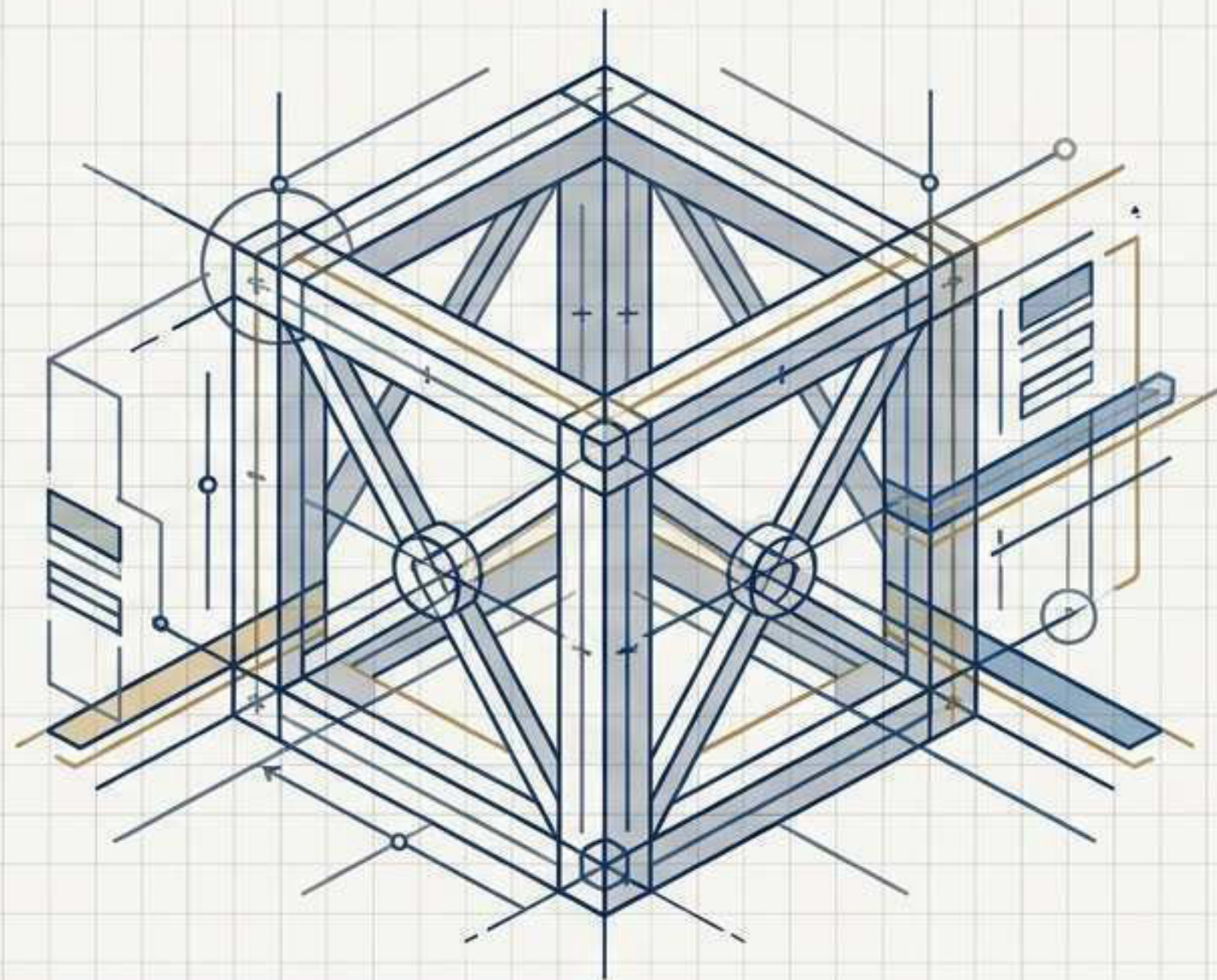


Governança de Dados de PEPs: O Equilíbrio Exato entre LAI e LGPD

Um **guia tático para gestores públicos**, DPOs e equipes de compliance sobre como tratar dados de Pessoas Expostas Politicamente sem comprometer a transparência ou a privacidade.

PEPs na Era da Governança de Dados

Equilibrando LGPD e LAI na Administração Pública



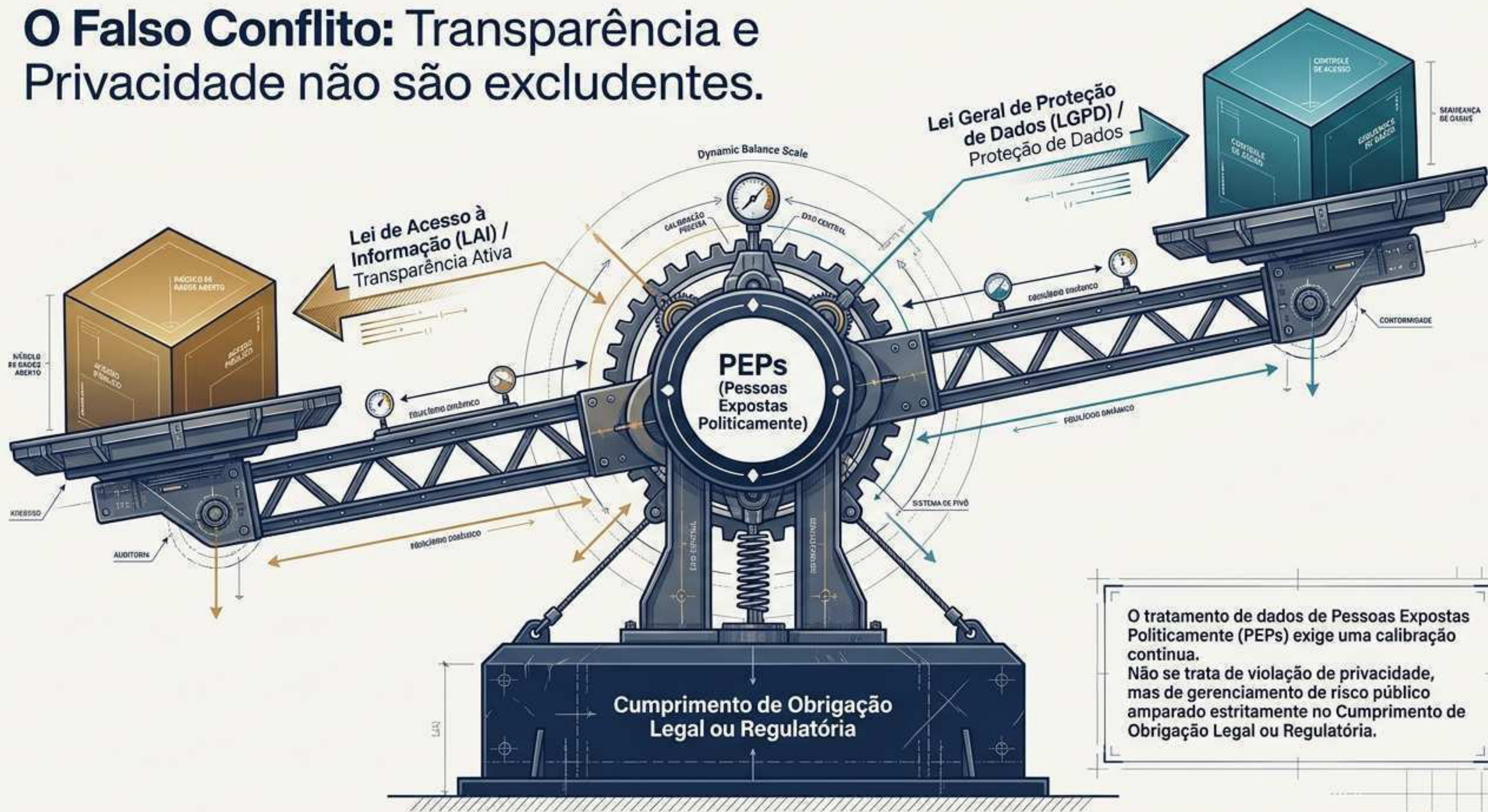
Um Guia Operacional de Melhores Práticas e Curadoria de Recursos



A Engenharia do Risco PEP

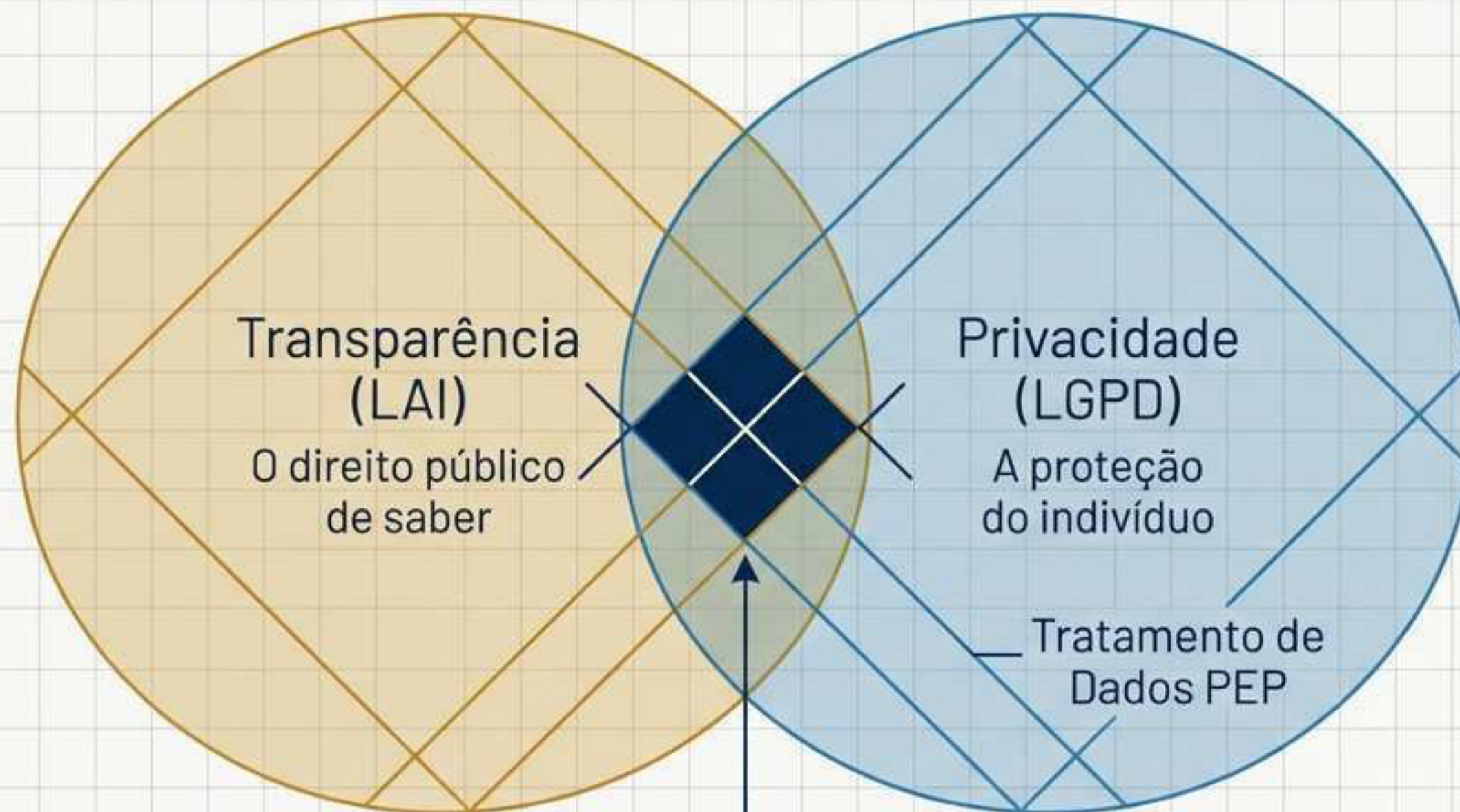
Equilibrando Transparência (LAI) e Privacidade (LGPD) na Governança Pública

O Falso Conflito: Transparência e Privacidade não são excludentes.



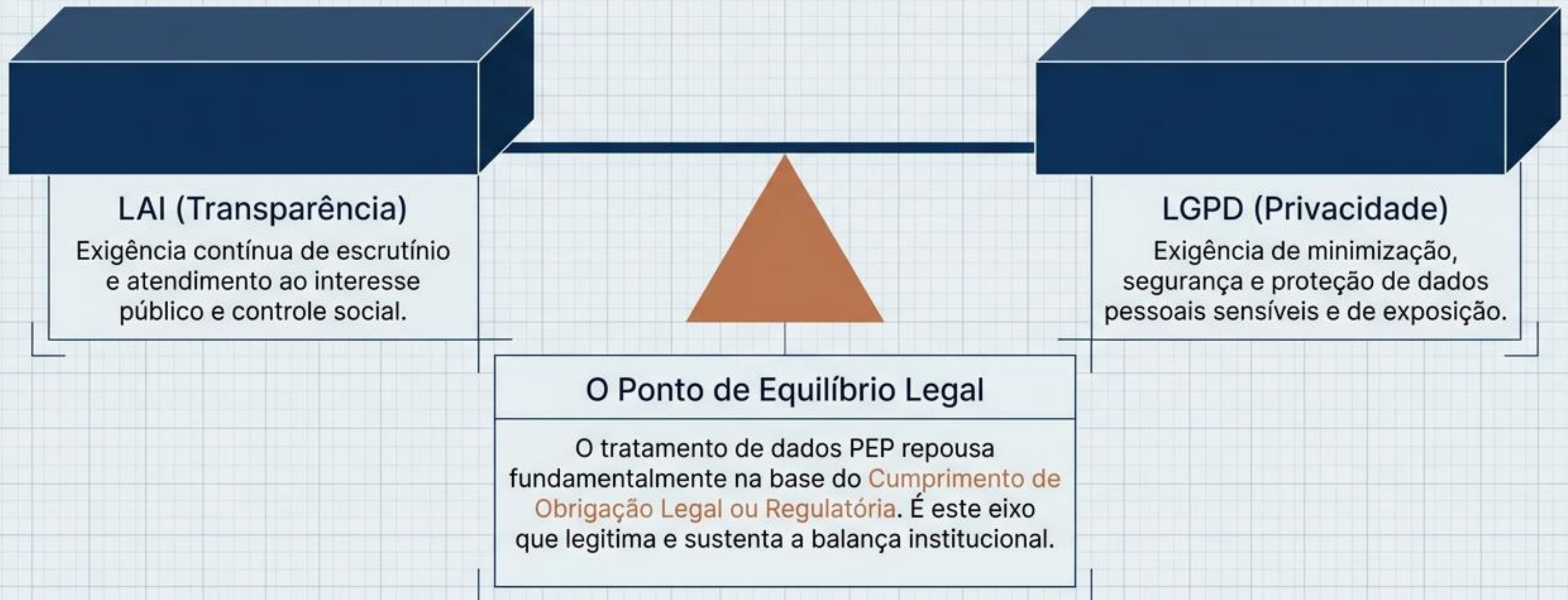
O tratamento de dados de Pessoas Expostas Politicamente (PEPs) exige uma calibração contínua. Não se trata de violação de privacidade, mas de gerenciamento de risco público amparado estritamente no Cumprimento de Obrigação Legal ou Regulatória.

O Grande Paradoxo Regulatório

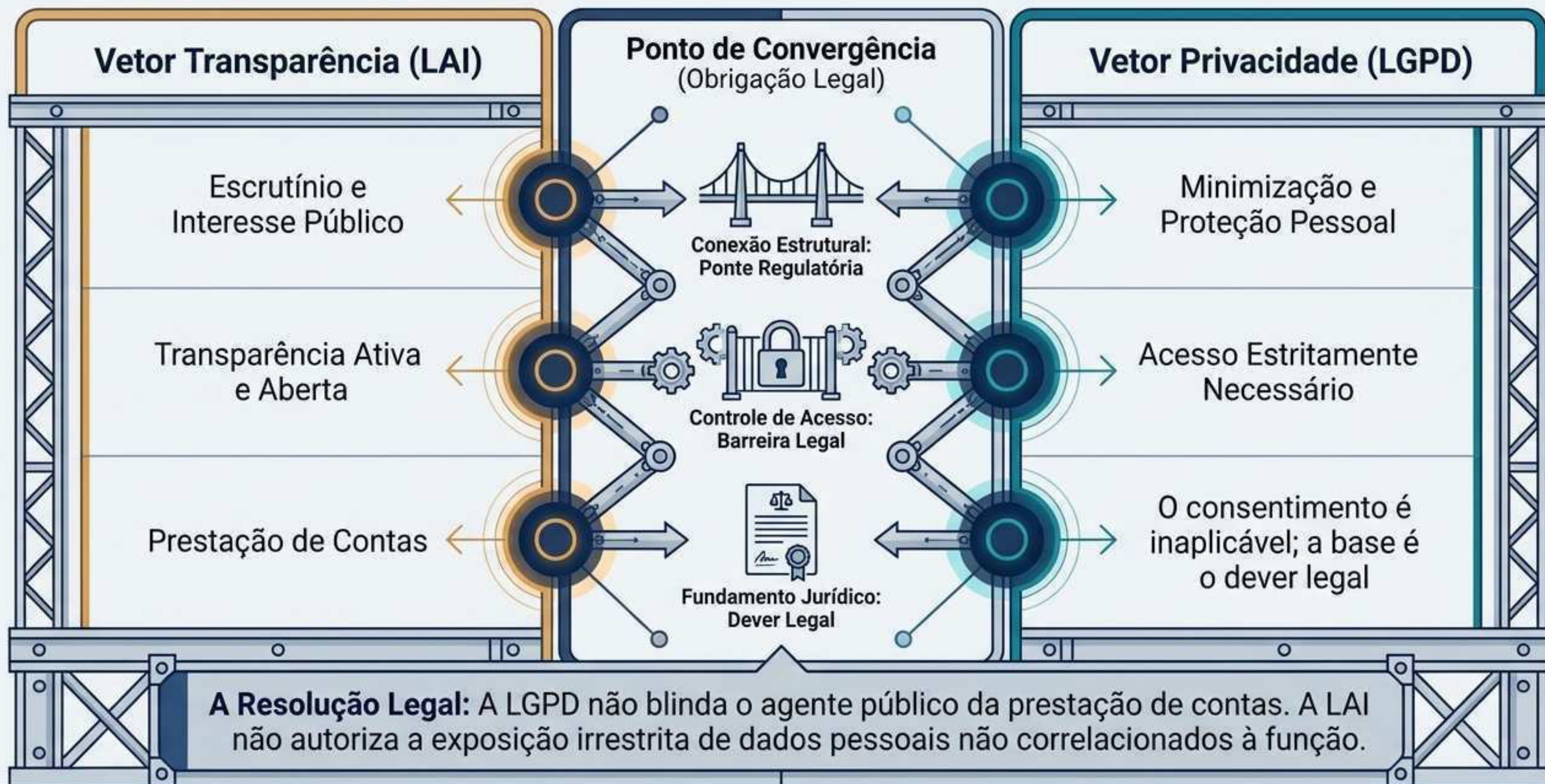


O tratamento de dados de Pessoas Expostas Politicamente (PEPs) exige navegar pela exata intersecção entre o dever de transparência pública e a garantia constitucional de proteção de dados pessoais.

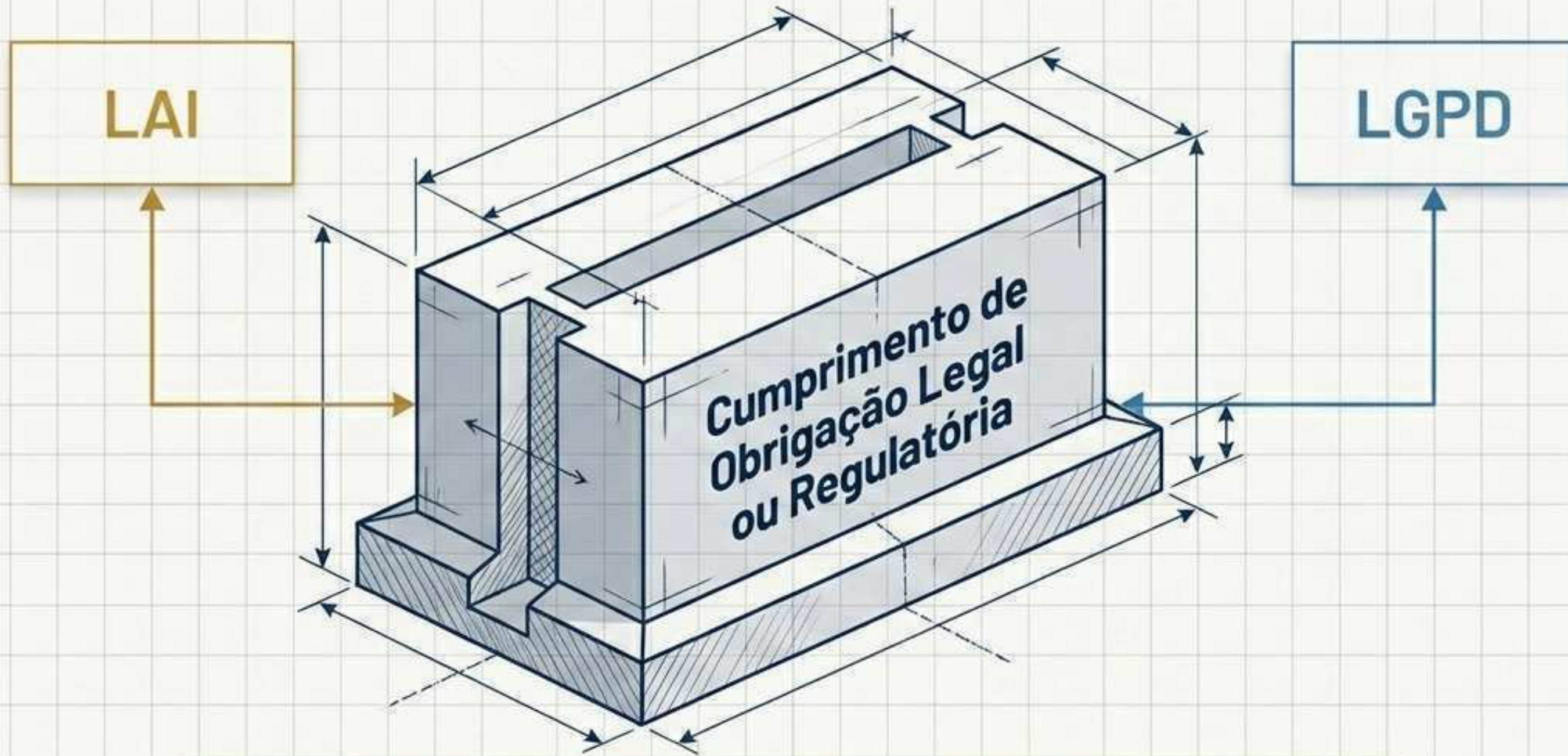
O Paradoxo Estrutural: LAI x LGPD



Matriz de Contenção Operacional



O Alicerce Jurídico Central



Esta é a base legal primária que permite e legitima o processamento de dados de PEPs. Ela atua como a ponte estrutural que satisfaz a transparência (LAI) enquanto justifica a necessidade de tratamento sob a ótica da privacidade (LGPD).

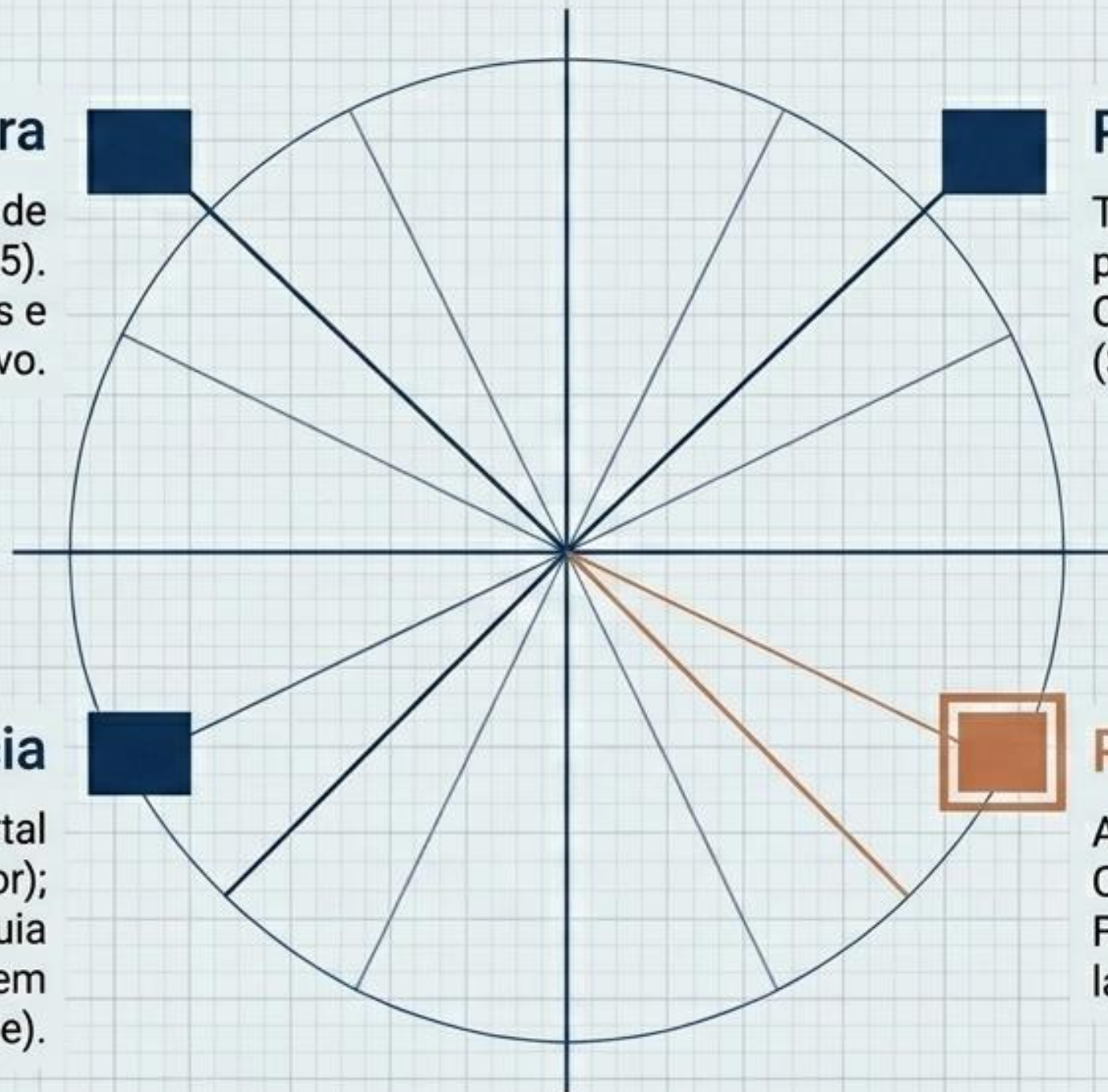
O Ecossistema de Recursos Oficiais

Governança Pura
Governo Digital (SGD) – Trilha de Governança de Dados (Vols. 1 a 5).
Foco: Estruturação de papéis e ecossistema no Executivo.

Privacidade Prática
TCE-RO – Guia Prático LGPD (20 passos para conformidade);
CODATA (PB) – Guia de Boas Práticas (Segurança e privacidade local).

Controle e Transparência
Banco Central (BACEN) – Portal LGPD (Papel do controlador);
Unifesp / Rede Ouvidorias – Guia de Boas Práticas (Tratamento em instâncias de controle).

Risco de Integridade
AML Reputacional – Guia Completo sobre PEPs.
Foco: Riscos de corrupção e lavagem de dinheiro (PLD).



O Ecossistema de Governança: Ferramentas Curadas

Resource Dashboard



Guia Prático LGPD (TCE-RO)

20 passos práticos para órgãos públicos atingirem a conformidade.



Trilha de Governança SGD (Governo Digital)

Estruturação de papéis, responsabilidades e ecossistema de dados no Executivo.



Guia sobre PEPs: Riscos e Lei (AML Reputacional)

Detalhamento de riscos de corrupção, PLD (Lavagem de Dinheiro) e listas de monitoramento.



Boas Práticas de Dados (CODATA-PB)

Orientações focadas no estado da Paraíba sobre segurança e privacidade.



Portal LGPD BACEN (Banco Central)

O papel do BACEN como controlador e a relação com o sistema financeiro.



Guia de LGPD para Ouvidorias (Unifesp)

Tratamento em instâncias de controle e transparência passiva.

O Ecossistema de Recursos Curados

Nenhum guia isolado cobre todas as complexidades. Esta curadoria compila frameworks da administração pública e órgãos de controle em um escudo unificado de conformidade.

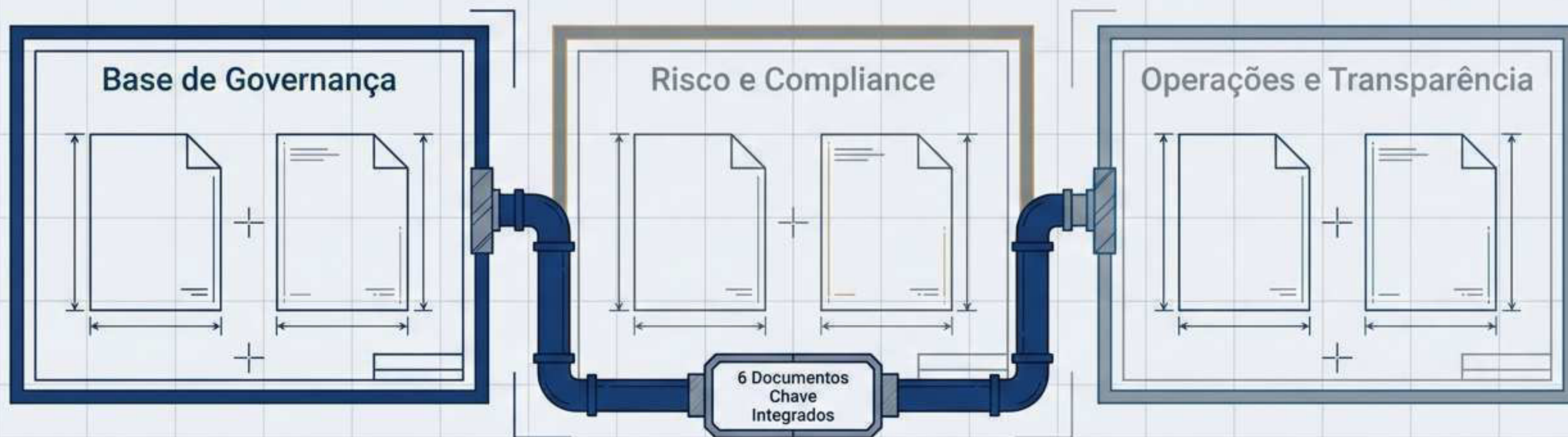
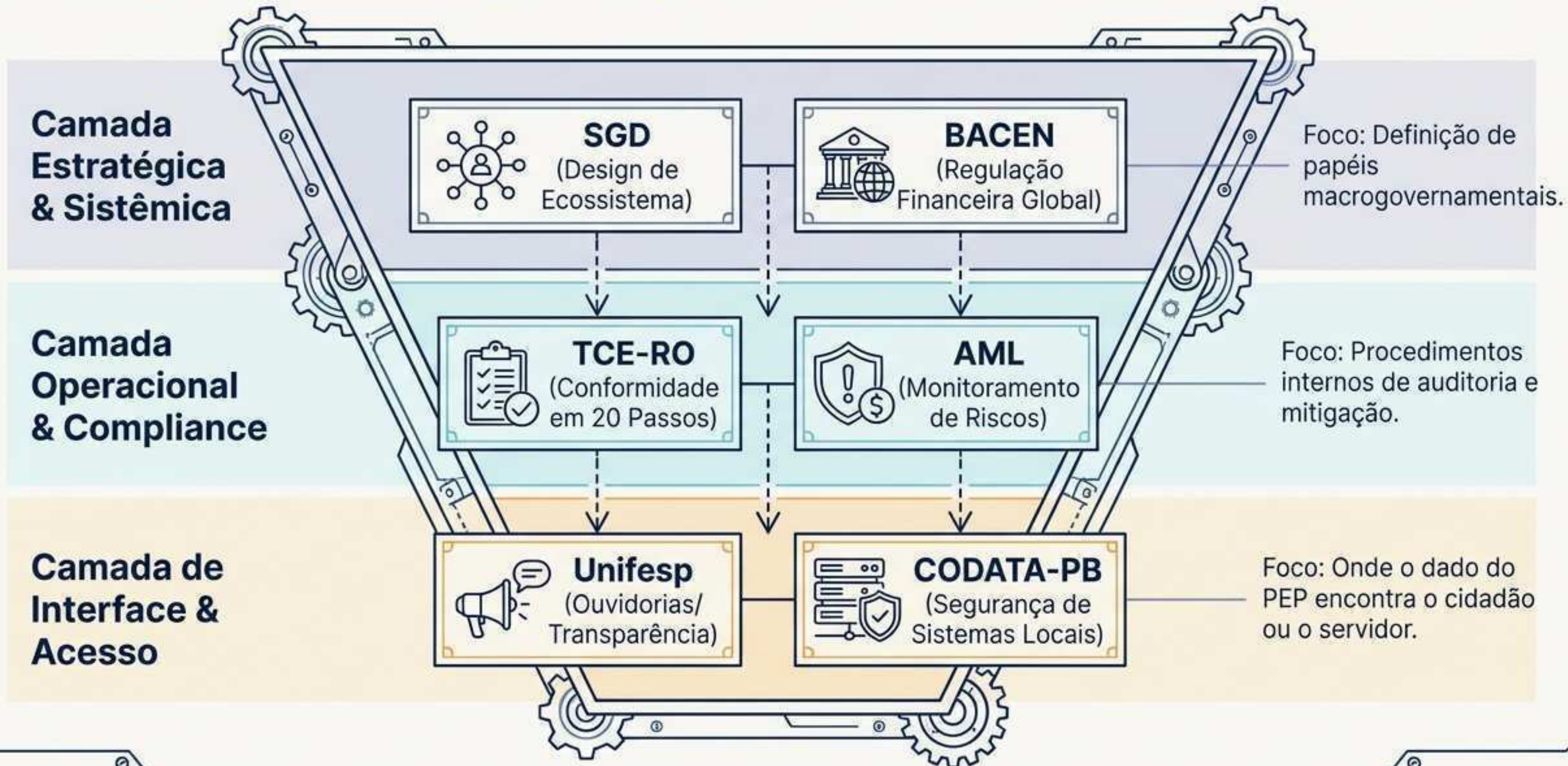
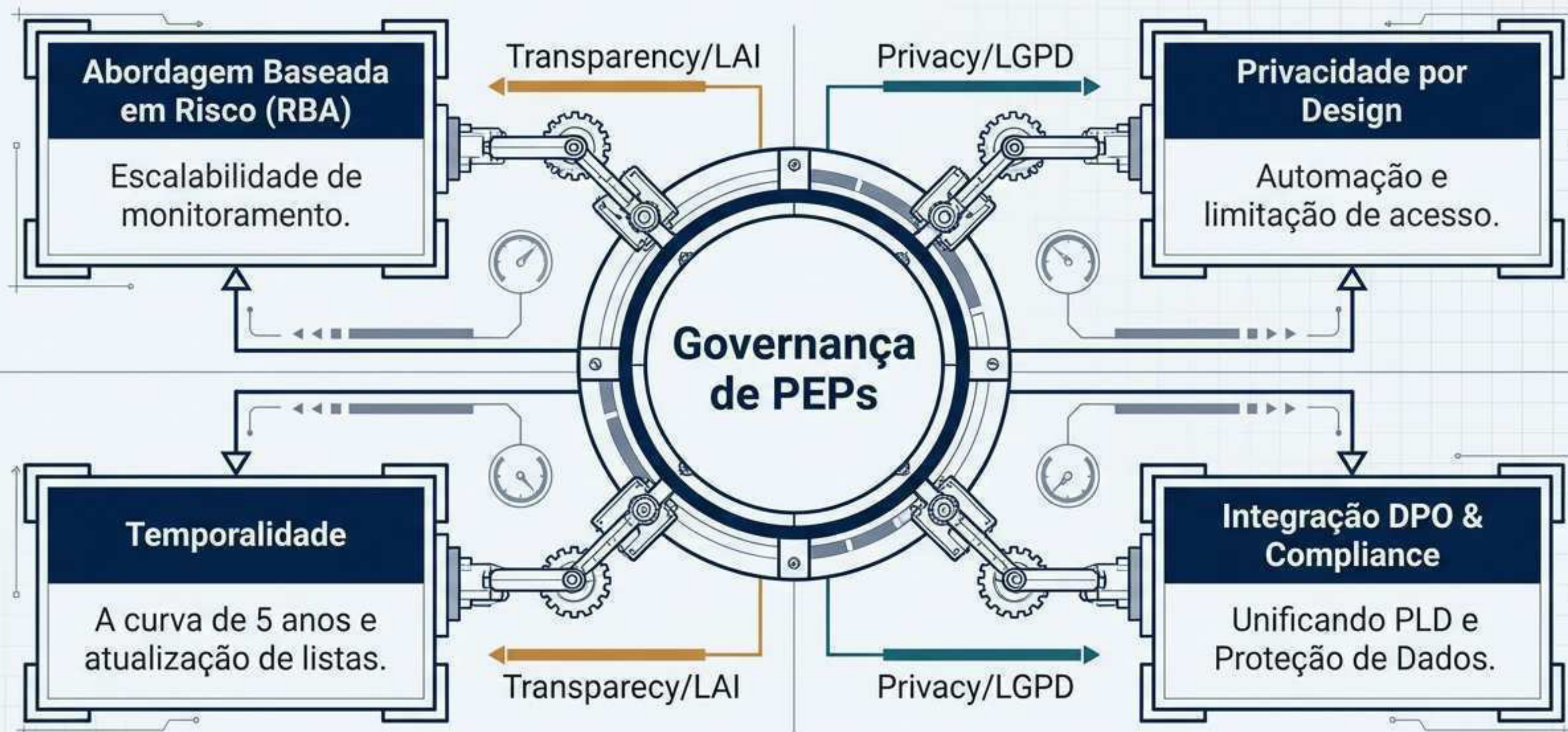


Diagrama de Aplicação Institucional



Os 4 Pilares de Implementação Estratégica



Diretrizes complementares para integrar as exigências do Tribunal de Contas (TCE-PB) aos frameworks nacionais.

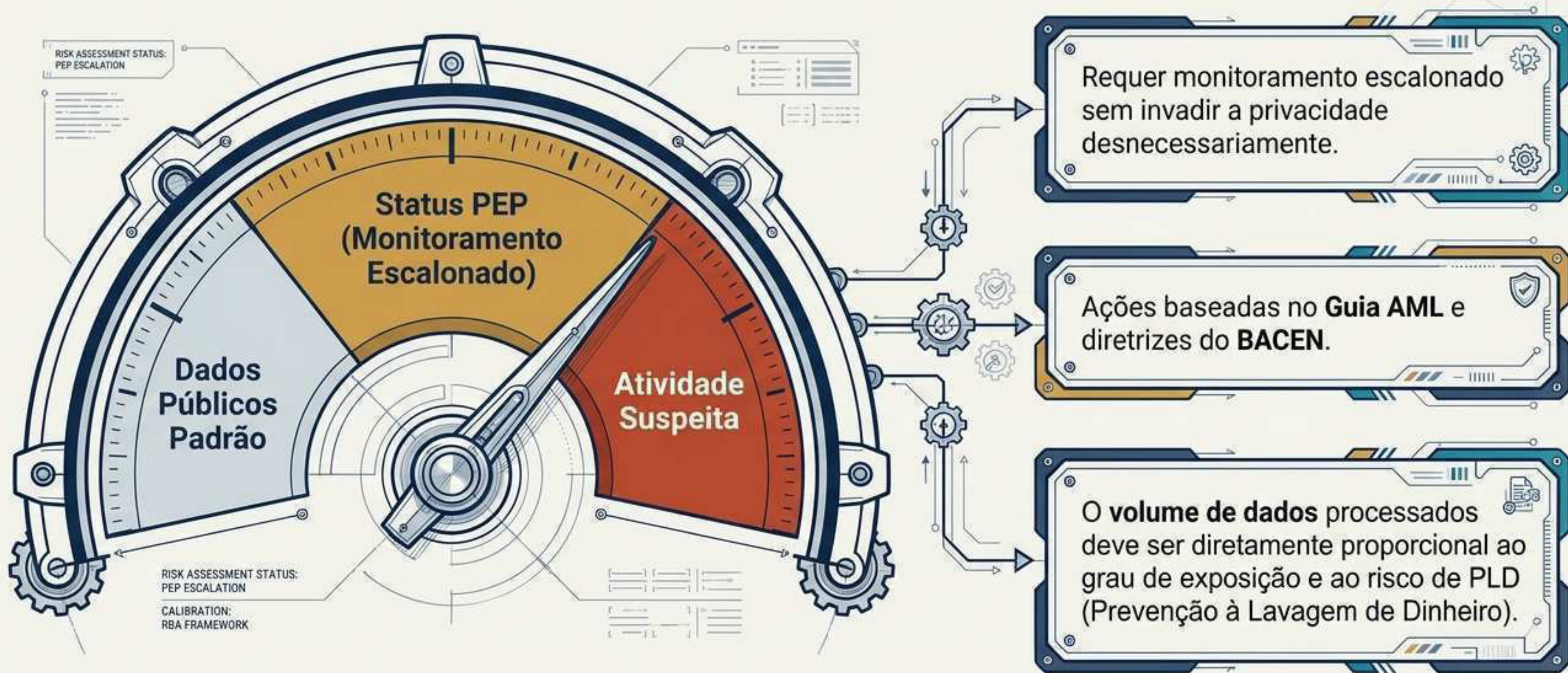
Os 4 Pilares de Implementação

A aplicação prática dos recursos exige quatro observações estratégicas para garantir que o monitoramento seja eficaz sem gerar violações desnecessárias.



Pilar 1: Abordagem Baseada em Risco (RBA)

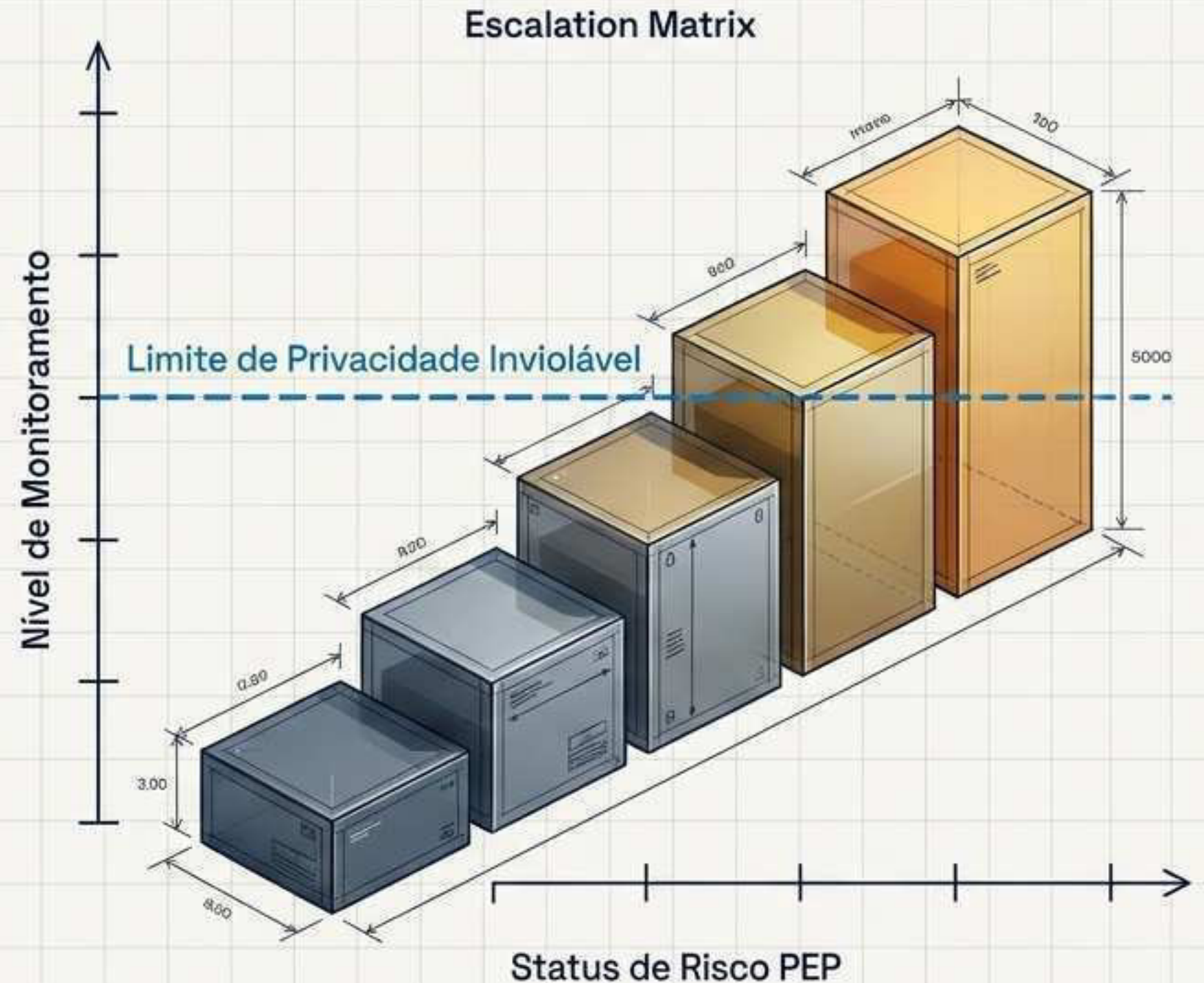
Ser PEP é um “status de risco”, não uma presunção de culpa.



Pilar 1: Abordagem Baseada em Risco (RBA)

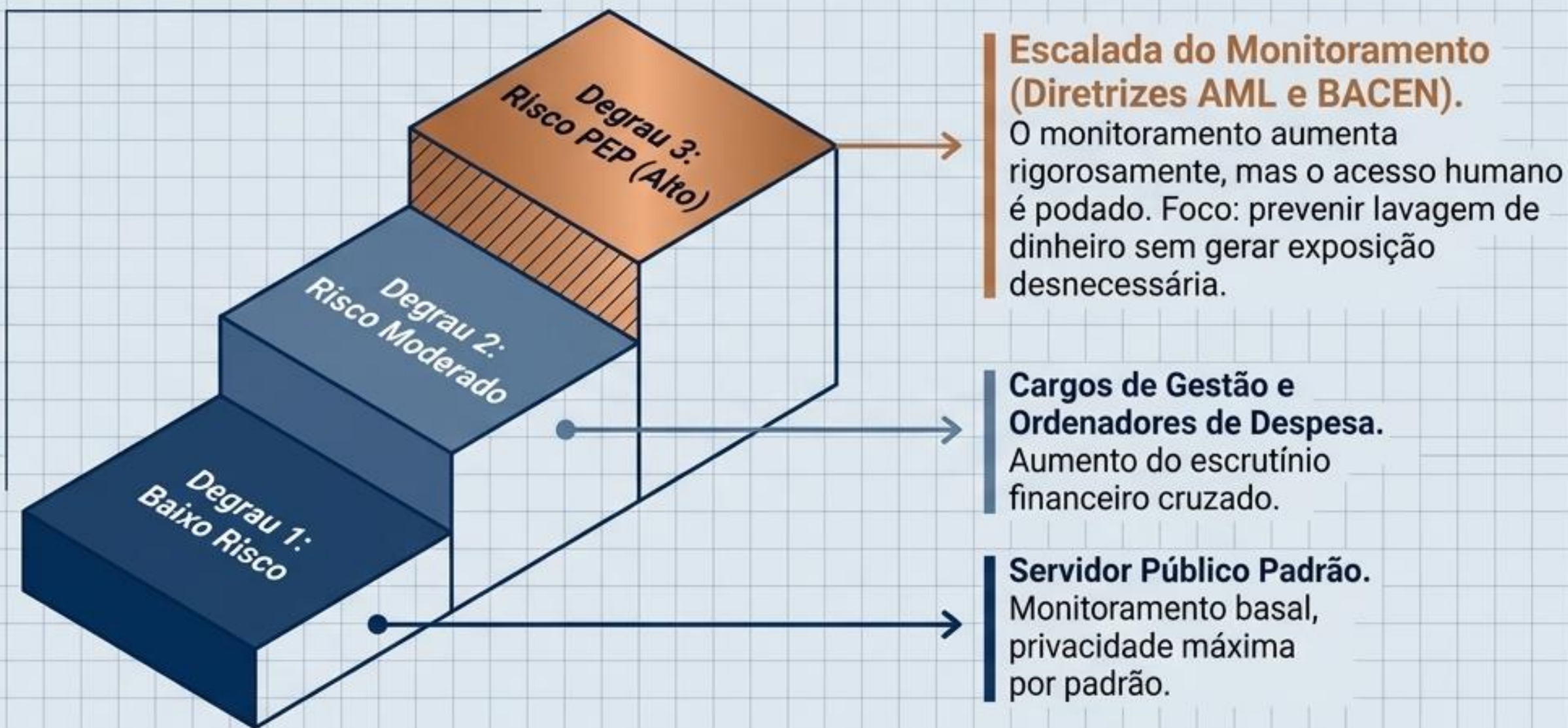
Ser um PEP é, por definição, assumir um 'status de risco'.

Seguindo as diretrizes da AML e do BACEN, o monitoramento deve ser escalado proporcionalmente ao risco identificado, garantindo a eficácia sem violar o núcleo de privacidade desnecessariamente.



Pilar 1: Abordagem Baseada em Risco (RBA)

Ser PEP não é uma infração, é um Status de Risco



Pilar 2: Privacidade por Design (PbD)

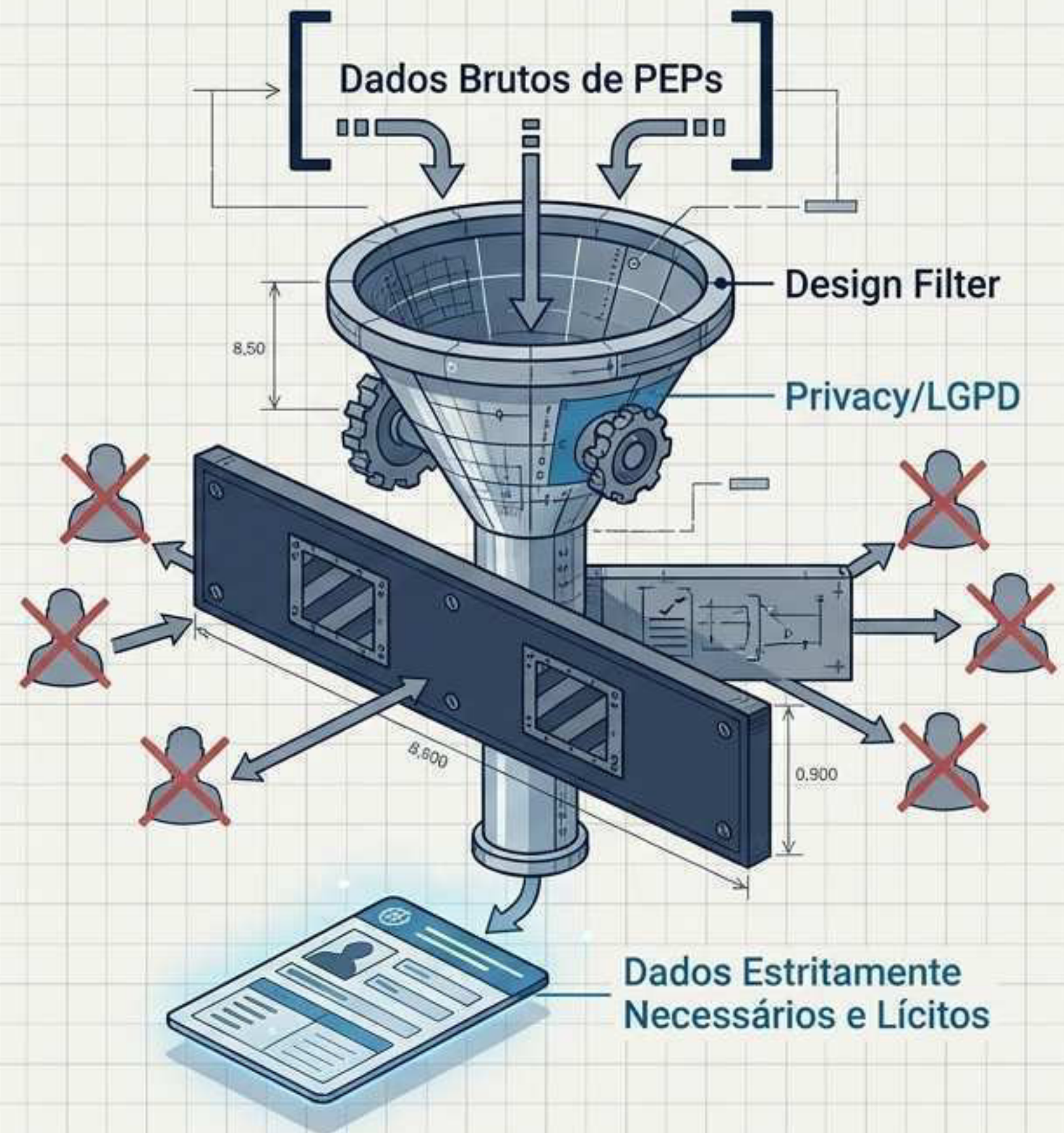
A arquitetura do sistema deve ser a primeira linha de defesa da privacidade.



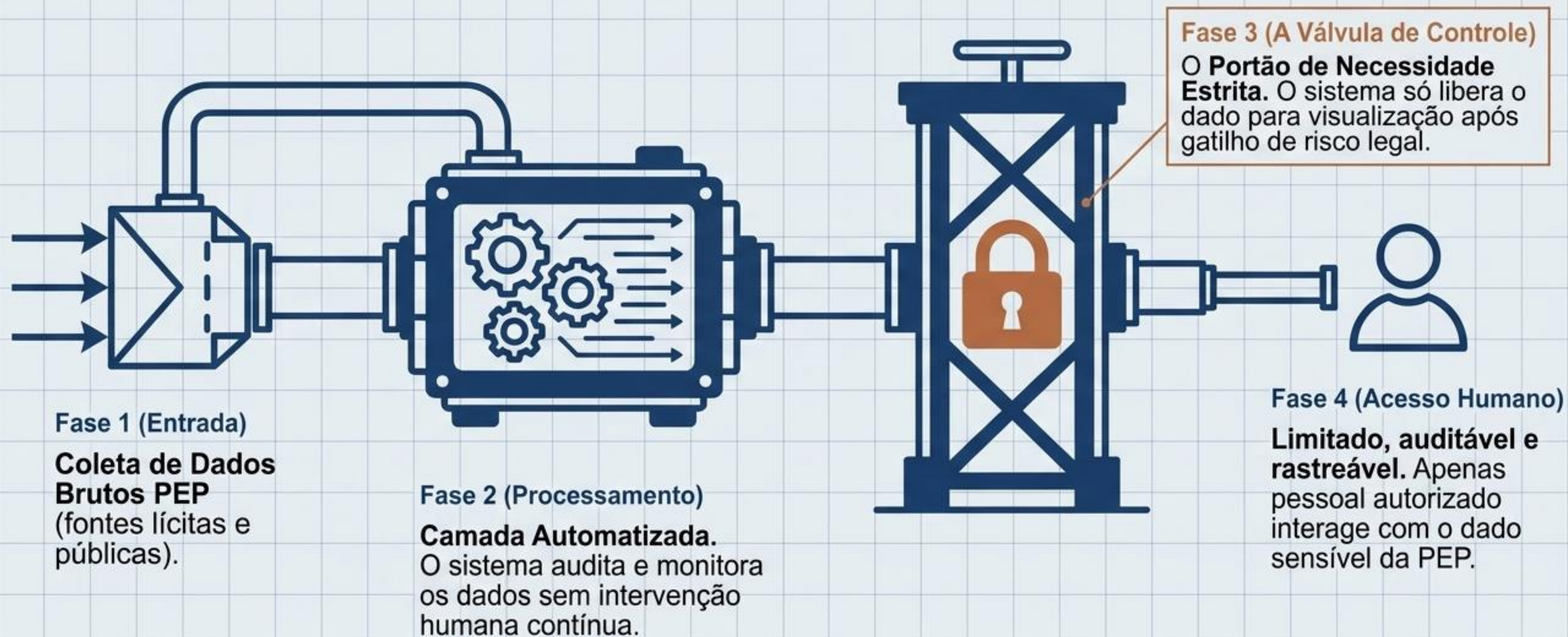
Pilar 2: Privacidade por Design

Conforme convergem os guias da CODATA e TCE-PB, a proteção se dá pela arquitetura do sistema.

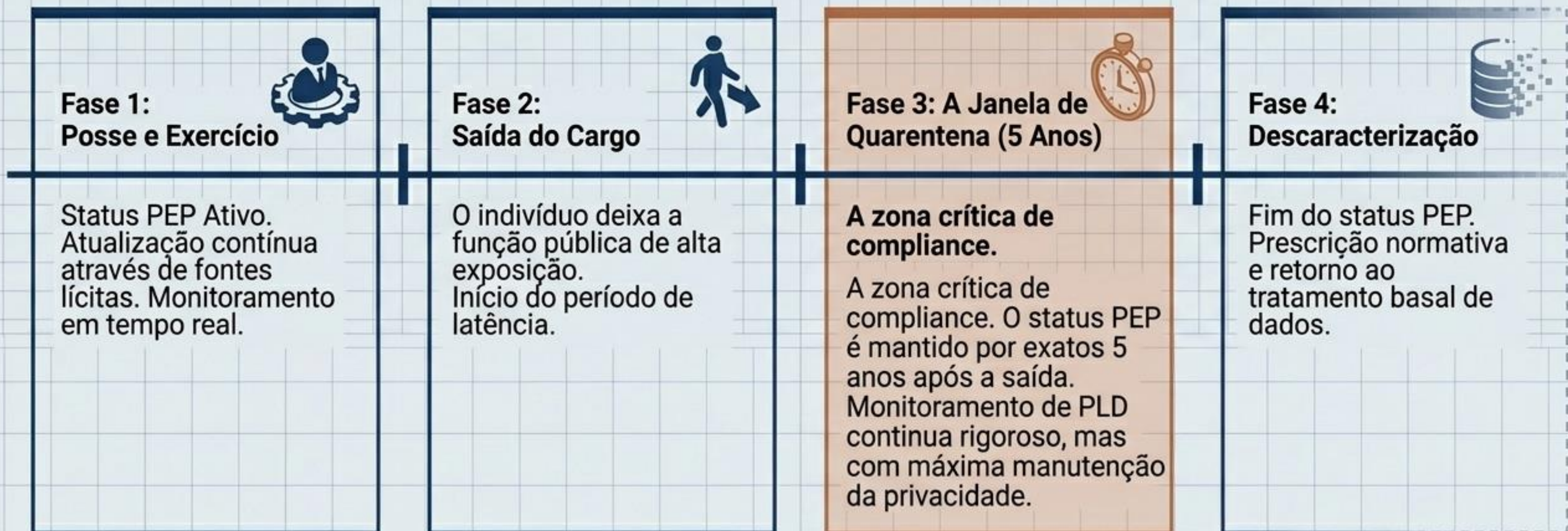
O acesso humano a dados sensíveis de PEPs deve ser tecnologicamente bloqueado, sendo substituído por automações que extraem apenas o estritamente necessário.



Pilar 2: Privacidade por Design na Prática

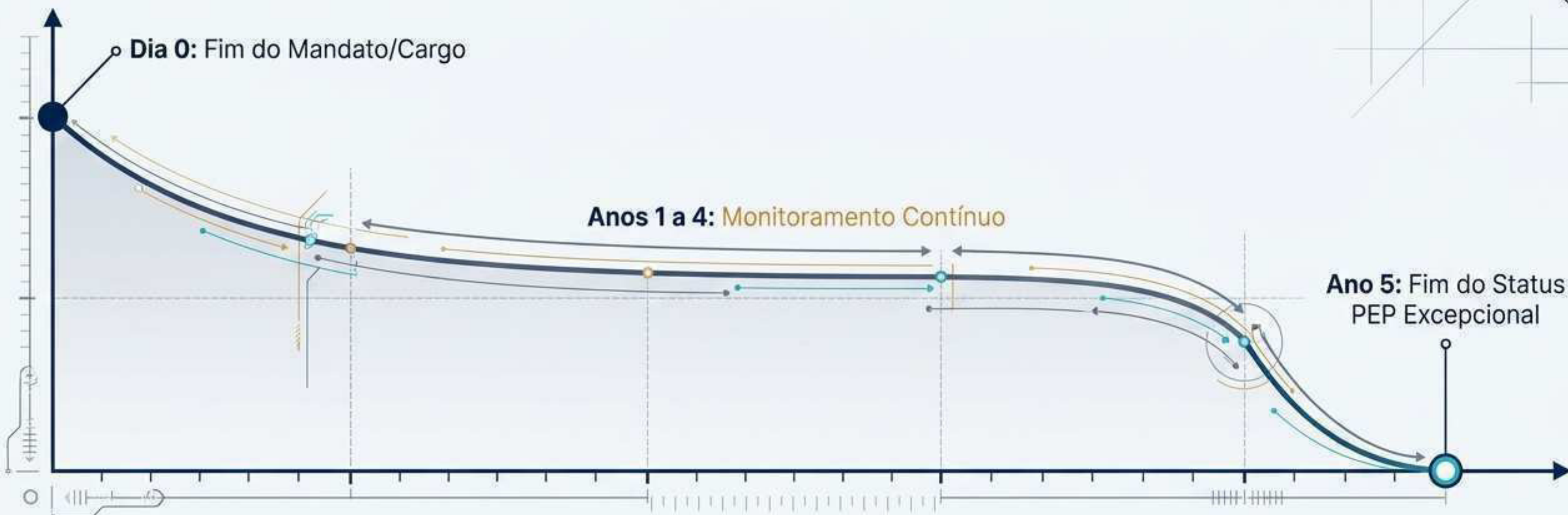


Pilar 3: A Cronologia do Risco (A Regra da Temporalidade)



Pilar 3: Temporalidade e Descontinuidade

O status de PEP e a justificativa para tratamento excepcional de dados têm data de validade.



Obrigatoriedade de respeito ao prazo legal de 5 anos após a saída do cargo público.

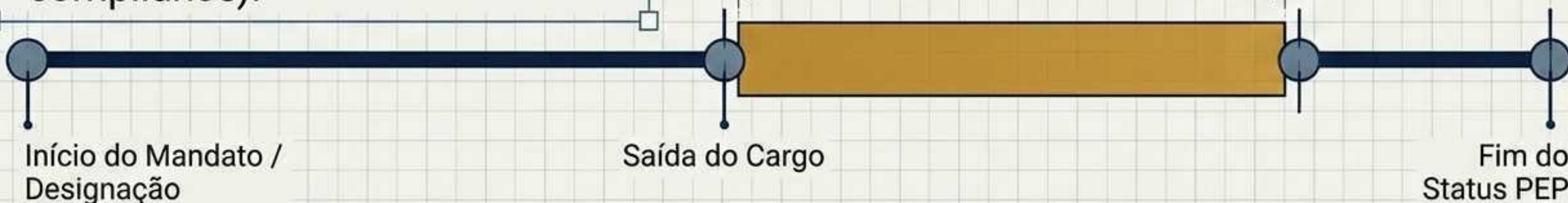
Necessidade crítica de seguir o fluxo contínuo de atualização de listas a partir de fontes lícitas e públicas.

Cessaçãõ do tratamento excepcional após o decurso do prazo, conforme manuais de compliance.

Pilar 3: A Regra da Temporalidade

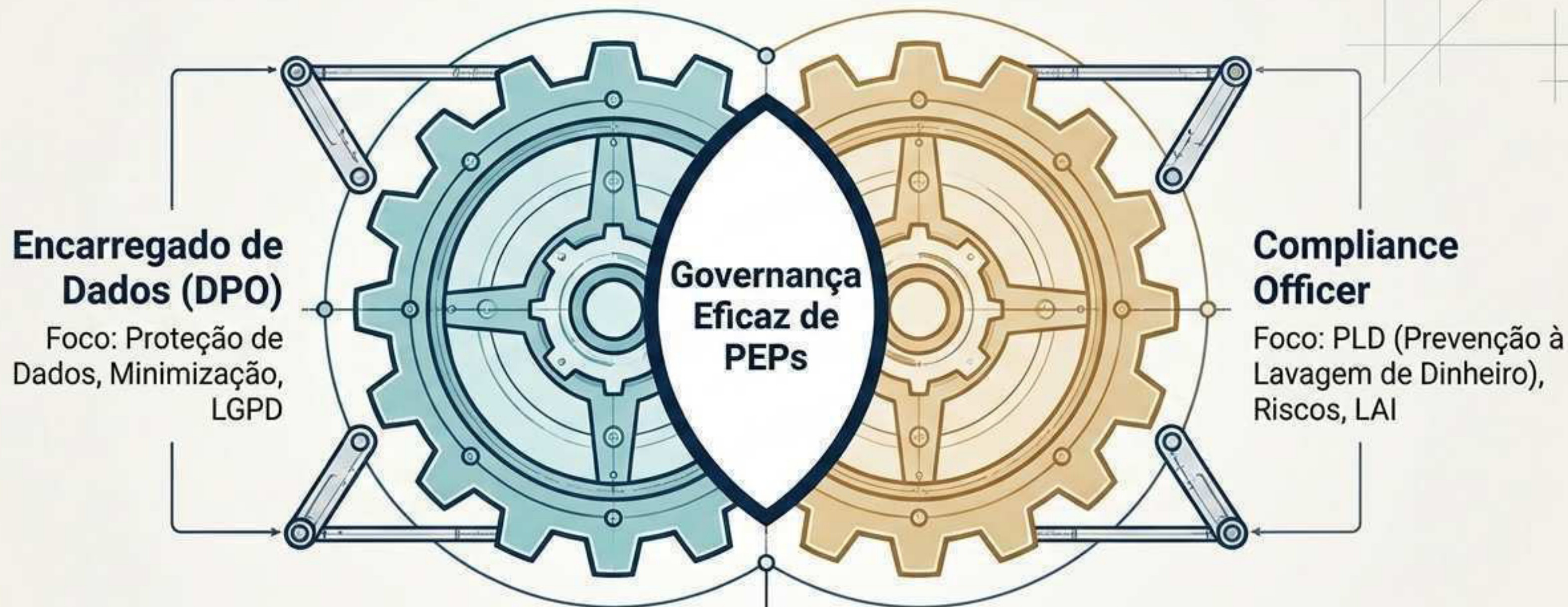
O status de PEP possui uma meia-vida legal. É imperativo rastrear a janela exata de 5 anos após a saída do cargo. Durante este período crítico de cauda, a atualização do monitoramento deve basear-se exclusivamente em fontes lícitas e listas públicas (manuais de compliance).

Janela de 5 Anos
de Monitoramento Pós-Cargo



Pilar 4: A Dupla Hélice da Governança

A conformidade não pode operar em silos.



A governança eficaz exige a união estrutural entre o mandato de privacidade (DPO) e o mandato de integridade financeira e anticorrupção (Compliance). Onde a LGPD e a PLD se encontram, o risco institucional é neutralizado.

Pilar 4: Sinergia Estratégica na Governança

Encarregado de Dados (DPO)	Compliance Officer
Foco: Privacidade e Proteção do Titular	Foco: Prevenção à Lavagem de Dinheiro (PLD) e Anticorrupção
Legislação Núcleo: LGPD	Legislação Núcleo: Normativas BACEN / Compliance
Objetivo Operacional: Minimização de Dados	Objetivo Operacional: Maximização de Risco Identificado

Sinergia: A governança eficaz não escolhe um lado. Ela unifica esses atores para criar uma barreira onde o compliance investigativo respeita os limites da minimização de dados.

Pilar 4: Integração de Perfis - DPO x Compliance

Encarregado de Dados (DPO)

- **Foco Central:** Minimização de dados, proteção de direitos dos titulares e garantia da base legal da LGPD.
- **Visão sobre PEP:** Dado sensível que requer contenção.

Compliance Officer

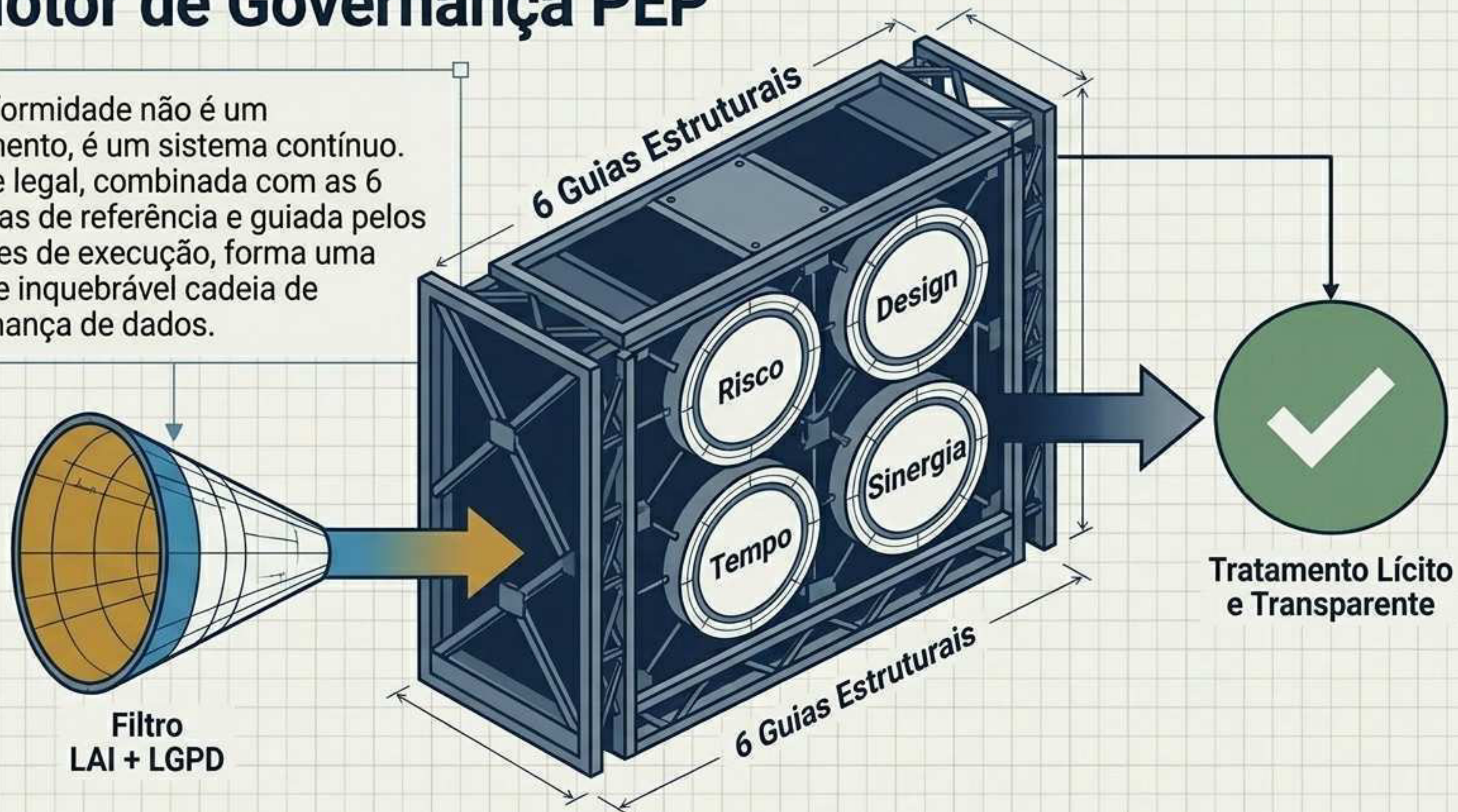
- **Foco Central:** Prevenção à Lavagem de Dinheiro (PLD), mapeamento de riscos operacionais e integridade da instituição.
- **Visão sobre PEP:** Vetor de risco que requer escrutínio.

A Sinergia da Governança PEP

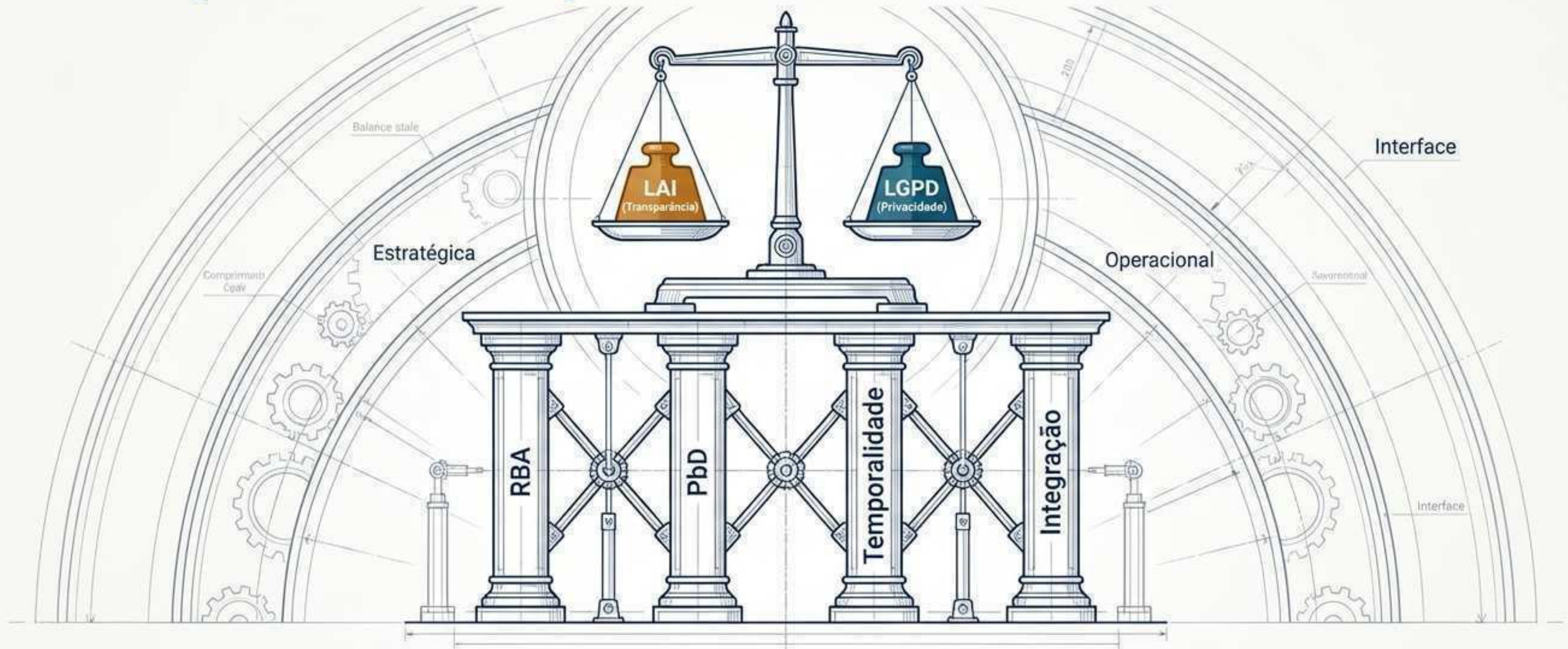
A governança eficaz exige atuação conjunta – o DPO cria o cofre seguro de dados que permite ao Compliance auditar o risco sem expor a instituição a vazamentos.

O Motor de Governança PEP

A conformidade não é um documento, é um sistema contínuo. A base legal, combinada com as 6 cartilhas de referência e guiada pelos 4 pilares de execução, forma uma única e inquebrável cadeia de governança de dados.



O Blueprint Final: Arquitetura Unificada



O cumprimento da LAI e da LGPD em relação aos PEPs não são atividades isoladas de departamentos diferentes. São engrenagens interdependentes do mesmo motor de integridade pública. A Obrigação Legal sustenta a balança, os Guias fornecem as ferramentas, e os 4 Pilares garantem a execução segura.

A Arquitetura do Equilíbrio: O Framework PEP Definitivo



Checklist Executivo: Próximos Passos

Ações Imediatas (Táticas)



Verificar fluxo de atualização de listas de PEPs em fontes lícitas e garantir o corte temporal de 5 anos.

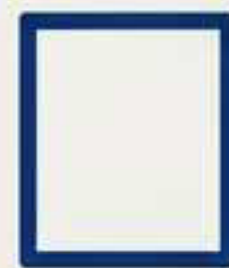


Estabelecer rotina conjunta entre o DPO e o Compliance Officer (PLD).

Ações Sistêmicas (Estratégicas)



Revisar arquitetura de sistemas de TI (com apoio da CODATA/TCE-PB) para automatizar limites de acesso humano.



Calibrar as métricas de monitoramento baseadas em risco, alinhando-as aos guias do BACEN e AML.

Diretrizes Táticas de Implementação Imediata

1

Auditar Sistemas

Revisar a arquitetura atual de dados PEP visando implementar o Privacy by Design. O objetivo: garantir que o monitoramento seja automatizado e o acesso humano seja restrito por gatilhos de necessidade.

2

Alinhar Áreas

Provocar uma reunião de alinhamento estratégico imediata entre o Encarregado de Dados (DPO) e as equipes de PLD/Compliance para estabelecer protocolos conjuntos de atuação.

3

Atualizar Processos

Revisar as rotinas de limpeza e expurgo de dados, garantindo que o rastreamento através de fontes lícitas e públicas obedeça estritamente à janela de temporalidade da quarentena de 5 anos.

Considerações Finais



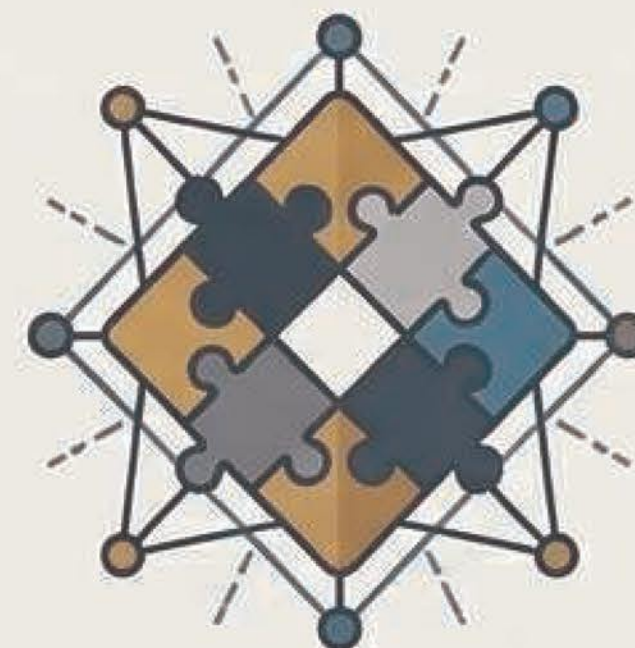
Equilíbrio

A conformidade é um ponto de equilíbrio, não um bloqueio. O "Cumprimento de Obrigação Legal" protege tanto o servidor quanto o cidadão.



Automação

Privacidade por Design é a melhor defesa. Limitar o acesso humano através de automação blindo o processo contra vazamentos e vieses.



Integração

Utilize a curadoria de guias como um kit de ferramentas vivo. Nenhuma lei ou manual funciona em silos; uma seu DPO e seu time de PLD.