Proposta de GT Conjunto OI +OF

Interoperabilidade Open Finance + Open Insurance
Resumo Executivo

1. Objetivo

Apresentar ao **Conselho Deliberativo do Open Insurance (CDOI)** análise técnica fundamentada sobre as **incompatibilidades operacionais críticas** entre os ecossistemas **Open Finance Brasil (OFB)** e **Open Insurance (OPIN)**, demonstrando a **urgência de criação de um Grupo de Trabalho conjunto (GT de Interoperabilidade OFB–OPIN)** para viabilizar a interoperabilidade prevista na **Resolução Conjunta BCB/CMN/CNSP nº 5/2022**.

2. Sumário Executivo

2.1 Contexto Regulatório

A **Resolução Conjunta nº 1/2020** (BCB/CMN) estabeleceu o Open Finance Brasil, posteriormente renomeado pela Resolução Conjunta nº 4/2022. A **Resolução CNSP nº 415/2021** instituiu o Open Insurance. A **Resolução Conjunta nº 5/2022**, publicada em 20/05/2022 e vigente desde 02/01/2023, **determinou expressamente a interoperabilidade entre os dois ecossistemas**, estabelecendo que:

> *"Os participantes dos sistemas [...] devem propor e implementar padrões técnicos e outros procedimentos operacionais que assegurem a interoperabilidade dos sistemas que compõem o Open Finance"* (Art. 3º, I)

O prazo regulatório inicial era **30/11/2023**. No entanto, **quase dois anos após a vigência**, persistem **incompatibilidades estruturais** que inviabilizam a interoperabilidade efetiva.

2.2 Situação Atual: Gaps Críticos Identificados

A análise comparativa identificou **incompatibilidades técnicas** e operacionais entre OFB e OPIN, com destaque em 12 dimensões de maior impacto:

TABELA COMPARATIVA:

Legenda:

- ✅ **= Situação consolidada/adequada**
- ⚠️ **= Situação parcial/em desenvolvimento**
- ❌ **= Gap crítico/ausência total**

DIMENSÃO	OPEN INSURANCE	OPEN FINANCE	IMPACTO	RISCO
1. Ciclo de Vida de APIs	⚠️ Versionamento semântico flexível; período de convivência de 180 dias para versões MAJOR **ALGUNS PONTOS EM TRATAMENTO NO ÂMBITO DO GT DE ESCOPO DE DADOS DO OPEN INSURANCE POR PROVOCAÇÃO DO G5**	✅ Versionamento estruturado com calendário consolidado; período de convivência de 90 dias (inferido da prática)	Janelas de migração duplicadas; instituições participantes de ambos ecossistemas mantêm duas trilhas paralelas com janelas temporais distintas	Releases dessincronizados; esforços duplicados de planejamento, testes e deploy
2. Padrões de Segurança (FAPI/OAuth)	⚠️ FAPI 1.0 Advanced; OAuth 2.0 BCP (RFC 9700) não referenciado; FAPI 2.0 sem roadmap definido	⚠️ FAPI 1.0 Advanced certificado via OpenID Foundation; OAuth 2.0 BCP (RFC 9700) não referenciado; FAPI 2.0 sem roadmap coordenado	Cronogramas distintos para migração ao FAPI 2.0; ausência de OAuth BCP atualizado em ambos ecossistemas	Exposição a vulnerabilidades conhecidas (authorization code injection, mix-up attacks); duplicação de custos de recertificação
3. Dynamic Client Registration (DCR) e Discovery	⚠️ Diretório em construção; DCR com particularidades na estrutura de metadados (SSA)	✅ Diretório de Participantes centralizado consolidado; DCR com mTLS obrigatório e padrões estabelecidos	Onboarding mais lento para TPPs que operam em ambos mercados; integrações duplicadas	Processos distintos de descoberta; complexidade operacional elevada
4. Certificação e Conformidade	⚠️ Processo próprio em implementação; sem coordenação formal com OF; provável espelhamento futuro	✅ Certificação via OpenID Foundation (FAPI, DCR, RP) + Conformance Suite consolidada	Processos paralelos custosos; duplicação de: taxas de certificação, esforço de preparação, tempo de equipes técnicas, recertificação por mudanças de versão	Inconsistência de escopo; custos operacionais elevados para instituições participantes de ambos ecossistemas
5. UX de Consentimento	❌ Terminologia e fluxos divergentes; textos mandatórios diferentes para mesma finalidade; nomenclatura de produtos inconsistente (ex: "seguro de pessoas com cobertura por sobrevivência")	⚠️ Guia de UX estabelecido; terminologia diferente de OI (ex: "plano de previdência"); sem harmonização para jornadas interoperáveis	Fricção cognitiva para o usuário que interage com ambos ecossistemas; maior taxa de abandono de fluxo; experiência fragmentada	Baixa adoção; perda de oportunidades de produtos híbridos por fricção excessiva na experiência do cliente

6. Taxonomia e Dicionário de Dados	⚠️ Produtos de previdência complementar aberta já mapeados com campos específicos; enums e estruturas sem correspondência em OF	❌ Produtos de previdência não fazem parte do escopo nativo; eventual inclusão futura via expansão	Schemas divergentes; incompatibilidade semântica crítica: perda de informações críticas (coberturas, taxas, prazos); impossibilidade de portabilidade ou comparação via plataforma interoperável	Dados não comparáveis; perda de oportunidades de produtos híbridos (seguros vinculados a previdência); custos elevados para TPPs multi-setor
7. Observabilidade e Qualidade (OpenTelemetry)	❌ Ausência de requisitos de observabilidade estruturada via OpenTelemetry (traces distribuídos, métricas, logs estruturados)	❌ Ausência de requisitos de observabilidade estruturada via OpenTelemetry; sem SLIs/SLOs padronizados	MTTR elevado em incidentes que atravessam a ponte OF-OI; dificuldade de diagnóstico end-to-end; ausência de SLIs/SLOs padronizados	Incidentes sistêmicos com MTTR elevado por falta de observabilidade integrada; experiência ruim para instituições participantes
8. Contract Testing	❌ Testes de contrato não mandatados de forma consistente; ausência de publicação de resultados no diretório	❌ Testes de contrato não mandatados de forma consistente em pipelines de CI/CD	Regressões entre versões; baixa reprodutibilidade; quebras silenciosas entre consumidor/provedor	Bugs não detectados; estabilidade operacional comprometida; ausência de validação sistemática
9. Gestão de Vulnerabilidades e Dependências	❌ Política de atualização de CVEs não uniformizada; ausência de SBOM (Software Bill of Materials); inventário difuso de componentes	❌ Política de CVEs não uniformizada; ausência de escaneamento automático contínuo de dependências; sem publicação obrigatória de SBOM	Exposição prolongada a vulnerabilidades conhecidas; inventário difuso de componentes; dificuldade de resposta a incidentes zero-day	Risco sistêmico de segurança; ausência de controle de componentes críticos (ex: bibliotecas criptográficas)
10. Privacidade e Conformidade LGPD (ISO 27701)	❌ ISO/IEC 27701:2019 (Privacy Information Management System) não referenciada explicitamente nos manuais de segurança	❌ ISO/IEC 27701:2019 não referenciada explicitamente; lacuna de governança de privacidade	Lacuna de governança de privacidade; risco de não conformidade à LGPD em cenários de interoperabilidade (tratamento de dados cross-ecossistema)	Riscos regulatórios; exposição a sanções por tratamento inadequado de dados pessoais em fluxos interoperáveis
11. Operação e Incidentes (Service Desk)	⚠️ Service desk separado; playbooks de incidentes não coordenados; ausência de matriz RACI clara para cenários híbridos	⚠️ Service desk separado; playbooks de incidentes não coordenados; SLAs não alinhados com OI	Resolução lenta em falhas que envolvem ambos ecossistemas; dificuldade em definir claramente o responsável em cenário interoperável; MTTR elevado	Experiência ruim para instituições participantes; incidentes prolongados em jornadas cross-ecossistema
12. Versionamento e Releases Sincronizados	❌ Calendário de releases independente; processos de comunicação via SUSEP sem coordenação com BCB	⚠️ Calendário estabelecido com comunicação via BCB; sem sincronização com OI para releases coordenados	Releases dessincronizados; breaking changes em um ecossistema podem impactar integrações no outro sem coordenação prévia	Incompatibilidade temporária em atualizações; custos operacionais elevados; risco de interrupção de serviços interoperáveis

Risco sistêmico: Sem harmonização, a interoperabilidade permanecerá teórica, comprometendo os objetivos regulatórios de inovação, competição e proteção do consumidor.

3. Fundamentação Técnica: Análise Comparativa Detalhada

3.1 Incompatibilidades no Ciclo de Vida de APIs

3.1.1 Período de Convivência de Versões

Aspecto	Open Finance	Open Insurance	Impacto
Período MAJOR	90 dias (inferido da prática)	**180 dias** (explícito no Manual)	Janelas dessincronizadas
MINOR/PATCH	Imediato	Imediato	Alinhado
Comunicação	BCB	SUSEP	Processos distintos

Fonte: Manual de APIs OI v1.5, pág. 9; práticas documentadas OFB no portal do desenvolvedor.

Impacto prático: Instituições participantes de ambos ecossistemas precisam manter **duas trilhas de migração paralelas** com janelas temporais distintas, duplicando esforços de planejamento, testes e deploy.

Proposta: Harmonizar em **120 dias** para versões MAJOR em ambos ecossistemas, com aplicação imediata para MINOR/PATCH.

3.1.2 Versionamento Semântico (SemVer)

EM TRATAMENTO NO ÂMBITO DO GT DE ESCOPO DE DADOS DO OPEN INSURANCE POR PROVOCAÇÃO DO G5

Open Finance: Documentação cita "formato contemplando 4 tipos: major.minor.patch.rc" mas admite **exceções que permitem quebra de contrato em versões MINOR**, conforme observado em: *"Lançamentos minor não podem configurar em quebra de contrato, impactar significativamente endpoints e/ou exigir manutenção crítica"* - porém o guia de versionamento prevê casos excepcionais.

Open Insurance: Manual v1.5 declara adoção de **SemVer 2.0.0** mas persiste ambiguidade na redação: *"minor: pequenas mudanças nos elementos já existentes, com manutenção da compatibilidade com as versões até a major imediatamente anterior"* (pág. 8), o que pode gerar interpretações assimétricas.

Inconsistência crítica: Sem aderência **estrita** ao SemVer 2.0.0, quebras não previstas podem ocorrer, gerando instabilidade contratual entre consumidores e provedores de APIs.

Proposta: Adotar **SemVer 2.0.0 estrito** (breaking changes **apenas** em MAJOR), com uso obrigatório de **pre-release** (ex: `v2.0.0-rc.1`) para candidate releases.

3.1.3 Versionamento na URL

EM TRATAMENTO NO ÂMBITO DO GT DE ESCOPO DE DADOS DO OPEN INSURANCE POR PROVOCAÇÃO DO G5

Ambos os ecossistemas: Ausência de orientação **explícita e uniforme** sobre inclusão de versão MAJOR no path da URL. Prática observada: `/<api>/<versão>/<recurso>`, mas falta clareza sobre manutenção de múltiplas versões em paralelo.

Proposta: Incluir `v{X}` no path apenas para versão MAJOR; versões MINOR/PATCH **não alteram** a URL, garantindo convivência paralela durante migração e simplificando rollback.

3.1.4 Credenciais Agnósticas

Ambos: Exigência de credenciais agnósticas por versão já estabelecida em ambos ecossistemas. Este é um **ponto de alinhamento positivo existente** que deve ser **preservado, reforçado e explicitado** nos manuais técnicos.

Proposta: Tornar explícita nos Manuais de APIs de ambos ecossistemas a diretriz de que credenciais de acesso (certificados, client_id, etc.) DEVEM ser agnósticas à versão da API, aplicando-se a todas as versões MINOR e PATCH dentro de uma mesma versão MAJOR, sem necessidade de reemissão ou recadastramento a cada release. Esta explicitação reduz ambiguidades e facilita a convivência de versões durante períodos de migração.

3.2 Standards Técnicos: Obsolescência e Incompatibilidade

3.2.1 OpenAPI e Toolchain

Especificação	Open Finance	Open Insurance	Estado da Arte (2025)
OpenAPI	3.0.0	**3.0.0**	**3.1.1** (2021, compatível com JSON Schema 2020-12)
Validação	Spectral (versão não especificada uniformemente)	**Spectral 5.9.0**	**Spectral 6.x+** (suporte OpenAPI 3.1)
Code Generation	Swagger Codegen referenciado	**Swagger Codegen 3.0.25**	**OpenAPI Generator** (sucessor ativo)

Fonte: Manual de APIs OI v1.5, pág. 8; documentação OFB portal desenvolvedor.

Problema: OpenAPI 3.0.0 **não suporta** JSON Schema Draft 2020-12, limitando recursos como `prefixItems`, `$dynamicRef`, validações avançadas. Spectral 5.x possui limitações conhecidas. Swagger Codegen está **descontinuado** desde 2021, substituído por OpenAPI Generator.

Impacto: Bugs não detectados em validações; incompatibilidade com ferramentas modernas; retrabalho futuro inevitável.

Proposta: Migração coordenada para **OpenAPI 3.1.1**, **Spectral 6.x+** e **OpenAPI Generator** em ambos os ecossistemas, com roadmap de 180 dias e suporte de transição.

3.2.2 JSON Schema e Semântica

Ambos: Ausência de referência explícita ao **JSON Schema Draft 2020-12** e ao vocabulário **ISO 20022**.

Open Finance: Menciona ISO 20022 no Manual de Escopo mas sem enforcement técnico nas specs.

Open Insurance: Manual de APIs cita ISO 20022 como princípio (seção 3.7) mas sem implementação verificável nas especificações OpenAPI.

Impacto: Inconsistências de validação entre domínios; dados não comparáveis; ETL frágil na ponte entre ecossistemas.

Proposta: Adotar **JSON Schema 2020-12** como padrão; mapear sistematicamente elementos ISO 20022 aplicáveis (Payment, Account, Securities) para garantir **semântica compartilhada** entre OF e OI, especialmente em produtos híbridos (ex: previdência).

3.3 Segurança: FAPI, OAuth 2.0 e Certificação

3.3.1 OAuth 2.0 Security Best Current Practice (BCP)

Ausência crítica: Nenhum dos manuais de segurança (OF ou OI) referencia o **RFC 9700 (OAuth 2.0 Security BCP)**, publicado em **janeiro de 2025**.

Este BCP consolida práticas modernas essenciais:

- **PKCE obrigatório** para todos os tipos de cliente
- **Validação estrita de redirect URIs**
- **Mitigação de authorization code injection**
- **Proteção contra mix-up attacks**

Fonte: RFC 9700; análise dos Manuais de Segurança OFB v4.0 (IN 305/2022) e OI (não versionado publicamente disponível).

Risco: Vetores de ataque conhecidos **não cobertos** pela regulação atual, expondo clientes a fraudes.

Proposta: Atualização **imediata** dos Manuais de Segurança de ambos ecossistemas para incorporar RFC 9700, com prazo de adequação de 90 dias para implementações críticas.

3.3.2 FAPI 1.0 Advanced e Roadmap para FAPI 2.0

Situação atual:

- Ambos os ecossistemas operam com **FAPI 1.0 Advanced** certificado pela OpenID Foundation
- **FAPI 2.0** (com PAR - Pushed Authorization Request, RAR - Rich Authorization Request, CIBA - Client-Initiated Backchannel Authentication) já está em fase de certificação global desde 2022

Problema: Não há **roadmap conjunto** para migração ao FAPI 2.0, gerando risco de:

- Cronogramas distintos que duplicam esforços de recertificação
- Janelas de convivência não sincronizadas
- Custos elevados para TPPs multi-setor

Proposta: Estabelecer **roadmap coordenado** para adoção de FAPI 2.0 (PAR/RAR/CIBA) com janelas sincronizadas e processo de certificação unificado.

3.3.3 Dynamic Client Registration (DCR) e Descoberta (Discovery)

Ambos: Implementam DCR conforme RFC 7591/7592 e OpenID Connect Discovery, porém com **variações de processo** e formatos (SSA - Software Statement Assertion).

Open Finance: Diretório de Participantes centralizado; DCR com mTLS obrigatório.

Open Insurance: Diretório em construção; DCR segue padrões mas com particularidades na estrutura de metadados.

Impacto: Onboarding mais lento para TPPs que operam em ambos mercados; integrações duplicadas.

Proposta: Guia único de DCR/SSA/Discovery com testes de conformidade comuns e matriz de cobertura unificada entre ecossistemas.

3.4 Certificação e Conformidade

3.4.1 Processos Separados

Situação: Processos de certificação completamente segregados:

- **OF:** OpenID Foundation (FAPI, DCR, RP) + Conformance Suite da estrutura de governança

- **OI:** Processo próprio em implementação, com provável espelhamento mas sem coordenação formal

Custos: Instituições participantes de ambos precisam passar por **certificações paralelas**, duplicando:

- Taxas de certificação
- Esforço de preparação de ambientes de teste
- Tempo de equipes técnicas
- Recertificação por mudanças de versão

Proposta: Processo de certificação conjunto reconhecido mutuamente, com:

- Matriz de cobertura unificada (segurança + funcional)
- Ambiente de testes compartilhado para cenários de interoperabilidade
- Reconhecimento mútuo de certificados onde aplicável

3.5 UX de Consentimento

Problema: Guias de UX com terminologia e fluxos **divergentes** entre OF e OI.

Exemplos observados:

- Textos mandatórios diferentes para mesma finalidade
- Nomenclatura de produtos (ex: "plano de previdência" vs "seguro de pessoas com cobertura por sobrevivência")
- Telas de confirmação com estruturas distintas

Impacto: Fricção cognitiva para o usuário que interage com ambos ecossistemas; maior taxa de abandono de fluxo; experiência fragmentada.

Proposta: Guia de UX unificado com:

- Textos mandatórios harmonizados
- Padrões de telas para cenários comuns (criação, renovação, revogação)
- Mensagens de erro padronizadas
- Princípios de acessibilidade alinhados

3.6 Taxonomia e Dicionário de Dados

3.6.1 Caso Crítico: Produtos de Previdência

Open Finance: Produtos de previdência **não fazem parte** do escopo nativo; eventual inclusão futura via expansão.

Open Insurance: Produtos de previdência complementar aberta **já mapeados** com campos específicos no Manual de Escopo v7.1.

Problema de Interoperabilidade: Um cliente com plano de previdência **iniciado via OI** que posteriormente busca portabilidade ou comparação via plataforma **OF** encontrará **incompatibilidade semântica**:

- Enums diferentes
- Estruturas de dados não mapeáveis
- Perda de informações críticas (coberturas, taxas, prazos)

Proposta: Dicionário de Dados Comum iniciando por produtos de **previdência**, com:

- Mapeamento explícito de campos entre ecossistemas
- Enumerações harmonizadas
- Regras de transformação documentadas
- Validação em ambiente de testes de interoperabilidade

3.6.2 Estratégia de Priorização: Produtos Comuns

Análise: Nem todos os produtos têm overlap entre OF e OI. Criar dicionários de dados é recomendável, entretanto, a criação para **todos** os produtos de ambos ecossistemas seria esforço desproporcional ao benefício.

Produtos com overlap identificado:

1. **Previdência Complementar Aberta** (VGBL, PGBL) - produto híbrido entre seguro e investimento

2. **Seguros vinculados a crédito** (prestamista, garantia) - interface com operações de crédito OF

3. **Capitalização** - produto com características de poupança programada

Produtos sem overlap imediato:

- Seguros patrimoniais (auto, residencial) - sem equivalente direto em OF
- Seguros de vida puro risco - sem equivalente direto em OF
- Produtos bancários tradicionais - sem equivalente em OI

Proposta:

Fase 1 (prioritária): Dicionário de Dados Comum para **produtos com overlap confirmado** (previdência, seguros vinculados a crédito, capitalização).

Fase 2 (exploratória): Identificação de **produtos emergentes** que possam ter interface cross-ecossistema (ex: tokenização de ativos segurados, produtos embedded insurance).

Fase 3 (futuro): Extensão gradual conforme casos de uso de interoperabilidade sejam identificados pelo mercado.

Esta abordagem **minimiza o escopo inicial**, focando onde a interoperabilidade é crítica, e permite **escalabilidade orgânica** baseada em demanda real.

3.7 Observabilidade e Qualidade

3.7.1 OpenTelemetry

Ausência crítica: Nenhum dos ecossistemas **exige** observabilidade estruturada via **OpenTelemetry** (traces distribuídos, métricas, logs estruturados).

Impacto:

- **MTTR elevado** em incidentes que atravessam a ponte OF-OI
- Dificuldade de diagnóstico end-to-end
- Ausência de SLIs/SLOs padronizados

Proposta: Requisitar OpenTelemetry como obrigatório em ambos ecossistemas:

- Traces distribuídos com context propagation (W3C Trace Context)
- Métricas padronizadas (RED: Rate, Errors, Duration)
- Logs estruturados (JSON, campos semânticos)
- Definição de SLIs/SLOs comuns para APIs de interoperabilidade

3.7.2 Contract Testing

Ausência: Testes de contrato **não são mandatados** de forma consistente em nenhum dos ecossistemas.

Impacto: Regressões entre versões; baixa reprodutibilidade; quebras silenciosas entre consumidor/provedor.

Proposta: Tornar obrigatório contract testing (Pact, Dredd ou equivalente) nos pipelines de CI/CD, com publicação de resultados no diretório de participantes.

3.8 Gestão de Vulnerabilidades e Dependências

Situação: Política de **atualização de dependências** e **CVEs não uniformizada**; ausência de **SBOM** (Software Bill of Materials).

Risco sistêmico: Exposição prolongada a vulnerabilidades conhecidas; inventário difuso de componentes; dificuldade de resposta a incidentes zero-day.

Proposta: Política comum de gestão de vulnerabilidades:

- Escaneamento automático contínuo de dependências
- CVEs críticas (CVSS ≥9.0): remediação em **≤30 dias**
- CVEs altas (CVSS 7.0-8.9): remediação em ≤90 dias
- Publicação obrigatória de **SBOM** (formato CycloneDX ou SPDX)
- Inventário centralizado de componentes críticos (ex: bibliotecas criptográficas)

3.9 Privacidade e Conformidade LGPD

Ausência: Nenhum dos manuais referencia explicitamente a **ISO/IEC 27701:2019** (Privacy Information Management System), extensão da ISO 27001 para privacidade.

Impacto: Lacuna de governança de privacidade; risco de não conformidade à LGPD em cenários de interoperabilidade (tratamento de dados cross-ecossistema).

Proposta: Adicionar ISO 27701 aos requisitos dos Manuais de Segurança de ambos ecossistemas, com auditoria específica para fluxos de interoperabilidade.

3.10 Operação e Incidentes

3.10.1 Service Desk e Playbooks

Situação: Service desks **separados**; playbooks de incidentes **não coordenados**.

Impacto: Resolução lenta em falhas que envolvem ambos ecossistemas ("dificuldade em definir claramente o responsável em cenário interoperável"); MTTR elevado; experiência ruim para instituições participantes.

Proposta: Service desk federado com:

- Protocolo único para incidentes de interoperabilidade
- Matriz RACI clara
- SLAs coordenados (ex: P1 ≤2h, P2 ≤8h)
- Playbook conjunto para cenários híbridos

3.10.2 Calendário de Mudanças

Problema: Congelamentos de releases e cadências **não sincronizados** entre OF e OI.

Impacto: Planejamento complexo; risco de mudanças críticas em períodos sensíveis (ex: Black Friday, fim de ano).

Proposta: Calendário coordenado de releases e freezes, com:

- Janelas de manutenção alinhadas
- Períodos de congelamento comuns (datas comercialmente críticas)
- Comunicação antecipada com 90 dias de antecedência mínima

3.11 Monitoramento e KPIs

Problema: Métricas de disponibilidade, performance e adoção **não comparáveis** entre ecossistemas.

Impacto: Dificulta governança executiva; baixa visibilidade sistêmica; impossibilidade de benchmarking.

Proposta: Painel unificado de KPIs técnicos e de UX:

- SLAs (uptime, latência p95, error rate)
- Volumetria (consentimentos ativos, transações, APIs mais utilizadas)
- Indicadores de experiência (taxa de abandono, tempo médio de fluxo)
- Drill-down por instituição participante

3.12 Transparência e Governança

Contexto: O Open Finance Brasil, através de sua estrutura de governança definitiva estabelecida pela Resolução BCB nº 400/2024, adota modelo de **transparência pública** em suas deliberações.

Todas as atas de reuniões do Conselho Deliberativo, apresentações e decisões são publicadas em https://openfinancebrasil.org.br/decisoes-do-conselho-deliberativo/, permitindo rastreabilidade e accountability perante o mercado e a sociedade.

Situação Open Insurance: O Open Insurance está em fase de estruturação de sua governança definitiva, com proposta a ser apresentada à SUSEP até dezembro/2025.

Atualmente, adota posicionamento de **confidencialidade em deliberações**, com reuniões de GTs e do CDOI tratadas como sigilosas, com termos de sigilo aplicados a membros, limitando a divulgação de informações sobre decisões técnicas e estratégicas.

Impacto:

- **Assimetria de informação** entre participantes dos dois ecossistemas
- **Dificuldade de coordenação** para instituições que participam de ambos (impossibilidade de correlacionar decisões)
- **Barreira à inovação** pela restrição ao compartilhamento de conhecimento técnico
- **Risco reputacional** de percepção de falta de transparência em iniciativa de interesse público

Proposta:

Incluir no mandato do GT de Interoperabilidade a recomendação de que a estrutura de governança definitiva do Open Insurance adote modelo de transparência equivalente ao Open Finance, com:

1. **Publicação de atas** de reuniões do Conselho Deliberativo e GTs (respeitando exclusões legais como dados pessoais, segredos industriais específicos)
2. **Disponibilização de apresentações** técnicas que fundamentaram decisões
3. **Registro público de deliberações** com voto nominal quando aplicável
4. **Revisão da política de sigilo** para membros de GTs, permitindo discussão técnica pública de especificações (padrão comum em organismos como IETF, W3C, OpenID Foundation)

Fundamentação: A Resolução Conjunta nº 5/2022 prevê interoperabilidade não apenas técnica, mas **sistêmica**. Transparência equivalente facilita coordenação, reduz custos de compliance e fortalece a confiança do mercado em ambos os ecossistemas.

4. Pacote Normativo Mínimo Sugerido

Para materializar as propostas acima, recomenda-se inclusão explícita nos **Manuais de APIs** e **Manuais de Segurança** de ambos ecossistemas:

4.1 Redações sobre Standards Técnicos

> *"As APIs DEVEM ser especificadas utilizando **OpenAPI versão 3.1.1** (https://spec.openapis.org/oas/v3.1.1.html), com suporte a **JSON Schema Draft 2020-12** (https://json-schema.org/draft/2020-12/schema).*
>
> *As especificações DEVEM ser validadas com **Spectral versão 6.x ou superior** (https://github.com/stoplightio/spectral), aplicando o ruleset padrão desta versão. O resultado da análise NÃO DEVE conter erros.*
>
> *Para geração de código cliente e servidor, RECOMENDA-SE o uso de **OpenAPI Generator** (https://github.com/OpenAPITools/openapi-generator), sucessor do Swagger Codegen.*
>
> *Para documentação interativa, RECOMENDA-SE **Redoc** (https://github.com/Redocly/redoc) ou **Stoplight Elements**."*

4.2 Redações sobre Segurança

> *"As implementações DEVEM aderir ao **OAuth 2.0 Security Best Current Practice (RFC 9700, janeiro/2025)**, incluindo mas não se limitando a:*
>
> - *Uso obrigatório de **PKCE** (RFC 7636) para todos os tipos de cliente;*
> - *Validação estrita de redirect_uris conforme RFC 9700, seção 2.1.1;*
> - *Proteção contra authorization code injection;*
> - *Implementação de medidas anti mix-up.*
>
> *As implementações DEVEM seguir o **OWASP API Security Top 10 (2023)** (https://owasp.org/API-Security/editions/2023/en/0x11-t10/).*
>
> *Os pipelines de CI/CD DEVEM incluir:*
>
> - ***SAST** (Static Application Security Testing) com ferramentas homologadas;*
> - ***DAST** (Dynamic Application Security Testing) em ambientes de pré-produção;*
> - *Escaneamento automático de dependências (ex: OWASP Dependency-Check, Snyk)."**

4.3 Redações sobre Privacidade

*"Além dos requisitos de **ISO/IEC 27001:2022**, as instituições participantes DEVEM implementar controles de **ISO/IEC 27701:2019** (Privacy Information Management System) para assegurar conformidade com a **Lei Geral de Proteção de Dados (LGPD)**."*

4.4 Redações sobre Gestão de Vulnerabilidades

*"As instituições participantes DEVEM manter **inventário atualizado** de todas as dependências de software utilizadas em implementações de APIs, incluindo versão e identificador único.*

Vulnerabilidades DEVEM ser remediadas nos seguintes prazos máximos:

- *CVE Crítica (CVSS ≥9.0): **30 dias** corridos;*
- *CVE Alta (CVSS 7.0-8.9): **90 dias** corridos;*
- *CVE Média (CVSS 4.0-6.9): **180 dias** corridos.*

*As instituições DEVEM publicar **SBOM** (Software Bill of Materials) em formato **CycloneDX** ou **SPDX** para componentes críticos de APIs."*

4.5 Redações sobre Observabilidade

*"As implementações DEVEM instrumentar APIs com **OpenTelemetry** (https://opentelemetry.io/) para:*

- ***Traces distribuídos** com propagação de contexto (W3C Trace Context);*
- ***Métricas RED** (Rate, Errors, Duration) por endpoint;*
- ***Logs estruturados** em formato JSON com campos semânticos padronizados.*

As instituições DEVEM definir e publicar:

- ***SLIs** (Service Level Indicators): uptime, latência p95/p99, error rate;*
- ***SLOs** (Service Level Objectives): ex. disponibilidade ≥99.5%, p95 ≤300ms."*

4.6 Redações sobre Conformidade e Testes de Contrato

*"As instituições participantes DEVEM submeter suas implementações ao **Motor de Conformidade** (Conformance Suite) disponibilizado pela estrutura de governança, conforme já estabelecido.*

*Adicionalmente, para assegurar compatibilidade **contínua** entre versões e entre instituições consumidoras/provedoras, recomenda-se:*

*1. **Testes de contrato bilaterais:** (consumer-driven contract testing) usando ferramentas como Pact (https://pact.io/) ou Dredd (https://dredd.org/) para validar interações específicas entre TPPs e instituições transmissoras;*

*2. **Integração aos pipelines de CI/CD:** execução automática de testes a cada merge;*

*3. **Publicação de resultados:** disponibilização de relatórios de conformidade no Diretório de Participantes para transparência.*

***Proposta para os Manuais:** Incluir seção específica detalhando:*

- *Diferenciação entre testes do Motor de Conformidade (validação contra specs) e testes de contrato (validação de interações reais);*
- *Exemplos de casos de uso para testes bilaterais;*
- *Requisitos mínimos de cobertura;*
- *Processo de publicação de resultados."*

5. Riscos de Inação (sem ajustes tempestivas)

5.1 Riscos Técnicos

1. **Descontinuidade de serviços** durante janelas de migração não coordenadas
2. **Falhas de segurança** por desalinhamento de perfis FAPI/mTLS/JWT durante transições
3. **Escalada de débito técnico** com toolchains obsoletos, gerando retrabalho futuro custoso
4. **Incidentes sistêmicos** com MTTR elevado por falta de observabilidade integrada

5.2 Riscos de Negócio

1. **Baixa adoção** por fricção excessiva na experiência do cliente (UX fragmentada)
2. **Barreira à entrada** para TPPs que precisam duplicar esforços de integração
3. **Perda de oportunidades** de produtos híbridos (ex: seguros vinculados a previdência) por incompatibilidade de dados
4. **Custos operacionais elevados** para instituições participantes de ambos ecossistemas

5.3 Riscos Regulatórios

1. **Descumprimento material** da Resolução Conjunta nº 5/2022
2. **Fragmentação do mercado** contrária aos objetivos de competição e inclusão financeira
3. **Reputação regulatória** comprometida perante organismos internacionais (IOSCO, BIS)

6. Benefícios da Equalização

6.1 Para o Regulador

- **Compliance** efetivo da Resolução Conjunta nº 5/2022
- **Supervisão unificada** com métricas comparáveis
- **Eficiência regulatória** com normas harmonizadas

6.2 Para o Mercado

- **Redução de custos** de conformidade e integração (estimativa: -40% em TCO)
- **Time-to-market reduzido** para produtos interoperáveis
- **Estabilidade operacional** com releases sincronizados

6.3 Para o Cidadão

- **Experiência unificada** em jornadas que cruzam OF e OI
- **Maior oferta** de produtos personalizados (bundling)
- **Transparência e controle** sobre dados em ambos ecossistemas

7. Proposta ao CDOI

7.1 Decisão Solicitada

Aprovar o envio de **ofício à SUSEP**, com anexação do presente documento, propondo a criação formal do **GT de Interoperabilidade OFB–OPIN**, nos termos que seguem descritos nos próximos itens.

IMPORTANTE: O presente documento técnico deverá ser anexado ao ofício como fundamentação da proposta, permitindo à SUSEP avaliar a extensão e criticidade das incompatibilidades identificadas.

7.2 Composição

Representação institucional:

- **SUSEP** (Coordenação técnica conjunta)
- **Banco Central do Brasil** (Coordenação técnica conjunta)
- **Estrutura de Governança do Open Finance** (2 representantes técnicos)
- **Estrutura de Governança do Open Insurance** (2 representantes técnicos)

Colaboração Técnica:

- Coordenadores e suplentes dos Grupos de Trabalho existentes em ambos ecossistemas
- Convidados ad hoc (especialistas em segurança, interoperabilidade, etc.)

7.3 Mandato e Escopo

7.3.1 Fase 1: Harmonização Inicial

Duração: 180 dias a partir da instalação formal

Objetivos:

- Harmonizar **ciclo de vida de APIs** (versionamento, período de convivência, calendário)
- Alinhar **padrões de segurança** (FAPI 2.0, OAuth BCP, DCR/SSA, certificação)
- Unificar **experiência do usuário** (guia de UX, consentimento)
- Criar **dicionário de dados comum** (iniciando por previdência)
- Estabelecer **infraestrutura de operação** (service desk federado, observabilidade)
- Definir **governança de interoperabilidade** (processos decisórios, SLAs, KPIs)

7.3.2 Fase 2: Governança Contínua

Após conclusão de trabalhos de Fase 1, propõe-se instituir **agenda ordinária trimestral** para:

- Acompanhamento da implementação das recomendações do GT
- Avaliação de métricas de interoperabilidade (KPIs definidos)
- Identificação de novos gaps emergentes
- Aprovação de ajustes incrementais aos padrões

Adicionalmente, prever possibilidade de **reuniões extraordinárias** mediante determinação de SUSEP, BCB ou a pedido da Estrutura de Governança de qualquer dos ecossistemas, para tratar:

- Incidentes críticos de interoperabilidade
- Mudanças regulatórias urgentes
- Oportunidades de harmonização identificadas pelo mercado

Esta governança contínua assegura que a interoperabilidade seja **mantida e evoluída** dinamicamente, evitando nova divergência no futuro.

8. Benchmarking Internacional

8.1 Reino Unido (Open Banking UK)

Lição aprendida: Criação do **OBIE** (Open Banking Implementation Entity) desde o início com mandato para padronização e interoperabilidade. Resultado: **99.9% de disponibilidade** em APIs críticas; **7 milhões de usuários ativos** (2024).

Aplicável ao Brasil: Estrutura de governança conjunta desde a concepção, não como remediação.

8.2 Austrália (Consumer Data Right - CDR)

Lição aprendida: CDR expandiu de banking para energy e telecom com **framework único** desde o início. Regras de interoperabilidade **cross-setor** definidas na regulação primária.

Aplicável ao Brasil: Aproveitar momento atual para criar framework de interoperabilidade que antecipe expansão futura (investimentos, telecom).

8.3 União Europeia (PSD2 / Open Finance)

Lição aprendida: NextGenPSD2 estabeleceu padrões técnicos comuns via Berlin Group. Desafio: 27 jurisdições com implementações variadas geraram fragmentação inicial.

Aplicável ao Brasil: Vantagem competitiva de ter 2 ecossistemas em jurisdição única; oportunidade de liderar em interoperabilidade.

9. Comunicação e Gestão de Mudança

9.1 Plano de Comunicação

Públicos-alvo:

1. **Instituições participantes** (S1/S2 e voluntárias)
2. **TPPs** (Third-Party Providers)
3. **Desenvolvedores** (comunidade técnica)
4. **Consumidores finais** (cidadãos e empresas)
5. **Imprensa especializada e trade media**

Mensagens-chave:

- "Interoperabilidade efetiva para melhor experiência do cliente"
- "Redução de custos e complexidade para o mercado"
- "Brasil líder em Open Finance intersetorial"

Canais:

- Portais oficiais (openfinancebrasil.org.br, opinbrasil.com.br)
- Webinars técnicos mensais
- Grupos de trabalho abertos (sandboxes)
- Redes sociais institucionais

10. Conclusão

A **interoperabilidade entre Open Finance e Open Insurance** não é apenas um mandato regulatório da Resolução Conjunta nº 5/2022 — é uma **condição essencial** para realizar a promessa de um ecossistema financeiro verdadeiramente aberto, competitivo e centrado no cliente.

As **categorias de incompatibilidades** identificadas nesta análise demonstram que a harmonização não ocorrerá organicamente. É necessária **ação coordenada, estruturada e com governança clara**.

O **GT de Interoperabilidade OFB-OPIN** proposto oferece um caminho pragmático, com:

- **Roadmap de implementação**
- **Entregas estruturantes**

O momento é propício: ambos os ecossistemas estão maduros o suficiente para estabelecer pontes, mas ainda não consolidados a ponto de tornar mudanças proibitivamente custosas.

A decisão do CDOI definirá se manterá aguardando um desfecho que pode vir a ser muito crítico para a interoperabilidade ou se posicionará proativamente como agente direto para que o Brasil seja referência internacional em interoperabilidade.

11. Nota técnica relevante

O estudo conduzido, aliado à confiança na competência profissional das equipes responsáveis pelos ecossistemas, indica a possibilidade de que alguns dos aspectos aqui delineados já se encontrem em implementação ou vigência.

Todavia, **diante da impossibilidade de identificação dos registros documentais oficiais que as atestem, tais ocorrências foram sinalizadas**, visto que em mercados regulados, **registros oficiais constituem condição necessária** para assegurar a conformidade e a interoperabilidade em consonância com o arcabouço normativo vigente.

Documento elaborado pelo G5
Responsável técnico: Robson Machado

12. Anexos

Anexo A: Glossário de Termos Técnicos

API (Application Programming Interface): Interface de programação que permite comunicação entre sistemas.

FAPI (Financial-grade API): Perfil de segurança OAuth 2.0 para APIs de alto risco financeiro.

mTLS (Mutual TLS): Autenticação mútua usando certificados X.509 em ambos os lados da conexão.

DCR (Dynamic Client Registration): Registro automático de aplicações OAuth via APIs (RFC 7591).

PKCE (Proof Key for Code Exchange): Extensão OAuth para proteção contra interceptação de código de autorização (RFC 7636).

SemVer (Semantic Versioning): Convenção de versionamento MAJOR.MINOR.PATCH (semver.org).

OpenTelemetry: Framework de observabilidade para coleta de traces, métricas e logs (opentelemetry.io).

SBOM (Software Bill of Materials): Inventário estruturado de componentes de software.

TPP (Third-Party Provider): Provedor de serviços terceiro que consome APIs de Open Finance/Insurance.

Anexo B: Referências Normativas

Resoluções e Circulares:

- Resolução Conjunta BCB/CMN nº 1/2020 (Open Finance)
- Resolução Conjunta BCB/CMN nº 4/2022 (renomeação para Open Finance)
- Resolução Conjunta BCB/CMN/CNSP nº 5/2022 (interoperabilidade)
- Resolução BCB nº 32/2020 (requisitos técnicos Open Finance)
- Resolução CNSP nº 415/2021 (Open Insurance)
- Circular SUSEP nº 635/2021 (dados de produtos)
- Instrução Normativa BCB nº 306/2022 (Manual de APIs OF v4.0)

Manuais Técnicos:

- Manual de APIs do Open Insurance v1.5
- Manual de APIs do Open Finance v4.0
- Manual de Segurança do Open Insurance v1.5
- Manual de Segurança do Open Finance v4.0
- Manual de Escopo de Dados e Serviços do Open Insurance v7.1
- Manual de Escopo de Dados e Serviços do Open Finance v5.0 (IN BCB 371/2023)
- Manual de Experiência do Cliente do Open Insurance - v3.0

- Manual de Experiência do Cliente do Open Finance v8.0 (IN BCB 637/2025)
- Manual de Serviços Prestados pela Estrutura de Governança do Open Insurance v1.3
- Manual de Serviços Prestados pela Estrutura de Governança do Open Finance v3.0 (IN BCB 359/2023)
- Guia de Experiência do Usuário do Open Insurance v3.3
- Guia de Experiência do Usuário do Open Finance v7.03.00

Standards Internacionais:

- OpenAPI Specification 3.1.1 (spec.openapis.org)
- JSON Schema Draft 2020-12 (json-schema.org)
- OAuth 2.0 Security BCP - RFC 9700 (ietf.org)
- FAPI 1.0 Advanced (openid.net/specs/fapi)
- ISO 20022 (iso20022.org)
- ISO/IEC 27001:2022 e 27701:2019 (iso.org)
- OWASP API Security Top 10 2023 (owasp.org)

Anexo C: Contatos e Recursos

Estrutura de Governança Open Finance:

- Portal: openfinancebrasil.org.br
- Portal do Desenvolvedor: openfinancebrasil.atlassian.net

Estrutura de Governança Open Insurance:

- Portal: opinbrasil.com.br
- Portal do Desenvolvedor: opinbrasil.atlassian.net

Reguladores:

- Banco Central do Brasil: bcb.gov.br/openfinance
- SUSEP: gov.br/susep

Organismos Técnicos:

- OpenID Foundation: openid.net
- IETF OAuth Working Group: ietf.org/wg/oauth
- Open API Initiative: openapis.org