GESTÃO ESTRATÉGICA DE TECNOLOGIA DA INFORMAÇÃO

MÓDULO III — UNIDADE III | 22/10/2026

Auditoria de sistemas orientada pelo COBIT

Técnicas e ferramentas de auditoria de sistemas orientadas pelo COBIT. A aula percorre a relação entre objetivos do negócio, riscos, controles, evidências e recomendações de auditoria.



O SISTEMA FUNCIONA, MAS ESTÁ SOB CONTROLE?

Uma empresa mantém seu sistema de vendas disponível e recebe pedidos normalmente.

Durante uma revisão, descobre-se que contas de funcionários desligados permanecem ativas e que alterações críticas não deixam registros suficientes.

A operação aparente não permite concluir que os riscos estejam controlados.

A auditoria verifica não apenas se a tecnologia entrega serviço, mas **se os controles são adequados, operam como previsto e produzem evidências confiáveis.**

O cenário é ilustrativo e será explicado pela professora, sem tarefa aos alunos.



REVISÃO SELETIVA — TERCEIRIZAÇÃO TAMBÉM EXIGE SUPERVISÃO

Na aula anterior, parcerias e terceirização foram tratadas como **decisões estratégicas de obtenção de capacidades de TI**, não como simples transferência de tarefas.

Contratos, níveis de serviço, riscos de dependência, custos totais e responsabilidades continuaram importantes mesmo quando a execução passou a um fornecedor.

A conexão com a auditoria é direta: **delegar a execução não elimina a necessidade de supervisão**, critérios de conformidade e evidências de que as obrigações estão sendo cumpridas.

Nesta aula, essas exigências passam a ser examinadas metodeticamente.

Executar fora ≠ deixar de controlar.



MAPA DA AULA — DA PERGUNTA À CONCLUSÃO

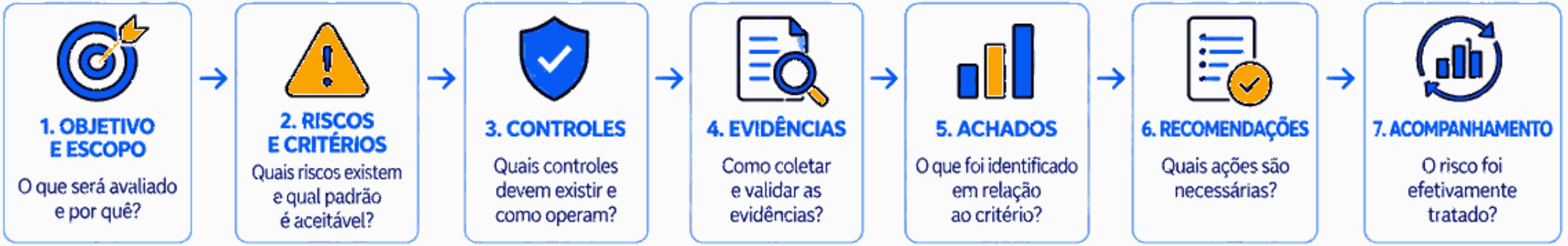
O **raciocínio da auditoria** pode ser entendido como um **encadeamento.**

Primeiro, definem-se **objetivo e escopo**: o que será avaliado e por quê. Depois, identificam-se **riscos e critérios**, para saber o que seria uma condição aceitável.

Em seguida, localizam-se **controles e coletam-se evidências**, mediante exame documental, entrevistas e testes. A comparação entre o critério e a situação observada fundamenta **achados, conclusões e recomendações**.

O **acompanhamento posterior** verifica se o risco foi efetivamente tratado.

O **COBIT** contribui como referência de objetivos e práticas de governança e gestão.



O QUE É AUDITORIA DE TI?

Auditoria de tecnologia da informação é um **processo sistemático de avaliação, sustentado por evidências**, de sistemas, práticas, controles e processos relacionados à informação e à tecnologia.

Seu propósito é oferecer uma **conclusão fundamentada** sobre aspectos como conformidade, confiabilidade, proteção de ativos, desempenho dos controles e exposição a riscos.

Não se limita a localizar erros em código: pode examinar **políticas, acessos, mudanças, continuidade, operações** e a forma como decisões tecnológicas são governadas.

Uma auditoria bem delimitada explicita **objeto, critérios, métodos e limitações** da conclusão.

AUDITORIA, MONITORAMENTO E GESTÃO: FUNÇÕES DIFERENTES

A **gestão implanta e opera controles**; o **monitoramento acompanha** o comportamento desses controles em intervalos definidos ou continuamente; a **auditoria avalia, com critérios e evidências,** se aquilo que foi estabelecido está adequadamente desenhado e funcionando.

Essas funções podem utilizar informações semelhantes, mas não têm o mesmo propósito.

Um painel operacional pode informar que o backup foi executado. A auditoria poderá verificar **se o backup abrange os dados críticos, se o registro é confiável e se a restauração atende ao requisito de recuperação.**

Também é necessário considerar a **independência e a objetividade** da função de auditoria.



GESTÃO

Implanta e opera controles

- Define políticas e procedimentos
- Executa as rotinas
- Mantém os controles em operação



MONITORAMENTO

Acompanha o comportamento

- Verifica se está ocorrendo
- Utiliza indicadores e alertas
- Identifica desvios em tempo hábil



AUDITORIA

Avalia com critérios e evidências

- Verifica se está adequado
- Analisa registros e testes
- Emite conclusão e recomendações

OBJETO, OBJETIVO, ESCOPO E CRITÉRIO

Objeto é o sistema, processo ou conjunto de controles examinado; **objetivo** é a pergunta que a auditoria pretende responder; **escopo** estabelece limites de unidades, sistemas, períodos e atividades; **critério** é o referencial usado para avaliar a condição observada.

Considere o acesso ao sistema financeiro: o objeto são os **controles de identidade e acesso**; o objetivo é **avaliar a adequação das permissões**; o escopo pode restringir-se a **contas privilegiadas de um trimestre**; os critérios podem incluir **política interna aprovada, obrigações aplicáveis e práticas selecionadas do COBIT**.

Sem essa distinção, a auditoria corre o risco de concluir além do que investigou.



AUDITORIA BASEADA EM RISCOS — ONDE CONCENTRAR A ATENÇÃO

Auditorias não conseguem examinar tudo com a mesma profundidade. O **planejamento orientado por riscos** procura priorizar processos e controles cuja falha possa produzir consequências relevantes para os objetivos da organização.

A análise considera, conforme o contexto, **impacto potencial, probabilidade, criticidade da informação, histórico de incidentes, exigências regulatórias e mudanças recentes**.

Um sistema que calcula cobranças ou trata dados sensíveis poderá exigir atenção distinta de uma página informativa de baixo impacto.

Priorização **não significa ignorar áreas menos críticas**; significa justificar o uso limitado de tempo e recursos de auditoria.



RISCO, CONTROLE E EVIDÊNCIA NÃO SÃO SINÔNIMOS

Risco é a possibilidade de que um evento ou condição comprometa objetivos.
Controle é uma medida de prevenção, detecção ou resposta a esse risco.
Evidência é a informação utilizada para avaliar se o controle existe, está adequadamente configurado e funciona.

Exemplo: o **risco** é um usuário desligado continuar acessando informações confidenciais;
o **controle** previsto é revogar o acesso de acordo com o desligamento;
a **evidência** pode combinar solicitação de RH, registros de desativação e amostra de contas.

A simples presença de uma política não prova que as revogações ocorreram tempestivamente.



RISCO
Possibilidade de que um evento ou condição comprometa objetivos.

Exemplo:
Usuário desligado continuar acessando informações confidenciais.

→



CONTROLE
Medida de prevenção, detecção ou resposta a esse risco.

Exemplo:
Revogar o acesso de acordo com o desligamento.

→



EVIDÊNCIA
Informação utilizada para avaliar se o controle existe, está configurado e funciona.

Exemplo:
Solicitação de RH, registros de desativação e amostra de contas.

CONTROLES PREVENTIVOS, DETECTIVOS E CORRETIVOS

Um **controle preventivo** tenta reduzir a ocorrência de uma falha, como exigir autenticação multifator para acesso privilegiado.

Um **controle detectivo** identifica uma situação potencialmente irregular, como alertas sobre autenticações anômalas ou alterações não autorizadas.

Um **controle corretivo** busca restaurar uma condição aceitável após o evento, como revogar credenciais comprometidas e restaurar serviços.

Essas categorias dizem respeito à função do controle; não afirmam, por si, que ele seja eficaz. A **auditoria precisa avaliar se cada mecanismo cobre o risco relevante, opera com periodicidade apropriada e gera registros verificáveis.**



PREVENTIVO

Reduz a ocorrência de uma falha.

Exemplo:
Exigir MFA para acesso privilegiado.



DETECTIVO

Identifica uma situação potencialmente irregular.

Exemplo:
Alertas sobre autenticações anômalas ou alterações não autorizadas.



CORRETIVO

Restaura uma condição aceitável após o evento.

Exemplo:
Revogar credenciais comprometidas e restaurar serviços.

DESENHO DO CONTROLE VERSUS OPERAÇÃO EFETIVA

Avaliar o **desenho de um controle** significa examinar se sua concepção, caso executada como previsto, **é suficiente para tratar o risco**.

Avaliar a **efetividade operacional** significa verificar se ele **realmente funcionou**, durante o período e nas condições examinadas.

Uma política que determina revisão trimestral de acessos pode estar formalmente bem estruturada, mas os relatórios e aprovações podem demonstrar **atrasos, omissões** ou **ausência de revisão de contas críticas**.

Não se deve confundir existência documental, execução registrada e redução efetiva de exposição. São **perguntas diferentes** e exigem **evidências diferentes**.

DESENHO DO CONTROLE



Foi concebido corretamente?

- Concepção adequada para tratar o risco
- Regras, procedimentos e responsabilidades definidos
- Se executado como previsto, seria suficiente

OPERAÇÃO EFETIVA



Funcionou na prática?

- Executado conforme o previsto
- Registros e aprovações disponíveis
- Funcionou no período e nas condições examinadas
- Reduziu a exposição ao risco

O QUE TORNA UMA EVIDÊNCIA ADEQUADA

A auditoria necessita de **evidências pertinentes** à pergunta investigada e **suficientemente confiáveis** para sustentar uma conclusão.

A pertinência depende de sua relação com o **critério e o risco**; a confiabilidade exige considerar **origem, integridade, independência da fonte, possibilidade de alteração e contexto de produção.**

Uma captura de tela isolada pode mostrar a configuração atual, mas não necessariamente comprova que ela permaneceu ativa nos últimos três meses. Para afirmar conformidade histórica, podem ser necessários registros com **data, identificação de responsável, trilha de mudanças e procedimentos de validação.**

Volume de arquivos, por si só, não equivale a força probatória.



PERTINÊNCIA

- Relacionada ao critério e ao risco
- Responde à pergunta investigada
- Relevante para a conclusão



SUFICIÊNCIA

- Quantidade adequada
- Cobre o período analisado
- Permite uma conclusão fundamentada



CONFIABILIDADE

- Origem identificável
- Integridade da informação
- Menor possibilidade de alteração
- Contexto de produção



INDEPENDÊNCIA

- Fonte não envolvida na execução do controle
- Menor risco de viés
- Preferência por fontes primárias

DOCUMENTOS E REGISTROS COMO FONTES DE EVIDENCIA

Políticas, procedimentos, inventários, solicitações, aprovações, relatórios de execução, contratos e logs podem compor a **base documental da auditoria.** Cada tipo responde a perguntas distintas.

Uma **política estabelece a regra**; uma **autorização identifica decisão**; um **log pode registrar evento**; um **relatório de exceções** evidencia situações que merecem investigação.

O auditor precisa confirmar se o documento corresponde ao **objeto e período do exame,** se há **rastreabilidade** e se o registro representa o **processo real**.

Documentos sem **versão, autor, data ou origem conhecida** podem demandar confirmação adicional antes de sustentar conclusões.



POLÍTICA
Define diretrizes e regras.

↓

Qual é a regra estabelecida?



PROCEDIMENTO
Detalha como executar a atividade.

↓

Como deve ser executado?



INVENTÁRIO
Lista ativos, recursos ou informações.

↓

O que existe no ambiente?



SOLICITAÇÃO E APROVAÇÃO
Registra demandas e decisões.

↓

Quem solicitou e quem aprovou?



RELATÓRIO
Apresenta resultados e exceções.

↓

O que foi executado e quais exceções ocorreram?



LOG
Registra eventos gerados por sistema.

↓

Qual evento foi registrado e quando ocorreu?

TRILHA DE AUDITORIA: RECONSTRUIR O QUE ACONTECEU

Uma **trilha de auditoria** é um **conjunto ordenado de registros** que permite reconstituir eventos relevantes, incluindo, quando disponíveis, identidade, ação, momento, objeto afetado e resultado.

Em um sistema de pagamentos, a trilha pode relacionar solicitação, aprovação, alteração de dados bancários e efetivação da transação.

Seu valor não depende apenas de armazenar eventos: **horários coerentes, integridade, controles de acesso** aos registros, **retenção adequada** e **possibilidade de correlação** são fundamentais.

Quando eventos são registrados sem **identidade confiável** ou podem ser **alterados sem controle,** a capacidade de investigação diminui.



EXAME DOCUMENTAL: VERIFICAR A REGRA E SUA EXECUÇÃO

O **exame documental** consiste em analisar políticas, configurações, registros, contratos e demais artefatos vinculados aos critérios.

Não se limita à leitura superficial: verifica **consistência entre versões, aprovações, datas, escopos e eventos correspondentes.**

Por exemplo, ao examinar mudanças em produção, o auditor pode conferir solicitação, avaliação de impacto, aprovação, evidência de teste e registro de implantação.

A ausência de uma etapa pode representar **exceção,** mas sua importância deve ser analisada **à luz do critério** definido.

A descrição de métodos de avaliação por exame, entrevista e teste é compatível com a abordagem do **NIST SP 800-53A.**



ENTREVISTA:
COMPREENDER E CONFRONTAR PROCESSOS

A **entrevista estruturada ou semiestruturada** permite compreender responsabilidades, fluxos e práticas que não estão suficientemente claros nos documentos.

O valor da entrevista está em **esclarecer o processo e orientar a busca de evidências**; declarações isoladas geralmente não comprovam, por si, a execução recorrente de um controle.

Se um gestor afirma que os acessos são revisados mensalmente, essa afirmação deve ser **confrontada com relatórios, datas de aprovação e exceções registradas**.

Perguntas abertas tendem a revelar como a atividade ocorre; **perguntas de confirmação** ajudam a identificar detalhes verificáveis.

A postura deve preservar **objetividade e respeito às pessoas** avaliadas.

RELATO

O que a pessoa diz



- Explica como o processo funciona
- Pode indicar responsáveis e práticas
- Ajuda a identificar pontos de atenção
- É um insumo para direcionar a busca de evidências

COMPROVAÇÃO

O que demonstra que aconteceu



- Registros, relatórios, aprovações e logs
- Evidências com data e período
- Confirma a execução recorrente do controle
- Pode mostrar exceções ou desvios
- Sustenta a conclusão da auditoria

TESTE DE CONTROLE:
COMPARAR COMPORTAMENTO ESPERADO E REAL

Testar um controle significa **executar um procedimento definido** para observar se o comportamento real corresponde ao comportamento requerido.

Em um **teste de acesso**, pode-se verificar, em ambiente autorizado, se uma conta sem privilégio é impedida de realizar uma ação reservada. Em **teste de recuperação**, verifica-se se o procedimento de restauração alcança o objetivo previsto.

Os testes devem ter **autorização, escopo controlado** e **cuidado** para evitar impacto indevido em produção.

A escolha do método depende do controle, do risco e da evidência esperada: **não existe teste universal que resolva toda avaliação**.

1. COMPORTAMENTO ESPERADO



- Qual é o requisito?
- Como o controle deve se comportar?
- Qual o critério de avaliação?

2. TESTE



- Executar o procedimento definido.
- Em ambiente autorizado.
- Com escopo controlado.

3. RESULTADO OBSERVADO



- O que aconteceu na prática?
- O comportamento foi conforme o esperado?
- Há exceções?

4. CONCLUSÃO



- Controle operou como requerido?
- Evidência obtida sustenta a conclusão?
- Há necessidade de ação adicional?

AMOSTRAGEM: AVALIAR SEM EXAMINAR CADA REGISTRO

Quando há grande volume de transações, contas ou mudanças, a auditoria pode selecionar itens por **métodos de amostragem** coerentes com objetivo, risco, população e período.

A escolha deve ser documentada: amostras direcionadas a itens críticos ajudam a investigar riscos específicos, mas **não representam automaticamente o comportamento de toda a população.**

Amostragens **estatísticas** permitem inferências sob condições e premissas próprias; amostragens **não estatísticas** exigem cuidado ainda maior com o alcance da conclusão.

Encontrar uma **exceção** demanda compreender sua natureza, causa possível e eventual necessidade de **ampliar testes**, sem generalização precipitada.

POPULAÇÃO

Conjunto completo de itens a que a auditoria se refere.



AMOSTRA

Subconjunto de itens selecionados para exame detalhado.



Itens escolhidos conforme critérios definidos.

PONTOS IMPORTANTES

- Definir objetivo, risco, população e período.
- Documentar o método e os critérios de seleção.
- Entender o alcance da conclusão.
- Tratar exceções e avaliar a necessidade de ampliar testes.

PAPÉIS DE TRABALHO E RASTREABILIDADE DA CONCLUSÃO

Os **papéis de trabalho** documentam o percurso entre pergunta de auditoria, critério, procedimento executado, evidências examinadas e conclusão.

Essa documentação possibilita **revisão, transparência metodológica** e **recuperação das bases do relatório.**

Em vez de escrever apenas "acessos inadequados", o registro deve indicar **quais permissões foram analisadas, em que período, contra qual regra e quais exceções** sustentaram a conclusão.

Informações sensíveis, dados pessoais e credenciais devem receber **proteção proporcional ao risco.** Organizar evidências não significa expor indiscriminadamente os dados coletados.

1. PERGUNTA DE AUDITORIA



Qual é o controle a ser avaliado?

2. PROCEDIMENTO



O que foi feito para obter a evidência?

3. EVIDÊNCIA



Quais registros, documentos ou testes foram examinados?

4. CONCLUSÃO



O que a evidência permite afirmar?

COBIT:
REFERENCIAL PARA GOVERNANÇA E AUDITORIA

O **COBIT**, mantido pela **ISACA**, é um framework para governança e gestão da informação e tecnologia corporativas.

Não é um software de auditoria, nem uma lista automática de conformidades.

Seu modelo reúne **objetivos de governança e gestão, práticas, atividades e componentes** que permitem discutir o que deve ser alcançado e como o sistema de governança pode ser estruturado.

Na auditoria, objetivos e práticas selecionados podem apoiar a **formulação de critérios, planejamento de procedimentos e identificação de evidências.**

A escolha deve considerar os **objetivos organizacionais, os riscos e o contexto**, sem exigir aplicação indistinta de todos os objetivos a cada auditoria.



REFERENCIAL

Fornece objetivos, práticas e componentes para estruturar governança e apoiar auditorias.

≠



SOFTWARE

Não é uma ferramenta que executa auditorias nem gera automaticamente listas de conformidade.

OBJETIVOS COBIT E CRITÉRIOS DE AVALIAÇÃO

O **COBIT 2019** apresenta um modelo central com **40 objetivos de governança e gestão,** conectados a propósitos, práticas e processos.

Esses elementos oferecem **linguagem estruturada para relacionar riscos e responsabilidades** a aspectos verificáveis.

Numa auditoria de mudanças em sistemas, por exemplo, o objetivo selecionado orienta a observação de **autorizações, testes, documentação e tratamento de mudanças.**

Não basta mencionar "conforme COBIT" de modo genérico: a análise deve **identificar o objetivo ou prática pertinente**, delimitar o critério específico, **executar procedimentos e registrar a evidência** encontrada.

O **critério concreto** deve ser comunicado de forma compreensível.

OBJETIVO COBIT



Resultado de governança ou gestão a ser alcançado.

PRÁTICA



Como o objetivo pode ser implementado.

CRITÉRIO



O que será verificado na auditoria.

EVIDÊNCIA



Registros, testes ou documentos que comprovam o critério.

DSS05:
SERVIÇOS DE SEGURANÇA GERENCIADOS

O objetivo **DSS05**, do modelo COBIT 2019, trata da **gestão de serviços de segurança.**

Numa abordagem de auditoria, ele pode servir de referência para organizar questões sobre **proteção de informação, controle de acesso, operação de mecanismos de segurança** e resposta relacionada à proteção dos serviços.

O foco da aula não é decorar todas as práticas desse objetivo, mas compreender a tradução metodológica: **risco identificado, controle esperado** e **evidência** capaz de demonstrar a operação.

Um cenário ilustrativo é a análise de **permissões privilegiadas** e da **revogação de contas** após desligamentos. Critérios locais e obrigações legais continuam necessários.

RISCO IDENTIFICADO

Acesso indevido e uso de contas privilegiadas.



- Contas privilegiadas sem necessidade.
- Contas não revogadas após desligamento.
- Uso indevido de acessos em sistemas críticos.

CONTROLE ESPERADO

Gestão de identidades e acessos.



- Concessão e revisão de acessos.
- Revogação tempestiva de contas.
- Monitoramento do uso de privilégios.

EVIDÊNCIA

Registros que comprovam a operação do controle.



- Registros de criação, alteração e revogação de acessos.
- Relatórios de revisão periódica de privilégios.
- Evidências de tratamento de contas após desligamento.

BAI06: MUDANÇAS GERENCIADAS

O objetivo **BAI06**, no COBIT 2019, refere-se a **mudanças de TI gerenciadas.**

Uma auditoria pode analisar se mudanças relevantes foram **solicitadas, avaliadas, aprovadas, testadas e registradas** segundo critérios estabelecidos, inclusive quando houver necessidade de tratamento emergencial.

O risco subjacente é que alterações insuficientemente controladas provoquem **indisponibilidade, erro, fraude ou exposição de dados.**

Para avaliar efetividade, o auditor **relaciona o registro da mudança ao momento da implantação e às aprovações aplicáveis,** evitando concluir conformidade apenas por existir um formulário padrão.

A natureza do processo e sua criticidade orientam **profundidade e seleção das evidências.**

SOLICITAÇÃO



Registro da necessidade e da justificativa.

AVALIAÇÃO



Análise de impacto, risco e impactos em serviços.

APROVAÇÃO



Autorização pelas instâncias responsáveis.

IMPLANTAÇÃO



Execução, teste e registro da implementação.

DSS04: CONTINUIDADE GERENCIADA

O objetivo **DSS04** está relacionado à continuidade, permitindo estruturar questões de auditoria sobre **preparação para interrupções e capaçidade de retomada dos serviços.**

Dispor de um plano de contingência **não equivale a comprovar** que ele poderá ser executado no tempo exigido pelo negócio.

A avaliação pode examinar **responsabilidades de acionamento, dependências, cópias de segurança, comunicação e registros de exercícios ou restaurações.**

Uma conclusão robusta precisa distinguir **plano existente, testes realizados e resultados alcançados,** respeitando limites de escopo.

Continuidade é relevante porque conecta a **capacidade técnica de recuperração ao impacto organizacional** da indisponibilidade.

1. INCIDENTE



Interrupção ou indisponibilidade do serviço.

2. ACIONAMENTO



Execução dos procedimentos e responsabilidades definidas.

3. RECUPERAÇÃO



Restauração dos serviços conforme o plano.

4. VALIDAÇÃO



Testes e registros que comprovam o resultado.

MEA02: CONTROLES INTERNOS GERENCIADOS

No COBIT 2019, o objetivo **MEA02** se refere ao **sistema de controles internos gerenciado.** Sua contribuição à auditoria é evidenciar a necessidade de acompanhar, avaliar é tratar **fragilidades de controles** dentro da organização.

Isso não significa que a área auditada e a auditoria independente exerçam a mesma função: **os responsáveis pelos processos** precisam manter seus controles, enquanto a auditoria realiza sua própria avaliação conforme mandato e escopo.

Quando uma falha é identificada, importam a **documentação da exceção, a atribuição de responsabilidade** e a **verificação de medidas corretivas.**

A simples abertura de um plano de ação **não prova sua efetividade.**



PLANO DE AÇÃO
Registra a intenção de corrigir a fragilidade.





CORREÇÃO COMPROVADA
Demonstra, por evidências, que o controle foi efetivamente implementado e está funcionando.

COMO NASCE UM ACHADO DE AUDITORIA

Um achado descreve uma **diferença relevante entre o critério de avaliação** e a **condição evidenciada**.

Para que seja útil, deve indicar com precisão a **situação observada, o requisito ou expectativa não atendida, os efeitos ou riscos associados** e, quando sustentado, a **causa provável**.

Exemplo ilustrativo: o procedimento exige revogação de acesso após desligamento; registros mostram contas ainda ativas além do prazo aplicável. A auditoria relata o **desvio comprovado e sua exposição,** sem imputar culpa pessoal ou afirmar consequências não demonstradas.

A formulação precisa separar **fato constatado de hipótese** que ainda requer validação.

CRITÉRIO DE AVALIAÇÃO



O que deveria ocorrer segundo norma, política ou procedimento.

CONDIÇÃO EVIDENCIADA



O que foi efetivamente observado nos registros, testes ou entrevistas.

RISCOS / EFEITOS



Quais impactos podem resultar da diferença identificada.

EVIDÊNCIA



Registros, dados ou testes que comprovam a condição observada.

CAUSA, EFEITO E RECOMENDAÇÃO: RIGOR NA INTERPRETAÇÃO

A **causa** explica por que uma falha ocorreu, mas nem sempre é possível estabelecê-la apenas com os registros inicialmente examinados.

O efeito pode representar uma **consequência observada** ou um **risco potencial:** essas duas situações devem ser diferenciadas.

Recomendações não deveriam limitar-se a "cumprir a política"; precisam **direcionar o tratamento da fragilidade, propor responsabilidade clara e permitir verificação posterior.**

Se as contas persistem ativas por falha de integração entre RH e identidade, uma resposta pode incluir **integração, controle de exceções e acompanhamento de revogação.**

A adequação dependerá da avaliação do **contexto e do risco residual.**



CONDIÇÃO

O que foi observado nos registros, testes ou entrevistas.



HIPÓTESE DE CAUSA

Por que a falha pode ter ocorrido (com base nas evidências disponíveis).



RESPOSTA VERIFICÁVEL

O que fazer, quem é responsável e como acompanhar para evitar recorrência.

RELATÓRIO:
COMUNICAR RISCO E EVIDÊNCIA PARA DECISÃO

O relatório de auditoria deve comunicar **objetivo, escopo, critérios, procedimentos** em nível apropriado, **constatações relevantes, conclusões e limitações.**

A clareza importa tanto quanto o rigor técnico: dirigentes precisam compreender qual **condição foi constatada, qual risco representa, o que sustenta a avaliação e qual decisão é requerida.**

A classificação de prioridade deve seguir critérios da organização ou da metodologia adotada, sem fabricar escalas universais.

Também é importante apresentar **contexto e manifestação dos responsáveis,** quando cabível, preservando a objetividade.

A auditoria produz **informação para governança e melhoria**; ela não substitui a responsabilidade da gestão por decidir e executar correções.



FOLLOW-UP:
VERIFICAR SE O RISCO FOI TRATADO

O acompanhamento de achados, também chamado **follow-up**, verifica se **medidas pactuadas foram efetivamente implementadas** e se respondem à fragilidade identificada.

A ação "publicar uma nova política" pode não resolver uma falha operacional de revogação de acessos; seria necessário observar **se o processo passou a funcionar e se novas exceções foram tratadas.**

Prazo, responsável, comprovação e situação atual precisam estar claros.

A auditoria não deve marcar um problema como resolvido apenas porque alguém informou sua conclusão.

A decisão sobre aceitação formal de risco remanescente deve observar as **autoridades definidas pela governança.**



AUDITORIA CONTÍNUA E USO DE DADOS

A auditoria contínua utiliza **procedimentos e análise de dados executados de forma mais frequente ou automatizada** para identificar condições que merecem verificação.

Regras de detecção podem sinalizar contas privilegiadas inativas, mudanças fora de janela autorizada ou ausência de registros de execução.

Isso amplia a cobertura temporal, mas **não elimina riscos de falsa indicação, falhas de dados ou interpretação inadequada.**

Painéis e alertas oferecem sinais; conclusões continuam exigindo **critérios, validação, julgamento profissional e documentação.**

É importante **diferenciar auditoria contínua de monitoramento contínuo** operado pela gestão, ainda que possam aproveitar tecnologias semelhantes.



IA E AUDITORIA: NOVOS OBJETOS, NOVAS CAUTELAS

Sistemas com inteligência artificial introduzem **questões auditáveis** como **origem e qualidade de dados, regras de acesso, supervisão humana, mudanças em modelos, rastreabilidade de resultados e gerenciamento de riscos de uso.**

Ferramentas de IA também podem **apoiar auditorias na triagem de documentos e identificação de padrões,** mas suas saídas exigem revisão e proteção de informações sensíveis.

A evolução profissional recente, refletida na **atualização do ITAF pela ISACA em 2026,** amplia a atenção à **governança de IA, análise de dados e mecanismos de avaliação contínua.**

Não se deve atribuir à IA capacidade automática de produzir **evidência independente e conclusão confiável.**

AUDITAR IA



Dados
Origem, qualidade e uso.

Controles
Acesso, supervisão humana e mudanças em modelos.

Rastreabilidade
Como os resultados são gerados e registrados.

Riscos de uso
Impactos e conformidade.

USAR IA NA AUDITORIA



Triagem de documentos
Classificação e organização.

Identificação de padrões
Análise de grandes volumes de dados.

Revisão humana
Validação das saídas e julgamento profissional.

Proteção de informações
Cuidado com dados sensíveis.

CASO DEMONSTRATIVO INTEGRADO: DESLIGAMENTO DE USUÁRIO

Considere um ambiente corporativo em que o RH comunica desligamentos, a equipe de identidade administra credenciais e aplicações registram os acessos.

Objetivo da auditoria: avaliar se os acessos de pessoas desligadas são revogados conforme o critério aprovado.
Risco: uso indevido de contas remanescentes.

Controle: fluxo documentado de comunicação e revogação.

Evidências: registros de desligamento, datas de solicitações, logs de desativação e amostra de contas, com tratamento adequado de dados pessoais.

Se os registros revelarem exceções, a conclusão deverá delimitar período, população examinada, regra aplicável e alcance dos testes.

Caso demonstrado pela professora, sem atividade discente.



LIMITES DA AUDITORIA E RESPONSABILIDADE PROFISSIONAL

Uma auditoria oferece **conclusões relativas ao objetivo, ao período, à amostra,** aos critérios e aos procedimentos executados; não representa garantia absoluta de inexistência de falhas ou fraudes.

Limitações de acesso, qualidade insuficiente de dados ou cobertura restrita precisam ser explicitadas, pois afetam o alcance das conclusões.

O auditor deve adotar cuidado com **confidencialidade, integridade das evidências, conflitos de interesse e registro fiel de resultados.**

Ao detectar um risco, não deve **extrapolar os fatos nem assumir a gestão operacional** do controle auditado.

Essa distinção sustenta **independência e utilidade da avaliação** para a governança.

SÍNTESE INTEGRADA:
AUDITAR É PRODUZIR CONFIANÇA JUSTIFICÁVEL

A aula articulou uma sequência de decisões e evidências.

O **objetivo e o escopo** definem a pergunta; **riscos e critérios** estabelecem o que merece atenção e contra qual padrão comparar; **controles** explicam como a organização trata o risco.

Exames, entrevistas e testes produzem evidências; **a análise** converte diferenças comprovadas em **achados e recomendações**; **o follow-up** verifica a resposta.

O **COBIT** auxilia a organizar objetivos e práticas relevantes, mas não substitui a avaliação.

Auditoria de TI é, portanto, um instrumento de **confiança justificável** e de **melhoria da governança**, sempre com limites declarados e decisões de correção atribuídas aos responsáveis.



REFERÊNCIAS E BASES DE FUNDAMENTAÇÃO



Fontes institucionais e técnicas

- **ISACA.** COBIT 2019 Framework: Introduction & Methodology e Governance & Management Objectives.
- **ISACA.** Exploring COBIT 2019's Value for Auditors. 21/08/2019.
- **ISACA.** Atualização do ITAF (2026).
- **NIST.** SP 800-53A Rev. 5. 2022 (atualização 2025).



Fontes curriculares

- **Plano de Ensino 2026.2** — Gestão Estratégica de Tecnologia da Informação.
- **Cronograma de Aulas 2026.2.**
- **Guia de Preparação de Aulas 2026.2.**
- **Ementas e Bibliografias do PPC.**



Bibliografia oficial de apoio

- **BITTENCOURT,** C. M. A. Governança Corporativa e Compliance: Planejamento e gestão estratégica. Crontentus, 2020.
- **NEVES,** E. C. Fundamentos de governança corporativa: riscos, direito e compliance. Intersaberes, 2021.
- **BLOK, M.** Compliance e governança corporativa. Freitas Bastos, 2023.

Links completos das referências apresentados ao final deste roteiro DOCX.
Nota: exemplos de sistemas e situações são hipotéticos e didáticos; não constituem evidências de ocorrências reais.

KAHOOT!

Hora da revisão interativa

Vamos revisar os principais conceitos da aula.

