

Cibersegurança no Sistema Financeiro: Aprimorando a Resiliência para Inovar com Segurança

ARISTIDES ANDRADE CAVALCANTE NETO

Departamento de Gestão Estratégica e
Supervisão Especializada – DEGEF
Banco Central do Brasil



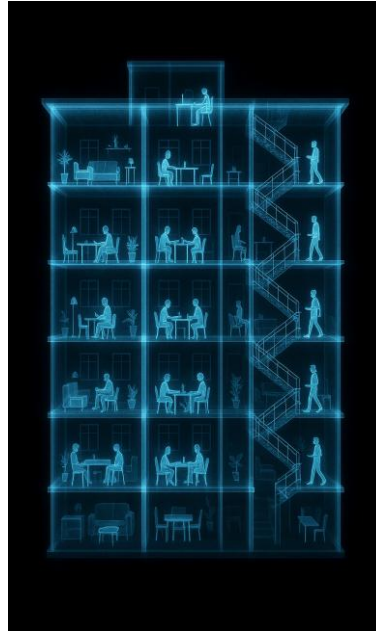
**Seminário BC/OCB
SNCC em transformação**

Supervisão auxiliar, modernização prudencial,
autorregulação e proteção

A Revolução Digital do Sistema Financeiro



Inovações tecnológicas



Foco do crime organizado
mudou para o SFN Digital



Novos padrões de consumo



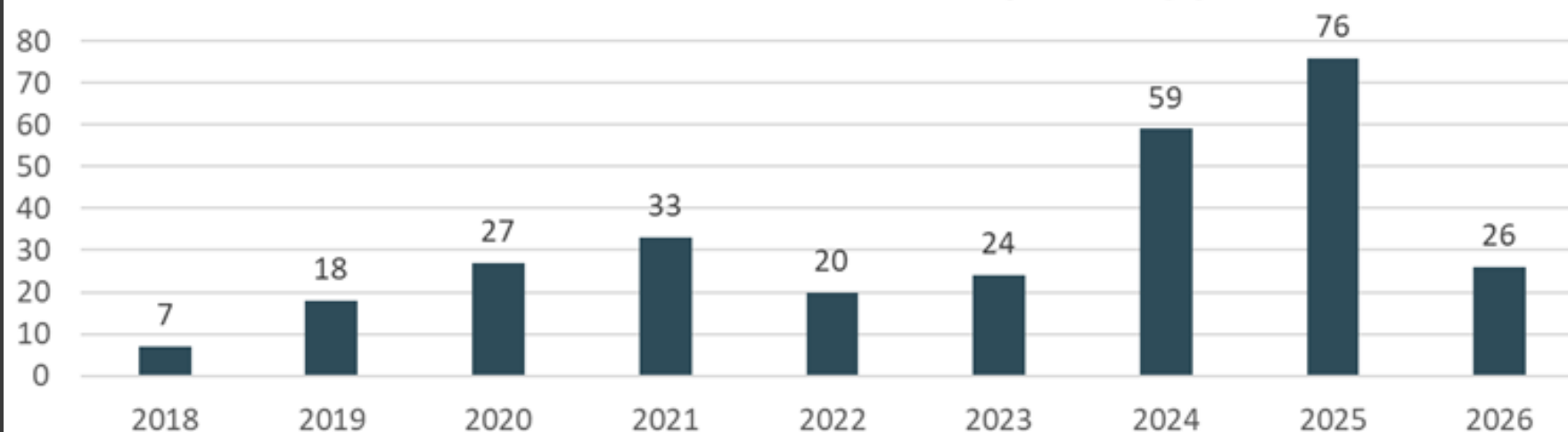
Novos ecossistemas



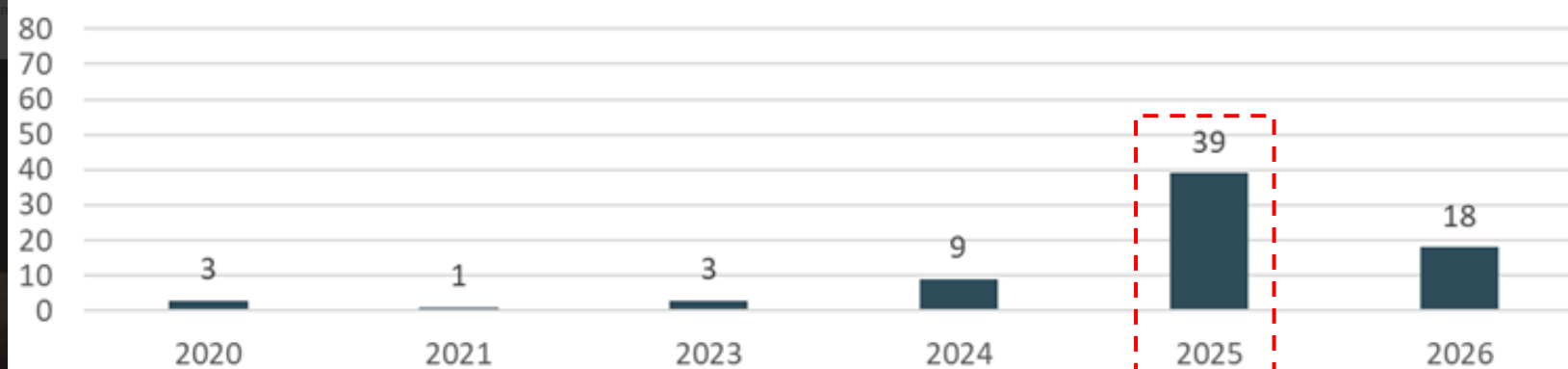
Maior interconectividade
Maior complexidade

Cibersegurança no Sistema Financeiro

Incidentes críticos comunicados por ano (*)



Incidentes críticos comunicados por ano que incluem a realização de transações fraudulentas



<https://cbn.globo.com/economia/noticia/2025/valor.gh.html>

<https://www.infomoney.com.br/brasil/ataque-hacker-afeta-infraestrutura-de-empresa-ligada-ao-pix-prejuizo-supera-r800-mil/>

Incidentes recentes – Táticas, Técnicas e Procedimentos (TTPs) Verificados

Conhecimento
avançado
sobre a
operação do
sistema
financeiro

- Estrutura da mensageria SPB
- Operação do piloto de reservas

Comprometi-
mento de
ambiente
computacional

- Acesso não autorizado
- Domínio da arquitetura da solução

Complexidade
das ações
desenvolvidas

- Desenvolvimento de agentes para injeção de mensagens
- Automação via APIs (pulverização de recursos)

Fatores que impactaram a resposta aos incidentes

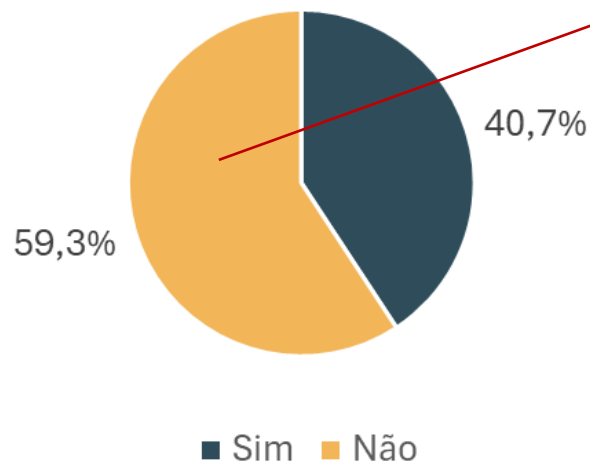
Ausência de logs
adequados

Falha no monitoramento

Ausência de conciliação de
operações

O fator humano: a importância de estabelecer controle de acesso

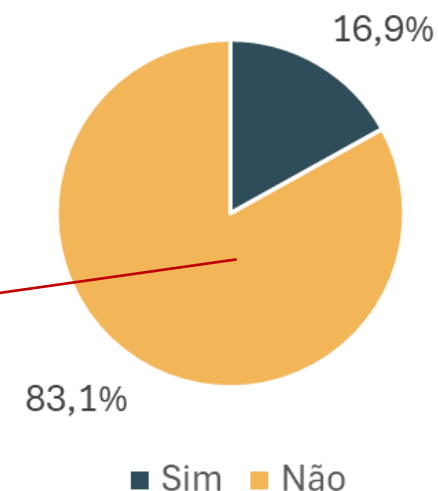
A instituição revisa periodicamente os acessos configurados?



Cenários de risco: acúmulo de permissões incompatíveis com as funções desempenhadas pelo funcionário / acesso indevido a sistemas e serviços de TI a partir de credenciais não revogadas.



Controle de acesso à rede para dispositivos (por ex., protocolo 802.1x)



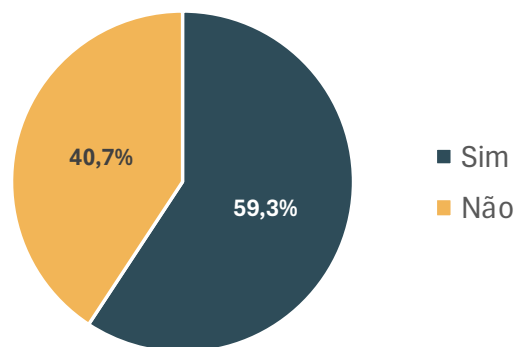
Cenário de risco: funcionários ou colaboradores terceirizados cooptados pelo crime podem instalar dispositivos conectados à rede corporativa para roubar informações

Dispositivos não autorizados podem ser conectados à rede corporativa.

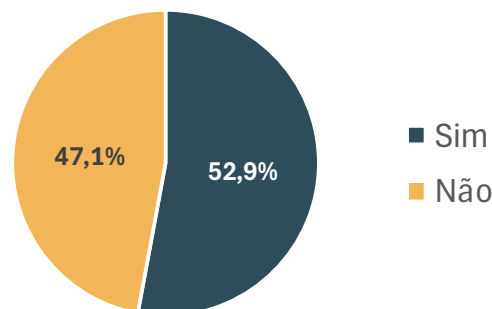
Ref.: 189 instituições (3 confederações, 4 centrais, 182 singulares)

Gestão do relacionamento com terceiros

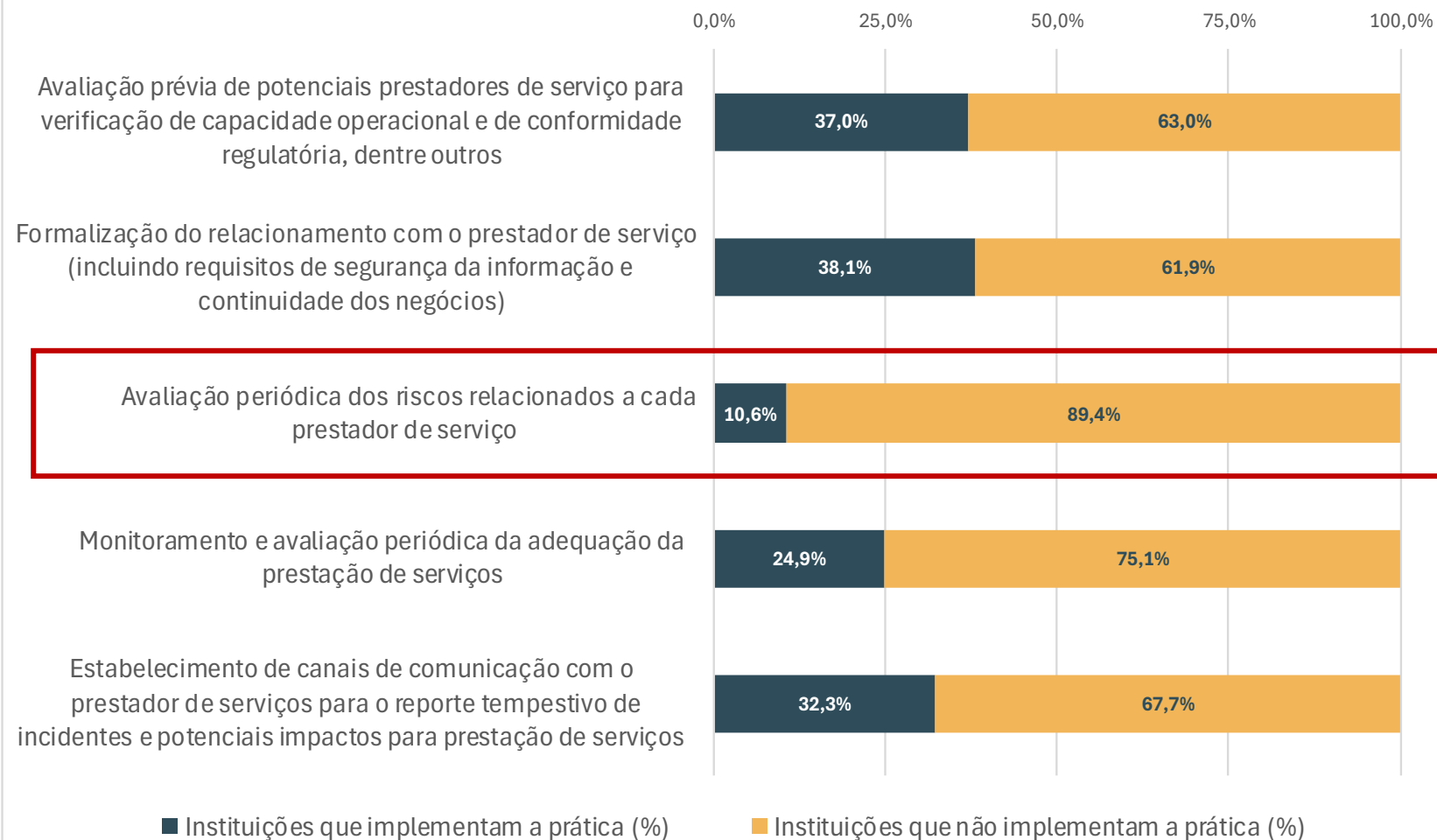
A instituição possui política(s) que trata(m) da gestão do relacionamento com terceiros?



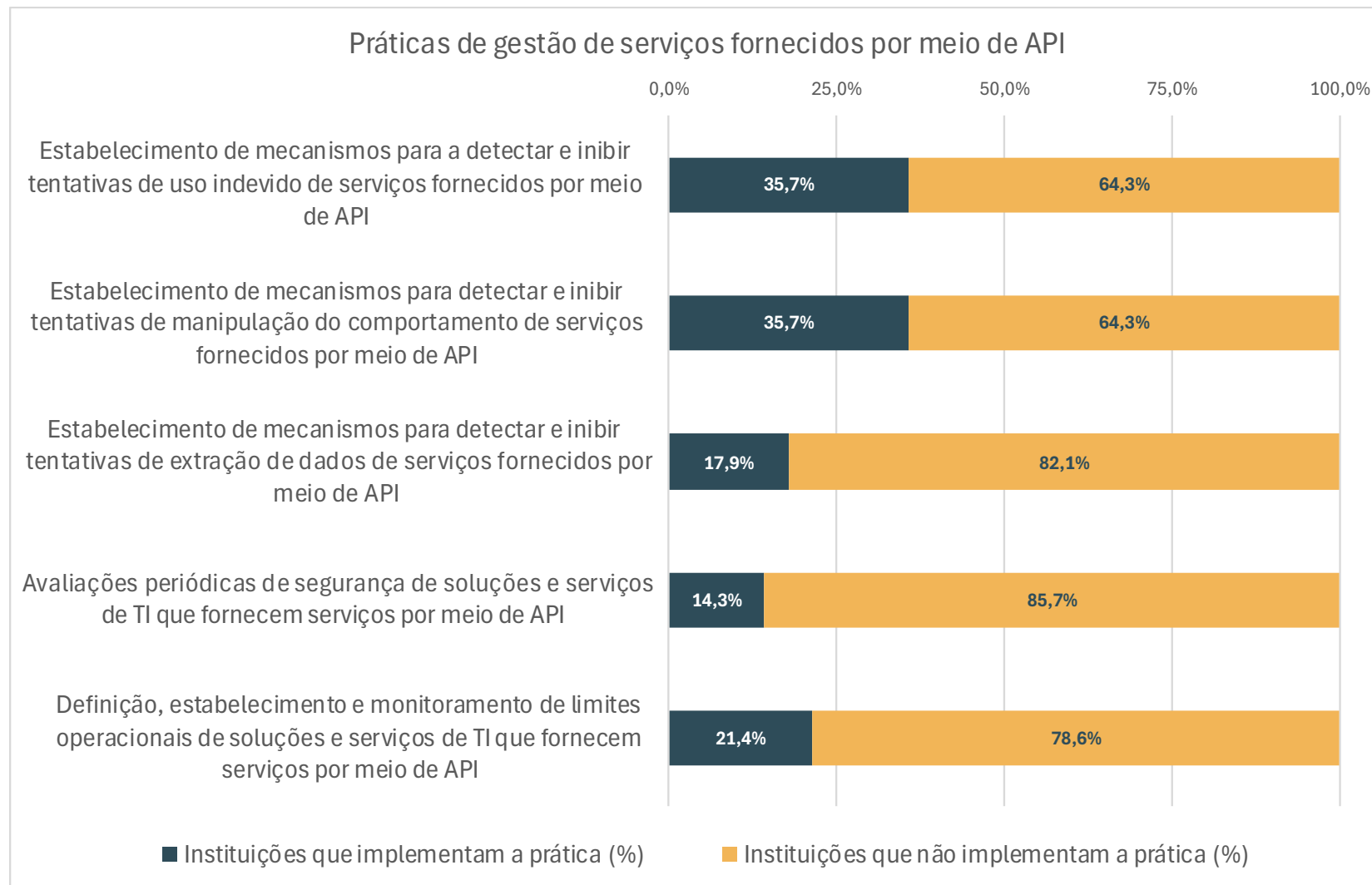
A instituição estabeleceu processo ou procedimentos para gerenciar o relacionamento com terceiros?



Práticas de gestão do relacionamento com terceiros



- 28 instituições informaram que fornecem serviços por meio de APIs

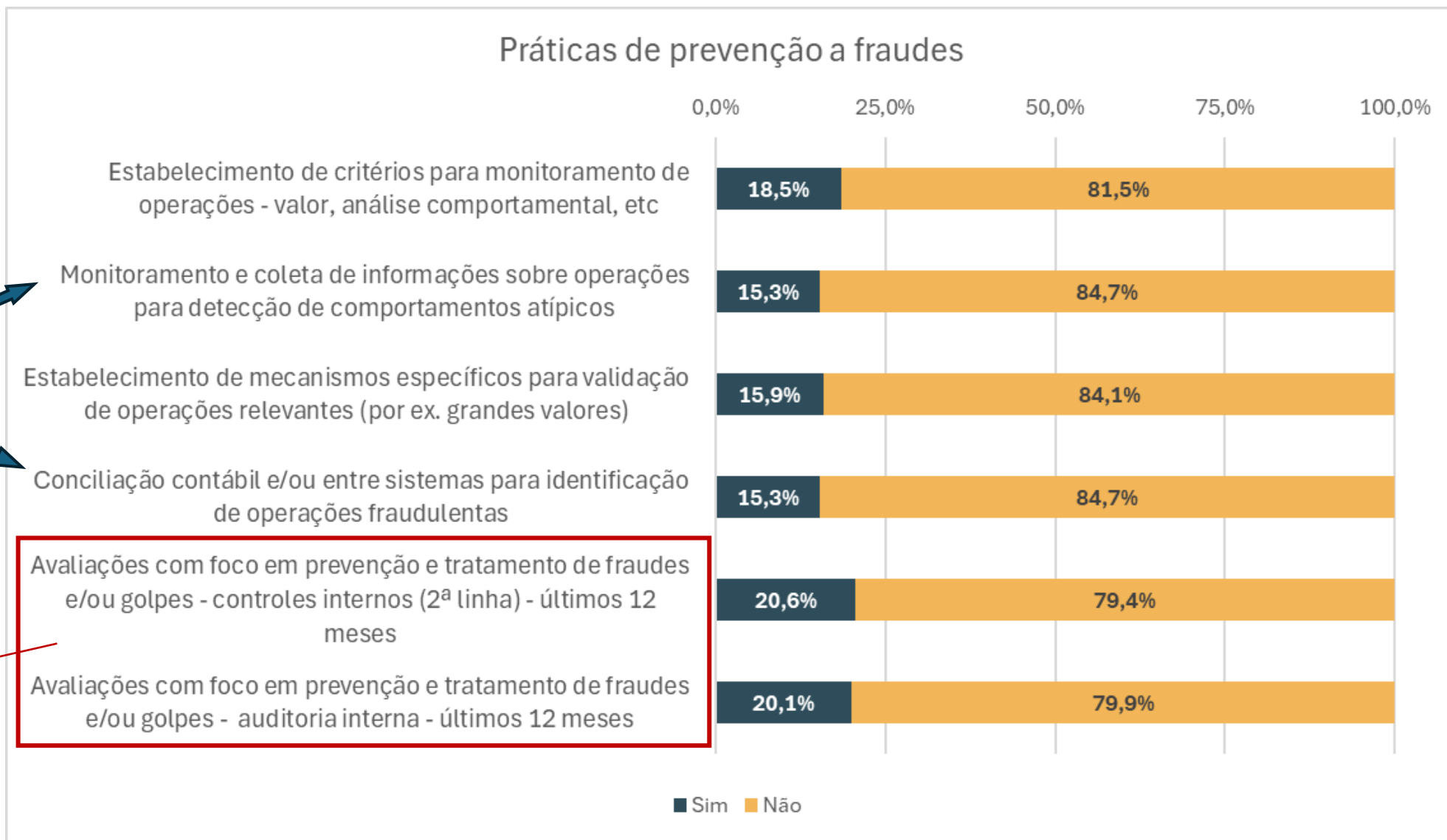


Monitoramento de operações

Práticas de prevenção a fraudes

Cenário de risco:
injeção de transações
fraudulentas.

É preciso aumentar
a atuação das linhas
de defesa



Ref.: 189 instituições (3 confederações, 4 centrais, 182 singulares)

➤ Publicação de novas regulamentações

- ✓ Credenciamento PSTIs
- ✓ Antecipação do prazo para autorização de IPs não autorizadas
- ✓ Estabelecimento de limites TED e PIX em instituições que se conectam por um terceiro
- ✓ Rejeitar transações de contas com fundada suspeita de fraude
- ✓ Obrigatoriedade de encerramento das “contas-bolsão”
- ✓ Nova regulamentação de capital mínimo
- ✓ Regulação de Banking-as-a-Service
- ✓ Regulação de Prestação de Ativos Virtuais

➤ Lançamento do “BC Protege+”

➤ Implementação de monitoramento de fluxos atípicos (PIX)

➤ Disponibilização do SPB-Web 2.0

➤ 5 Workshops de conscientização por segmento: +3500 profissionais participantes



Acessos não-autorizados

- Autenticação e Controle de Acesso (art. 3º, §9º)
- Mecanismos de rastreabilidade (art. 3º, §7º)
- Perfis de configuração segura de ativos de TI (art. 3º, §10º)
- Mecanismos de proteção da rede (art. 3º, §11º)

Prestadores de Serviço

- Adoção de controles para prevenção e tratamento de incidentes (art. 3º, incisos V-a)
- Vedação de acesso às chaves privadas (art. 3º-A, incisos I-f)
- Verificação da capacidade do prestador de serviço (art. 12º, incisos II)

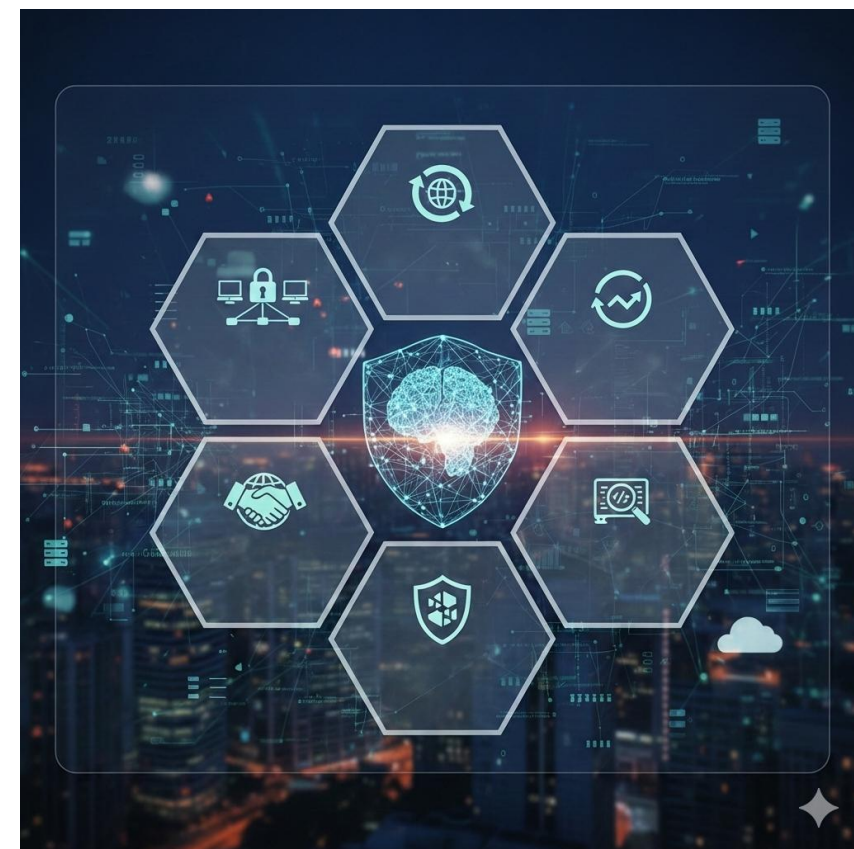
Integração de Serviços por meio de APIs

- Requisitos de segurança para integração de serviços (art. 3º, §2º, incisos XIII e art. 24º, inciso IV)

Monitoramento de Operações e Informações

- Ações de inteligência cibernética na Deep Web e na Dark Web (art. 3º, §2º, incisos XIV)
- Monitoramento de conexões (art. 3º, §11º, incisos II e III)
- Monitoramento e gestão dos certificados e assinaturas digitais (art. 3º, §12º)

- ✓ Avaliação de 100% das entidades supervisionadas sobre a implementação dos novos requisitos definidos nas Res. CMN 4893/21 e Res. BCB 85/21
- ✓ Aprimoramentos regulatórios orientados a temas específicos como, por exemplo, provedores de serviço e integração de serviços (APIs)



OBRIGADO!



Um cooperado nunca está só.

Fique por dentro das mudanças no cooperativismo e aprenda com quem faz acontecer no segmento de crédito.