GESTÃO ESTRATÉGICA DE TECNOLOGIA DA INFORMAÇÃO

Unidade III
Revisão seletiva

Unidade IV
Lei Sarbanes-Oxley (SOX)



O PERCURSO DA REVISÃO ATÉ A SOX

Na **Unidade III,** estudamos quatro decisões: **escolher** como obter serviços de TI; **contratar** com responsabilidades definidas; **medir** custos e resultados; e **auditar** riscos e controles por evidências.

Na **Unidade IV,** aplicaremos esse raciocínio aos sistemas que registram **vendas, pagamentos e lançamentos contábeis.** A questão deixa de ser apenas "o serviço funciona?" e passa a incluir: **"como demonstrar que a informação financeira gerada é confiável?".**

Percurso:  **DECIDIR** →  **MEDIR** →  **AUDITAR** →  **COMPROVAR**

SOURCING: ESCOLHA E RESPONSABILIDADE

Sourcing é a decisão sobre como obter capacidades e serviços de TI. **Make** significa desenvolver ou operar internamente; **Buy** adquirir uma solução ou serviço de mercado; **Partner** integrar competências internas e externas em uma parceria.

A escolha depende de **criticidade, competência disponível, custo total, riscos e necessidade de controle.** Ao terceirizar uma execução, a organização não transfere automaticamente a responsabilidade por seus objetivos, dados ou decisões estratégicas.

Exemplo: se um parceiro opera o sistema financeiro, a contratante ainda precisa definir requisitos, supervisionar riscos e avaliar resultados.



MAKE
Desenvolver ou operar internamente.



BUY
Adquirir uma solução ou serviço de mercado.



PARTNER
Integrar competências internas e externas em uma parceria.



Execução externa ≠ ausência de responsabilidade.

SLA e dependência: desempenho não é controle

SLA (Service Level Agreement, Acordo de Nível de Serviço) é o **compromisso contratual sobre padrões de serviço**, como disponibilidade, prazo de atendimento ou recuperação. Cumprir um SLA demonstra o alcance das metas pactuadas; não prova, sozinho, que acessos e alterações de dados estejam sob controle.

Vendor lock-in (dependência ou aprisionamento ao fornecedor) ocorre quando substituir ou trazer um serviço de volta se torna caro, demorado ou arriscado.

Exemplo: o sistema financeiro fica disponível 99,9% do tempo, mas permite alterações sem autorização. A contratante precisa de supervisão, registros verificáveis e alternativas de saída.



SLA atendido | ≠ **controle demonstrado** | ≠  **dependência resolvida**

PRODUTIVIDADE, TCO E FINOPS: VALOR REAL

Produtividade em TI relaciona recursos utilizados aos resultados entregues; contar tickets ou linhas de código não demonstra, por si, qualidade, estabilidade e valor.

TCO *(Total Cost of Ownership,* Custo Total de Propriedade) considera aquisição, integração, suporte, operação, segurança e eventual migração ou saída — não apenas o preço inicial.

FinOps é uma prática colaborativa de gestão financeira de tecnologia, envolvendo TI, finanças e negócio para tornar o consumo visível e orientar gasto por valor. **Exemplo:** reduzir custo de nuvem não é ganho real se a economia compromete a continuidade de um processo financeiro crítico.



volume ≠ valor



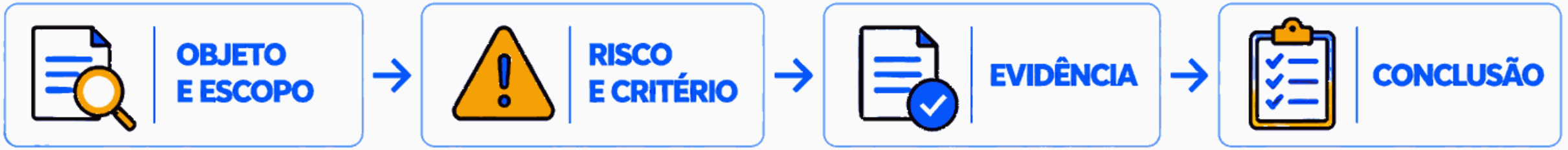
preço ≠ custo total

AUDITORIA ORIENTADA POR RISCO E CRITÉRIO

Auditoria de TI é uma avaliação sistemática de processos e controles baseada em critérios e evidências. Primeiro, define-se o **objeto** (o que será examinado), o **objetivo** (qual pergunta responder) e o **escopo** (sistemas e período). Depois, priorizam-se **riscos** e estabelecem-se **critérios** para comparar o esperado com o observado.

COBIT é um framework de governança e gestão da informação e tecnologia mantido pela ISACA. Seus objetivos e práticas podem **orientar critérios de auditoria**, mas não são um software nem substituem exames, entrevistas, testes e julgamento profissional.

Exemplo: auditar permissões de acesso ao ERP segundo a política aprovada e as obrigações aplicáveis.



CONTROLE PREVISTO NÃO É CONTROLE COMPROVADO

Controle é uma medida para **prevenir, detectar ou corrigir** um risco. Avaliar seu **desenho** significa verificar se a regra é adequada; avaliar sua **operação** significa demonstrar que funcionou no período observado.

Exemplo: a política exige aprovação antes de mudanças no sistema. O desenho parece adequado, mas só registros de solicitação, autorização, implantação e logs permitem verificar a execução real. Um documento sem data ou um print isolado não comprova necessariamente meses de conformidade.

Evidência de auditoria precisa ser **pertinente, confiável e suficiente** para fundamentar uma conclusão delimitada.



DESENHO:
regra adequada?



OPERAÇÃO:
há evidência de que funcionou?

DO ACHADO DE AUDITORIA À AÇÃO CORRETIVA

Um **achado de auditoria** descreve uma diferença relevante entre o critério definido e a condição demonstrada pelas evidências. Deve indicar o fato observado, o risco envolvido e, quando sustentado, sua possível causa.

Exemplo: a regra exige revogar o acesso após desligamento, mas os registros mostram uma conta ainda ativa fora do prazo. A recomendação pode propor melhorar a comunicação entre RH e TI e registrar exceções.

Follow-up é o acompanhamento posterior: verifica se a medida foi implementada e realmente reduziu o risco. Abrir um plano de ação ou encerrar um chamado não prova correção eficaz.



ALINHAMENTO E RESPONSABILIDADE: A PONTE NECESSÁRIA

Alinhamento entre TI e negócio significa orientar sistemas e investimentos para os resultados que a organização precisa alcançar. Aqui, o resultado relevante é registrar e divulgar **informações financeiras confiáveis.**

A TI mantém aplicações, acessos, mudanças e registros; áreas de negócio definem regras e validam transações; a administração responde pela qualidade das informações divulgadas, conforme suas obrigações. **As atribuições precisam estar claras para evitar lacunas de controle.**

Não basta afirmar "o financeiro cuida dos números" se sistemas e pessoas de outras áreas também podem alterá-los.



POR QUE SURGIU A LEI SARBANES-OXLEY?

SOX é a sigla de Sarbanes-Oxley Act (Lei Sarbanes-Oxley), promulgada nos Estados Unidos em **2002** após grandes escândalos contábeis e corporativos, como **Enron** e **WorldCom**. Seu contexto foi a perda de confiança de investidores em demonstrações financeiras e na supervisão das empresas.

A lei reforçou **regras de prestação de contas, responsabilidade de executivos, auditoria e controles relacionados à divulgação financeira**. Não é uma lei criada apenas para exigir ferramentas de segurança cibernética.

Para a TI, a ligação é prática; receitas, despesas e lançamentos dependem de aplicações e bases de dados que precisam produzir **registros íntegros e verificáveis**.



Escândalos contábeis e corporativos →  Perda de confiança de investidores →  **2002** | Confiança nas informações financeiras

O ALCANCE DA SOX E OS CONTROLES FINANCEIROS

A **SOX** reúne obrigações aplicáveis a companhias sujeitas à regulação do mercado de capitais dos EUA, incluindo certos emissores estrangeiros. **Não se aplica automaticamente a toda empresa brasileira.** A obrigação exata depende do enquadramento e das regras da SEC (Securities and Exchange Commission, regulador do mercado de valores mobiliários dos EUA).

ICFR (Internal Control over Financial Reporting) significa **Controles Internos sobre Relatórios Financeiros:** políticas e procedimentos para oferecer segurança razoável quanto à confiabilidade dos registros e demonstrações.

"Segurança razoável" não significa garantia absoluta contra erro ou fraude; significa controles apropriados aos riscos financeiros relevantes.



ALCANCE DA SOX
Depende do emissor e das regras da SEC.



ICFR
Controles Internos sobre Relatórios Financeiros.



SEGURANÇA RAZOÁVEL
Não é garantia absoluta contra erro ou fraude.

SEÇÃO 302:
A DIREÇÃO PRECISA CERTIFICAR

A **Seção 302 da SOX** fundamenta regras de certificação, pelo principal executivo e pelo principal responsável financerio, das informações apresentadas nos relatórios periódicos exigidos. **Eles confirmam, com base em seu conhecimento,** a adequação das informações divulgadas e assumem deveres relativos a controles e procedimentos de divulgação.

Também devem **comunicar aos auditores e ao comitê de auditoria** deficiências relevantes e certas ocorrências de fraude conforme as regras aplicáveis.

Exemplo: o fornecedor opera o ERP, mas isso não transfere ao fornecedor a obrigação de certificação da alta direção.



DIREÇÃO EXECUTIVA
(principal executivo)

+



DIREÇÃO FINANCEIRA
(principal responsável financeiro)

→



CERTIFICAÇÃO
das informações nos relatórios periódicos exigidos.

SEÇÃO 404: AVALIAR OS CONTROLES INTERNOS

A **Seção 404 da SOX** trata de controles internos sobre relatórios financeiros (ICFR). Pela **404(a)**, a administração deve apresentar, no relatório anual aplicável, **uma avaliação da eficácia desses controles** e assumir responsabilidade por sua manutenção.

A **404(b)** prevê, quando exigido para a categoria do emissor, **atestação do auditor independente** sobre a avaliação dos controles internos. Há companhias dispensadas dessa atestação; portanto, não é correto dizer que toda empresa deve contratar essa auditoria.

O que se verifica? Se o controle é apropriado ao risco e se existem evidências suficientes de que operou de maneira eficaz.



404(a)

Administração avalia

apresenta, no relatório anual aplicável, a avaliação da eficácia e assume responsabilidade por sua manutenção.



404(b)

Auditor independente atesta quando aplicável

prevê atestação sobre a avaliação dos controles internos. Há companhias dispensadas dessa atestação.



O que se verifica?

Se o controle é apropriado ao risco e se existem evidências suficientes de que operou de maneira eficaz.

ONDE A TI ENTRA NOS CONTROLES DA SOX?

ITGC (Information Technology General Controls, Controles Gerais de Tecnologia da Informação) sustentam a **operação confiável de sistemas que participam do relatório financeiro.** Sua relevância depende do risco que a aplicação pode causar às informações contábeis.

Acessos: limitar quem consulta ou altera lançamentos e dados bancários. **Mudanças:** exigir análise, testes e aprovação antes de modificar regras de cálculo ou integrações. **Operações:** acompanhar processamentos, falhas e registros necessários ao fechamento financeiro.



Acessos

Limitar quem consulta ou altera lançamentos e dados bancários.



Mudanças

Exigir análise, testes e aprovação antes de modificar regras de cálculo ou integrações.



Operações

Acompanhar processamentos, falhas e registros necessários ao fechamento financeiro.



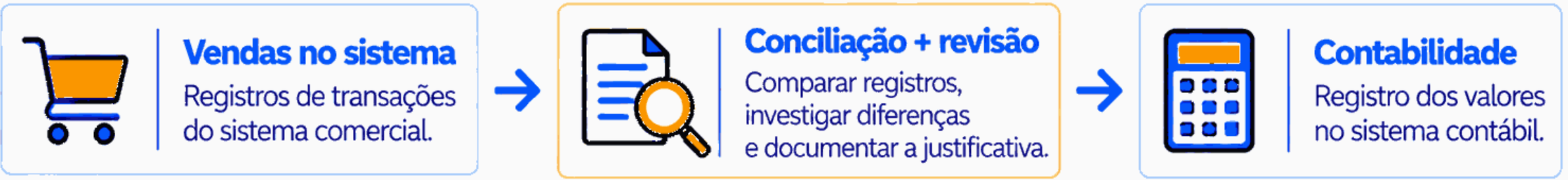
Exemplo: uma alteração não autorizada no cálculo de tributos pode afetar valores reportados. A SOX não prescreve a compra de um software específico.

ICFR: DO SISTEMA AO RELATÓRIO FINANCEIRO

Um controle financeiro deve ajudar a verificar se valores produzidos por sistemas são **completos, corretos e levados adequadamente à contabilidade.** Conciliação é comparar registros de fontes relacionadas para identificar e investigar diferenças.

Exemplo didático: comparar o total de vendas do sistema comercial com o valor registrado no sistema contábil. Se houver divergência, o responsável investiga, documenta a justificativa e registra a revisão.

Evidências podem incluir relatórios de conciliação, identificação de quem revisou, datas e tratamento das exceções. Esse é um exemplo de controle possível para um risco específico, não uma exigência padronizada da SOX para todas as empresas.



CASO APLICADO:
MUDANÇA INDEVIDA NO ERP FINANCEIRO

ERP (Enterprise Resource Planning, Sistema Integrado de Gestão Empresarial) reúne processos como compras, pagamentos e contabilidade.

Caso didático: um usuário sem competência autorizada altera os dados bancários de um fornecedor. A falha pode gerar pagamento indevido e comprometer registros de contas a pagar.
Risco: transações incorretas ou fraudulentas alcançarem o processo financeiro.

Controles possíveis: restringir privilégios, exigir aprovação independente para alteração cadastral, registrar quem mudou os dados e revisar exceções. A auditoria verifica solicitações, autorizações e logs. Se o serviço for terceirizado, o dever de supervisionar esses riscos permanece com a contratante.



Alteração indevida
Usuário sem competência autorizada altera os dados bancários de um fornecedor.



Risco financeiro
Pagamento indevido e transações incorretas ou fraudulentas.

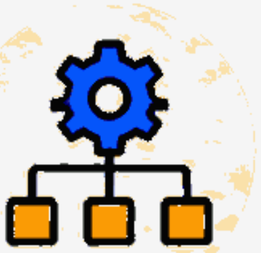


Aprovação + trilha
Controles, registros e revisão de exceções para evidência.

SOX, COBIT E LGPD: NÃO CONFUNDIR



SOX (Sarbanes-Oxley Act)
é lei dos EUA, com exigências relevantes de responsabilização corporativa, divulgação e controles financeiros.



COBIT é um framework de governança e gestão de informação e tecnologia, desenvolvido e mantido pela ISACA. Ele pode orientar práticas, critérios e responsabilidades, mas não é uma lei nem garante, por si, conformidade com a SOX.



LGPD (Lei Geral de Proteção de Dados Pessoais, Lei brasileira nº 13.709/2018) disciplina o tratamento e a proteção de dados pessoais.
Uma organização pode ter obrigações relacionadas aos três temas, mas cada um possui finalidade e alcance diferentes.

SÍNTESE PARA A VERIFICAÇÃO: TRÊS PERGUNTAS



1. QUE INFORMAÇÃO PRECISA SER CONFIÁVEL?

Identificar registros e sistemas que alimentam relatórios financeiros.



2. QUAL RISCO E QUAL CONTROLE IMPORTAM?

Avaliar acessos, alterações, conciliações ou operações relevantes e suas evidências.



3. QUEM RESPONDE E COMO DEMONSTRA?

Definir responsabilidades, comprovar execução e acompanhar exceções.



Na SOX, a **Seção 302** trata de certificações da direção; a **404**, de avaliação de controles internos sobre relatórios financeiros, com atestação externa quando aplicável. Na **Unidade III**, revisamos contratação, produtividade, custos, auditoria e ação corretiva.

CHEGOU O MOMENTO DAS AVALIAÇÕES

Antes de iniciar:

- **Guarde o celular** dentro da bolsa; ou
- **Deixe o celular** na mesa da professora.



O celular **não pode permanecer sobre a sua mesa** durante a avaliação.