Táticas de Busca e Apreensão Digital

O guia definitivo sobre métodos, logística e preservação forense de dados corporativos.

Baseado na metodologia de
Agenor Zaparoli | Perito Judicial

O Cenário Operacional

Caso Real: Alegação de dupla clonagem de software corporativo.

Alvos Físicos: Duas filiais de uma mesma empresa (mesmo CNPJ).

Escopo de Apreensão: Equipamentos informáticos, telemáticos, mídias digitais e arquivos físicos.

O Objetivo da Missão

- ☑ Coletar evidências inquestionáveis sem margem para impugnação.
- ☑ Definição técnica e tática delegada ao perito para execução do mandado.
- ☑ Equilibrar a coleta de provas com a preservação legal via rígida **Cadeia de Custódia**.

Paradigmas de Atuação: Força Bruta vs. Inteligência Forense

A Força Policial (Ação Ostensiva)

Tática: Abordagem pé na porta. Arrombamento e força física.

Coleta: Confisco imediato, desordenado.

Retorno: Sem prazo para devolução. Paralisação total do alvo.

A Perícia Judicial (Ação Humanizada)

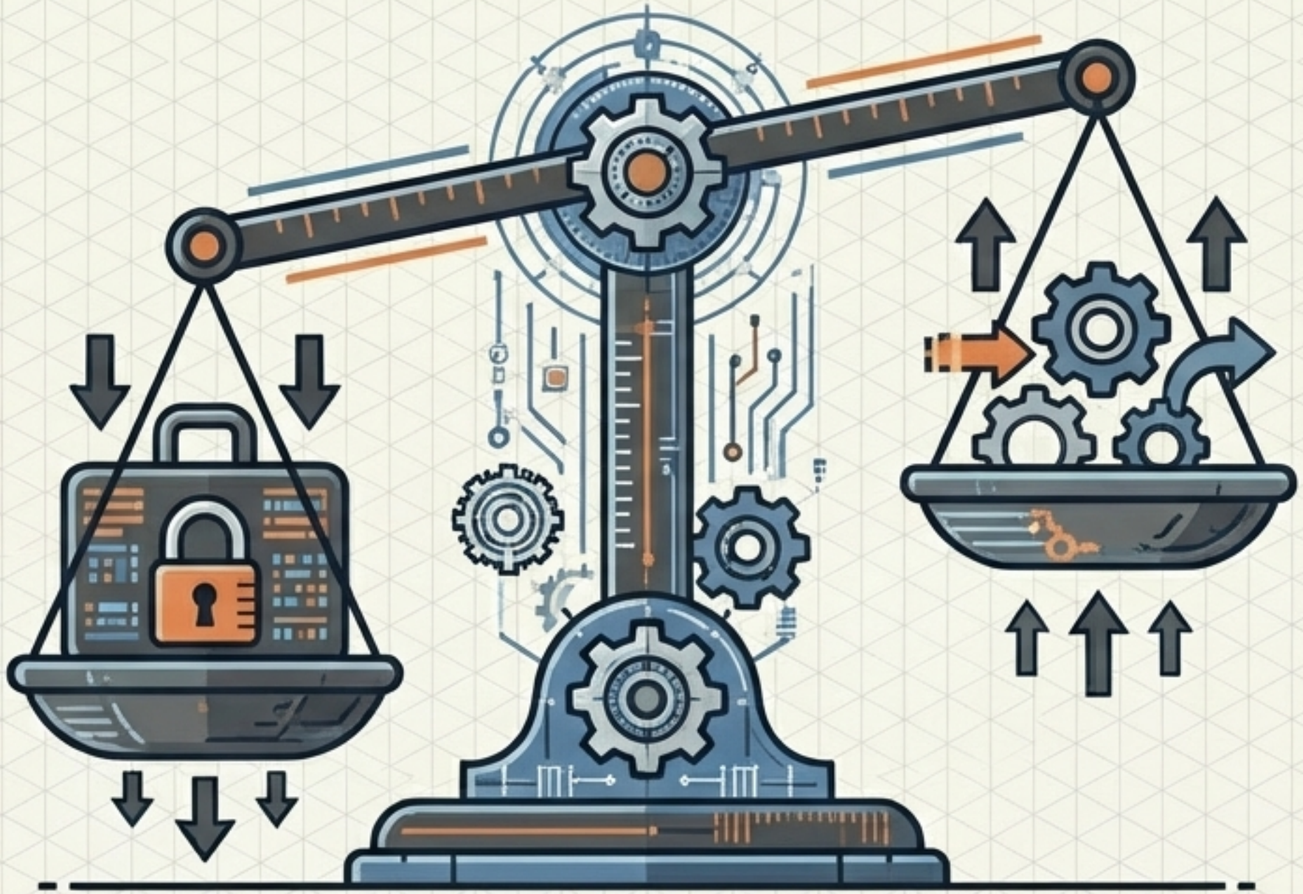
- **Tática:** Abordagem planejada (ex: uso de chaveiro profissional).
- **Coleta:** Logística metódica junto às partes envolvidas.
- **Retorno:** Foco na continuidade do negócio dentro do escopo legal.

O Dilema Central da Apreensão Digital

Toda operação de busca exige calibrar uma balança crítica. O método escolhido dependerá da autorização judicial e do orçamento do autor.

Preservação Máxima

100% de garantia de coleta, mas ao custo de paralisar a empresa alvo.

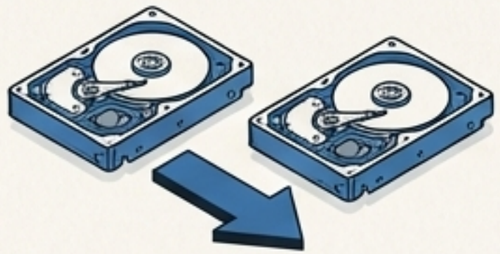


Continuidade do Negócio

Empresa continua operando, mas eleva o custo de campo e reduz o escopo da busca.

O Core Técnico: Espelhamento e Cadeia de Custódia

O rigor técnico obrigatório antes de qualquer equipamento ser devolvido.



1. Cópia Bit-a-bit

Copia da posição 1 do HD original para o destino, incluindo espaços vazios.

```
1TB lido != 999MB gravados.
Se houver erro, refaz do zero.
```

2. Validação de Hash

A chave alfanumérica do HD cópia deve bater 100% com a original.

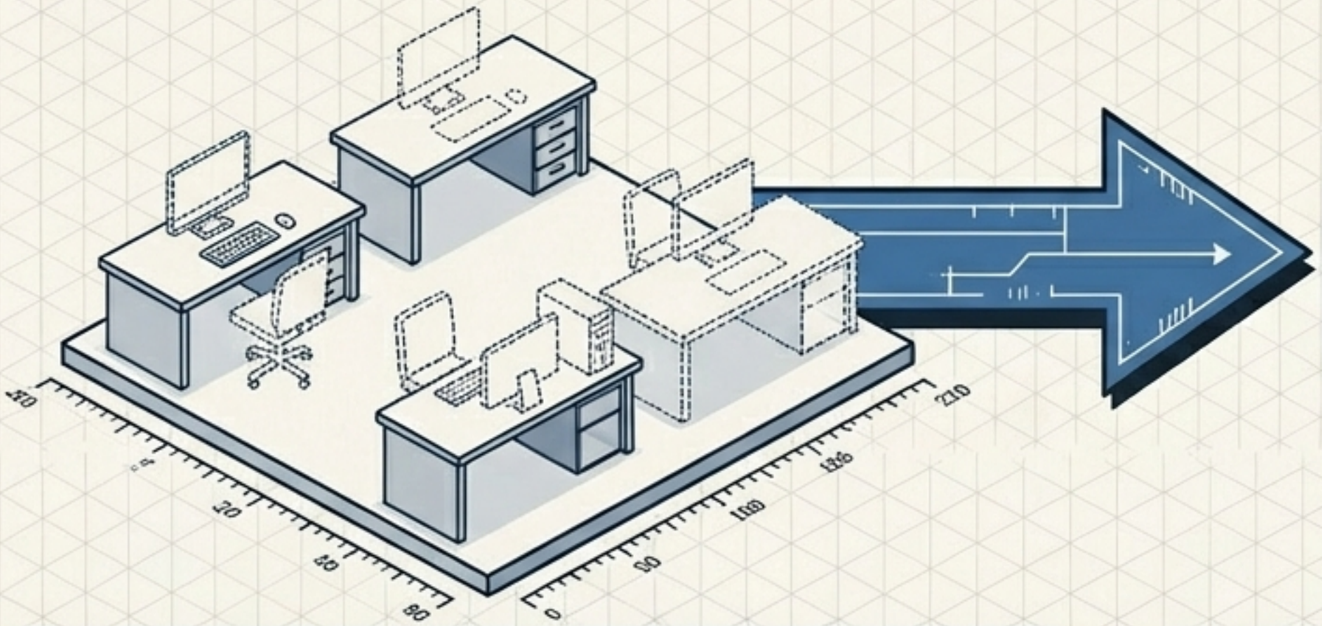
```
Algoritmos: MD5, SHA-512, SHA-1024
```

3. Backup Forense

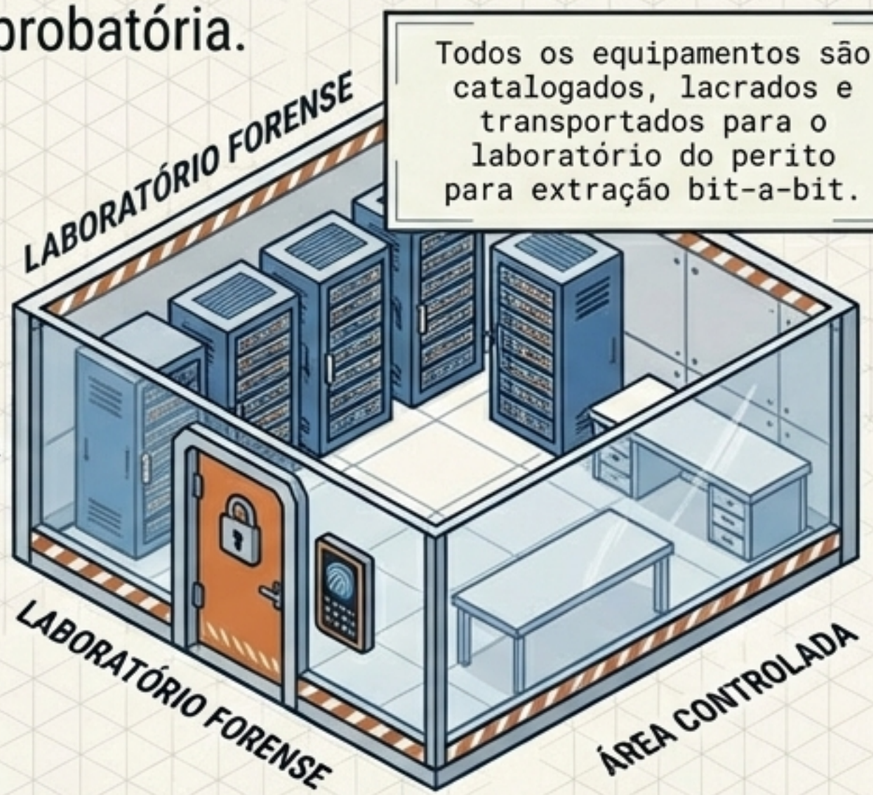
Criação da 'Cópia da Cópia'. Mantém-se a original intacta e um backup de segurança validado.

Método 1: Sequestro Total + Duplicação em Laboratório

A abordagem tradicional e mais garantida para coleta probatória.



Todos os equipamentos são catalogados, lacrados e transportados para o laboratório do perito para extração bit-a-bit.



100% de garantia de coleta.
Operação controlada em laboratório.

A empresa alvo fica **inoperante** e “depenada” por semanas.

Método 2: Duplicação Forense em Campo

Operação *In Loco* sem a remoção definitiva dos bens.

A empresa é paralisada temporariamente.
Cria-se uma sala lacrada e monitorada no local.
Equipamentos voltam a operar gradativamente.

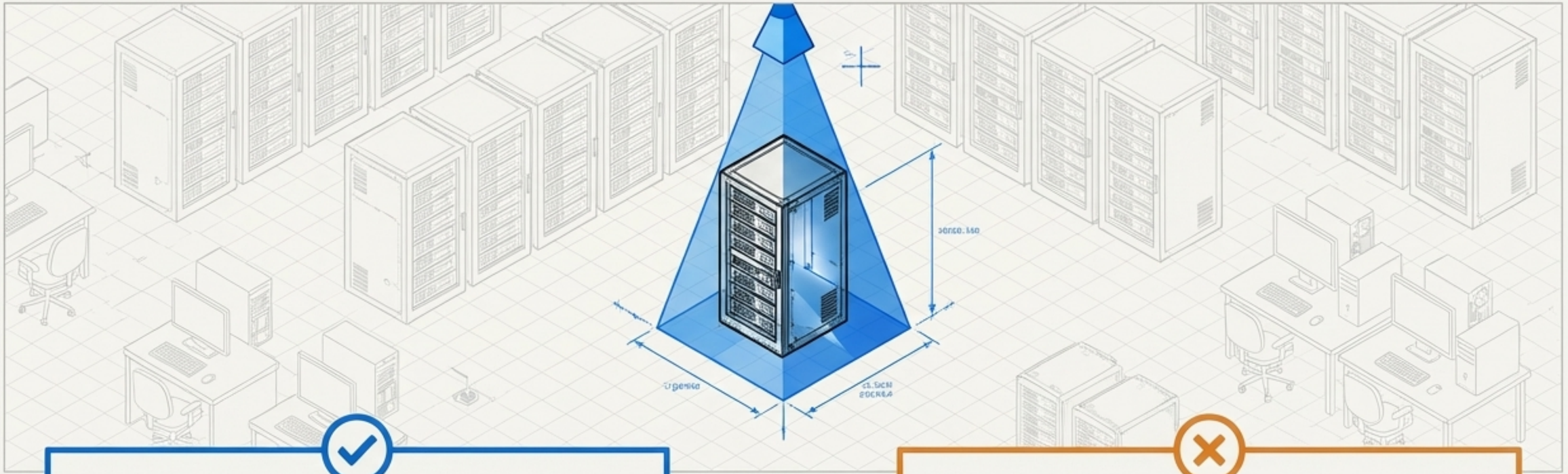
✓ Os bens não saem da empresa, gerando menos atrito.

✗ Exige equipe numerosa, dias dormindo em campo e altíssimo custo com HDs e duplicadores.

Método 3: Abordagem Específica em Campo

A operação cirúrgica baseada em testemunho técnico local.

A equipe identifica e duplica apenas a máquina exata com o software alvo, na frente do técnico da empresa, ainda no local.



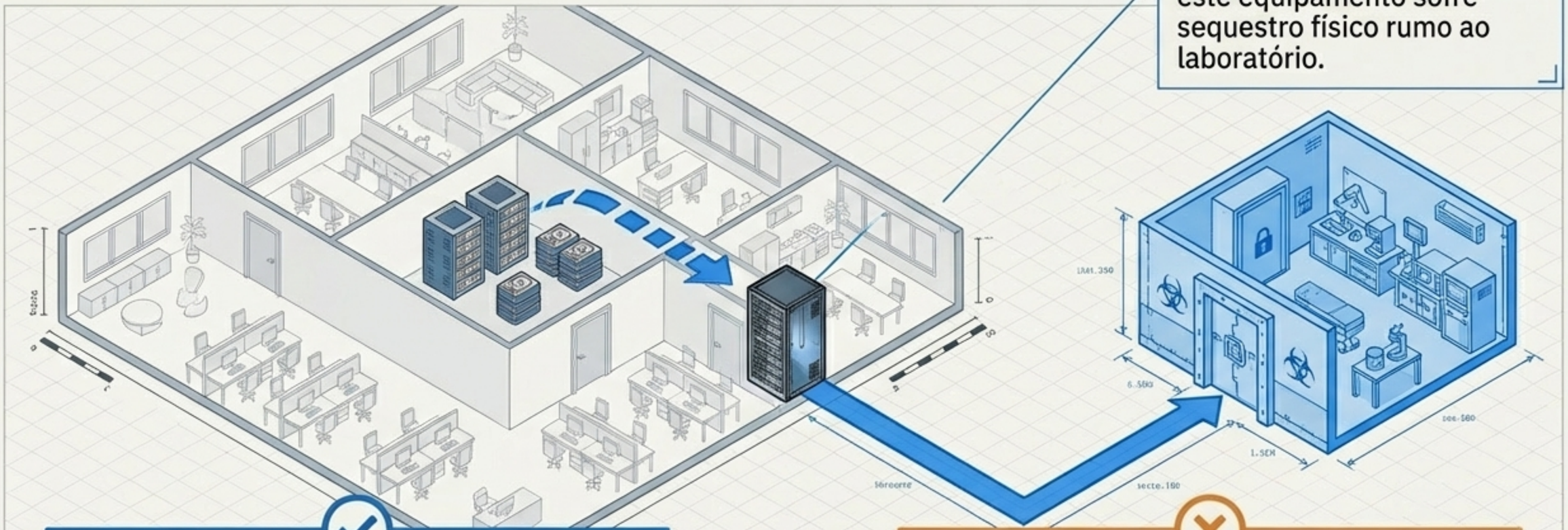
Rápido, barato para o autor e gera mínimo impacto operacional ao alvo.

Risco de ignorar vestígios ocultos em máquinas secundárias da rede.

Método 4: Sequestro Específico com Extração

Precisão de alvo com a segurança laboratorial.

Identifica-se cirurgicamente a máquina alvo. Em vez de duplicar em campo, apenas este equipamento sofre sequestro físico rumo ao laboratório.



Combina baixo custo de campo com o ambiente controlado do laboratório. Empresa perde apenas 1 equipamente.

Ainda carrega o risco menor de deixar evidências secundárias na rede.

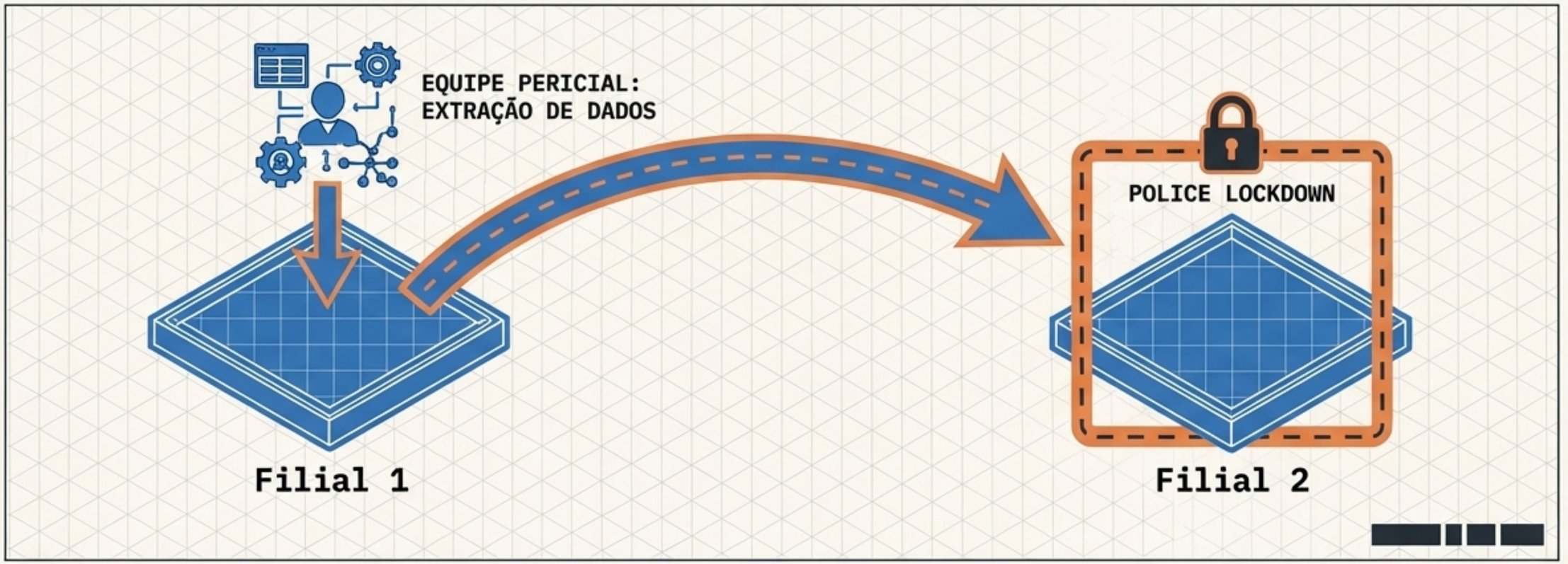
SYNTHESIS: Matriz de Decisão Forense

Framework comparativo para definição da estratégia de apreensão.

	Método 1 (Seq. Total)	Método 2 (Campo Amplo)	Método 3 (Campo Específico)	Método 4 (Seq. Específico)
Custo Financeiro p/ Autor	 Médio	 Altíssimo	 Baixo	 Baixo
Duração da Missão (Campo)	 Rápido	 Muito Lento	 Rápido	 Muito Rápido
Impacto Operacional no Alvo	 Paralisante	 Alto	 Baixo	 Moderado
Abrangência de Vestígios	 Máxima	 Máxima	 Restrita	 Restrita

Estudo de Caso Real: Logística Multi-Filial

Neutralizando o risco de destruição remota de provas em empresas de mesmo CNPJ.



1. Sincronia:
Ação deflagrada simultaneamente.

2. Congelamento:
Polícia isola operações de TI da Filial 2.

3. Atuação:
Equipe executa extração inteiramente na Filial 1.

4. Deslocamento:
Time pericial avança para a Filial 2, mantida sob custódia.

O Veredito do Especialista

A Escolha Tática:
Método 4 (Sequestro Específico com Extração).

A Justificativa:

Como o objeto pericial já possui **alocação provável centralizada**, uma **varredura sistêmica** apenas geraria **montanhas de laudas, atraso processual** e **custos desproporcionais**. O **sequestro cirúrgico** garante a **cadeia de custódia inquestionável** de laboratório com **precisão tática** no alvo.

Ecossistema de Inteligência Pericial

Ferramentas operacionais e networking para Peritos.

Acesso Restrito

+350 especialistas ativos debatendo táticas.

fala.host/grupos

Ferramentas de Autoridade

Crie seu Cartão Virtual e integre-se ao diretório.

fala.host/cartao

Blindagem de Honorários

Simulador avançado para evitar impugnação de valores.

fala.host/calculadora

Acesse a Área de Membros para treinamentos avançados de campo que cursos teóricos tradicionais não ensinam.