risklab.

PLAYBOOK EXECUTIVO

Claude Code na Auditoria Interna

Como transformar procedimentos, controles, bases de dados e evidências em rotinas de análise e testes automatizados.

De Documentos para Execução: A Engenharia de Auditoria

A Auditoria Interna ainda trata muitos testes operacionais como artesanato manual. O Claude Code surge como a camada operacional para inaugurar uma nova era: transformar o trabalho repetitivo, manual e quebradiço em engenharia de dados e automação.

O Modelo Tradicional (Artesanato)

- **Foco:** Copiar e organizar evidências.
- **Análise:** Planilhas manuais, amostragem limitada e leitura humana exaustiva.
- **Resultado:** Achados escritos no escuro, baseados em fragmentos de dados.

O Modelo risklab + IA (Engenharia)

- **Foco:** Avaliar o risco real.
- **Análise:** Testes automatizados via scripts (Python/SQL), análise massiva de dados e validação algorítmica.
- **Resultado:** Conclusões 100% sustentadas por dados e rastreáveis.

A IA é o motor que limpa a lama operacional da trilha.
O auditor permanece como o juiz absoluto.

Capítulo 1: Operacionalização e Testes de Controle

01. Automatização de Testes de Controle

- **Conceito**: Substituição de filtragens e amostragens manuais em planilhas por scripts que executam a regra do controle.
- **Contexto**: Ideal para controles volumosos (ex: aprovações financeiras) onde a auditoria testa 100% da população em vez de amostras pontuais.
- **Dados**: Bases de pagamentos (CSV/Excel) e logs de aprovação.

```
Atuando como auditor técnico, leia a base 'pagamentos.csv'. Construa um script em Python que identifique transações acima de R$ 50 mil sem duas aprovações distintas nos logs. Gere um output com id_pagamento, valor, aprovadores e o motivo da exceção, além de um resumo técnico.
```

- **Entregáveis**: Planilha de achados e resumo técnico do teste.
- **Governança**: A IA levanta as exceções lógicas; o auditor julga a materialidade e o contexto do desvio.

02. Transformar Descrição em Lógica Testável

- **Conceito**: Quebrar políticas nebulosas em roteiros algorítmicos executáveis.

- **Contexto**: Traduzir normativos como revisão periódica de acessos em perguntas parametrizáveis para sistemas.
- **Dados**: Manuais, políticas corporativas e matrizes descritivas.

```
Analise a seguinte descrição de controle manual: [INSERIR TEXTO]. Quebre esta diretriz em uma lógica estruturada de teste contendo: periodicidade exata, bases comprobatórias necessárias, chaves de cruzamento e regras para classificar exceções.
```

- **Entregáveis**: Roteiro técnico de teste e checklist de extração de dados.
- **Governança**: O auditor deve validar se a interpretação lógica da IA reflete a verdadeira intenção do risco mitigado.

03. Geração de Scripts para Bases

- **Conceito**: Criação de rotinas (Python/SQL) para cruzar bases corporativas sem depender de fila de TI.
- **Contexto**: Encontrar duplicidades, registros órfãos ou quebras de padrão em bases de ERPs, RH ou compras.
- **Dados**: Exportações brutas (CSV, logs de sistema, cadastros).

```
Leia 'pagamentos.csv' e 'aprovacoes.csv'. Crie um script robusto em Python para correlacionar as bases via 'id_pagamento'. Identifique pagamentos críticos sem aprovação dupla. Exporte os achados documentando o status e o motivo da exceção, incluindo comentários no código.
```

- **Entregáveis**: Script executável e arquivo consolidado de desvios.
- **Governança**: O código gerado atua como apoio analítico; os achados devem ser submetidos à checagem e ceticismo do auditor.

Capítulo 2: Acessos, Evidências e Documentação

04. Auditoria de Acessos e SoD

- **Conceito:** Mapeamento em massa de conflitos de Segregação de Funções (SoD) e acessos indevidos.
- **Contexto:** Cruza bases de RH (altivos/desligados) com logs para barrar acessos genéricos ou acúmulo de funções.
- **Dados:** Matriz SoD, logs de acesso e base de colaboradores.

```
Analise a 'matriz_sod.xlsx' e a 'base_acessos.csv'. Crie um script para identificar usuários com perfis conflitantes, genéricos ou sem vínculo ativo. O output deve agrupar exceções por área/risco e gerar um sumário executivo detalhando as violações.
```

- **Entregáveis:** Resumo executivo de exceções e abas detalhadas por tipo de conflito.
- **Governança:** A IA mapeia o conflito sistêmico; a avaliação sobre o impacto de negócios do acesso indevido é estritamente humana.

05. Leitura e Análise de Evidências

- **Conceito:** Estruturação de dados extraídos de PDFs, atas e prints (via OCR/texto).
- **Contexto:** Transforma um amontoado de documentos informais em uma matriz auditável (Critério x Evidência x Conclusão).
- **Dados:** Contratos, relatórios exportados, e-mails, atas.

```
Utilizando leitura de texto, analise os PDFs da pasta de evidências. Extraia: data, responsável, sistema e conclusão. Crie uma matriz consolidada e sinalize com uma flag arquivos incompletos, inconsistentes ou fora do período auditado.
```

- **Entregáveis:** Matriz estruturada de verificação documental.
- **Governança:** O auditor deve revisar amostras das evidências processadas para atestar a precisão da extração da IA.

06. Papéis de Trabalho Padronizados

- **Conceito:** Geração automática da estrutura de documentação GRC baseada nos testes realizados.
- **Contexto:** Elimina a variação narrativa entre auditores, garantindo uniformidade e qualidade técnica no registro.
- **Dados:** Scripts executados, planilhas de exceção e escopo.

```
Com base no script executado e na tabela de exceções gerada, redija um papel de trabalho em Markdown. Inclua estritamente: objetivo, critério técnico, procedimentos, população, amostra, detalhamento das exceções e a conclusão.
```

- **Entregáveis:** Documento estruturado pronto para anexo sistêmico.
- **Governança:** A IA redige a arquitetura do documento, mas a conclusão formal e a assinatura do papel de trabalho são invioláveis.

Capítulo 3: Planejamento, Monitoramento e Ação

07. Planejamento Baseado em Dados

- **Conceito:** Uso de IA para cruzar histórico e definir prioridades antes do trabalho de campo.
- **Contexto:** Direciona o Plano Anual de Auditoria (PAA) focando em reincidência, exposição residual e volume financeiro crítico.
- **Dados:** Histórico de achados, planos de ação e Matriz de Riscos.

```
Processe a base de achados dos últimos 3 anos, a matriz de riscos e os planos de ação. Crie um modelo analítico para priorizar processos no plano anual, baseado em criticidade, reincidência e atrasos. Entregue um ranking top 10 com justificativas.
```

- **Entregáveis:** Análise preditiva e proposta quantitativa de priorização do PAA.
- **Governança:** A decisão final do Plano de Auditoria requer julgamento estratégico humano e alinhamento do Comitê.

08. Monitoramento Contínuo

- **Conceito:** Criação de rotinas autônomas que apontam exceções no momento em que a operação pulsa.
- **Contexto:** Transforma a auditoria retrospectiva em observação em tempo real (ex: transações noturnas, trocas bancárias anômalas).
- **Dados:** Feeds de dados de ERPs e logs operacionais.

```
Com base nas regras do controle de fornecedores, escreva um script de monitoramento contínuo em SQL que rode diariamente para identificar alterações cadastrais sensíveis feitas fora do fluxo aprovado, gerando um alerta automatizado.
```

- **Entregáveis:** Scripts de monitoramento contínuo e parâmetros de alerta.
- **Governança:** A IA acelera a detecção preliminar; o auditor atua na investigação qualificada do alerta gerado.

09. Análise de Planos de Ação

- **Conceito:** Avaliação em lote da qualidade, aderência e atraso das medidas de remediação propostas pelas áreas.
- **Contexto:** Varre cronogramas para expor ações genéricas, causas-raiz desconexas ou áreas com excesso de backlog.
- **Dados:** Planilha de gestão de achados e planos de ação.
planos de ação.

```
Analise o arquivo de planos de ação pendentes. Classifique e sinalize planos com descrições genéricas, prazos incompatíveis com a criticidade ou causa-raiz desconexa da ação proposta. Gere um relatório consolidado por área responsável.
```

- **Entregáveis:** Régua de priorização e relatório de qualidade dos planos.
- **Governança:** O auditor utiliza o insight para cobrar os gestores, mas jamais altera os planos sem alinhamento com a 1ª linha.

Capítulo 4: Reporte Técnico, Consistência e Cadeia de Valor

10. Apoio na Redação de Achados

- **Conceito**: Conversão de exceções técnicas brutas em linguagem executiva padronizada.
- **Contexto**: Evita que o achado vire ficção elegante, focando no bisturi analítico das falhas sistêmicas.
- **Dados**: Planilhas de teste de auditoria e matriz de riscos.

```
A partir da relação de exceções do teste, elabore minutas de achados seguindo estritamente a estrutura: Condição, Critério, Causa provável, Consequência operacional, Nível de Risco associado e Recomendação técnica.
```

- **Entregáveis**: Minutas de achados de auditoria altamente estruturadas.
- **Governança**: A IA propõe o texto inicial; a revisão humana é obrigatória para calibrar o impacto real de negócios.

11. Revisão de Consistência de Matrizes

- **Conceito**: Varredura algorítmica em Matrizes de Riscos e Controles para identificar amarrações frouxas.
- **Contexto**: Localiza riscos sem controle, testes incompatíveis com a natureza do controle, ou critérios contraditórios.
- **Dados**: Matriz de Riscos, Controles e Procedimentos.

```
Efetue uma revisão de coerência lógica na matriz de riscos e controles. Para cada linha, valide se o teste descrito efetivamente mitiga o risco associado. Classifique o alinhamento como 'Adequado', 'Parcial' ou 'Inadequado', justificando as falhas.
```

- **Entregáveis**: Diagnóstico arquitetônico e de maturidade da Matriz de Riscos.
- **Governança**: A ferramenta expõe as inconsistências lógicas; o auditor sênior aprova o redesenho metodológico do controle.

12. Auditoria de Terceiros e Due Diligence

- **Conceito**: Cruzamento de bases relacionais para expor anomalias na cadeia de fornecedores e contratos.
- **Contexto**: Identifica fornecedores pagos sem contrato, CNPJs compartilhando contas bancárias ou concentração excessiva.
- **Dados**: Cadastros de fornecedores, base de contratos e faturamentos.

```
Cruze as bases 'fornecedores.csv', 'contratos.xlsx' e 'pagamentos.csv'. Identifique anomalias como: fornecedores pagos sem contrato ativo ou CNPJs distintos compartilhando dados bancários. Gere um dossiê analítico de exceções.
```

- **Entregáveis**: Relatório de red flags operacionais de fornecedores.
- **Governança**: A IA mapeia os desvios transacionais; o auditor investiga indícios de fraude com rigoroso ceticismo profissional.

Capítulo 5: Compliance Regulatório e Inteligência Executiva

13. Auditoria de Compliance Regulatório

- **Conceito:** Acompanhamento algorítmico de obrigações legais, prazos, licenças e penalidades.

- **Contexto:** Avalia se o cadastro de obrigações possui donos claros, ausência de evidências ou licenças críticas expirando no curto prazo.

- **Dados:** Bases de obrigações legais, licenças ambientais/operacionais e certidões.

```
Cruze a base de obrigações regulatórias com o calendário corporativo. Destaque obrigações vencidas, licenças próximas do limite sem evidência atualizada e pendências severas sem responsável direto atribuído.
```

- **Entregáveis:** Dashboard preliminar de status regulatório e alertas de quebra.

- **Governança:** A interpretação de normas legais complexas e a gestão do risco regulatório continuam sob chancela exclusivamente humana.

14. Dashboards e Relatórios Executivos

- **Conceito:** Consolidação e modelagem de bases de testes para consumo em ferramentas de BI.

- **Contexto:** Automatiza a engenharia de dados para expor achados, reincidências e tempos médios de remediação aos Comitês.

- **Dados:** Tabelas históricas de testes, exceções e planos de ação.

```
Transforme a base de testes e achados em um modelo tabular normatizado para Power BI. A tabela deve conter dimensões (área, processo, risco) e métricas (status, dias em atraso). Forneça o script Python e a estrutura final consolidada.
```

- **Entregáveis:** Modelo de dados higienizado pronto para consumo visual.

- **Governança:** A apresentação executiva e a narrativa gerada devem ser revisadas pelo gestor antes do reporte ao Conselho.

15. Bibliotecas de Testes Reutilizáveis

- **Conceito:** Criação de um repositório proprietário de scripts de auditoria em constante evolução.

- **Contexto:** Impede que a auditoria comece do zero, consolidando um arsenal silencioso e letal de testes padronizados.

- **Dados:** Scripts passados, lógicas de GRC corporativo.

```
Com base no script de SoD recém-criado, parametrize o código Python para que ele se torne um módulo genérico reutilizável. Extraia as variáveis dinâmicas (nomes de arquivos, limites financeiros) para um arquivo de configuração JSON padronizado.
```

- **Entregáveis:** Pacotes internos de testes de rotina versionados.

- **Governança:** O versionamento e a segurança do código fonte da biblioteca corporativa devem seguir estritamente as diretrizes de TI.

Capítulo 6: Automação Híbrida e Arquitetura de Testes

16. Conversão de Procedimentos em Automações

- **Conceito:** Decomposição arquitetônica de testes manuais em esteiras automatizáveis (Data + IA + Humano).
- **Contexto:** Separa o que é scriptável (dados puros), o que é OCR (documentos) e o que exige cognição humana.
- **Dados:** Manuais metodológicos e procedimentos em Word/PDF.

```
Transforme o procedimento manual fornecido em uma rotina híbrida. Separe claramente as etapas testáveis por dados, as que exigem análise documental (visão computacional) e as que exigem julgamento humano. Proponha a estrutura do output.
```

- **Entregáveis:** Fluxograma operacional e arquitetura técnica do teste.
- **Governança:** A IA desenha o processo proposto, mas a eficácia da automação de controle deve ser homologada pela liderança técnica.

17. Validação de Qualidade de Dados (Profiling)

- **Conceito:** Checagem de higidez algorítmica das bases recebidas antes da execução dos testes.
- **Contexto:** Evita que a auditoria gaste dias processando planilhas corrompidas com campos nulos ou chaves quebradas.
- **Dados:** Qualquer extração crua (raw data) fornecida pelas áreas de negócio.

```
Elabore uma rotina preliminar de 'data profiling' para a base recebida. Mapeie campos nulos, formatos de data inconsistentes, duplicidades sistêmicas e registros fora do escopo temporal. Entregue um relatório de saúde dos dados.
```

- **Entregáveis:** Diagnóstico de integridade da base recebida (Health Check).
- **Governança:** Garante que a IA atue apenas sobre informações íntegras, blindando a auditoria contra conclusões baseadas em lixo sistêmico.

18. Simulação de Trilha de Auditoria

- **Conceito:** Construção de mapas de evidência relacionando a origem primária do dado à conclusão final.
- **Contexto:** Mapeia de qual sistema a informação flui, quais chaves cruzar e quais limitações inerentes existem no teste.
- **Dados:** Inventário de sistemas corporativos e escopo do teste.

```
Com base no escopo fornecido, monte um mapa lógico da trilha de auditoria. Indique a origem dos dados, chaves primárias para cruzamentos, regras de validação, limitações operacionais e as evidências que sustentarão o parecer.
```

- **Entregáveis:** Mapa rastreável e defensável do fluxo da auditoria.
- **Governança:** A rastreabilidade documentada assegura que cada achado resistirá a revisões rigorosas por auditores independentes ou reguladores.

Priorização Estratégica: A Matriz de Valor

Onde iniciar a implementação do Claude Code para garantir retorno imediato em produtividade, cobertura e precisão técnica.

[1] Automatização de Testes de Controle

O motor de escala. Reduz drasticamente o trabalho manual de amostragem cega e amplia imediatamente a cobertura da auditoria para 100% da população de dados analisada.

[2] [V] Análise de Acessos e SoD

O ganho rápido (Quick Win).
Campo de altíssimo impacto, risco severo e fácil padronização algorítmica. Ideal para estabelecer a confiança da equipe técnica na capacidade analítica de cruzamentos da IA.

[3] [SD] Validação de Evidências

A organização do caos.
Reduz o retrabalho extenuante de leitura humana de documentos despadronizados, PDFs e atas, melhorando substancialmente o lastro documental do trabalho.

[4] [E-SU] Monitoramento Contínuo

A mudança definitiva de paradigma.
Tira a auditoria do ciclo puramente retrospectivo e reativo, permitindo a identificação cirúrgica de exceções no momento exato em que a operação pulsa.

[5] [N-SIL] Papéis de Trabalho Automáticos

O salto de produtividade.
Gera ganho de tempo imediato ao criar a estrutura narrativa, organizacional e documental dos testes simultaneamente à execução técnica.

Governança de IA: O Fator Humano

A automação via Claude Code amplia exponencialmente a capacidade técnica, mas não revoga os princípios fundamentais, a ética e a responsabilidade da profissão de Auditoria.

- **Confidencialidade e Dados Sensíveis:** Dados PII ou informações corporativas estratégicas jamais devem ser inseridos em prompts abertos sem anonimização prévia robusta ou uso de ambientes corporativos seguros (Enterprise).
- **Rastreabilidade e Versionamento:** Todo script gerado por IA utilizado para conclusões oficiais deve deve ser validado tecnicamente, salvo no repositório oficial da auditoria e estritamente documentado no papel de trabalho.
- **Revisão e Materialidade Obrigatória:** A IA possui capacidade impecável de processar os dados e propor o texto, mas a materialidade do achado e o impacto nos negócios exigem calibração humana irrevogável.
- **O Limite Frontal da Ferramenta:** O Claude Code constrói a engenharia operacional e analítica do teste; o auditor provê o Ceticismo Profissional.

"A grande aplicação do Claude Code não é substituir o auditor, mas substituir a parte mais ingrata do ritual: o trabalho repetitivo, manual e quebradiço entre a evidência e a conclusão. Menos tempo copiando evidências, mais tempo avaliando riscos. Bem-vindo à auditoria baseada em execução."