POLÍTICA DE MONITORAMENTO DE CONFORMIDADE

1. Introdução

1.1. Propósito

Esta Política de Monitoramento de Conformidade (“Política”) estabelece diretrizes, regras e responsabilidades para o monitoramento contínuo, avaliação, auditoria e supervisão das obrigações legais, regulatórias e normativas aplicáveis à OPENBANX, especialmente no que se refere ao Sistema de Gestão de Privacidade da Informação (PIMS), Sistema de Gestão de Segurança da Informação (SGSI), Lei Geral de Proteção de Dados (LGPD), Resoluções do Conselho Monetário Nacional (CMN) e Banco Central do Brasil (BACEN), bem como às regras de governança e segurança do Open Finance Brasil.

O propósito central desta Política é garantir que todos os processos, sistemas, operações e tratamentos de dados pessoais — incluindo dados financeiros compartilhados via Open Finance — estejam permanentemente em conformidade com:

- ISO/IEC 27701:2025 (cláusulas 9 e 10)
- ISO/IEC 27001:2022 (monitoramento e auditoria)
- LGPD (arts. 46 a 50 – segurança, boas práticas e governança)
- Resolução CMN nº 4.893/21 (segurança cibernética e Open Finance)
- Resolução CMN nº 4.968/21 (compartilhamento de dados)
- Normativos técnicos do Open Finance Brasil

1.2. Escopo

Esta Política se aplica a:

- Todos os colaboradores, estagiários, prestadores de serviços e fornecedores da OPENBANX.
- Todas as áreas envolvidas em tratamento de dados pessoais, dados financeiros ou qualquer operação vinculada ao ecossistema Open Finance.
- Todos os sistemas, APIs, bases de dados, componentes de infraestrutura e ferramentas que armazenam, processam ou transmitem dados pessoais, dados sensíveis ou dados obtidos via Open Finance.
- Todos os processos sujeitos à supervisão da ANPD, Bacen, CMN e demais órgãos reguladores.

1.3. Princípios Fundamentais

O monitoramento de conformidade será conduzido observando os seguintes princípios:

1. Transparência – Evidenciar, registrar e demonstrar conformidade regulatória

O princípio da Transparência determina que todos os processos, controles, procedimentos, atividades de tratamento de dados, operações técnicas e decisões organizacionais devem ser claramente documentados, registrados, comunicados e disponíveis para auditoria, sempre que necessário.

Isso inclui:

- Evidências formais de implementação de controles.
- Registro de decisões de risco, aprovações e mudanças.
- Relatórios de conformidade prontos para Bacen, ANPD e auditorias ISO.
- Visibilidade clara sobre o uso, acesso e compartilhamento de dados.
- Disponibilização de informações relevantes a titulares, parceiros, reguladores e auditores.
- Esse princípio atende diretamente aos requisitos de accountability da LGPD (art. 6º, X) e às cláusulas de documentação das normas ISO 27001 e ISO 27701.

2. Rastreabilidade – Garantir logs completos, íntegros e auditáveis

A rastreabilidade assegura que todas as ações, acessos, autenticações, transações, operações, integrações e modificações relacionadas a dados, sistemas e infraestrutura estejam devidamente registradas em logs completos, imutáveis e auditáveis.

Elementos essenciais:

- Logs criptografados e protegidos contra alteração (WORM).
- Registro de usuário, IP, timestamp, recurso acessado e operação realizada.
- Rastreabilidade de consentimentos e escopos no Open Finance.
- Integração a sistemas de auditoria contínua (SIEM, UEBA, SOAR).

- Retenção conforme reguladores (mín. 5 anos para dados financeiros regulatórios).
- Garantir rastreabilidade é requisito explícito do Bacen, das normas FAPI, das certificações ISO 27001/27701 e da LGPD (art. 6º, VI).

3. Accountability – Evidenciar responsabilidade em todos os níveis organizacionais

Accountability significa demonstrar que a organização adota medidas efetivas, documentadas e verificáveis para proteger dados pessoais, assegurar segurança da informação e cumprir requisitos legais e regulatórios.

Inclui:

- Designação de responsáveis (DPO, Gestores, Comitês).
- Atribuição clara de papéis e obrigações.
- Registros formais de ações, decisões e conformidade.
- Métricas, indicadores e relatórios periódicos.
- Governança estruturada e validada pelas diretorias e órgãos responsáveis.
- Este princípio é central na LGPD (art. 6º, X) e obrigatório na implementação do PIMS da ISO 27701.

4. Privacidade e Segurança by Design – Aplicação preventiva de requisitos de privacidade e segurança

Significa que controles de segurança e privacidade devem ser implementados desde o início da concepção de processos, projetos, produtos, sistemas, integrações ou mudanças, e não apenas após sua implementação.

Inclui:

- Avaliação de impacto (DPIA/LIA) antes de iniciar novos tratamentos.
- Arquiteturas seguras por padrão.
- Minimização de dados já no desenho inicial.
- Definição antecipada de controles de acesso, criptografia, logs e segregação.
- Testes de segurança contínuos antes da produção.
- Configurações de privacidade habilitadas por padrão (by default).
- Atende diretamente aos princípios da LGPD (art. 46 e art. 50) e clausulados essenciais da ISO 27701.

5. Melhoria Contínua – Atualização permanente do PIMS e SGSI

A Melhoria Contínua determina que controles, políticas, processos, procedimentos, tecnologias e práticas de segurança sejam avaliados, atualizados e aprimorados continuamente, para acompanhar mudanças:

- Tecnológicas
- Reguladoras
- Operacionais
- De risco
- Da infraestrutura
- Do ecossistema Open Finance
- Inclui atividades como:
- Auditorias internas frequentes
- Revisões de controles
- Atualização de políticas.

- Planos de ação corretiva
- Monitoramento de conformidade
- LIções aprendidas pós-incidente
- Avaliação periódica de riscos
- Esse princípio é a base dos sistemas de gestão ISO (cláusula 10 — Improvement).

6. Proporcionalidade e Necessidade – Monitoramento adequado aos riscos envolvidos no tratamento

Esse princípio determina que todas as medidas de proteção, monitoramento, controle e auditoria devem ser proporcionais:

- Ao nível de risco
- À criticidade dos dados tratados
- Ao tipo de operação
- Ao potencial impacto para o titular e para a organização
- Assim, processos e controles devem:
- Ser mais rigorosos para dados sensíveis ou financeiros.
- Ser mais leves quando o tratamento envolver informações não pessoais de baixo impacto.
- Evitar excesso de coleta, retenção ou monitoramento desnecessário.
- Justificar qualquer tratamento adicional que não seja indispensável.
- Esse princípio decorre da LGPD (art. 6º, III e art. 6º, V) e da ISO 27701, que exigem proporcionalidade e adequação para cada tipo de dado e finalidade.

2. Papéis e Responsabilidades

2.1. Encarregado (DPO)

- Monitorar o cumprimento da LGPD e coordenar verificações de privacidade.
- Avaliar riscos de privacidade e emitir pareceres.
- Integrar evidências de conformidade ao PIMS.
-

2.2. Comitê de Segurança e Privacidade (CSP)

- Aprovar critérios, indicadores e planos de auditoria.
- Avaliar riscos críticos e incidentes relevantes.
- Supervisão geral do PIMS, SGSI e Open Finance.

2.3. Área de Segurança da Informação

- Monitorar continuamente eventos de segurança e riscos cibernéticos.
- Revisar logs, alertas, eventos e trilhas de auditoria.
- Implementar ferramentas de SIEM, SOAR e controles técnicos mandatórios.

2.4. Áreas de Negócio e Tecnologia

- Garantir conformidade operacional com políticas internas e normativas regulatórias.
- Manter evidências de execução dos controles.
- Reportar desvios ou irregularidades ao CSP.

2.5. Fornecedores e Terceiros Críticos

- Atender aos requisitos de Bacen, LGPD e Open Finance aplicáveis.
- Permitir auditorias e avaliações de conformidade.

3. Processo de Monitoramento de Conformidade

3.1. Monitoramento Contínuo

A OPENBANX executará monitoramento contínuo para garantir aderência aos controles previstos na ISO 27701, ISO 27001, LGPD, CMN e Open Finance, incluindo:

1. Avaliação diária de logs de sistemas críticos.
2. Monitoramento automatizado de riscos, APIs, consentimentos e acessos.
3. Verificação de integridade e disponibilidade de serviços Open Finance.
4. Acompanhamento regulatório de novas normas da ANPD, Bacen, CMN e Open Finance Brasil.

3.2. Indicadores e Métricas (KPIs/KRIs)

Serão monitorados indicadores específicos, incluindo:

1. Tempo de resposta a solicitações de titulares (LGPD).
2. Conformidade com SLAs regulatórios do Bacen.
3. Taxa de incidentes de privacidade e segurança.
4. Taxa de revogação, expiração e gestão de consentimentos no Open Finance.
5. Proporção de controles implementados do Anexo A da ISO 27701.
6. Status de planos de ação corretiva abertos e concluídos.

Os indicadores serão revisados trimestralmente pelo CSP.

3.3. Auditorias Internas

1. Auditorias internas serão realizadas anualmente, no mínimo.
2. A auditoria abrangerá:

- Conformidade com a ISO 27701 e ISO 27001.
- Obrigações da LGPD e ANPD.
- Serviços e APIs do Open Finance.
- Controles definidos no PIMS e SGSI.

3. Os resultados serão consolidados em relatório e submetidos ao CSP e Diretoria.

3.4. Auditorias de Terceiros e Avaliações Regulatórias

A OPENBANX permitirá auditorias das instituições participantes do Open Finance, bem como:

1. Avaliações de segurança por instituições transmissoras e receptoras.
2. Auditorias dos organismos certificadores ISO.
3. Solicitações de supervisão do Bacen ou ANPD.

4. Monitoramento Técnico e Operacional

4.1. Logs e Trilhas de Auditoria

1. Todos os acessos, transações, chamadas de API e operações de dados serão registrados.
2. Logs devem ser íntegros, imutáveis e armazenados conforme requisitos regulatórios (mínimo de 5 anos para dados financeiros).
3. Alertas automáticos devem ser configurados para:

- Tentativas de acesso indevido;
- Escalonamento de privilégios;
- Múltiplas falhas de autenticação;
- Comportamento anômalo em APIs do Open Finance.

4.2. Conformidade com Padrões do Open Finance

1. Monitoramento contínuo das APIs conforme especificações técnicas vigentes.
2. Validação periódica de consentimento, autenticação e escopo.
3. Verificação de aderência à jornada de usuário (CX) exigida pelo Open Finance Brasil.

5. Ações Corretivas e Preventivas

1. Desvios identificados devem ser registrados e avaliados quanto ao risco.
2. Deve ser conduzida análise de causa raiz (RCA).
3. Planos de ação corretiva serão definidos com prazos e responsáveis.
4. A eficácia das ações será verificada no ciclo de auditorias.

6. Revisão e Vigência

Esta Política será revisada pelo Comitê de Segurança e Privacidade:

- Anualmente, ou
- Sempre que houver mudanças significativas nas normas do Bacen, ANPD, CMN, exigências do Open Finance ou estrutura organizacional.

Versão: 1.0

Aprovado por: Comitê de Segurança e Privacidade (CSP) da OPENBANX

7. Referências

Esta Política foi elaborada com base nas seguintes normas e diretrizes:

1. ISO/IEC 27701:2025 — Privacy Information Management System (PIMS).
2. ISO/IEC 27001:2022 — Information Security Management Systems.
3. Lei nº 13.709/2018 — Lei Geral de Proteção de Dados (LGPD).
4. Resolução CMN nº 4.893/2021 — Requisitos de segurança cibernética e Open Finance.
5. Resolução CMN nº 4.968/2021 — Compartilhamento de dados no Open Finance.
6. Regulamentos técnicos, manuais operacionais e guias do Open Finance Brasil.
7. Comunicações, Ofícios e Circulares vigentes do Banco Central do Brasil.