ANÁLISE REGULATÓRIA

Governança cibernética no mercado latino-americano

O mapa regulatório que toda empresa com operação regional precisa ler antes de desenhar seu programa de segurança e privacidade.

SÉRIE	EDIÇÃO	PÁGINAS	PÚBLICO
Inteligência regulatória	Junho 2026	6	CISOs, DPOs, jurídico e compliance

SUMÁRIO EXECUTIVO

A América Latina deixou de ser um vazio regulatório. O problema agora é o oposto: seis jurisdições relevantes, seis ritmos diferentes e nenhuma delas espera pela outra.

Entre 2018 e 2026, a região saiu de um cenário onde só a Argentina tinha tradição consolidada em proteção de dados para um ambiente com leis gerais em vigor nos seis maiores mercados, duas autoridades novas em operação, uma lei marco de cibersegurança pioneira no Chile e regulação setorial financeira cada vez mais dura no Brasil e no México. Para empresas com operação em mais de um país, o erro mais caro é tratar a região como um bloco único: prazos de notificação, exigência de encarregado e tetos de multa variam de forma material. Esta análise organiza o cenário por jurisdição, identifica os pontos de convergência que permitem um programa unificado e aponta o que muda até 2027.

6
jurisdições com lei geral de proteção de dados em vigor entre os maiores mercados da região
BR · MX · CL · CO · AR · PE

3 dias úteis
prazo de comunicação de incidente à ANPD no Brasil desde a Resolução CD/ANPD 15/2024
regulamento de incidentes · BR

até 4%
da receita anual: teto sancionatório da nova lei chilena 21.719 para infrações gravíssimas
vigência plena em 2026 · CL

1 O retrato em uma página

A leitura abaixo consolida cinco dimensões de maturidade regulatória. Duas observações antes do quadro: "consolidado" significa norma em vigor com autoridade ativa e prática sancionatória ou fiscalizatória real, não apenas lei publicada. E a coluna de lei marco de cibersegurança é a que mais separa os países hoje: o Chile saiu na frente da região com uma lei dedicada, enquanto os demais ainda tratam o tema por normas setoriais e estratégias nacionais sem força de obrigação ampla.

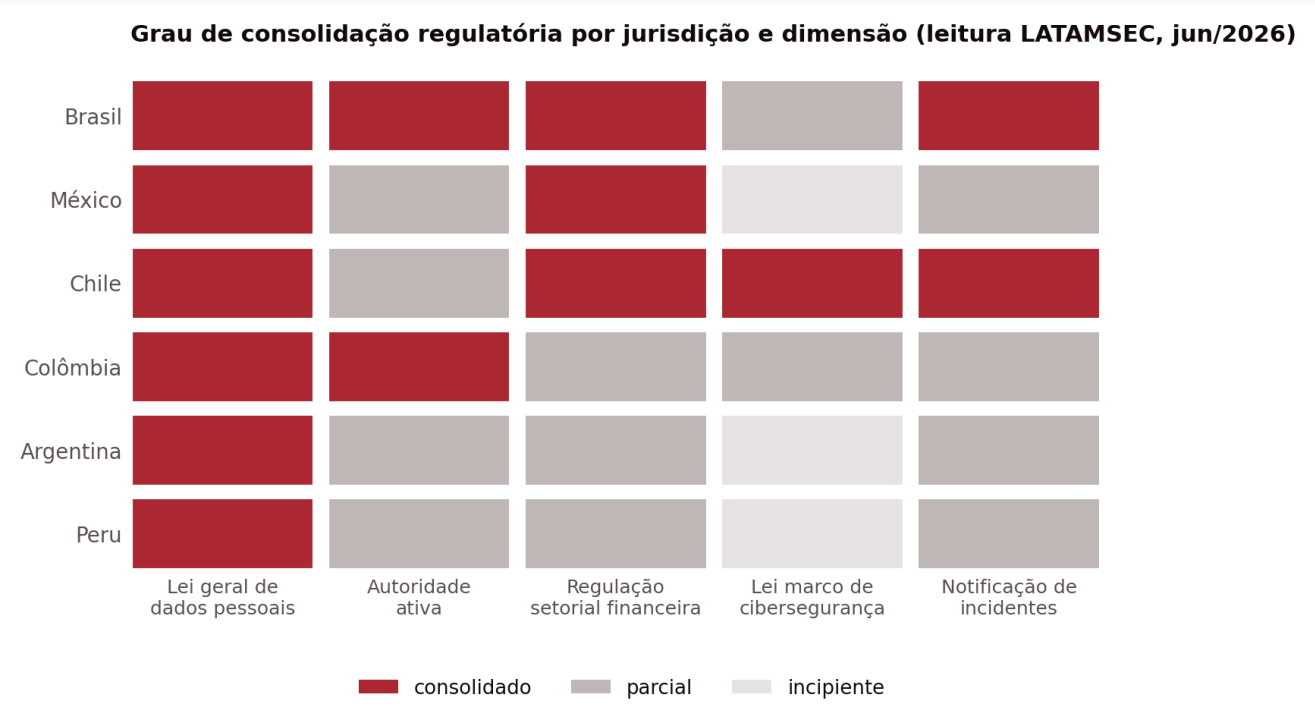

Figura 1 · Consolidação regulatória por dimensão. Leitura analítica da LATAMSEC com base em normas em vigor em junho de 2026.

2 Jurisdição por jurisdição

Brasil. A LGPD (Lei 13.709/2018) está madura: a ANPD regulamentou dosimetria de sanções, comunicação de incidentes (Resolução CD/ANPD 15/2024, com prazo de três dias úteis) e transferências internacionais. As multas chegam a 2% do faturamento no Brasil, limitadas a R$ 50 milhões por infração. No setor financeiro, a Resolução CMN 4.893/2021 e a Resolução BCB 85/2021 exigem política formal de cibersegurança, requisitos para contratação de nuvem e comunicação de incidentes relevantes ao Banco Central. Na prática, instituições financeiras brasileiras já operam sob duplo regime: dados pessoais com a ANPD e resiliência operacional com o BACEN.

Chile. O caso mais importante para acompanhar. A Lei Marco de Cibersegurança 21.663 (2024) criou a ANCI, agência nacional com poder de fiscalização sobre serviços essenciais e operadores de importância vital, incluindo dever de reporte de incidentes significativos em prazos curtos a partir do conhecimento do fato. Em paralelo, a Lei 21.719 (2024) modernizou a proteção de dados, criou a Agencia de Protección de Datos Personales e estabeleceu multas que alcançam 4% da receita anual nas infrações gravíssimas, com exigibilidade plena em dezembro de 2026. Empresas com operação chilena têm, neste momento, a janela de adequação mais apertada da região.

México. A reforma de 2025 da LFPDPPP redesenhou a arquitetura institucional: o INAI foi extinto e suas funções de proteção de dados migraram para a estrutura do Executivo federal, o que gera um período de transição com fiscalização menos previsível. A regulação setorial, porém, segue firme: a CNBV impõe requisitos de segurança da informação e reporte de incidentes às instituições financeiras, e contratos com o setor público carregam exigências próprias. O risco mexicano hoje é menos a multa de privacidade e mais a assimetria entre norma geral em transição e norma setorial exigente.

Colômbia. A Ley 1581/2012 segue como base, com a Superintendencia de Industria y Comercio (SIC) entre as autoridades mais ativas da região em fiscalização de tratamento de dados, registro de bases (RNBD) e sanções a empresas de todos os portes. Não há lei marco de cibersegurança, mas os documentos CONPES de segurança digital e as exigências da Superintendencia Financiera aproximam o setor regulado das práticas internacionais.

Argentina e Peru. A Argentina mantém a Ley 25.326/2000 e o status de adequação reconhecido pela União Europeia, um ativo relevante para fluxos de dados com a Europa; projetos de reforma para alinhamento ao GDPR tramitam há anos sem aprovação definitiva. O Peru opera sob a Ley 29733/2011 com autoridade vinculada ao Ministério da Justiça e fiscalização crescente, ainda que com tetos sancionatórios modestos em comparação regional.

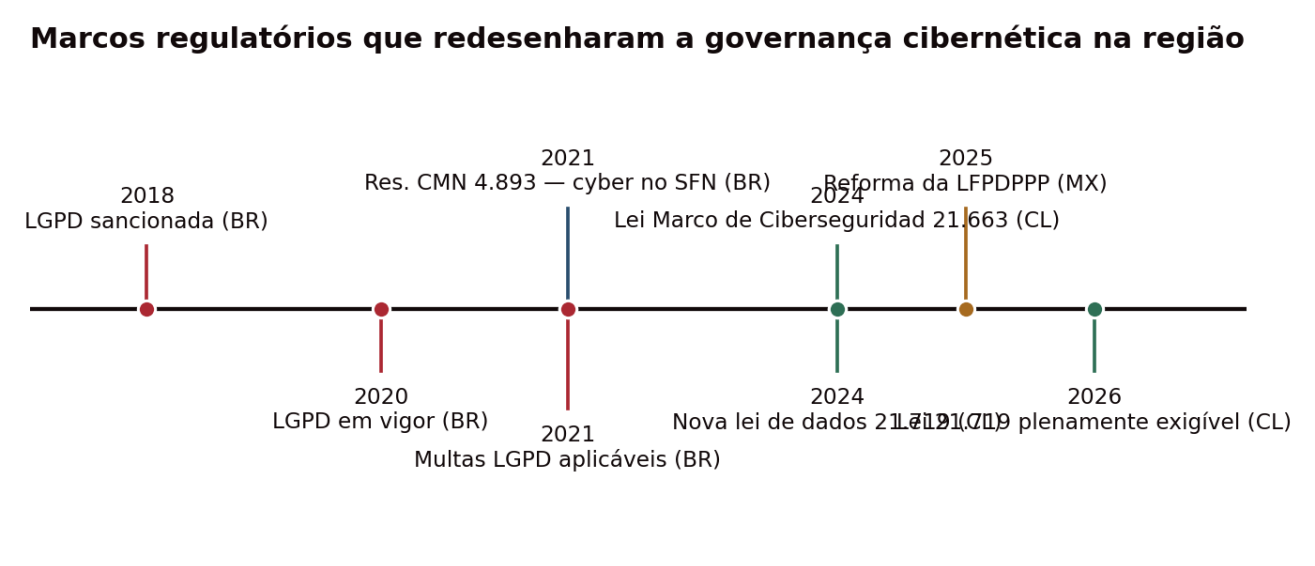

Figura 2 · A aceleração é visível: metade dos marcos relevantes da região é posterior a 2023.

3 A assimetria que custa dinheiro

Três variáveis concentram o risco de quem padroniza demais: prazo de notificação de incidentes, exigência de encarregado e teto sancionatório. Uma política regional calibrada pela norma mais branda viola a mais dura; uma calibrada pela mais dura gera custo desnecessário onde a exigência não existe. A resposta madura é um padrão corporativo único de processo com parâmetros locais: o fluxo de resposta a incidentes é um só, mas o relógio e o destinatário da notificação mudam por país.

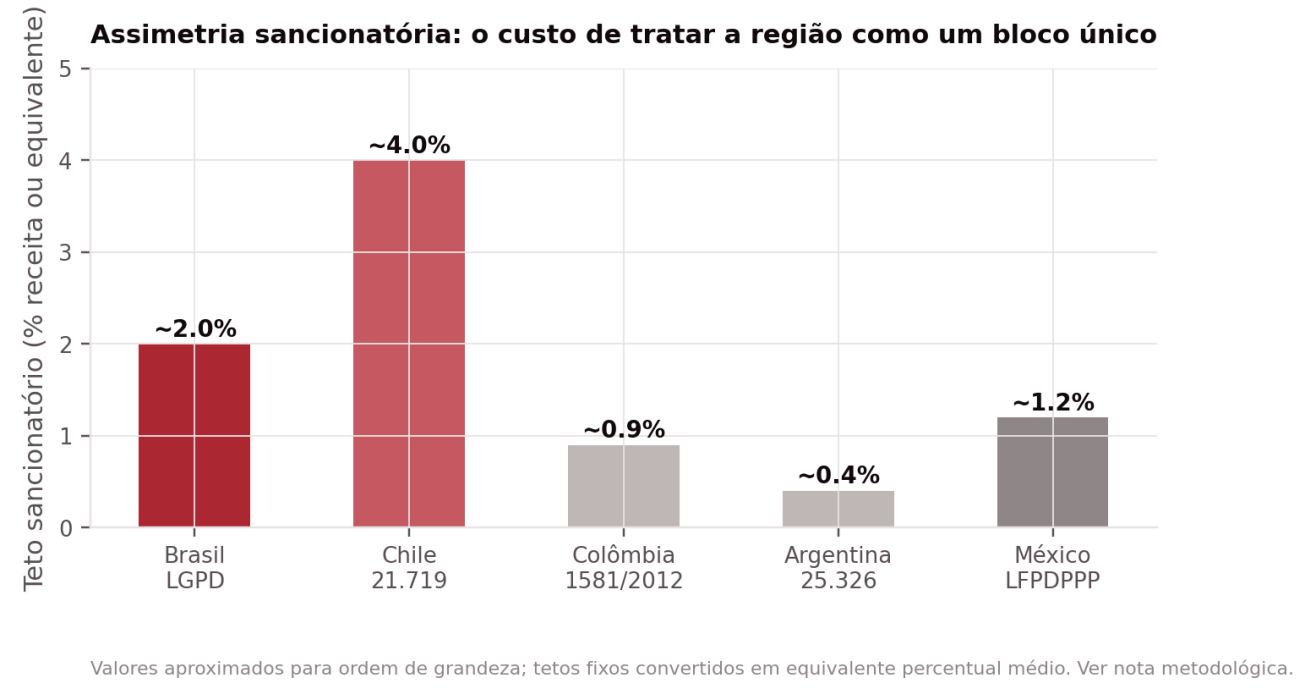

Figura 3 · Tetos sancionatórios em ordem de grandeza. Nota metodológica: tetos fixos (como os 2.000 salários mínimos colombianos ou as unidades fiscais argentinas) foram convertidos em equivalente percentual médio apenas para comparação visual.

DIMENSÃO	ONDE ESTÁ MAIS DURO	IMPLICAÇÃO PRÁTICA
Notificação de incidente	Brasil (3 dias úteis à ANPD) e Chile (reporte em horas à ANCI para entes regulados).	O playbook de resposta precisa de um passo de qualificação jurídica nas primeiras horas, não no fim.
Encarregado / DPO	Brasil exige indicação de encarregado para controladores em geral.	Estrutura regional com encarregado central e pontos focais locais atende ao conjunto com um só desenho.
Transferência internacional	Brasil (regulamento ANPD com cláusulas-padrão) e Argentina (regime de adequação).	Inventário de fluxos transfronteiriços deixa de ser exercício teórico e vira pré-requisito contratual.
Setor financeiro	Brasil (CMN/BCB) e México (CNBV), com Chile se aproximando via ANCI.	Bancos e fintechs respondem a dois reguladores por país; a trilha de evidências precisa servir aos dois.

4 Convergência: onde um programa único funciona

A boa notícia é que as normas da região bebem das mesmas fontes. Princípios de finalidade, necessidade e segurança aparecem em todas as leis gerais; as exigências técnicas setoriais convergem para o vocabulário de ISO 27001, NIST CSF e CIS Controls. Isso permite uma arquitetura de conformidade em camadas: um conjunto único de controles corporativos mapeado, controle a controle, para cada requisito local. Quando o controle "gestão

de acesso privilegiado" tem dono, evidência e data de revisão, ele responde simultaneamente à LGPD, à 21.719 chilena, à circular da SIC e ao questionário do regulador financeiro. O custo de conformidade cai porque a evidência é produzida uma vez e reutilizada em todas as frentes.

> **TESE LATAMSEC**
> O padrão que separa empresas maduras: tratar cada nova norma como uma **coluna nova na matriz de mapeamento**, não como um projeto novo de conformidade. Quem mantém controles e evidências organizados absorve regulação nova em semanas; quem não mantém recomeça do zero a cada lei.

5 O que muda até 2027

Quatro movimentos merecem monitoramento ativo. Primeiro, a exigibilidade plena da lei chilena 21.719 ao fim de 2026, que deve inaugurar a prática sancionatória mais agressiva da região. Segundo, a consolidação da fiscalização da ANCI sobre operadores de importância vital, criando o primeiro corpo de jurisprudência de cibersegurança obrigatória da América Latina. Terceiro, a tendência de regulamentação de inteligência artificial: o Brasil discute marco legal com obrigações de gestão de risco para sistemas de alto impacto, e a experiência regulatória europeia pressiona o desenho regional. Quarto, a elevação da responsabilidade de administradores: reguladores financeiros já exigem aprovação de políticas de cibersegurança em nível de conselho, e a tendência é essa lógica transbordar para os demais setores. Conselheiro que aprova política sem entender o risco está assinando responsabilidade.

6 Implicações para o seu programa

HORIZONTE	AÇÃO RECOMENDADA
Imediato (30 dias)	Inventariar em qual célula da Figura 1 a empresa opera, com quais entidades legais e quais fluxos de dados cruzam fronteiras.
Curto prazo (90 dias)	Unificar o playbook de resposta a incidentes com matriz de notificação por país: prazo, autoridade, gatilho e responsável jurídico.
Médio prazo (12 meses)	Construir a matriz de mapeamento controle-a-requisito cobrindo LGPD, 21.719, normas setoriais aplicáveis e frameworks contratuais.
Contínuo	Manter evidências vivas, com dono e validade, para que auditoria e fiscalização sejam leitura de plataforma, não projeto de coleta.

É exatamente esse desenho que o módulo de compliance da LATAMSEC implementa: controles corporativos únicos mapeados contra LGPD, ISO 27001, NIST CSF, CIS Controls e requisitos setoriais, com evidências versionadas, validade controlada e relatórios prontos para auditoria e regulador. A regulação da região vai continuar acelerando. A pergunta é se a sua estrutura de evidências acompanha.