AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

AUDITORIA DE SISTEMAS
CONCEITOS DE AUDITORIA

ALGUNS CONCEITOS BÁSICOS

relacionados com qualquer tipo de auditoria

CAMPO

Compõe-se de aspectos como Objeto a ser fiscalizado, período e natureza da auditoria

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

CONTROLE

É a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos ou sobre produtos, para que não se desviem das normas preestabelecidas.

AUDITORIA DE SISTEMAS
CONCEITOS DE AUDITORIA

Controles Preventivos

Prevenir erros (senhas de acesso)

Controles Detectivos

Detectar erros, omissões ou atos fraudulentos (tentativas de acessos não autorizados)

Controles Corretivos

Reduzir impacto ou corrigir erros detectados

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

PROCEDIMENTOS DE AUDITORIA

Lista de pontos a serem verificados durante a auditoria (manuais de auditoria – TCU)

AUDITORIA DE SISTEMAS
CONCEITOS DE AUDITORIA

ACHADOS DE AUDITORIA

Fatos significativos observados pelo auditor durante a execução da auditoria.

→ Não só falhas e irregularidades, mas também pontos fortes. Para que conste no relatório, deve ser relevante e baseado em fatos e evidências irrefutáveis.

AUDITORIA DE SISTEMAS
CONCEITOS DE AUDITORIA

PAPEIS DE TRABALHO

São registros que evidenciam atos e fatos observados pelo auditor (planilhas, tabelas, etc.)

RELATÓRIO

São feitas as recomendações da auditoria.

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

PONTO DE CONTROLE

Situação do ambiente computacional considerada pelo auditor como sendo de interesse para validação e avaliação

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

NATUREZA DA AUDITORIA

Auditoria Interna

Realizada por departamento interno responsável pela verificação e avaliação de sistemas e procedimentos internos de uma entidade. Deve ser independente e prestar contas diretamente à direção da instituição

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

Auditoria Externa

Realizada por instituição externa e independente da entidade fiscalizada

Auditoria Articulada

Trabalho conjunto de auditorias internas e externas.

AUDITORIA DE SISTEMAS
CONCEITOS DE AUDITORIA

FORMA DE ABORDAGEM

Auditoria Horizontal

Com tema específico realizada em várias entidades ou serviços paralelamente.

Auditoria Orientada

Focada em uma atividade específica qualquer ou em atividade com fortes indícios de erros ou fraudes.

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

CONTROLE INTERNO

Verificação e validação dos seguintes parâmetros do Sistema de Informação:

- Fidelidade da informação em relação ao dado
- Segurança física
- Segurança lógica
- Confidencialidade
- Obediência à legislação em vigor
- Eficiência
- Eficácia
- Obediência às políticas e às regras de negócio da organização

AUDITORIA DE SISTEMAS

CONCEITOS DE AUDITORIA

QUANTO AO TIPO OU ÁREA ENVOLVIDA

Auditoria contábil

Auditoria programas de governo

Auditoria planejamento estratégico

Auditoria administrativa

Auditoria de sistemas

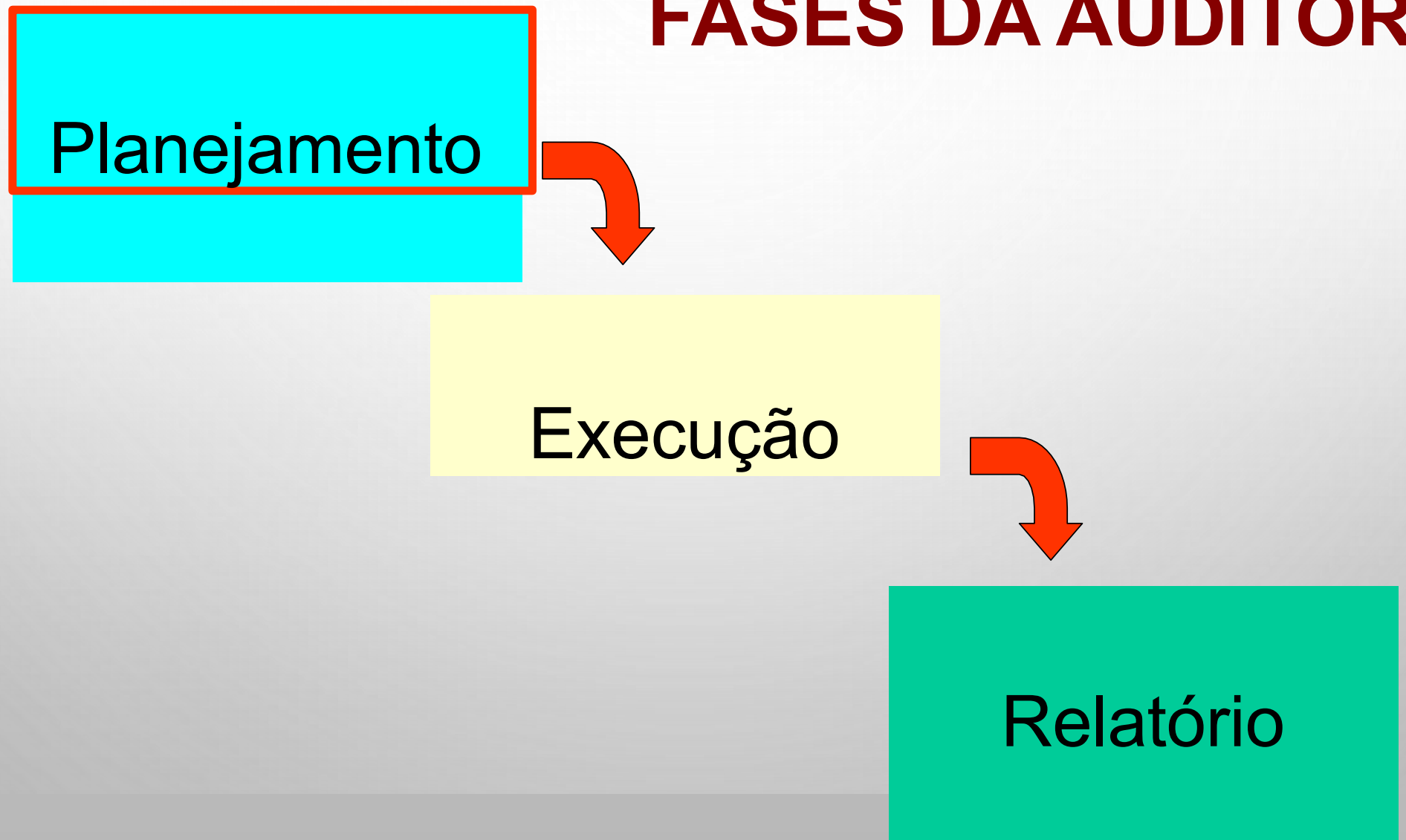
FASES DA AUDITORIA

Planejamento

Execução

Relatório

FASES DA AUDITORIA



PLANEJAMENTO DA AUDITORIA

Pesquisar Fontes de Informação

Definir Campo, Âmbito e Sub-Áreas

Definir os Recursos Necessários

Metodologia

Definir Objetivos e Procedimentos

PESQUISAR FONTES DE INFORMAÇÃ

- DEIXAR O MÁXIMO DE INFORMAÇÕES DISPONÍVEIS.
- ESTABELECER OS RECURSOS E CONHECIMENTOS TÉCNICOS NECESSÁRIOS.
- EXEMPLOS: HARDWARE, SO, SISTEMAS DE SEGURANÇA, APLICATIVOS E RESPONSÁVEIS PELA ÁREA.

DEFINIR OS RECURSOS NECESSÁRIOS

Humanos: equipe escolhida de acordo com o grau de complexidade, componentes e ferramentas utilizadas.

Econômicos: previsão de gastos.

Técnicos: levantar dispositivos de hardware, software e documentos técnicos a serem utilizados.

DEFINIR A METODOLOGIA

Entrevistas: utilizadas para apresentação, coleta de dados, discussão e encerramento.

Técnicas e Ferramentas

Verificação de Controles de Sistemas: sistemas operando de forma correta e produzindo dados fidedignos.

Exemplo: simulações, comparação de programas, mapeamento e rastreamento do processamento.

Análise dos Dados: Amostragens e Logs.

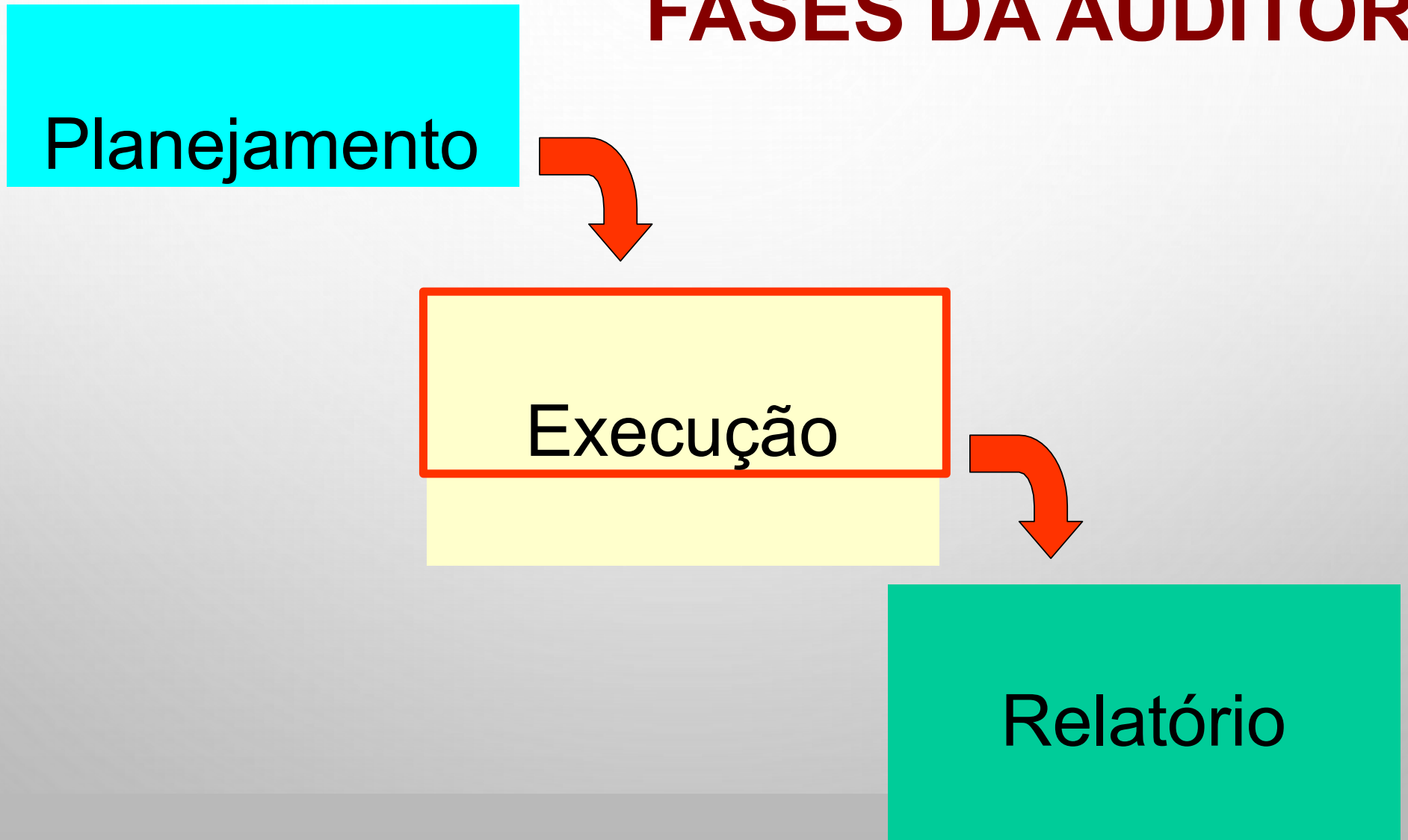
DEFINIR OBJETIVOS E METODOLOGIA

Norteiam a auditoria em várias áreas especializadas e organizacionais.

Avaliador deve utilizar um modelo normativo, um conjunto de padrões, de como a atividade deveria estar sendo feita.

O modelo normativo é traduzido em objetivos de controle a serem avaliados pelo auditor em cada área específica.

FASES DA AUDITORIA



EXECUÇÃO DA AUDITORIA

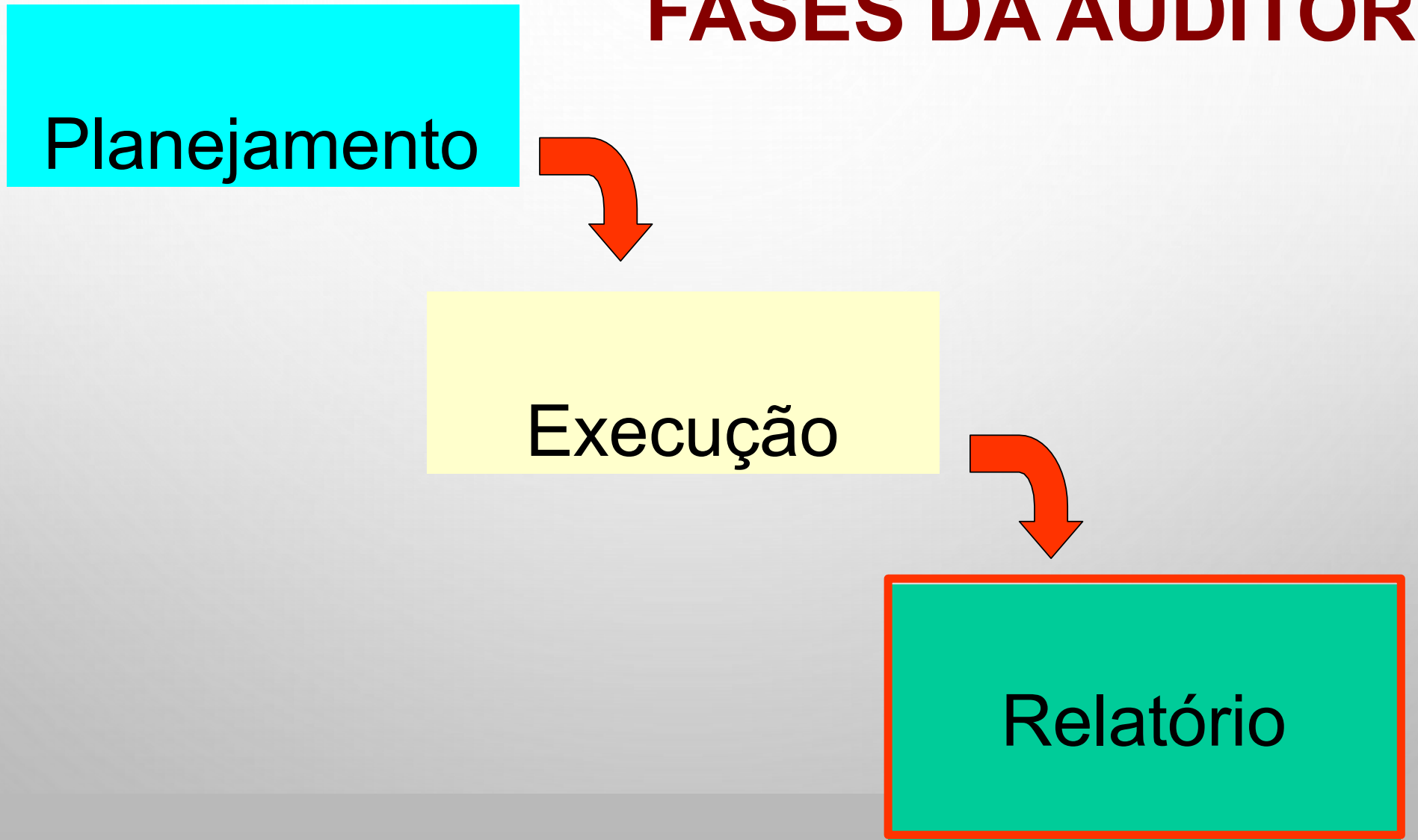
- EQUIPE DEVE REUNIR **EVIDÊNCIAS CONFIÁVEIS**, RELEVANTES E ÚTEIS PARA OS OBJETIVOS DA AUDITORIA.
- TODAS ESSAS EVIDÊNCIAS DEVEM ESTAR **ORGANIZADAS NOS PAPÉIS DE TRABALHOS**, PARA FACILITAR A ELABORAÇÃO DO RELATÓRIO.

EXECUÇÃO DA AUDITORIA

Tipos de Evidências:

- Físicas
- Documentárias
- Fornecidas pelo Auditado
- Analíticas (comparações, cálculos, etc)

FASES DA AUDITORIA



RELATÓRIO

O relatório final deve conter evidências, conclusões, recomendações e determinações.

Deve ser claro, objetivo, sem uso exagerado de termos técnicos.

Estrutura Típica:

- Dados da entidade auditada
- Resumo
- Dados da auditoria
- Não-conformidades detectadas
- Conclusão

LEVANTAMENTO

- Informações iniciais
  - Objetivos institucionais
  - Legislação aplicável
  - Estrutura organizacional
- Avaliação dos Controles Internos
  - O auditor, para determinar a extensão e o alcance da fiscalização, deve examinar e avaliar o grau de confiabilidade dos controles internos

(Normas de Auditoria da Intosai)

AVALIAÇÃO DOS CONTROLES DE TI

- Avaliação limitada: avaliação menos profunda dos controles gerais e de aplicativos, que pode ser realizada por equipes compostas somente por auditores que não detenham conhecimentos específicos de TI. Os controles pertinentes são examinados na extensão necessária para o atendimento dos objetivos da auditoria.

AVALIAÇÃO DOS CONTROLES DE TI

- Controles Gerais
- Controles de Aplicativos
- Análise de Dados

CONTROLES GERAIS

- Políticas e padrões organizacionais, especialmente relacionados à TI
- Organização e administração da TI
- Segregação de funções
- Procedimentos de Segurança
- Controles físicos (de acesso e de ambiente)
- Controles lógicos de acesso

CONTROLES GERAIS

- Desenvolvimento de sistema e alterações de programas
- Plano de Continuidade de Negócios
- Computação de usuário final

CONTROLES DE APLICATIVOS

- Controles e procedimentos que garantem que apenas as transações válidas são processadas e registradas
- Controle no(a):
  - Entrada de Dados
  - Processamento de Dados
  - Saída de Dados

CONTROLE DE APLICATIVOS

- SÃO ESPECÍFICOS DOS SISTEMAS E SÃO IMPLEMENTADOS PARA PREVENIR, DETECTAR E CORRIGIR ERROS E IRREGULARIDADES EM TRANSAÇÕES DURANTE A ENTRADA, PROCESSAMENTO E SAÍDA DE DADOS
- POSSUI COMO OBJETIVO GARANTIR UM PROCESSAMENTO CONFIÁVEL E EXATO, A PARTIR DE CONTROLES INCORPORADOS DIRETAMENTE EM PROGRAMAS APLICATIVOS, NAS TRÊS ÁREAS DE OPERAÇÃO: ENTRADA, PROCESSAMENTO E SAÍDA DE DADOS

ANÁLISE DE DADOS

- Segundo princípios geralmente aceitos de auditoria, quanto menor a confiabilidade dos controles gerais ou de aplicativo (ou se esses não forem avaliados), maior a extensão dos testes necessários para determinar a confiabilidade dos dados
- Papel da evidência:
  - Única evidência para fundamentar um achado
  - Evidência auxiliar ou de ratificação
  - Informação geral (histórico, descrições etc.)

PLANEJAMENTO

- Nesta fase, deve ser definido:
  - Objetivo da auditoria
  - Objeto da auditoria
  - Universo a ser auditado (escopo)
  - Técnicas e procedimentos a serem utilizados
  - Critérios de auditoria
  - Etapas e cronogramas
  - Recursos humanos e materiais

ETAPAS DO PLANEJAMENTO

- Visão geral
- Avaliação dos Controles Internos
- Elaboração da Matriz de Planejamento

  – A Avaliação dos Controles Internos deve ser feita caso não tenha sido realizada a fase de Levantamento

VISÃO GERAL

- Objetivos institucionais
- Estrutura Organizacional
- Legislação Aplicável
- Práticas Administrativas
- Planos Estratégicos
- Descrição do Objeto da Fiscalização

CONHECENDO O AUDITADO

- Compreender o negócio é essencial para identificar os riscos e controles
- Direcionar os esforços da auditoria de forma mais eficiente
- Entender o negócio
  - Processos
  - Pessoas
  - Tecnologia

CONHECENDO O AUDITADO

- Algumas questões a serem respondidas
  - Existem problemas que o auditor deveria conhecer melhor?
  - Há alguma previsão de mudança na organização?
  - Quais são os principais sistemas e bases de dados?
  - Quem o auditor deve entrevistar para obter as informações de que necessita?

CONHECENDO O AUDITADO

- Fontes de informação:
  - Levantamento de auditorias anteriores
  - Relatórios de auditorias realizadas
  - Relatórios de auditoria interna
  - Discussão com a gerência e com outros auditores que já realizaram trabalhos na unidade a ser auditada
  - Orçamento da unidade auditada
  - Documentos de estratégia de TI ou Plano Diretor de TI
  - Legislação e normas aplicáveis
  - Entrevistas
  - Internet

MATRIZ DE PLANEJAMENTO

- Instrumento para organizar as informações relevantes do planejamento de um auditoria
- Homogeneização do entendimento da equipe e demais envolvidos quanto a:
  - O objetivo do trabalho
  - Os passos a serem seguidos
  - A estratégia metodológica a ser adotada
- Orienta os integrantes da equipe nas fases de execução e de elaboração do relatório

MATRIZ DE PLANEJAMENTO

Questões de Auditoria	Informações requeridas	Fontes de Informação	Detalhamento do Procedimento	Objetos	Membro responsável	Período	Possíveis Achados
Apresentar, em forma de perguntas, os diferentes aspectos que compõem o escopo da fiscalização e que devem ser investigados com vistas à satisfação do objetivo	Identificar as informações necessárias para responder à questão de auditoria	Identificar as fontes de cada item de informação requerida da coluna anterior. Estas fontes estão relacionadas com as técnicas empregadas	Descrever as tarefas que serão realizadas, de forma clara, esclarecendo os aspectos a serem abordados (itens de verificação ou *check list*)	Indicar o documento, o projeto, o programa. O processo ou o sistema no qual o procedimento será aplicado. Exemplos: contrato, folha de pagamento, base de dados, ata, edital, ficha financeira, processo licitatório, orçamento.	Pessoa(s) da equipe encarregada(s) da execução de cada procedimento	Dia(s) em que o procedimento será executado	Esclarecer com precisão que conclusões ou resultados podem ser alcançados

ELABORAÇÃO DA MATRIZ DE PLANEJAMENTO

- Elaborar o objetivo da auditoria, após o diagnóstico da situação, e determinar a linha de investigação, mediante a formulação das questões de auditoria
- Determinar, para cada questão de auditoria, possíveis achados, ou seja, onde se deseja chegar com a investigação
- Identificar as informações requeridas e onde as obter (fontes de informação)

ELABORAÇÃO DA MATRIZ DE PLANEJAMENTO

- Elaborar procedimentos e descrevê-los passo a passo, para colher informações, analisá-las e obter as evidências com objetivo de responder às questões de auditoria
- Identificar o membro da equipe responsável pelo procedimento
- Especificar o período de realização do procedimento (cronograma)
- Identificar os objetos que foram analisados (fase de execução)

EXECUÇÃO DA AUDITORIA

- Etapas da fase de execução:
  - Aplicação dos Procedimento definidos
  - Acumulação de Evidências
  - Desenvolvimento dos Achados
  - Elaboração da Matriz de Achados

DESENVOLVIMENTO DOS ACHADOS

- Consiste no acúmulo organizado de informações (ou evidências) apropriadas e necessárias para esclarecê-los e sustentá-los

ATRIBUTOS DE UMA ACHADO

- Condição (Situação Encontrada)
- Critério (Situação Desejada)
- Causas
- Efeitos

PREMISSAS DOS ACHADOS

- Os achados da auditoria devem levar em conta o nível de risco associado
- Bom senso em apresentar achados de baixo risco
- Deve-se ser realista, usar a empatia
- Cada falha apontada deve estar suportada por evidências e papéis de trabalho

MATRIZ DE ACHADOS

- Composta das seguintes informações:
  - Achado
  - Situação Encontrada
  - Critério
  - Evidência
  - Causas
  - Efeitos
  - Encaminhamento (Proposta)

MATRIZ DE ACHADOS

Achado	Situação Encontrada	Critério	Evidência	Causas	Efeitos	Encaminhamento
Correspondência com o Achado constante na Matriz de Planejamento	Situação existente, identificada e documentada durante a fase de execução da auditoria	Legislação, norma, jurisprudência, entendimento doutrinário ou padrão adotado	Informações obtidas durante a auditoria no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe	O que motivou a ocorrência do achado	Consequências do achado	Propostas da equipe de auditoria. Deve conter identificação do(s) responsável (is)
A1	...					
A2	...					
A*n*	...					

ELABORAÇÃO DO RELATÓRIO

- O Relatório de Auditoria é o instrumento formal e técnico por intermédio do qual a equipe de auditoria comunica:
  - O objetivo do trabalho
  - A metodologia (como foi executado)
  - Os achados (resultado obtido)
  - As conclusões (avaliações e opiniões)
  - A proposta (recomendações e determinações)

REQUISITOS DE UM RELATÓRIO EFETIVO

- Clareza
- Convicção
- Concisão
- Exatidão
- Relevância
- Tempestividade
- Objetividade

MONITORAMENTO

- Etapas da fase de monitoramento
  - Verificações das Ações Tomadas
  - Aplicação dos Procedimentos
  - Acumulação das Evidências
  - Elaboração da Matriz de Achados
  - Elaboração do Relatório

CONTROLES GERAIS DE TI

- Objetivo dos Controles
  - Prevenir fraudes, erros, desperdícios, abusos
  - Proteger o ativo
  - Assegurar a obediência às diretrizes, planos, normas e procedimentos
  - Assegurar a validade e integridade dos dados para tomada de decisão
  - Caráter preventivo
  - Voltados para a correção de desvios
  - Instrumentos auxiliares de gestão em todos os níveis hierárquicos

CONTROLES GERAIS DE TI

- Consistem na estrutura, políticas e procedimentos que se aplicam aos sistemas aplicativos e base de dados de uma organização
- Influem no ambiente em que os sistemas aplicativos e os controles irão operar
- Buscam garantir a integridade dos sistemas com um todo, incluindo todos os aplicativos, dados e arquivos.

CONTROLES GERAIS DE TI

- Durante uma auditoria em que seja necessário avaliar algum sistema ou base de dados em particular, é preciso inicialmente avaliar os controles gerais que atuam sobre a estrutura computacional da unidade auditada
- Um ambiente de controle estável e bem gerenciado reforça a efetividade dos controles de aplicativos

CONTROLES GERAIS DE TI

- Políticas e padrões organizacionais, especialmente relacionados à TI
- Organização e administração da TI
- Segregação de funções
- Procedimentos de Segurança
- Controles Físicos (de Acesso e Ambiente)
- Controles Lógicos de Acesso

CONTROLES GERAIS DE TI

- Desenvolvimento de sistema e alterações de programas
- Plano de Continuidade de Negócios (PCN)
- Computação de usuário final

NORMAS E PADRÕES EM AUDITORIA DE TI

- Constituição Federal
- Legislação Brasileira
- CobIT – Governança de TI
- NBR ISO/IEC 38500 – Governança de TI
- ITIL – Serviços de TI
- NBR ISO/IEC 20000 – Serviços de TI
- Série NBR ISO/IEC 27000 – Segurança da Informação
- Outros padrões