TLP:CLEAR

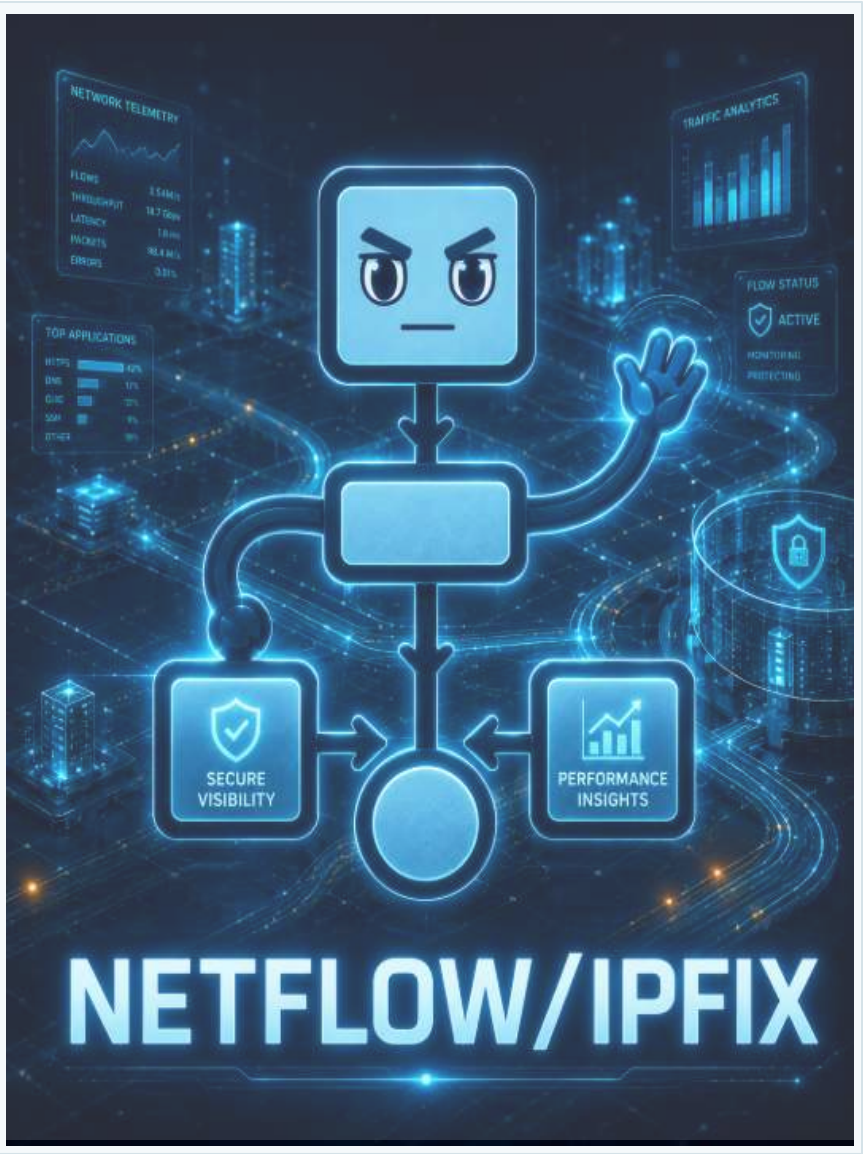
cert.br
Fórum de CSIRTs

RESOLUÇÕES

# CMN nº 5.274/2025 e BCB nº 538/2025

## e NetFlow no setor financeiro: visibilidade de rede, rastreabilidade e resposta a incidentes

Da exigência regulatória à detecção, investigação e evidência




**Edney Fernandes**
Administrador de Redes, Gerente Executivo de Produção e Infraestrutura
Membro do CSIRT, Evangelizador IPv6,
www.linkedin.com/in/edneyfer

TLP:CLEAR

# O prazo passou. A exigência agora é operacional.

**18 DEZ 2025**

## Normas editadas

Controles e procedimentos reforçados

**1º MAR 2026**

## Adequação prevista

Prazo definido nas duas resoluções

**OPERAÇÃO CONTÍNUA**

## Capacidade demonstrável

Detectar · investigar
responder · evidenciar

## A regulação desloca o foco de possuir controles para provar que eles funcionam.

Fonte: Res. CMN nº 5.274/2025 e Res. BCB nº 538/2025, arts. 2º e 3º.

TLP:CLEAR

# Duas normas convergem nas mesmas capacidades técnicas.

## CMN 5.274/25

Altera a CMN 4.893/2021

**Instituições financeiras** e demais instituições autorizadas a funcionar pelo Banco Central.

### NÚCLEO COMUM

**Rastreabilidade**
**Proteção da rede**
**Eventos atípicos**
**Vulnerabilidades**
**Ambientes críticos**

## BCB 538/25

Altera a BCB 85/2021

Instituições de **pagamento**, **corretoras** e distribuidoras de **títulos e valores mobiliários** e **corretoras de câmbio** autorizadas pelo BCB.

**Não presumir aplicação cumulativa**

Fonte: ementas e art. 1º das Res. CMN nº 5.274/2025 e BCB nº 538/2025.

TLP:CLEAR

# Os 14 controles formam um sistema integrado.

**IDENTIDADE E CONFIANÇA**

Autenticação · Criptografia
Controles de acesso · Certificados digitais

**PROTEÇÃO CONTRA AMEAÇAS**

Intrusão · Vazamento
Software malicioso · **Proteção da rede**

**POLÍTICA DE SEGURANÇA CIBERNÉTICA**

**RESILIÊNCIA E CONFIGURAÇÃO**

Cópias de segurança · Vulnerabilidades
Configuração segura de ativos

**RASTREABILIDADE E INTELIGÊNCIA**

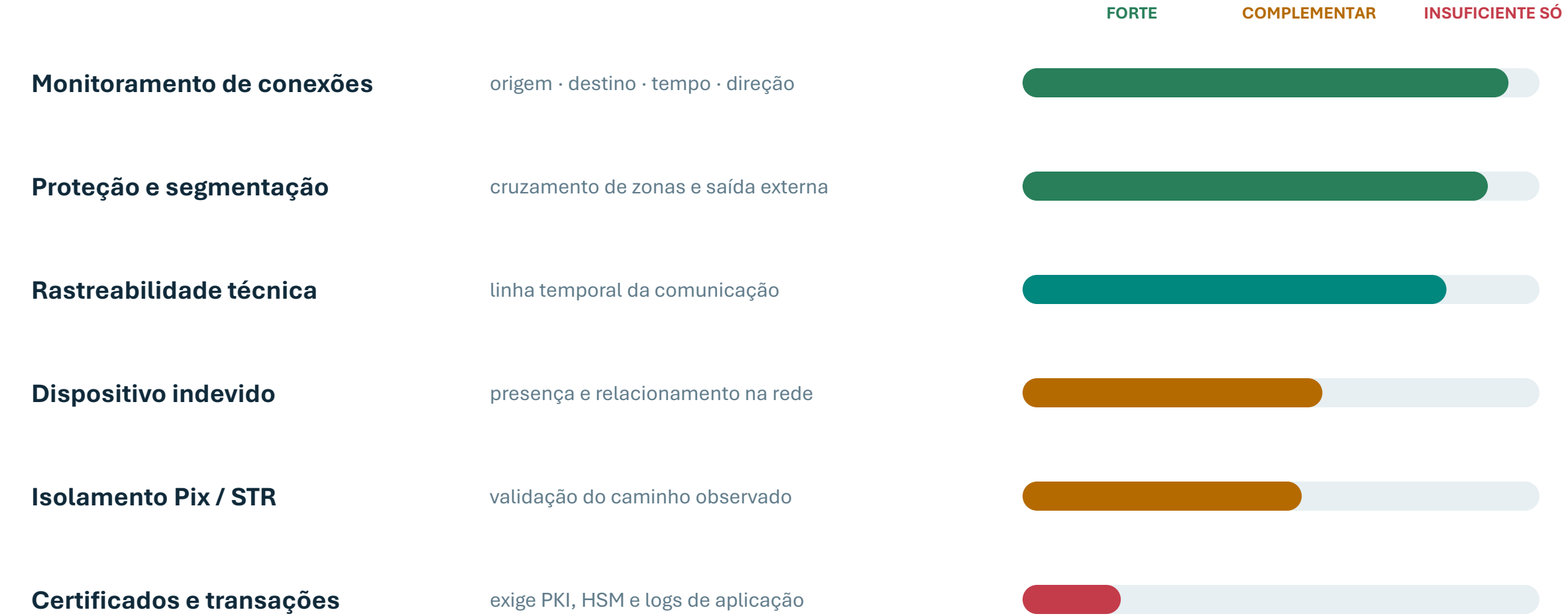
**Rastreabilidade** · Integrações eletrônicas
Inteligência cibernética

**Estabelecer princípios, responsabilidades, procedimentos e controles de forma coordenada.**

Fonte: art. 3º, §2º, incisos I a XIV, das Resoluções alteradas.

TLP:CLEAR

# NetFlow é mais forte quando a pergunta está na rede.




Fonte: art. 3º, §§7º, 8º, 11 e 12, e art. 3º-A.

TLP:CLEAR

# Um fluxo é o passaporte da comunicação - não a conversa.


Base técnica: IPFIX - RFC 7011 e RFC 7012. Campos variam conforme versão, template e exportador.

TLP:CLEAR

# O fluxo mostra a comunicação; o contexto explica.

## VISÍVEL NO FLUXO

- ✓ Endpoints e portas
- ✓ Início, fim e duração
- ✓ Bytes e pacotes
- ✓ Direção e interfaces
- ✓ Frequência e relacionamento

## PERMANECE OCULTO

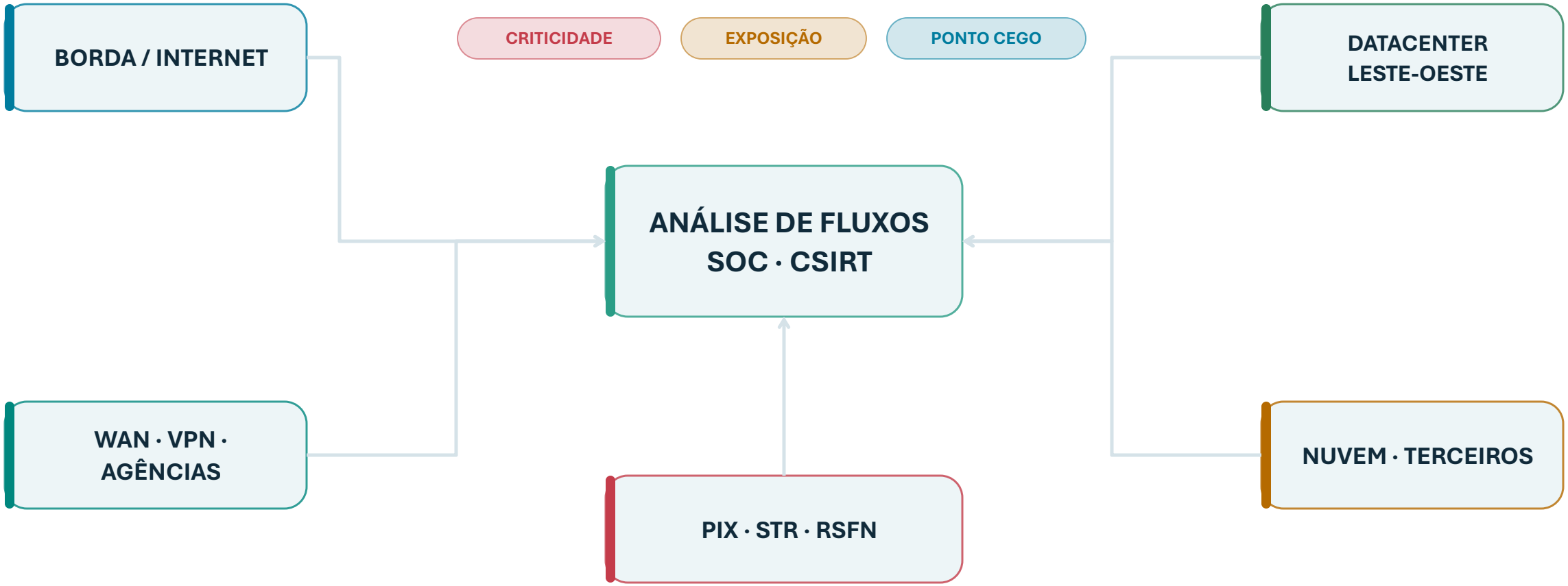
- × Conteúdo ou payload
- × Usuário autenticado
- × Sucesso da autenticação
- × Operação executada
- × Uso do certificado
- × Contexto de negócio

**FLUXO + DNS + CMDB + IAM/PAM + EDR + FIREWALL = CONTEXTO**

Base técnica: IPFIX - RFC 7011/7012. Fontes complementares conforme arquitetura da instituição.

TLP:CLEAR

# Colete onde uma comunicação indevida teria maior impacto.

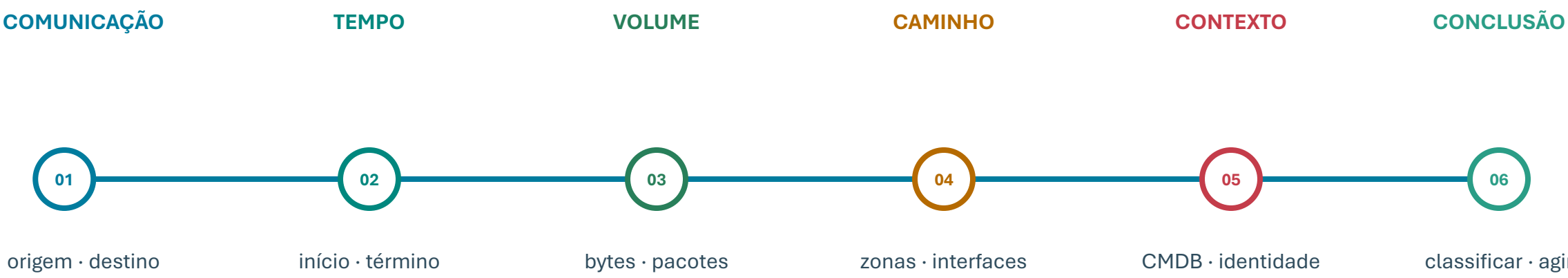



**Prioridade** = criticidade + cruzamento de zonas + valor investigativo

Fonte: art. 3º, §11, e art. 3º-A. Nos ambientes RSFN, observar os requisitos técnicos próprios do SFN.

TLP:CLEAR

# O fluxo organiza a investigação em uma linha temporal.




**Pergunta investigativa: o comportamento era esperado para aquele ativo, naquele horário, naquele segmento e com aquele volume?**

Fonte: art. 3º, §7º. NetFlow apoia a trilha técnica da comunicação, não substitui logs transacionais.

TLP:CLEAR

# A telemetria revela o caminho realmente utilizado.

## ARQUITETURA ESPERADA


caminho autorizado

FLUXOS MOSTRAM CAMINHOS PERMITIDOS

## COMPORTAMENTO OBSERVADO


atalho indevido observado

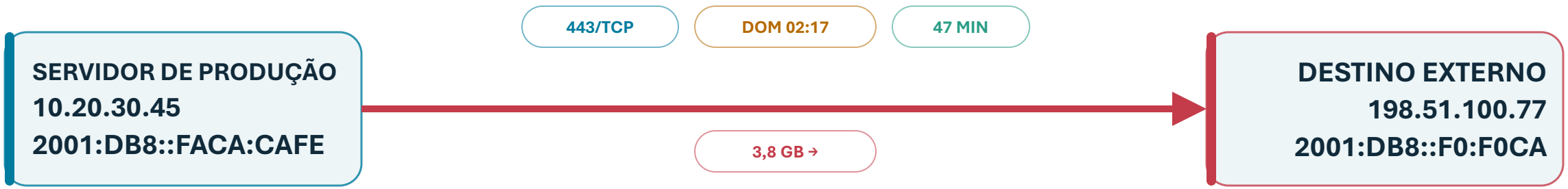
BLOQUEIOS EXIGEM LOGS DE FIREWALL/IPS

Fonte: art. 3º, §11, incisos I a VI.

TLP:CLEAR

# Caso 1: HTTPS não torna a comunicação legítima.

CENÁRIO FICTÍCIO




**SINAIS QUE ELEVAM A PRIORIDADE**

**Ativo crítico + destino sem histórico + dia não útil + alto volume de saída**

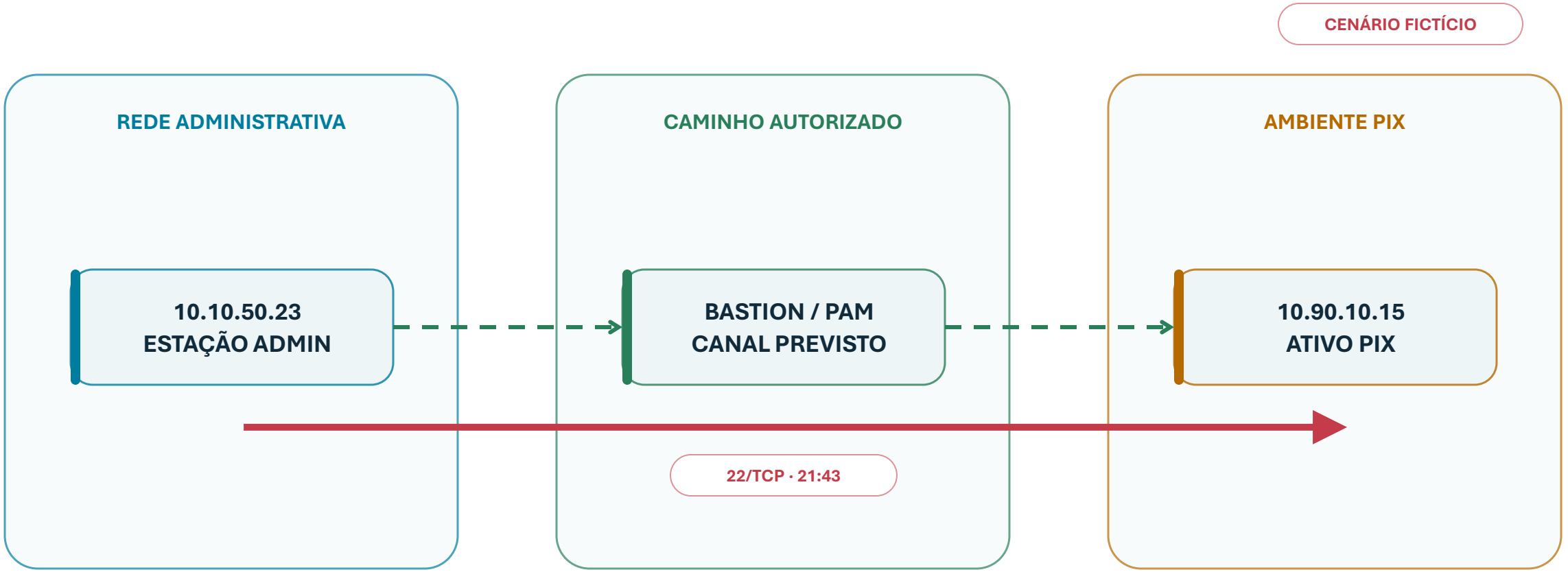
**HIPÓTESES A VALIDAR**

Backup ou integração autorizada · túnel HTTPS exfiltração · serviço comprometido

Endereços e valores fictícios. 198.51.100.0/24 e 2001:DB8::/32 são reservados para documentação.

TLP:CLEAR

# Caso 2: o fluxo mostra o desvio; os registros provam o acesso.




**Correlacionar: firewall · VPN · IAM · PAM · EDR · mudança · autenticação no destino**

Fonte regulatória: art. 3º, §11, e art. 3º-A, inciso I. Endereços fictícios.

TLP:CLEAR

# Caso de uso e playbook transformam dados em resposta.

**01 PERGUNTA DE RISCO**

O que precisa ser detectado?

**02 DADOS + CONTEXTO**

Fluxo · CMDB · DNS · IAM

**COMUNICAÇÃO EXTERNA DE ATIVO CRÍTICO FORA DA JANELA**

**03 SEVERIDADE**

Criticidade · novidade · volume

**04 PLAYBOOK + EVIDÊNCIA**

Validar · conter · preservar

**Sem caso de uso, NetFlow vira armazenamento.**

**Com regra e playbook, vira capacidade operacional.**

Fonte: art. 3º, §11, inciso V. Lógica ilustrativa; limiares devem ser definidos pela instituição.

TLP:CLEAR

# A arquitetura deve preservar contexto, qualidade e evidência.

## 1 · COLETA

- Exportadores
- Flow logs
- Coletores redundantes
- Saúde da coleta

## 2 · DADOS E CONTEXTO

- Normalização
- CMDB + DNS
- IAM/PAM + EDR
- Retenção

## 3 · OPERAÇÃO

- Analytics / SIEM
- SOAR
- Dashboards
- SOC + CSIRT

**CONTROLES TRANSVERSAIS**

NTP | RBAC | INTEGRIDADE | CAPACIDADE | PERDAS

Arquitetura técnica recomendada; os componentes devem ser ajustados ao ambiente e ao risco institucional.

TLP:CLEAR

# A confiabilidade da telemetria está abaixo do dashboard.

VISÍVEL

**DASHBOARDS · ALERTAS · CONSULTAS**

ABAIXO DA LINHA D'ÁGUA

### COBERTURA

Só na borda

Sem leste-oeste

Ambientes críticos cegos

### QUALIDADE

Amostragem inadequada

NAT e assimetria

Perdas e relógios divergentes

### CONTEXTO E PROCESSO

CMDB desatualizada

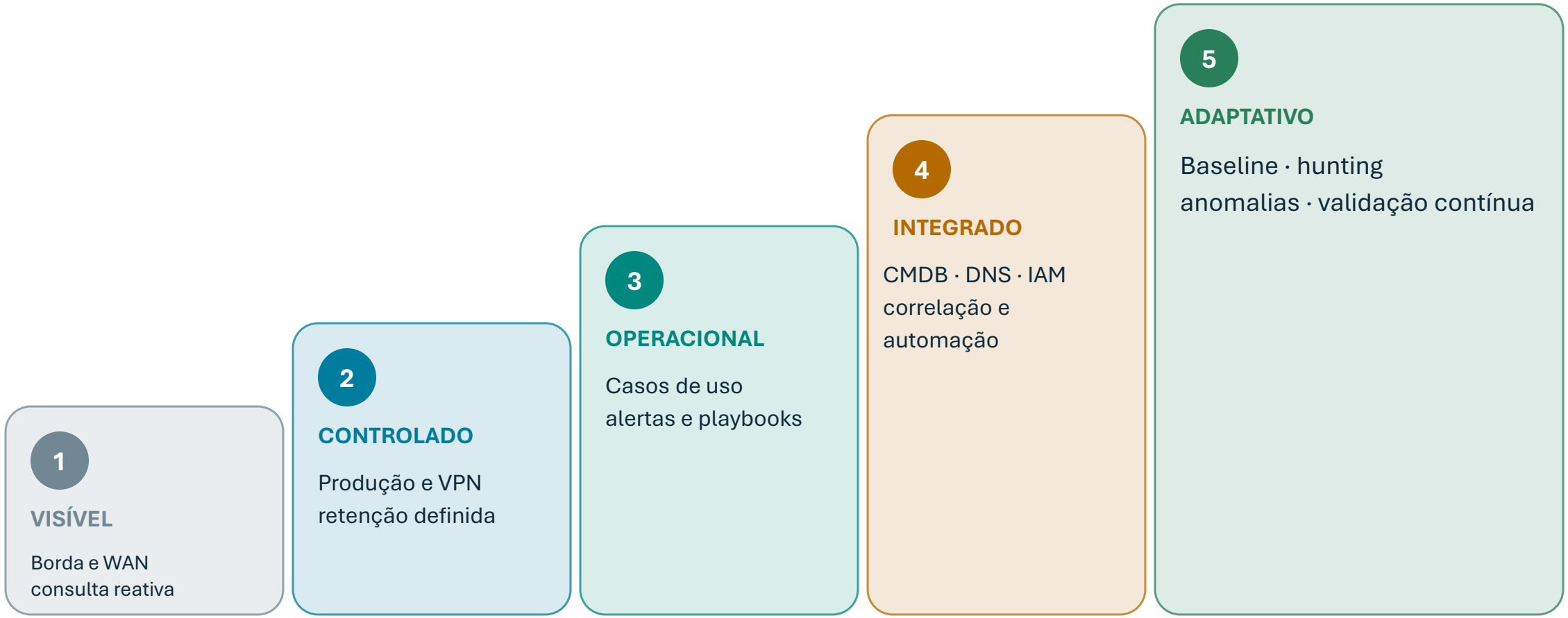
Retenção indefinida

Sem casos de uso ou testes

**O maior risco é confiar em uma telemetria incompleta sem perceber a lacuna.**

TLP:CLEAR

# A maturidade evolui da coleta para a decisão.




**Maturidade = capacidade de converter telemetria em decisão consistente**

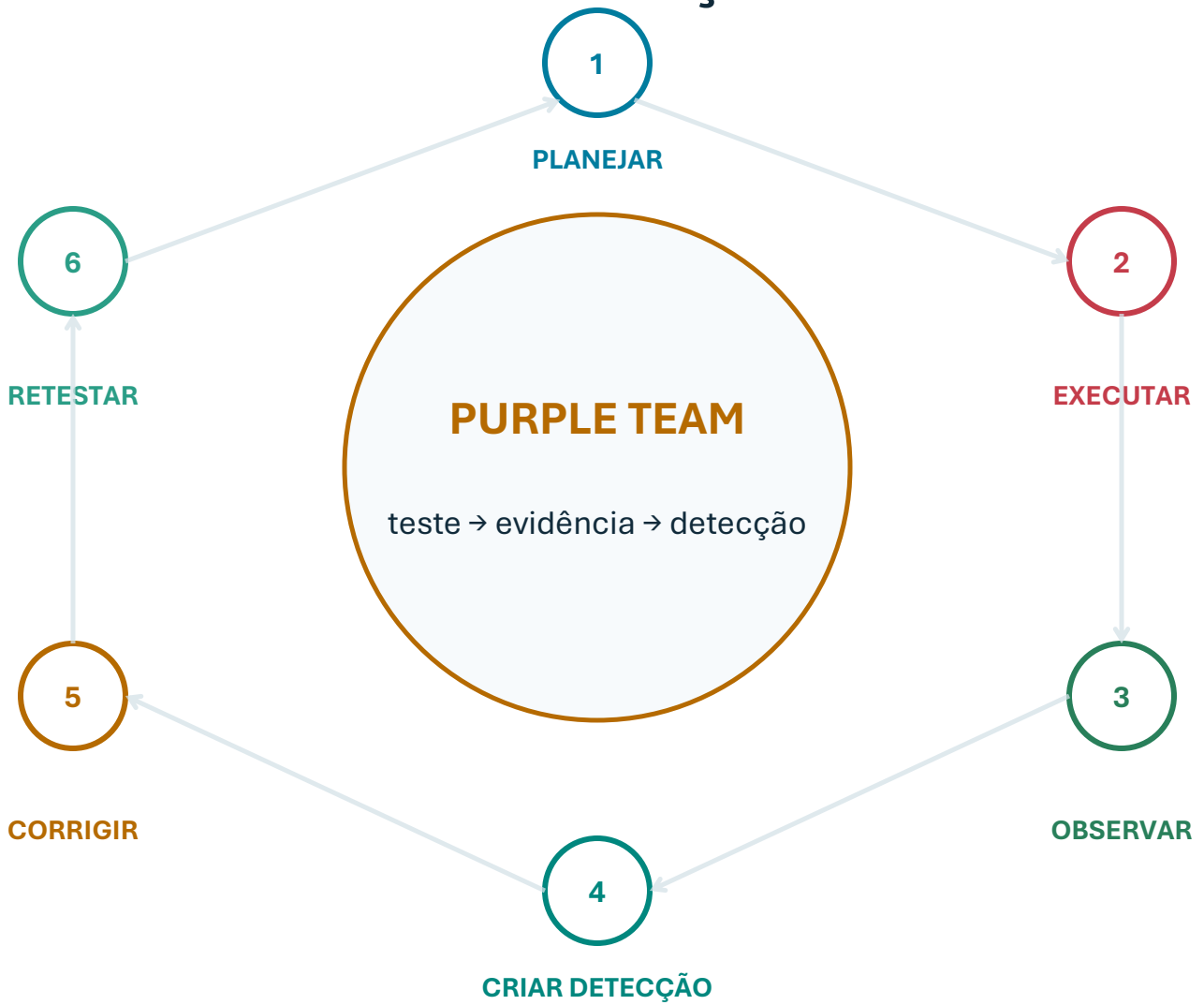
Modelo proposto para discussão; não representa classificação normativa.

TLP:CLEAR

# O pentest deve testar resistência e detecção.

## Requisitos normativos

- MÍNIMO ANUAL
- INDEPENDÊNCIA
- RESULTADO DOCUMENTADO




## Resultados Esperados

- PLANO DE AÇÃO
- NOVAS DETECÇÕES
- RETESTE

**A telemetria permite observar caminhos explorados e transformar técnicas do teste em casos de detecção.**

Fonte: art. 3º, §8º; art. 8º, §1º, V; art. 22-A e art. 23, X.

TLP:CLEAR

# Comece pelas perguntas de maior risco.

## 01 MAPEAR

Ativos e processos críticos

Fluxos autorizados

Pontos cegos

Responsáveis

## 02 IMPLEMENTAR

Normalização e contexto

Retenção

Casos de uso

Playbooks

## 03 VALIDAR

Simulações e testes

Qualidade dos dados

Ajuste de regras

Reporte

MÉTRICAS

COBERTURA CRÍTICA | PERDAS | TEMPO DE DETECÇÃO | TEMPO DE INVESTIGAÇÃO | FALSOS POSITIVOS | CASOS TESTADOS

Prática recomendada. As três etapas não representam prazo ou obrigação normativa.

TLP:CLEAR

CONCLUSÃO

# A pergunta não é “temos NetFlow?”

## É: conseguimos detectar, investigar e evidenciar?

### VER

Cobertura e qualidade

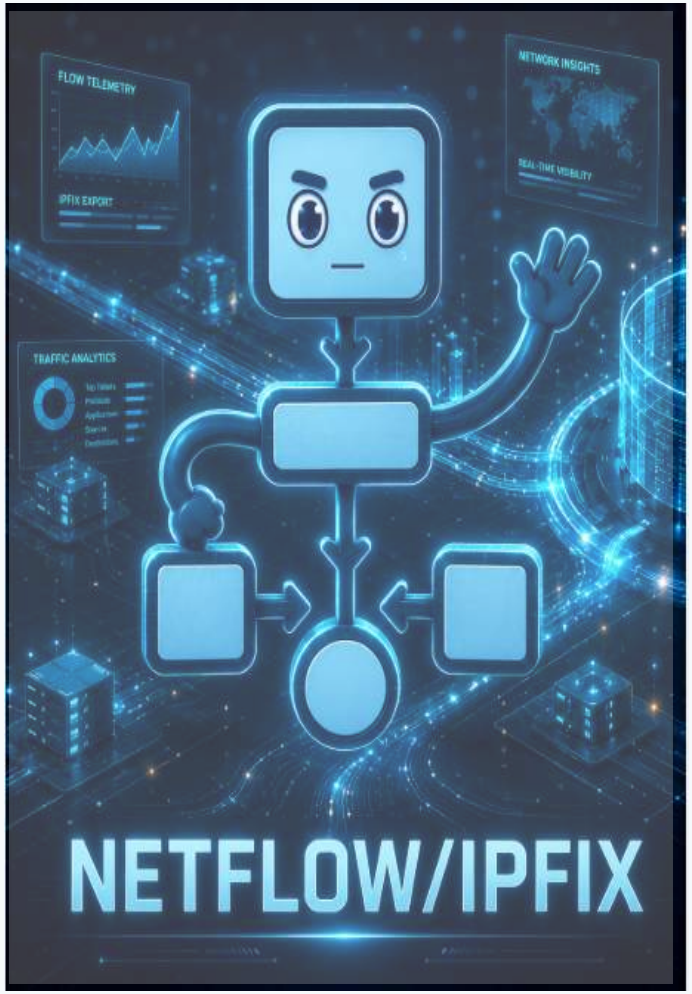
### COMPREENDER

Contexto e correlação

### RESPONDER

Playbook e evidência

**Sem telemetria adequada do fluxo, perde-se velocidade para detectar, contexto para investigar e consistência para evidenciar.**



cert.br
Fórum de CSIRTs

TLP:CLEAR

# Obrigado!

**Edney Fernandes**
www.linkedin.com/in/edneyfer

TLP:CLEAR

# Matriz de correlação entre norma e telemetria.

| DISPOSITIVO | PERGUNTA OPERACIONAL | CONTRIBUIÇÃO DO FLUXO | COMPLEMENTOS | CONTRIBUIÇÃO TÉCNICA |
|---|---|---|---|---|
| **§7º · Rastreabilidade** | Quem comunicou, quando e em qual direção? | Linha temporal e relacionamento entre endpoints | Aplicação · transação | ALTA |
| **§8º · Vulnerabilidades** | Há dispositivo ou conexão não inventariada? | Presença, primeira observação e destinos | NAC · CMDB · scanner | MÉDIA |
| **§11 · Proteção da rede** | Houve cruzamento de zona ou saída indevida? | Segmentos, interfaces, volume e horário | Firewall · IPS | ALTA |
| **§12 · Certificados** | Quem usou qual certificado e com que resultado? | Apenas endpoints e contexto temporal | PKI · HSM · TLS | BAIXA |
| **3º-A · Pix/STR/RSFN** | O caminho administrativo respeitou o isolamento? | Validação do trajeto observado | PAM · MFA · logs RSFN | MÉDIA |

Fontes: Res. CMN nº 5.274/2025 e Res. BCB nº 538/2025.

TLP:CLEAR

# Antes de confiar no alerta, valide a telemetria.

**01 COBERTURA**
Borda, leste-oeste e ambientes críticos

**02 AMOSTRAGEM**
Taxa compatível com o caso de uso

**03 TEMPLATES**
Versões, campos e expiração controlados

**04 NAT / ASSIMETRIA**
Ponto de observação documentado

**05 SINCRONIZAÇÃO**
Relógios e fuso coerentes

**06 PERDAS**
Exportador, transporte e coletor monitorados

**07 CAPACIDADE**
Picos, filas e armazenamento dimensionados

**08 RETENÇÃO**
Matriz formal e recuperação testada

**09 ACESSO**
RBAC e trilha das consultas

**10 CASOS TESTADOS**
Alertas e playbooks exercitados