Reforma das Exigências de Segurança Cibernética do Banco Central

O que as instituições precisam fazer até março de 2026

LCSEC

Introdução

O Sistema Financeiro Nacional está passando por uma mudança importante na forma como a segurança cibernética é tratada. O Banco Central deixou claro que **não basta mais ter políticas e documentos**. Agora, as instituições precisam **provar, com evidências técnicas e operacionais**, que os controles funcionam, são monitorados e fazem parte da rotina.

As novas regras reforçam a resiliência digital, especialmente em ambientes críticos como **Pix e STR**, que passam a ser tratados como **infraestrutura crítica**. Esta transformação representa uma elevação significativa do padrão de segurança exigido de todas as instituições financeiras operando no Brasil, alinhando o país com as melhores práticas internacionais de governança e gestão de riscos cibernéticos.

Este material explica, de forma simples e objetiva, **o que mudou, por que isso importa e como se preparar**. Você encontrará orientações práticas, requisitos técnicos detalhados e recomendações estratégicas para garantir que sua instituição esteja plenamente adequada às novas exigências regulatórias até o prazo estabelecido.

CAPÍTULO 1

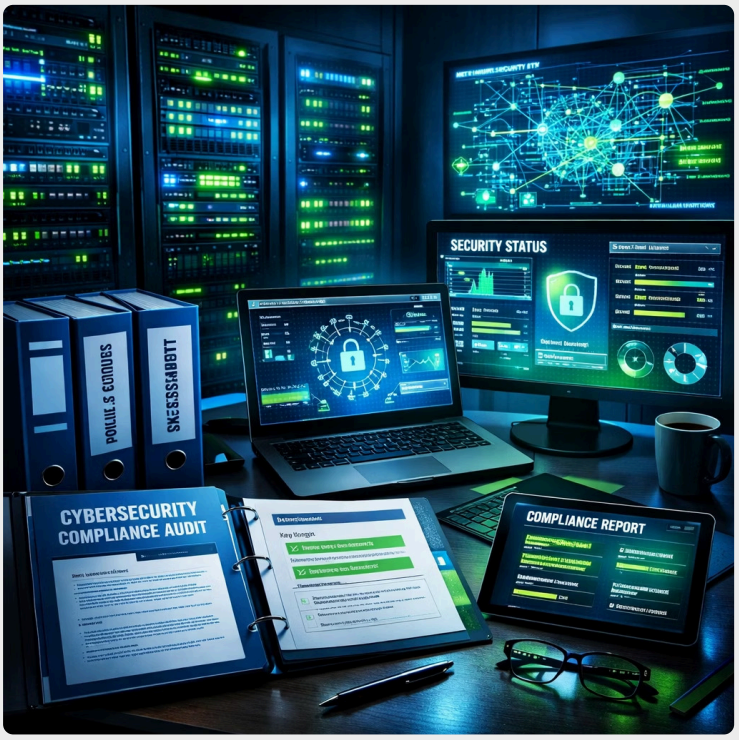
Segurança deixa de ser diretriz e vira obrigação técnica

O que é

O Banco Central substituiu o modelo baseado em "boas práticas" por **requisitos técnicos obrigatórios**, auditáveis e contínuos.

Por que é importante

Isso reduz interpretações subjetivas e eleva o nível mínimo de segurança em todo o setor financeiro.



Como aplicar

- Revisar políticas de segurança existentes
- Transformar diretrizes em controles técnicos implementados
- Definir responsáveis claros por cada controle

Ganhos esperados

- Menor risco regulatório
- Padronização da segurança
- Mais clareza para auditorias

Riscos se não aplicar

- Multas significativas
- Restrição operacional
- Responsabilização da alta gestão

A mudança de paradigma representa uma evolução natural do mercado financeiro brasileiro. Enquanto anteriormente as instituições podiam demonstrar conformidade através de documentação e políticas bem elaboradas, agora o regulador exige comprovação técnica de que os controles estão implementados, funcionando adequadamente e sendo continuamente monitorados. Esta abordagem elimina a lacuna entre a teoria e a prática, garantindo que a segurança cibernética seja uma realidade operacional, não apenas um conjunto de intenções documentadas.

CAPÍTULO 2

Da política à evidência operacional

01

Implementar logs e trilhas de auditoria

Estabelecer sistemas robustos de registro que capturem todas as atividades críticas e mantenham histórico completo

02

Monitorar controles continuamente

Configurar alertas automáticos e painéis de controle para supervisão em tempo real da efetividade dos controles

03

Manter evidências organizadas e rastreáveis

Criar repositórios estruturados de evidências com versionamento e rastreabilidade completa para auditorias

O que é

A segurança passa a ser tratada como **processo contínuo**, com evidências reais de funcionamento. Esta mudança fundamental transforma a forma como as instituições financeiras gerenciam e demonstram sua postura de segurança cibernética.

Por que é importante

Documentos não impedem incidentes. **Controles ativos e monitorados, sim.** A diferença entre ter uma política escrita e ter um controle operacional pode ser crítica durante um ataque cibernético.

Ganhos esperados

- Conformidade regulatória demonstrável
- Detecção precoce de falhas e anomalias
- Maior maturidade operacional
- Resposta mais rápida a incidentes

Riscos se não aplicar

- Não conformidade em fiscalizações
- Falhas invisíveis até o incidente ocorrer
- Tempo de resposta comprometido

A transição da política para a evidência operacional representa uma mudança cultural profunda nas organizações financeiras. Não se trata apenas de implementar novas ferramentas ou tecnologias, mas de criar uma mentalidade onde a segurança é medida, verificada e continuamente aprimorada. As instituições precisam estabelecer processos que garantam que cada controle seja não apenas implementado, mas também testado, monitorado e documentado de forma que qualquer auditor ou regulador possa verificar sua efetividade a qualquer momento.

CAPÍTULO 3

Controles mínimos agora são mais completos

O Banco Central ampliou significativamente o conjunto mínimo de controles obrigatórios, estabelecendo um padrão abrangente que cobre todas as áreas críticas de segurança cibernética. Esta expansão reflete a evolução das ameaças e alinha o Brasil com frameworks internacionais reconhecidos.

Autenticação e Acesso

Autenticação multifator (MFA) obrigatória e controle rigoroso de acessos, incluindo gestão de privilégios e terceiros

Criptografia

Proteção de dados em repouso e em trânsito com algoritmos aprovados e gestão adequada de chaves criptográficas

Segurança de Rede

Detecção e prevenção de intrusão, segmentação de rede e proteção de perímetro com monitoramento contínuo

Proteção contra Malware

Sistemas avançados de detecção e resposta a ameaças com atualizações automáticas e varredura em tempo real

Logs e Rastreabilidade

Registro completo de eventos críticos com retenção adequada e capacidade de análise forense

Backups

Cópias de segurança regulares com testes de restauração e armazenamento geograficamente distribuído

Controles Adicionais

- **Hardening e configuração segura:** Aplicação de benchmarks de segurança em todos os sistemas
- **Proteção de APIs:** Autenticação, autorização e rate limiting em todas as interfaces
- **Inteligência de ameaças:** Integração com feeds de ameaças e análise proativa

Implementação Estratégica

Avaliar gaps técnicos através de assessment completo, priorizar controles críticos baseado em análise de riscos, e medir continuamente a eficácia através de métricas e KPIs estabelecidos.

O alinhamento com ISO 27001 e NIST facilita a implementação e demonstra maturidade para stakeholders.

CAPÍTULO 4

Segurança aplicada ao desenvolvimento, terceiros e nuvem

A segurança passa a ser exigida **desde o desenvolvimento** e se estende a **fornecedores, parceiros e ambientes em nuvem**. Esta abordagem reconhece que a superfície de ataque moderna vai muito além do perímetro tradicional da organização. Grande parte dos incidentes nasce fora do ambiente interno convencional, tornando essencial a extensão dos controles de segurança para toda a cadeia de valor digital.

Desenvolvimento Seguro

Implementar secure coding nas fases de desenvolvimento com revisões de código, testes de segurança automatizados e validação rigorosa de integrações. Todas as aplicações devem passar por análise de vulnerabilidades antes do deploy.

Gestão de Terceiros

Estabelecer programa formal de gestão de riscos da cadeia de fornecedores com due diligence, contratos com cláusulas de segurança, auditorias periódicas e monitoramento contínuo de conformidade.

Segurança em Nuvem

MFA obrigatório para todos os acessos administrativos, isolamento rigoroso de ambientes críticos, controle detalhado de credenciais e certificados, e visibilidade completa sobre configurações de segurança.

Ganhos Estratégicos

- Redução significativa do risco sistêmico
- Menor incidência de falhas em integrações
- Responsabilidade clara e rastreável sobre terceiros
- Maior controle sobre ambientes híbridos e multinuvem

Riscos da Não Conformidade

- Incidentes originados por fornecedores comprometidos
- Comprometimento de ambientes críticos via cadeia de suprimentos
- Perda de visibilidade sobre ativos em nuvem
- Responsabilização por falhas de terceiros

A gestão integrada de segurança através de desenvolvimento, terceiros e nuvem requer maturidade organizacional e ferramentas adequadas. As instituições devem estabelecer processos de governança que garantam que os mesmos padrões de segurança aplicados internamente sejam exigidos e verificados em toda a cadeia de valor. Isso inclui mecanismos de auditoria, cláusulas contratuais específicas e capacidade técnica de monitorar a conformidade de forma contínua.

CAPÍTULO 5

Pix e STR como infraestrutura crítica

Pix e STR passam a ter **exigências mais rigorosas**, equivalentes a sistemas críticos nacionais. Esta classificação reconhece o papel fundamental que esses ambientes desempenham na sustentação de operações essenciais da economia brasileira, processando trilhões de reais diariamente e conectando milhões de usuários e instituições.

A disponibilidade, integridade e confidencialidade desses sistemas são agora tratadas como questão de segurança nacional financeira, exigindo controles de nível mais elevado e supervisão intensificada pelo regulador.

Isolamento

Segregação física e lógica completa dos ambientes Pix e STR com controles de acesso rigorosos e segmentação de rede avançada

Monitoramento

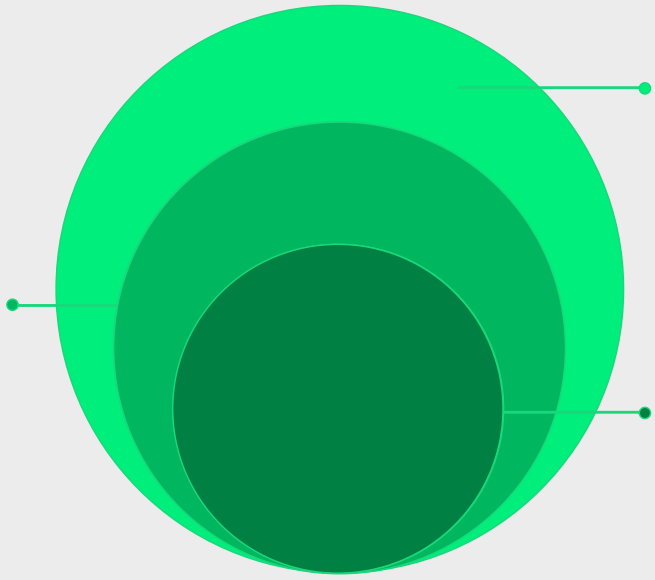
Supervisão contínua 24x7 com detecção de anomalias em tempo real e capacidade de resposta imediata a qualquer desvio

Proteção Criptográfica

Gestão reforçada de chaves e certificados com HSM, rotação automática e controles de acesso multicamada

Validação de Integridade

Verificação ponta a ponta da integridade das transações com controles redundantes e trilhas de auditoria imutáveis



Isolamento de rede
Segmentação e controles de acesso

Monitoramento contínuo
Detecção em tempo real e logs

Validação de integridade
Verificação de mensagens e assinaturas

A implementação desses controles reforçados garante alta disponibilidade operacional, confiança sistêmica e redução significativa do risco de interrupções ou comprometimentos. As penalidades para não conformidade nesta área são particularmente severas, podendo incluir restrições operacionais que impactam diretamente a capacidade da instituição de participar do ecossistema de pagamentos instantâneos e liquidação bruta em tempo real.

CAPÍTULO 6

Testes, governança e prazo até 2026

Pentests anuais passam a ser obrigatórios, com **documentação mantida por cinco anos**. Esta exigência transforma os testes de invasão de atividades pontuais e opcionais em elemento permanente da governança de segurança cibernética. Os testes devem ser conduzidos por profissionais qualificados, independentes, e cobrir todos os sistemas críticos da instituição.

1 **Até Junho 2024**

Diagnóstico completo de gaps e planejamento estratégico de adequação

2 **Até Dezembro 2024**

Implementação dos controles prioritários e início dos testes

3 **Até Junho 2025**

Conclusão da implementação técnica e evidências operacionais

4 **Até Dezembro 2025**

Testes de conformidade, ajustes finais e preparação de documentação

5 **1º Março 2026**

Prazo final - conformidade total obrigatória

Requisitos de Testes

- Contratar testes independentes de empresas especializadas
- Documentar todas as vulnerabilidades identificadas
- Registrar ações corretivas e prazos de remediação
- Manter evidências por cinco anos
- Tratar pentest como processo contínuo, não pontual

Governança Integrada

Os resultados dos pentests devem ser reportados à alta administração e ao comitê de riscos, integrando-se ao ciclo de gestão de vulnerabilidades da instituição.

A não conformidade pode resultar em responsabilização direta de administradores, inabilitação para gestão e restrições operacionais severas.

Benefícios da Abordagem Estruturada

Visão real e atualizada da exposição a riscos cibernéticos, melhoria contínua da postura de segurança, evidência clara e documentada para apresentação ao regulador, e demonstração de compromisso com a gestão proativa de riscos para clientes e parceiros.

Resumo Executivo – O que realmente muda

Mudança de Paradigma
Segurança passa de documento para operação contínua com evidência técnica obrigatória

Infraestrutura Crítica
Pix e STR tratados com rigor de sistemas essenciais nacionais

Escopo Ampliado
Terceiros e nuvem entram definitivamente no escopo regulatório

Prazo Final

1º de Março de 2026

Data limite para conformidade total com todas as exigências do Banco Central

Controles Técnicos Obrigatórios
Implementação verificável de controles mínimos abrangendo MFA, criptografia, detecção de intrusão, proteção contra malware, logs, backups, gestão de acesso e proteção de APIs

Evidência Operacional Contínua
Monitoramento permanente com trilhas de auditoria, logs organizados e capacidade de demonstrar efetividade dos controles a qualquer momento

Testes como Governança
Pentests anuais obrigatórios com documentação mantida por cinco anos, integrando-se ao ciclo de gestão de vulnerabilidades

Segurança na Cadeia de Valor
Controles estendidos a desenvolvimento, fornecedores e ambientes em nuvem com gestão de riscos de terceiros

---

Mais do que cumprir uma exigência regulatória, a adequação às novas normas do Banco Central representa uma **oportunidade estratégica de elevar a maturidade organizacional, reduzir riscos sistêmicos e fortalecer a confiança de clientes, parceiros e stakeholders no negócio**.

O foco agora não é apenas **ter controles**, mas **provar que eles funcionam, são mantidos e fazem parte da operação diária**. As instituições que abraçarem essa transformação não apenas atenderão ao regulador, mas construirão vantagem competitiva sustentável em um mercado cada vez mais digital e exigente.

Próximos Passos Recomendados

1. Realizar assessment completo de gaps técnicos e documentais
2. Estabelecer comitê multidisciplinar de adequação com patrocínio executivo
3. Desenvolver roadmap detalhado alinhado ao prazo de março de 2026
4. Iniciar implementação priorizando ambientes críticos (Pix, STR)
5. Estabelecer processos de monitoramento e evidenciação contínuos