A Nova Era da Fraude de Identidade

Em 2025, a fraude digital passou por uma transformação profunda. Ataques rudimentares cederam espaço para operações sofisticadas que combinam inteligência artificial, engenharia social e identidades artificiais — exigindo das empresas uma postura de defesa igualmente evoluída.

LCSEC

RESUMO EXECUTIVO

O Que Está em Jogo

A fraude de identidade está entrando em uma nova fase. O problema não é apenas a quantidade de ataques, mas a sua qualidade. Deepfakes, identidades sintéticas, phishing avançado, bots e abusos pós-KYC estão tornando a fraude mais difícil de detectar — e mais cara quando passa despercebida.

Na América Latina, esse cenário é amplificado pelo crescimento acelerado de fintechs, pagamentos digitais, e-commerce, apostas online e serviços financeiros. O mercado exige proteção: **95% dos consumidores afirmaram que escolheriam um provedor apenas se ele tivesse medidas antifraude robustas.**

Para empresas, o caminho é claro: criar uma defesa em camadas, integrando verificação de identidade, biometria, MFA, análise comportamental, proteção contra bots, monitoramento contínuo e resposta estruturada. Segurança antifraude não é uma barreira ao crescimento — é um habilitador de confiança.

Impactos Críticos

- **Perdas financeiras diretas**
- **Danos à reputação da marca**
- **Exposição regulatória e de compliance**
- **Erosão da confiança do cliente**

LCSEC

CAPÍTULO 1

A Nova Fraude de Identidade

O que é

Fraude de identidade acontece quando criminosos usam dados reais, falsos ou manipulados para se passar por outra pessoa — abrindo contas, acessando serviços, movimentando dinheiro ou cometendo abusos em plataformas digitais. Em 2025, o nível de sofisticação aumentou radicalmente, com crescimento de **180%** **nas fraudes sofisticadas** em relação a 2024.

Por que é importante

Uma conta criada com identidade falsa pode ser usada para lavagem de dinheiro, golpes financeiros, abuso de promoções, chargebacks, invasão de contas e danos à reputação. O impacto vai muito além da transação individual — compromete a integridade do negócio.

Como Prevenir

Verificação Documental

Validação de documentos com fontes confiáveis

Biometria

Prova de vida e reconhecimento facial

Análise Comportamental

Monitoramento de dispositivo e padrão de uso

Revisão Humana

Casos críticos com análise manual especializada

Frameworks recomendados: NIST Cybersecurity Framework, ISO/IEC 27001:2022, CIS Controls v8 e SOC 2 Type II. Classifique riscos por impacto no negócio e aplique controles proporcionais.

CAPÍTULO 2

Deepfakes e IA Generativa

Deepfakes são imagens, vídeos ou áudios falsos criados com inteligência artificial para imitar pessoas reais. No contexto de fraude, são usados para enganar verificações de selfie, chamadas de vídeo, centrais de atendimento e processos de prova de vida. **O Brasil registrou crescimento de 126%** em deepfakes em relação ao ano anterior, e países como México, Panamá, Guatemala e Suriname também reportaram aumentos expressivos.

🎭 Verificação Visual Não Basta

Um vídeo aparentemente real pode ser manipulado. Uma voz pode ser clonada. Uma selfie pode ser gerada por IA. Controles visuais simples falham diante dessas ameaças.

🔬 Detecção Avançada

Use vivacidade avançada, biometria multimodal e análise comportamental. Avalie contexto, dispositivo, localização, padrão de navegação e histórico de risco — não apenas a aparência da imagem.

🏦 Setores em Risco

Bancos digitais, fintechs, e-commerces, plataformas de apostas, criptoativos e serviços financeiros estão sob maior pressão e precisam de controles específicos contra deepfakes.

CAPÍTULO 3

Identidades Sintéticas

O que é uma identidade sintética?

Uma identidade fabricada que mistura dados reais e falsos: nome, CPF, endereço, data de nascimento, selfie manipulada e informações artificiais criadas para parecerem legítimas. Na América Latina, o uso de dados pessoais falsos quase triplicou, representando **7,3% das fraudes analisadas**.

Por que é perigoso?

Identidades sintéticas podem passar despercebidas por controles simples. Em muitos casos, são usadas por semanas ou meses antes de o fraudador executar o golpe principal — tornando a detecção tardia extremamente custosa.

Estratégia de Prevenção — Princípio de Confiança Zero

01

Cruzamento de dados cadastrais

Valide com fontes externas confiáveis e bureaus de dados

02

Validação documental e prova de vida

Biometria combinada com análise de consistência documental

03

Reputação de dispositivo

Identifique dispositivos suspeitos, emuladores e proxies

04

Monitoramento pós-cadastro

Nunca presuma que uma conta é segura após o primeiro cadastro

Ganhos esperados: redução de contas falsas, melhoria nos processos de KYC e AML, proteção contra abuso de benefícios e fortalecimento da qualidade da base de clientes.

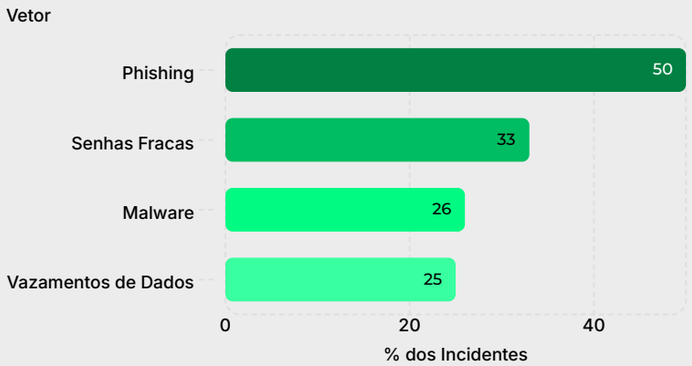
CAPÍTULO 4

Phishing e Engenharia Social

Phishing é o principal vetor de ataque entre consumidores na América Latina. Criminosos usam mensagens falsas para roubar senhas, dados bancários ou códigos de acesso. Engenharia social vai além — é a manipulação psicológica que leva a vítima a agir contra sua própria segurança.

Mesmo com tecnologia avançada, **pessoas continuam sendo alvos centrais**. Uma única credencial roubada pode abrir portas para invasão de contas, fraudes financeiras e acesso indevido a dados sensíveis em toda a organização.

Principais Vetores — América Latina



Conscientização Contínua

Campanhas frequentes para ensinar usuários e colaboradores a reconhecer mensagens suspeitas, links falsos, anexos perigosos e pedidos urgentes.

MFA e Senhas Fortes

Implemente autenticação multifator, gerenciadores de senha, bloqueio por tentativa incorreta e monitoramento de acessos suspeitos em todos os sistemas.

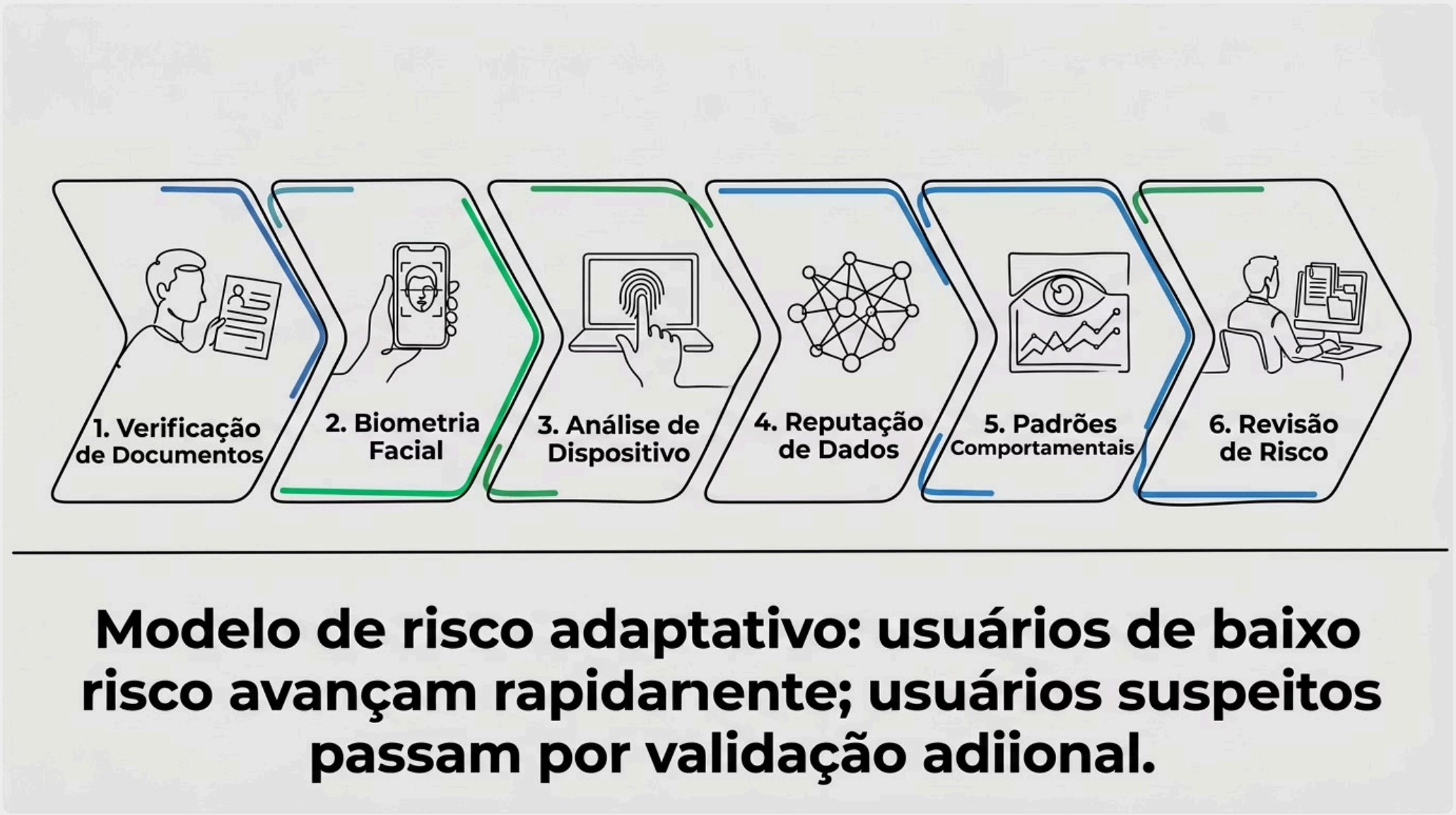
Monitoramento de Acessos

Detecte logins suspeitos em tempo real, identifique padrões anormais e acione fluxos de resposta imediata para eventos de alto risco.

CAPÍTULO 5

Segurança no Onboarding Digital

O onboarding digital é a porta de entrada da empresa. Se ele falha, contas fraudulentas entram no ambiente e geram prejuízos em transações, acessos, promoções, crédito e suporte. O relatório revela que **42% das fraudes na América Latina envolvem inconsistências entre selfie e documento** — a maior categoria identificada.



Ganhos Esperados: Aumento da taxa de aprovação legítima, redução de fraudes no cadastro e melhoria da experiência do cliente confiável sem atrito desnecessário.

Riscos sem Controle: Onboarding fraco permite entrada de fraudadores, contas sintéticas, deepfakes e redes organizadas de fraude que exploram o ambiente meses depois.

CAPÍTULO 6

Monitoramento Pós-KYC

KYC não termina no cadastro. Monitoramento pós-KYC é acompanhar o comportamento da conta após a aprovação — identificando mudanças suspeitas, acessos incomuns, transações fora do padrão e sinais de abuso. O relatório destaca que fraudes pós-KYC e abusos orquestrados estão substituindo golpes simples, exigindo defesas contínuas e não apenas verificações estáticas.

Login e Dispositivo

Monitore padrões de login, dispositivos utilizados, localização geográfica e velocidade de acesso para identificar anomalias.

Transações e Movimentações

Analise volume, frequência e valor de transações. Identifique movimentações fora do padrão histórico do usuário.

Alterações Cadastrais

Monitore trocas de senha, alterações de MFA, mudanças de e-mail ou telefone — sinais frequentes de tomada de conta.

Alertas e Resposta

Crie alertas com níveis de risco e fluxos claros. Casos críticos devem gerar bloqueio preventivo ou revalidação de identidade.

⚠ Sem monitoramento pós-KYC, a empresa só percebe a fraude depois do prejuízo — quando o dinheiro já saiu, a conta foi abusada ou o cliente foi afetado. A detecção tardia multiplica o custo do incidente.

CAPÍTULO 7

Proteção contra Bots e Automação Maliciosa

Entre empresas da América Latina: **87%** relatam phishing e engenharia social, **65%** relatam roubo de identidade, e **33%** enfrentam testes de cartão e ataques automatizados por bots.

O Problema da Escala

Bots são programas automatizados que executam ações em grande escala — testando cartões, tentando senhas, criando contas falsas e simulando comportamentos legítimos. Um ataque que seria lento manualmente pode ser executado milhares de vezes em minutos, gerando custos, indisponibilidade e desgaste operacional.

Camadas de Proteção Recomendadas

- **Análise comportamental e detecção de padrões anormais**
- **Limitação de tentativas e reputação de IP e dispositivo**
- **Autenticação adaptativa baseada em risco**
- **Integração de logs de aplicações, APIs e antifraude**
- **Identificação de ataques distribuídos e coordenados**

LCSEC

CAPÍTULO 8

Governança, Compliance e Resposta a Incidentes

Governança antifraude é o conjunto de processos, responsabilidades, métricas e controles que orientam como a empresa previne, detecta, responde e aprende com incidentes. **71% das empresas** usam modelo híbrido de prevenção, combinando equipes internas e fornecedores externos — porém o mesmo percentual ainda depende de processos manuais, revelando lacunas críticas de automação.

Fraude é um Problema Multidisciplinar

Sem governança, cada time reage de um jeito — e isso atrasa a resposta, amplifica o impacto e dificulta o aprendizado organizacional. Jurídico, compliance, atendimento, financeiro, segurança, produto, risco e liderança executiva precisam estar alinhados em torno de um único programa integrado.

Métricas Essenciais de Governança

Tempo de Detecção

Mean time to detect (MTTD)

Tempo de Resposta

Mean time to respond (MTTR)

Fraudes Bloqueadas

Taxa de prevenção efetiva

Falsos Positivos

Impacto em usuários legítimos

Frameworks de Referência

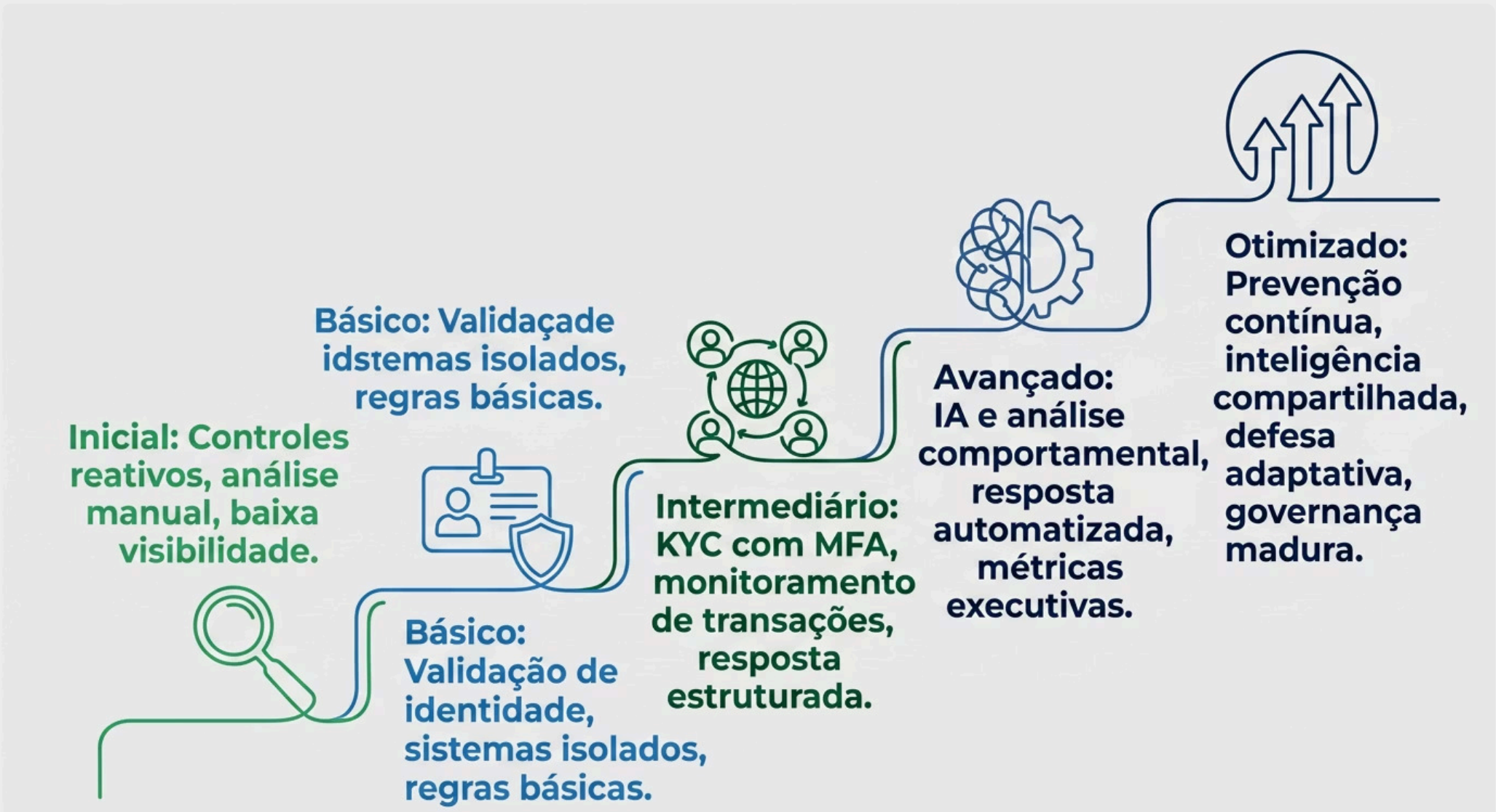
- ISO/IEC 27001:2022
- NIST Cybersecurity Framework
- CIS Controls v8
- SOC 2 Type II
- LGPD / GDPR

Elementos do Playbook

- Papéis e responsabilidades definidos
- Fluxos de escalação claros
- Comunicação regulatória padronizada
- Revisão pós-incidente estruturada

Modelo de Maturidade Antifraude

Avalie em qual nível sua organização se encontra e defina o caminho de evolução prioritário. Cada dimensão recebe uma nota de 1 a 5, ponderada pelo seu peso estratégico no programa de prevenção à fraude.



Cálculo do Índice de Maturidade

Dimensão	Peso	Foco de Evolução
Identidade e Onboarding	25%	Verificação multicamadas
Monitoramento Pós-KYC	20%	Alertas e resposta automatizada
Proteção contra Bots	15%	Detecção comportamental
Governança e Resposta	20%	Playbooks e métricas
Conscientização e Acessos	20%	MFA e cultura de segurança

📊 Abaixo de 3,0

Priorize controles básicos, integração de sistemas e validação de identidade. Foco imediato em eliminar pontos cegos no onboarding.

📈 Entre 3,0 e 4,0

Foque em automação de resposta, análise comportamental e integração entre áreas. Reduza dependência de processos manuais.

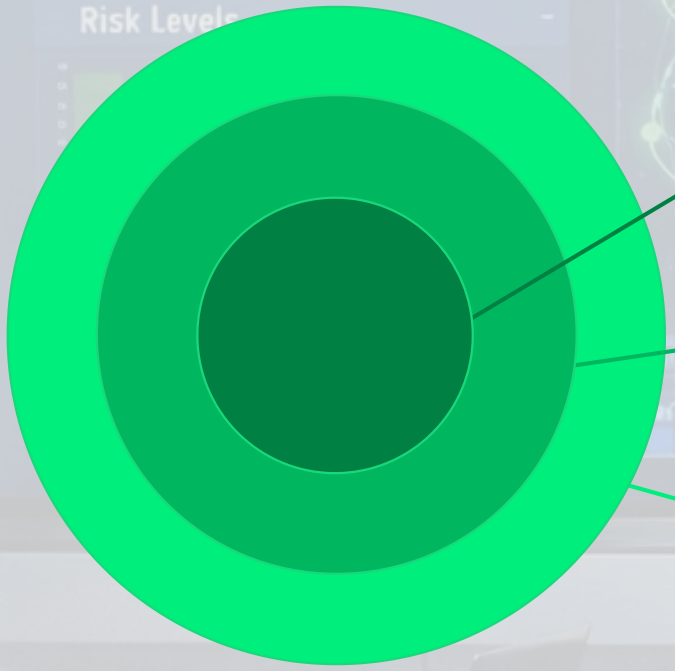
🚀 Acima de 4,0

Evolua para inteligência preditiva, redução de falsos positivos, defesa adaptativa e melhoria contínua baseada em dados.

LCSEC

Próximos Passos Recomendados

A prevenção à fraude precisa evoluir na mesma velocidade dos ataques. Quem combina tecnologia, governança e educação consegue transformar risco em vantagem competitiva — protegendo receita, reduzindo perdas e fortalecendo a confiança do cliente.



Rever
Auditar onboarding e monitoramento.

Implementar
Controlos para contas e transações.

Evoluir
IA, analítica comportamental e governança.

Segurança como Vantagem Competitiva: Quando bem aplicada, a estratégia antifraude protege receita, reduz perdas operacionais, melhora a experiência do cliente e fortalece a posição da empresa perante reguladores e parceiros.

Comece hoje: Revise seus processos de onboarding, autenticação e monitoramento pós-cadastro. Implemente controles por prioridade, focando nos pontos de maior impacto: contas sensíveis, transações financeiras e APIs críticas.

Avaliar Maturidade da Empresa

LCSEC