DOCUMENTO TÉCNICO / CBR CONSULTORIA

Maturidade de Segurança para Fintechs em 2026

Um raio-x prático dos requisitos que reguladores e auditores mais cobram hoje — e como priorizar investimento em segurança sem travar a operação.

CBR.Consultoria

Tecnologia & Segurança da Informação
Edição 2026

01 — Contexto

Por que maturidade de segurança virou pauta de board

O setor financeiro regulado opera hoje sob um volume de exigência que cresce mais rápido do que a maioria das estruturas internas consegue acompanhar. Este guia organiza, de forma prática, onde concentrar esforço primeiro.

Fintechs, instituições de pagamento e plataformas de crédito digital compartilham um mesmo desafio: crescer rápido sem deixar brechas que um auditor, um regulador ou um invasor possam explorar. A pressão vem de várias direções ao mesmo tempo — exigências do Banco Central, adequação à LGPD, expectativa de parceiros e investidores, e a superfície de ataque que aumenta a cada novo produto lançado.

O erro mais comum não é a ausência de controles, mas a falta de priorização: empresas investem esforço disperso em vários pontos e deixam lacunas exatamente onde auditorias e incidentes mais cobram — governança documentada, gestão de acesso e resposta a incidentes.

3
frentes regulatórias que mais geram apontamento em fintechs

3 dias úteis
prazo regulamentar para comunicação de incidentes sujeitos à notificação à ANPD, ressalvada legislação específica

01
política documentada é o item mais cobrado em auditoria inicial

> Este documento não substitui aconselhamento jurídico ou auditoria formal. O objetivo é dar um ponto de partida estruturado para priorizar investimento em segurança e governança.

02 — Panorama regulatório

O que cada frente realmente exige

Três frentes concentram a maior parte da cobrança regulatória sobre tecnologia e segurança em instituições financeiras.

Apesar de linguagens diferentes, as três exigem essencialmente a mesma coisa: documentação viva (que reflete o processo real, não um modelo genérico), rastreabilidade (saber quem acessou o quê, quando) e capacidade de resposta comprovada (não basta ter um plano, é preciso mostrar que ele já foi testado).

FRENTE	O QUE COBRA NA PRÁTICA	ONDE FINTECHS MAIS FALHAM
Banco Central (Res. 4.893)	Política de segurança cibernética formal, plano de continuidade de negócios, gestão de incidentes relevantes e contratos de terceirização auditáveis.	Política existe no papel mas não reflete o processo real; PCN nunca foi testado.
LGPD / ANPD	Base legal para cada tratamento de dado, mapeamento de fluxo de dados pessoais, e notificação de incidente em prazo definido.	Ausência de inventário de dados atualizado; ninguém sabe exatamente onde o dado pessoal trafega.
ISO 27001 / PCI DSS	Sistema de gestão de segurança da informação com escopo definido, controles mapeados a risco e evidência de operação contínua.	Controles implementados isoladamente, sem processo de revisão periódica nem dono formal.

O padrão comum entre as três frentes

Política de segurança · Gestão de acesso · Continuidade de negócio · Resposta a incidentes · Gestão de terceiros

03 — Modelo de maturidade

Quatro estágios de maturidade em segurança

Use este modelo para identificar em qual estágio sua operação está hoje e o que muda no próximo nível.

Estágio 1 — Reativo

Segurança tratada caso a caso, sem política formal. Decisões dependem de uma ou duas pessoas. Não há registro sistemático de incidentes.

Estágio 2 — Documentado

Existem políticas e processos escritos, mas a aderência real varia. Auditoria encontra gaps entre o que está no papel e o que acontece na operação.

Estágio 3 — Gerenciado

Processos são seguidos de forma consistente, com indicadores e responsáveis definidos. A empresa consegue demonstrar evidência de controle para um auditor externo.

Estágio 4 — Otimizado

Segurança é parte do ciclo de desenvolvimento e das decisões de negócio. Métricas de risco alimentam decisões do board. Resposta a incidentes é testada periodicamente.

> A maioria das fintechs em crescimento acelerado está entre os estágios 1 e 2 — o que já é suficiente para operar, mas insuficiente para resistir a uma auditoria aprofundada ou a um incidente real sem dano reputacional.

04 — Priorização

Por onde começar quando o orçamento é limitado

Nem toda fintech tem orçamento para atacar tudo ao mesmo tempo. Esta é a ordem que costuma gerar mais redução de risco por real investido.

- [ ] **Inventário de dados e acessos.** Sem saber onde o dado pessoal e financeiro está e quem acessa, nenhum controle posterior é confiável.
- [ ] **Política de segurança documentada e aprovada pela liderança.** É o primeiro item que qualquer auditor pede, e a base para todo o resto.
- [ ] **Gestão de identidade e acesso (IAM).** Autenticação forte, revisão periódica de permissões e desligamento de acesso ágil.
- [ ] **Plano de resposta a incidentes testado.** Ter o documento não basta — é preciso simular um incidente e medir o tempo de resposta real.
- [ ] **Gestão de fornecedores e terceiros críticos.** Boa parte dos incidentes em fintechs entra pela cadeia de fornecedores, não pelo perímetro próprio.
- [ ] **Continuidade de negócio.** Plano formal, com testes periódicos, para os sistemas que não podem parar.

Sinais de que é hora de agir

Auditoria ou parceiro pediu evidência que a empresa não tinha pronta; crescimento de equipe tornou controle de acesso informal insustentável; um incidente pequeno revelou ausência de processo de resposta.

O que não fazer

Comprar ferramenta antes de mapear processo; copiar política de outra empresa sem adaptar à realidade operacional; tratar segurança como projeto de TI isolado do negócio.

05 — Sobre este material

Quem preparou este documento

A CBR Consultoria estrutura, opera e protege ambientes de tecnologia para fintechs e negócios sob alta regulação — com gestão de projetos, alocação de especialistas e resposta a incidentes, no Brasil e no exterior.

CA

Claudio Araujo

Diretor Executivo da CBR Consultoria. Mais de 31 anos de carreira em Tecnologia e Segurança da Informação, com atuação em governança, gestão de risco e conformidade regulatória para o setor financeiro.

Quer aplicar este modelo na sua operação?

Agende um diagnóstico gratuito e sem compromisso com um de nossos especialistas.