MERCGROUP

APRESENTAÇÃO · APLICAÇÃO PRÁTICA

No Open Finance, o consentimento precisa ser *auditável*.

Com cinco anos de operação, dezenas de milhões de consentimentos ativos e escopo em expansão para crédito, investimentos e portabilidade, o Open Finance deixou de ser projeto para virar infraestrutura. Quando dados sensíveis fluem entre participantes por consentimento do cliente, o ciclo de vida do consentimento, a segurança das APIs e a rastreabilidade dos controles deixam de ser tema exclusivo de tecnologia — viram objeto de asseguração. Este material transforma o compartilhamento de dados em agenda de controles verificáveis.

SÃO PAULO · BRASIL · 2026

SUMÁRIO EXECUTIVO

O que este material te *entrega*.

- **O ciclo de vida do consentimento destrinchado:** concessão, uso conforme finalidade, renovação e revogação efetiva — e por que a revogação que não interrompe o fluxo de dados é a falha de controle mais crítica do ecossistema.

- **A segurança das APIs como controle, não como recurso técnico:** autenticação, autorização, proteção de dados em trânsito e rastreabilidade — o que precisa existir para que o compartilhamento seja confiável entre participantes.

- **A lógica da asseguração aplicada ao ecossistema:** como o espírito das normas de asseguração de controles em prestadores de serviço (ISAE 3402/SOC) se traduz em relatórios que um participante pode confiar sobre os controles de outro.

- **Um diagnóstico editável de 12 perguntas** para áreas de tecnologia, segurança, compliance e auditoria interna avaliarem a maturidade dos controles de consentimento e compartilhamento de dados.

- **Próximos passos objetivos** com a MERC: asseguração independente de controles de consentimento e segurança de APIs, avaliação da interface com a LGPD e preparação de relatórios de controles para o diálogo entre participantes.

Material de aplicação prática elaborado pela MERC Group a partir do artigo “Asseguração no Open Finance: consentimento, segurança de APIs e controles no compartilhamento de dados entre participantes”, publicado em julho de 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, a confiança de um participante repousa nos controles de outro. Quando o dado do cliente flui por consentimento, o controle sobre esse consentimento não é detalhe técnico — é a moeda de *confiança* de todo o ecossistema.

MERCGROUP

CONTEXTO

O ecossistema amadureceu. Os *controles* têm de acompanhar.

O QUE ACONTECEU

O Open Finance brasileiro chegou à maturidade operacional: cinco anos de implantação, dezenas de milhões de consentimentos ativos e escopo em expansão contínua — de dados cadastrais e transacionais para crédito, investimentos, câmbio e serviços de iniciação de pagamento. O que começou como compartilhamento de informação evoluiu para uma infraestrutura de dados e transações entre centenas de participantes.

A lógica do sistema é o consentimento do cliente: o dado só flui entre instituições porque o titular autorizou, para uma finalidade e por um prazo. Essa arquitetura desloca o eixo do controle para o ciclo de vida do consentimento — como ele é concedido, usado dentro da finalidade, renovado e, sobretudo, revogado de forma efetiva.

A camada técnica é a interface de programação de aplicações (API), que conecta os participantes. Autenticação, autorização, proteção dos dados em trânsito, controle de acesso e rastreabilidade das chamadas deixam de ser preocupação isolada de segurança da informação e passam a ser controles cuja efetividade sustenta a confiança de todo o ecossistema.

Aqui entram a asseguração e a interface com a proteção de dados. O espírito das normas de asseguração de controles em prestadores de serviço — na linha da ISAE 3402 / NBC TO 3402 e dos relatórios do tipo SOC — oferece a estrutura para que um participante confie nos controles de outro com base em evidência independente, enquanto a LGPD dá o enquadramento de licitude, finalidade e direitos do titular.

O QUE MUDA NA PRÁTICA

A revogação precisa interromper o fluxo de fato. Consentimento revogado que continua permitindo acesso a dados é a falha mais grave do modelo. A efetividade da revogação — e não apenas o registro dela — precisa ser testada e evidenciada.

O consentimento precisa respeitar finalidade e prazo. Uso de dados além da finalidade autorizada ou após o prazo é violação de controle e de LGPD ao mesmo tempo. Controles que amarrem escopo, finalidade e prazo à chamada de API são o que separa conformidade de intenção.

A segurança das APIs vira objeto de evidência. Autenticação forte, autorização granular, criptografia em trânsito e logs íntegros precisam existir e ser demonstráveis — controle que não deixa trilha não é auditável, e o que não é auditável não é confiável para o outro participante.

A asseguração organiza a confiança entre participantes. Relatórios de controles no espírito ISAE 3402/SOC permitem que uma instituição confie nos controles de outra sem auditar cada uma individualmente — e definem claramente os controles complementares que cabem ao usuário do serviço.

IMPACTO POR PERFIL

Como isso afeta a *sua* companhia.

INSTITUIÇÃO TRANSMISSORA DE DADOS

Você guarda o dado que o cliente autoriza a compartilhar. Garanta que o consentimento seja validado a cada chamada, que a revogação interrompa o acesso imediatamente e que cada compartilhamento deixe trilha — a responsabilidade sobre o dado não termina quando ele sai da sua fronteira.

INSTITUIÇÃO RECEPTORA DE DADOS

Você usa dados de terceiros por consentimento. Assegure que o uso respeite finalidade e prazo, que a base de tratamento sob LGPD esteja clara e que você confie nos controles da transmissora com base em evidência — não em presunção de conformidade do ecossistema.

FINTECH E INICIADORA DE TRANSAÇÃO DE PAGAMENTO

Nascer no ecossistema não dispensa maturidade de controle. Autenticação, autorização e rastreabilidade das chamadas são o que sustenta a confiança de parceiros e reguladores — formalize o ciclo de vida do consentimento antes que a escala transforme exceção em incidente.

PRESTADOR DE SERVIÇO DE TECNOLOGIA DO ECOSSISTEMA

Se você opera infraestrutura para participantes, seus controles entram no perímetro de confiança deles. Relatórios de asseguração no espírito ISAE 3402/SOC, com controles complementares do usuário bem definidos, são o que permite ao cliente institucional confiar e comprovar.

COMPLIANCE, SEGURANÇA E AUDITORIA INTERNA

Consentimento e segurança de API precisam estar no plano de controles com abordagem baseada em risco. Testem a efetividade da revogação, a aderência à finalidade e a integridade dos logs — e leiam criticamente os relatórios de asseguração dos parceiros do ecossistema.

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. Existe mapa do ciclo de vida do consentimento (concessão, uso, renovação e revogação) com controles em cada etapa?	☐	☐	
02. A revogação do consentimento interrompe o acesso aos dados de forma efetiva e tempestiva, e isso é testado?	☐	☐	
03. O uso dos dados é amarrado à finalidade e ao prazo autorizados pelo titular?	☐	☐	
04. As chamadas de API exigem autenticação forte e autorização granular por escopo?	☐	☐	
05. Os dados em trânsito são protegidos por criptografia e controles de integridade adequados?	☐	☐	
06. Cada compartilhamento de dados deixa trilha íntegra e rastreável (logs auditáveis)?	☐	☐	
07. A base legal de tratamento sob a LGPD está definida e documentada para cada fluxo de dados?	☐	☐	
08. Os direitos do titular (acesso, revogação, informação) são operacionalizados e evidenciados?	☐	☐	
09. A instituição obtém e revisa relatórios de asseguração de controles dos participantes e prestadores relevantes?	☐	☐	
10. Os controles complementares do usuário (CUECs) dos prestadores são identificados e implementados?	☐	☐	
11. Incidentes de segurança e de dados têm processo formal de resposta, comunicação e avaliação de impacto?	☐	☐	
12. O plano de auditoria interna cobre consentimento, segurança de APIs e compartilhamento com abordagem baseada em risco?	☐	☐	

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 independente de controles de consentimento e de segurança de APIs no Open Finance, avaliação da interface entre os controles do ecossistema e a LGPD, e preparação de relatórios de controles no espírito ISAE 3402 para sustentar a confiança entre participantes.

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

- Regulação do Open Finance (Banco Central do Brasil) — estrutura, escopo e regras de compartilhamento por consentimento.
- Lei 13.709/2018 (LGPD) — licitude, finalidade, direitos do titular e segurança no tratamento de dados.
- NBC TO 3402 — asseguração de controles em organizações prestadoras de serviços.
- Resolução CMN 4.893/2021 — política de segurança cibernética e contratação de serviços em nuvem.
- NBC TA 315 (revisada) — entendimento do ambiente de TI e dos controles gerais na auditoria.

REFERÊNCIAS INTERNACIONAIS

- ISAE 3402 — Assurance Reports on Controls at a Service Organization.
- SOC 2 (AICPA) — Trust Services Criteria (segurança, disponibilidade, confidencialidade e privacidade).
- ISO/IEC 27001 — gestão de segurança da informação; padrões de API security (OAuth 2.0 / FAPI).

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.