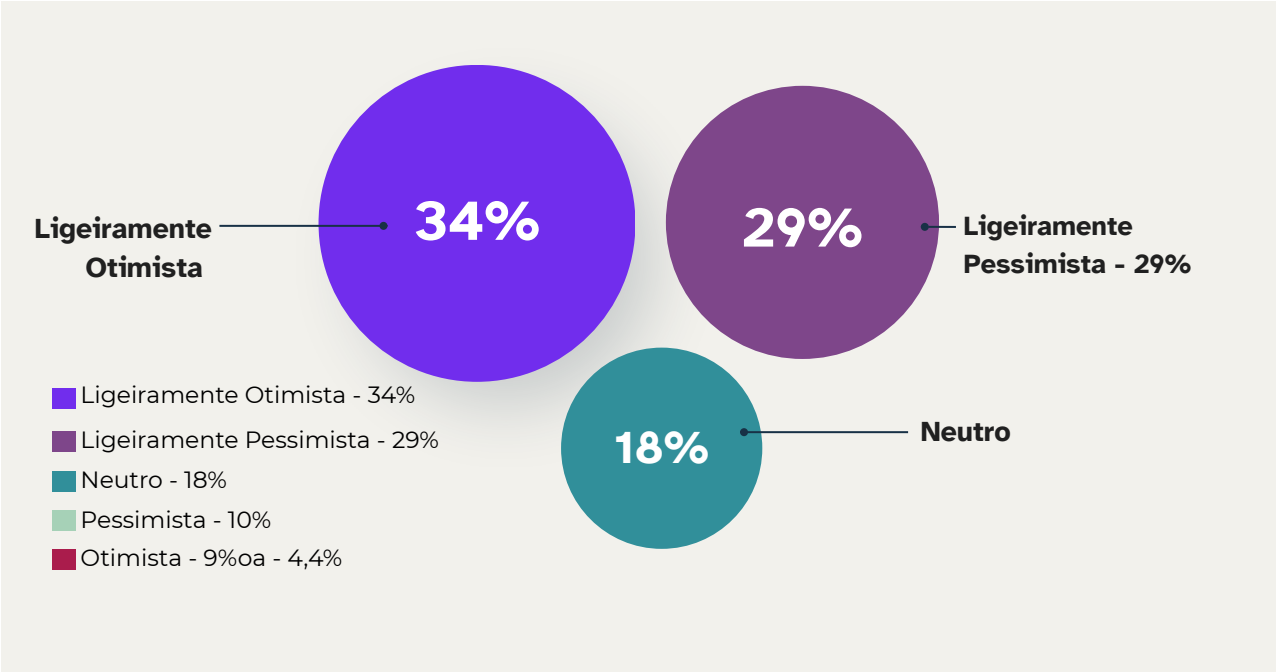
- **A adoção de frameworks reconhecidos internacionalmente**, como a norma ABNT NBR ISO/IEC 42001 — voltada especificamente à governança de IA —, pode oferecer uma base estruturada para lidar com os riscos e obrigações dessa nova fronteira tecnológica.

- Além disso, **o uso de ferramentas tecnológicas que automatizem e monitorem processos de governança** contribui para aumentar a eficiência e reduzir o risco de não conformidade.

Em síntese, quando conduzida com planejamento, capacitação e suporte institucional, **a integração entre a governança de proteção de dados e a de inteligência artificial promove uma abordagem mais ética, transparente e estratégica no uso da tecnologia,** alinhada às expectativas legais e sociais do mundo contemporâneo.

9. O que esperar do Futuro?

O otimismo quanto a capacidade da sociedade proteger os dados pessoais no futuro



A pergunta da PNPD25 sobre **o nível de otimismo em relação ao futuro da proteção de dados pessoais** revelou um cenário de **expectativas moderadas** entre os profissionais da área. A maioria dos respondentes se declarou ligeiramente otimista (231 respostas), enquanto uma parcela quase equivalente demonstrou ligeiro pessimismo (198 respostas), mostrando um resultado interessante, pois embora a expectativa tenha resultado como moderada, as respostas majoritárias foram antagônicas. **Essa divisão reflete uma percepção de que, embora avanços tenham sido alcançados nos últimos anos**, ainda há **incertezas relevantes** quanto à capacidade de a sociedade — incluindo usuários, empresas e o poder público — garantir efetivamente **a proteção de dados nos próximos cinco a dez anos.**

Um dos principais fatores que sustentam esse otimismo contido é a velocidade com que surgem novas tecnologias, como a inteligência artificial generativa, a Internet das Coisas, os sistemas biométricos e, futuramente, a computação quântica. Esses avanços, embora promissores, ampliam de forma exponencial a quantidade de dados gerados, a complexidade dos fluxos de tratamento e a opacidade dos processos automatizados. Isso gera benefícios inegáveis, mas também impõe novos riscos. A governança sobre esse ecossistema se torna cada vez mais desafiadora.

No **campo regulatório, o Brasil avançou consideravelmente com a consolidação da LGPD** como referência legal, o fortalecimento institucional da ANPD e a proposição de normativas específicas, como o Projeto de Lei 2338/2023, que trata do uso ético da inteligência artificial. Ainda assim, **a regulamentação continua a caminhar em ritmo mais lento do que a inovação tecnológica, o que cria lacunas e incertezas na aplicação prática da lei**. Essa **defasagem entre regulação e tecnologia** representa um risco estrutural para a efetividade das normas e a proteção dos titulares.

Outro ponto de atenção é a **maturidade da sociedade brasileira diante do tema**. Embora o interesse por privacidade e proteção de dados tenha crescido nos últimos anos, especialmente com a entrada em vigor da LGPD e com a repercussão de casos de vazamento, **o conhecimento técnico da população sobre seus direitos ainda é limitado**. A educação digital não é amplamente disseminada e, muitas vezes, não chega de forma acessível às camadas mais vulneráveis. Isso compromete o empoderamento dos cidadãos e enfraquece sua capacidade de agir como sujeitos ativos na defesa de sua privacidade.

Diante desse contexto, **o cenário desenhado pela pesquisa é de realismo com espaço para progresso**. Houve avanços significativos, especialmente no arcabouço legal e institucional, mas permanecem atentos às limitações estruturais que ainda desafiam a **consolidação de uma cultura robusta de proteção de dados no país**. O futuro dependerá do equilíbrio entre três pilares fundamentais: uma regulação eficaz, capaz de acompanhar a velocidade da inovação; tecnologias desenvolvidas de forma ética e com mecanismos de explicabilidade e controle; e uma sociedade consciente, bem informada e participativa, capaz de exercer plenamente seus direitos no ambiente digital. **O momento atual é, portanto, uma oportunidade para amadurecer essa convergência e fortalecer as bases da privacidade como valor democrático e estratégico.**

10. Insights

Principais reflexões e considerações

I

A Proteção de dados não deve ser tratada como um projeto pontual, mas como um **programa contínuo de governança,** que assegura manutenção, evolução constante e, acima de tudo, engajamento ativo da liderança.

II

Apesar de reconhecido como essencial, o **inventário de operações (ROPA) segue sendo um desafio central**, impactado por baixa automação, falta de envolvimento das áreas e processos pouco integrados.

III

O engajamento organizacional, sobretudo da alta liderança, continua sendo um **desafio importante**, que pode ser trabalhado com uma **abordagem mais orientada ao negócio** – e não apenas regulatória.

IV

Plataformas especializadas têm potencial grande de transformar a gestão dos programas de governança em proteção de dados.

V

Cresce a aplicação da LGPD nas decisões judiciais, mas ainda há lacunas de aprofundamento conceitual e pouca articulação com as diretrizes da ANPD, o que impacta a segurança jurídica

VI

Há expectativa de protagonismo do DPO na governança interna, especialmente liderando comitês de proteção de dados, mas isso requer autonomia funcional, capacitação e equilíbrio de responsabilidades.

VII

A população começa a compreender seus direitos, mas o exercício ativo ainda é limitado. A educação digital é chave para transformar conhecimento em cidadania.

VIII

A integração entre proteção de dados e governança de IA é cada vez mais necessária. Ambas compartilham princípios e riscos, exigindo estruturas conjuntas, times multidisciplinares e marcos regulatórios compatíveis.

IX

Profissionais do setor reconhecem avanços, mas enxergam desafios na maturidade institucional, no acompanhamento regulatório da inovação e na educação da sociedade.

X

O momento atual representa uma chance decisiva de consolidar a proteção de dados como valor estratégico, com base em regulação eficaz, tecnologias responsáveis e um ecossistema social consciente e engajado.

Agradecimento

Nosso especial agradecimento a toda a **comunidade envolvida, direta ou indiretamente, com a proteção de dados**, que contribuiu generosamente respondendo à nossa pesquisa. Sem esse apoio fundamental, essa iniciativa não teria avançado.
Muito obrigado!

A Pesquisa Nacional de Proteção de Dados 2025 foi realizada com o apoio de:

Netuno Network

Fórum de Proteção de Dados do Interior Paulista

Podium

SimpleWay
CyberSecurity & Privacy & AI Governance and Management

Pesquisa Nacional de *Proteção de Dados* 2025