MERCGROUP

APRESENTAÇÃO · APLICAÇÃO PRÁTICA

# Open Finance: o dado compartilhado exige *controle*.

O que o ecossistema de compartilhamento de dados e serviços do Banco Central exige das instituições participantes — consentimento, APIs, segurança, responsabilidade — e como auditoria e asseguração entram nesse fluxo.

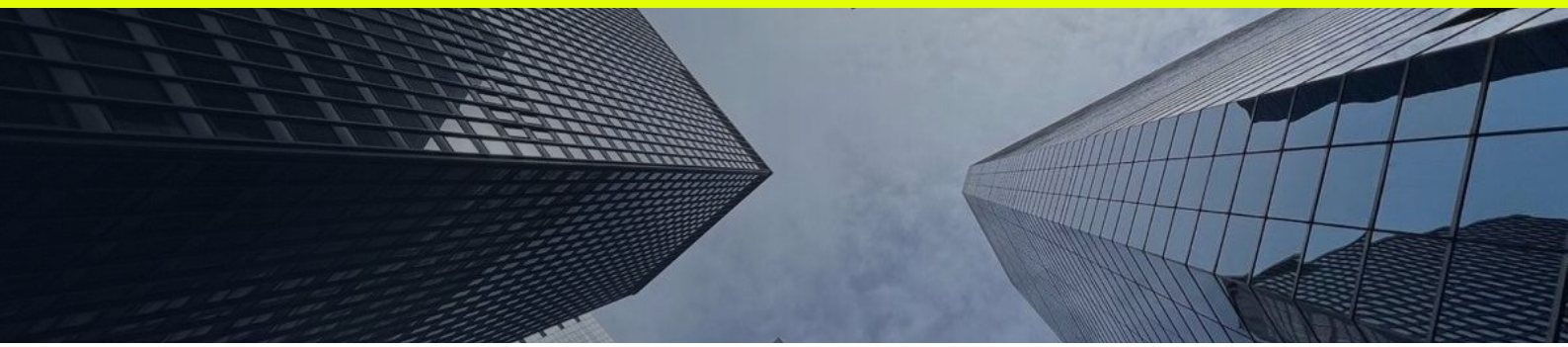
SÃO PAULO · BRASIL · 2026

SUMÁRIO EXECUTIVO

# O que este material te *entrega*.

- **O desenho do Open Finance brasileiro:** fases, papéis (transmissora, receptora, iniciadora) e a base normativa da Resolução Conjunta nº 1/2020 e regulamentação complementar do BCB.
- **O ciclo de vida do consentimento:** obtenção, autenticação, confirmação, revogação e prazo — e por que cada etapa é um controle a testar, não um requisito de tela.
- **Os controles que sustentam a participação:** segurança de APIs, disponibilidade, qualidade de dados, trilhas de auditoria e a responsabilidade pelos dados recebidos de terceiros.
- **Um diagnóstico editável de 12 perguntas** sobre a conformidade e a operação do seu ambiente de Open Finance.
- **Próximos passos objetivos** com a MERC: asseguração de controles e prontidão para supervisão no ecossistema.

Material de aplicação prática elaborado pela MERC Group a partir do artigo “Open Finance: auditoria e controles”, publicado em 2026 em www.mercgroup.com.br/insights. Este documento tem caráter informativo e não substitui avaliação profissional específica.



Este material não é sobre teoria. É sobre *decisão prática*.

No Open Finance, o dado do cliente circula entre instituições. A confiança do sistema depende do controle que cada participante consegue *demonstrar*.

MERCGROUP

CONTEXTO

# Um ecossistema construído sobre *consentimento*.

## O QUE ACONTECEU

O **Open Finance** brasileiro — instituído pela Resolução Conjunta CMN/BCB nº 1/2020 e regulamentação complementar — obriga grandes instituições e permite às demais compartilhar, mediante consentimento do cliente, dados cadastrais, transacionais e serviços como iniciação de pagamentos.

O ciclo do **consentimento** é o núcleo do regime: pedido com finalidade determinada, autenticação do cliente na instituição transmissora, confirmação, prazo de validade e revogação a qualquer tempo — tudo com registro e trilha. Falha nesse fluxo não é bug: é descumprimento regulatório com dano potencial ao cliente.

A operação exige **APIs padronizadas** com requisitos de disponibilidade, desempenho e segurança (certificados, criptografia, autorização), participação na estrutura de governança do ecossistema e reporte de métricas ao BCB — a instituição responde pela qualidade do que transmite e pelo uso do que recebe.

Com o Open Finance no centro da agenda estratégica do BCB — ao lado de PIX, Drex e tokenização —, a supervisão sobre segurança de dados, incidentes e uso indevido tende a se aprofundar, e a asseguração independente de controles (na lógica ISAE 3402 / SOC 2) vira diferencial competitivo para quem participa do ecossistema.

## O QUE MUDA NA PRÁTICA

**Consentimento vira objeto de teste.** Amostras de consentimentos ativos, revogados e expirados, confrontados com os dados efetivamente compartilhados — é assim que se evidencia conformidade.

**Segurança de API é controle contínuo.** Gestão de certificados, tokens, logs de acesso e resposta a incidentes precisam de dono, monitoramento e evidência — não de configuração feita uma vez.

**Dados recebidos criam responsabilidade.** A receptora responde pelo uso conforme a finalidade consentida e pela guarda segura — LGPD e Open Finance se sobrepõem aqui, e o auditor lê os dois.

**Métricas reportadas precisam conciliar.** Disponibilidade e volumetria reportadas à estrutura do ecossistema devem bater com os logs internos — divergência em reporte regulatório é achado sério.

IMPACTO POR PERFIL

# Como isso afeta a *sua* companhia.

### BANCO TRANSMISSOR DE DADOS

Obrigatoriedade plena: consentimento, APIs, disponibilidade e qualidade de dado sob supervisão — o custo de conformidade se administra com controles automatizados e testados.

### INSTITUIÇÃO DE PAGAMENTO RECEPTORA

Usar dado de Open Finance para crédito e ofertas exige governança de finalidade, guarda e descarte — o benefício comercial vem com responsabilidade regulatória.

### INICIADORA DE TRANSAÇÃO DE PAGAMENTO

A ITP toca o dinheiro do cliente sem custodiá-lo: autenticação, limites e trilha de cada iniciação são o produto — e o controle é o negócio.

### FINTECH QUE CONSOME DADOS VIA PARCEIROS

Arranjos indiretos não transferem a responsabilidade: contratos, segregação e monitoramento do parceiro entram no perímetro de controles da autorizada.

### INSTITUIÇÃO EM EXPANSÃO DE PRODUTOS

Crédito com dado transacional, agregação financeira e carteiras digitais nascem do Open Finance — cada produto novo precisa entrar na avaliação de riscos e controles.

DIAGNÓSTICO RÁPIDO

# Onde a sua companhia está *hoje*?

Responda Sim ou Não. Cada "Não" é um ponto de atenção prioritário. Os campos deste formulário são editáveis.

| | SIM | NÃO | OBSERVAÇÕES |
|---|---|---|---|
| **01.** O papel da instituição no ecossistema (transmissora, receptora, iniciadora) está formalmente mapeado? | ☐ | ☐ | |
| **02.** O ciclo de consentimento (obtenção, confirmação, revogação, expiração) tem trilha completa e testável? | ☐ | ☐ | |
| **03.** Os dados compartilhados são conciliados com os consentimentos ativos correspondentes? | ☐ | ☐ | |
| **04.** Certificados, tokens e chaves das APIs têm gestão formal de ciclo de vida? | ☐ | ☐ | |
| **05.** Logs de acesso e compartilhamento são retidos, protegidos e monitorados? | ☐ | ☐ | |
| **06.** As métricas de disponibilidade e desempenho reportadas conciliam com os logs internos? | ☐ | ☐ | |
| **07.** Incidentes de segurança e indisponibilidade têm processo de resposta, registro e comunicação? | ☐ | ☐ | |
| **08.** O uso dos dados recebidos respeita a finalidade consentida, com governança de acesso interno? | ☐ | ☐ | |
| **09.** Descarte e anonimização de dados após expiração do consentimento estão implementados? | ☐ | ☐ | |
| **10.** A sobreposição com a LGPD (bases legais, direitos do titular, DPO) está tratada de forma integrada? | ☐ | ☐ | |
| **11.** Parceiros tecnológicos e arranjos indiretos passam por diligência e monitoramento contínuo? | ☐ | ☐ | |
| **12.** Os controles do ambiente Open Finance já passaram por avaliação ou asseguração independente? | ☐ | ☐ | |

MERCGROUP

PRÓXIMOS PASSOS

# Do diagnóstico à *ação*, com a MERC.

**MERC Valuation — valuation.mercgroup.com.br**

Avaliação de empresas com metodologia de mercado financeiro: DCF, múltiplos e modelagem avançada, com trilha de premissas auditável.

**MERC DF — df.mercgroup.com.br**

Elaboração e revisão de demonstrações financeiras em conformidade com CPC e IFRS, prontas para auditoria, credores e investidores.

**MERC Lastros — lastros.mercgroup.com.br**

Verificação independente de lastros para securitizadoras, FIDCs e operações estruturadas, com evidência e rastreabilidade.

**Auditoria & Advisory especializada**

Asseguração de controles no ecossistema Open Finance — consentimento, APIs, segurança e qualidade de dados — na lógica ISAE 3402/SOC 2, para instituições transmissoras, receptoras e iniciadoras.

**AGENDAR REUNIÃO**

Fale com o nosso time: **contato@mercgroup.com.br**

Ou fale diretamente com nossos sócios: **gabriel.carolei@mercgroup.com.br** · **bruno.zamboni@mercgroup.com.br**

FONTES NORMATIVAS

# Referências deste material.

## NORMAS E REGULAÇÃO BRASILEIRAS

- Resolução Conjunta CMN/BCB nº 1/2020 — implementação do Open Finance.
- Resolução BCB nº 32/2020 e regulamentação complementar — requisitos técnicos e operacionais.
- Lei nº 13.709/2018 (LGPD) — tratamento de dados pessoais.
- Instruções e comunicados do BCB sobre a estrutura de governança do Open Finance.

## REFERÊNCIAS INTERNACIONAIS

- ISAE 3402 — Assurance Reports on Controls at a Service Organization (IAASB).
- SOC 2 — Trust Services Criteria (AICPA).
- Padrões abertos de API e segurança (FAPI/OpenID Foundation) adotados pelo ecossistema.

As referências acima indicam o arcabouço normativo aplicável na data de elaboração deste material (julho de 2026) e podem ser alteradas pelos órgãos emissores. A aplicação a casos concretos exige análise específica. MERC Group — Auditoria do Mercado Financeiro Brasileiro · São Paulo · Brasil.