CHECKLIST TÉCNICO / CBR CONSULTORIA

Checklist de Conformidade para Fintechs

Um guia rápido de autoavaliação: os controles que reguladores e auditores mais verificam primeiro em instituições financeiras.

BACEN 4.893 | LGPD / ANPD | ISO/IEC 27001 | PCI DSS

CBR.Consultoria

Tecnologia & Segurança da Informação
Edição 2026

Como usar este checklist

Autoavaliação rápida, sem enrolação

Marque o que sua empresa já tem implementado **e documentado** — não vale o que "existe na cabeça de alguém". Ao final, some os itens marcados para ter uma leitura honesta do seu estágio.

Governança | Acesso | Dados | Continuidade | Terceiros

1 Governança e política

- [ ] Política de segurança da informação formalizada e aprovada pela liderança.
- [ ] Estrutura de responsabilidades definida — quem responde por segurança, quem aprova exceções.
- [ ] Revisão periódica da política (mínimo anual) com registro de data e responsável.
- [ ] Treinamento de conscientização aplicado a todos os colaboradores, com evidência de participação.

2 Gestão de identidade e acesso

- [ ] Autenticação multifator obrigatória para sistemas críticos e acesso remoto.
- [ ] Revisão periódica de permissões (quem tem acesso a quê, e por quê).
- [ ] Processo formal de desligamento que revoga acesso no mesmo dia.
- [ ] Princípio de menor privilégio aplicado — acesso mínimo necessário por função.

3 Dados pessoais e LGPD

- [ ] Inventário de dados pessoais atualizado — onde estão, quem acessa, para que servem.
- [ ] Base legal documentada para cada tipo de tratamento de dado.
- [ ] Processo de resposta a incidentes capaz de notificar a ANPD dentro do prazo exigido.
- [ ] Contratos com fornecedores incluem cláusulas de proteção de dados.

4 Continuidade de negócio

- [ ] Plano de continuidade de negócios (PCN) formal, cobrindo os sistemas críticos.
- [ ] Teste do PCN executado nos últimos 12 meses, com relatório de resultado.
- [ ] Backup testado — não basta existir, é preciso comprovar que restaura corretamente.
- [ ] RTO e RPO definidos para cada sistema crítico (tempo e ponto de recuperação aceitáveis).

5 Resposta a incidentes

- [ ] Plano de resposta a incidentes documentado, com papéis e fluxo de escalonamento claros.
- [ ] Simulação de incidente (tabletop ou real) realizada no último ano.
- [ ] Canal de notificação definido para reguladores, clientes e parceiros afetados.
- [ ] Registro histórico de incidentes, mesmo os de baixo impacto, com lição aprendida.

6 Terceiros e cadeia de fornecedores

- [ ] Avaliação de risco aplicada antes de contratar fornecedores com acesso a dados ou sistemas críticos.
- [ ] Cláusulas contratuais de segurança exigidas de fornecedores críticos, com direito de auditoria.
- [ ] Inventário de terceiros críticos mantido atualizado, com plano de contingência se um deles falhar.

Leitura rápida do resultado

18 itens no total

Até 8 marcados: estágio inicial, priorize governança e inventário de dados. De 9 a 14: base sólida, foque em testar o que já existe no papel. 15 ou mais: maturidade avançada, o próximo passo é formalizar evidência para auditoria externa.