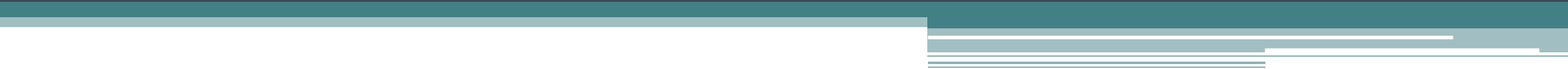


CONDUZINDO UMA AUDITORIA / AUDITORIA INTERNA E EXTERNA EM TI E SISTEMAS DE INFORMAÇÃO

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending from the left side of the slide towards the right, positioned below the main title.

Introdução

- Normalmente, as auditorias envolvem 4 fases e cada uma delas é dividida em seus respectivos estágios. São elas:
 - Planejamento.
 - Trabalho de campo.
 - Relatório de auditoria.
 - Acompanhamento.

Planejamento



Comunicação Inicial: O auditor notifica o cliente ou a entidade envolvida sobre a auditoria e seus objetivos por meio de uma carta ou e-mail.



Reunião Inicial de Preparação da Auditoria Interna: Clientes, auditores e outras partes interessadas realizam uma reunião de abertura na qual o cliente descreve as áreas a serem revisadas, recursos disponíveis, processos organizacionais e outras informações relevantes.



Levantamento Preliminar: Nesta etapa, o auditor coleta os dados necessários para obter uma compreensão abrangente da auditoria.

Planejamento




Análise da Estrutura de Controle Interno: Esta fase, que pode ser detalhada e apoiada por ferramentas e técnicas especializadas, ajuda o auditor a identificar as áreas prioritárias.




Elaboração do Programa de Auditoria: Este programa serve como um manual de processo, delineando o trabalho de campo necessário.

Trabalho de Campo

Testes para os controles internos críticos: Este processo avalia a precisão das transações selecionadas aleatoriamente.



Atualizações regulares sobre o progresso da auditoria para o cliente: O auditor periodicamente fornece relatórios ao cliente, principalmente por meio de comunicações verbais. O cliente também pode colaborar na resolução de questões levantadas.



Compilação da auditoria: Após a conclusão de todos os trabalhos de campo, o auditor resumirá suas descobertas, apresentará conclusões e oferecerá recomendações para abordar as questões identificadas.



Preparação dos papéis de trabalho: Esses documentos desempenham um papel fundamental na sustentação da opinião do auditor sobre a situação do cliente.

Relatório de Auditoria



Elaboração de relatório de auditoria: o relatório é analisado pela equipe de auditoria antes de apresentá-lo ao cliente. Às vezes, o projeto é apresentado ao cliente para revisão.



Criação do projeto de auditoria formal: comentários e sugestões, a partir do primeiro rascunho, são aplicados ao projeto formal.



Distribuição dos relatórios finais de auditoria para as pessoas envolvidas.

Acompanhamento



Revisão da auditoria de acompanhamento: a resposta do cliente será revista. As descobertas podem ser testadas e resolvidas.



Relatórios sobre a auditoria de acompanhamento. Os efeitos dos resultados resolvidos serão concluídos. Enquanto isso, os resultados não resolvidos também serão incluídos nos relatórios de acompanhamento.

Recomendações adicionais

Revisar o organograma do departamento ou divisão que será auditado.

Estudar as funções e nomes dos participantes da reunião de abertura.

Reafirmar o escopo da auditoria, conforme descrito no memorando de pré-auditoria da gestão.

Fornecer um cronograma detalhado do trabalho dentro do departamento e uma lista específica de processos a serem verificados.

Identificar o principal ponto de contato com o auditor.



Solicitar perguntas dos participantes sobre qualquer aspecto da auditoria.

Estimular a comunicação entre o departamento de auditoria e o departamento ou divisão auditados.

Confirmar a disponibilidade de espaço e conectividade necessários para conduzir a auditoria.

Ter um checklist com todos os critérios a serem auditados, considerando normas e procedimentos vigentes.

Utilizar perguntas abertas, como "O quê? Como? Quem? Quando? Por quê? Onde?".

Evitar questionar excessivamente e fazer observações.

Ir além das perguntas listadas.

Conversar com todos os níveis hierárquicos, não apenas com os superiores.

Utilizar termos como "fale-me" e "mostre-me" durante a auditoria.

Comportamento do Auditor

O profissional responsável pela auditoria deve ser imparcial, focando na avaliação do processo e suas etapas, incluindo o comportamento humano.

A ênfase deve ser na busca de oportunidades de melhoria, não na identificação de culpados ou não conformidades.

Antes da auditoria, é importante definir metas de pontos-chave em uma reunião com a equipe qualificada para a tarefa.

A auditoria é uma ferramenta valiosa para identificar melhorias, e todas as não conformidades devem ser registradas e tratadas com ações para atender aos critérios estabelecidos.

Pontos que não devem ser esquecidos

1

Determinar a conformidade do sistema com os requisitos especificados.

2

Determinar a eficácia do sistema.

3

Proporcionar ao auditado possibilidades de melhoria no sistema.

4

Auditoria não tem conotação punitiva, mas sim ação corretiva de aprimoramento.

Auditoria interna e externa em tecnologia da informação e/ou sistemas de informação

- Os tipos mais comuns de auditoria são classificados de acordo com os seguintes aspectos:
 - Quanto ao órgão fiscalizador.
 - Forma de abordagem do tema.
 - Tipo ou área envolvida.

Quanto ao órgão fiscalizador

- **Auditoria interna:** realizada pelo departamento interno responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade.
 - **Objetivo:** reduzir as probabilidades de fraudes, erros, práticas ineficientes ou ineficazes.
- **Auditoria externa:** realizada por instituição externa e independente daquela fiscalizada.
 - **Objetivo:** emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e a regularidade de suas operações.
- **Auditoria articulada:** trabalho conjunto de auditorias internas e externas.

Quanto à forma de abordagem do tema



Auditoria horizontal: auditoria com tema específico realizada em várias entidades ou serviços paralelamente.



Auditoria orientada: auditoria focada em uma atividade específica qualquer ou em atividades com fortes indícios de erros ou fraudes.

Quanto ao tipo ou área envolvida



Auditoria de programas de governo: acompanhamento, exame e avaliação da execução de programas e projetos governamentais específicos.



Auditoria do planejamento estratégico: verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias de aquisição, utilização e alienação de recursos são respeitadas.



Auditoria administrativa: engloba o plano da organização, seus procedimentos e documentos de suporte à tomada de decisão.



Auditoria contábil: relativa à salvaguarda dos ativos e à fidedignidade das contas da instituição. Tem como finalidade fornecer certa garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.



Auditoria financeira ou auditoria das contas: consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas.



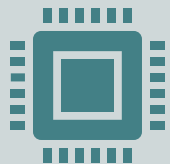
Auditoria de legalidade: também conhecida como auditoria de regularidade ou de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.



Auditoria operacional: incide em todos os níveis da gestão, nas fases de programação, execução e supervisão, sob o ponto de vista da economia, eficiência e eficácia. Analisa a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.



Auditoria integrada: inclui simultaneamente a auditoria financeira e a operacional.



Auditoria da tecnologia da informação: essencialmente operacional. Os auditores analisam os sistemas de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências. É também conhecida como auditoria informática, computacional ou de sistemas.

Auditoria interna

A auditoria interna, que anteriormente estava predominantemente ligada às finanças e frequentemente terceirizada, agora é um componente essencial para muitas organizações, exigindo a manutenção de um departamento de auditoria interna.

Para implementar e melhorar continuamente o sistema de gestão de segurança da informação, é necessário um programa anual de auditorias. Isso pode envolver auditorias únicas ou combinadas quando diferentes sistemas de gestão são auditados juntos.

O apoio da alta direção é crucial para o sucesso dos programas de auditoria, assim como a aplicação do ciclo **PDCA (Planejar, Fazer, Checar e Agir)** para garantir a melhoria contínua.

- O programa de auditoria deve definir objetivos relacionados a estratégias, conformidade com normas, requisitos dos clientes e regulamentações.
- A abrangência do programa varia de acordo com o tamanho, complexidade da organização e outras considerações.
- As responsabilidades do programa devem ser atribuídas a colaboradores qualificados, enquanto os recursos, incluindo financeiros, técnicos e humanos, devem ser alocados.

- Os procedimentos de auditoria devem ser definidos e abranger planejamento, seleção de equipes, acompanhamento e comunicação de resultados.
- Além disso, as empresas frequentemente estabelecem um **Comitê Corporativo de Segurança da Informação** e um **Security Officer** para garantir a eficácia das políticas de segurança e monitorar o progresso.

Auditoria externa

O auditor externo atua de forma independente, sem vínculo empregatício com a empresa, e colabora com o auditor interno para avaliar a eficácia dos sistemas. Geralmente, desempenha um papel de consultor.

A auditoria externa tem como objetivo verificar os controles dos sistemas da organização contratante, oferecer soluções e melhorias, emitir parecer sobre os processos auditados.

É um processo similar à auditoria interna, mas é conduzido por uma empresa ou instituição externa, que é imparcial e independente em relação aos resultados, evitando influências ou favorecimentos internos ou externos.

Metodologia de auditoria de tecnologia da informação

- Para operar em ambientes informatizados, os auditores precisam adquirir um conjunto específico de conhecimentos e habilidades. Isso inclui:
 - **Auditoria de Sistemas em Desenvolvimento:** Compreensão da metodologia de desenvolvimento de sistemas, técnicas de prototipação, elaboração de planos diretores de informática, documentação de sistemas e conhecimento em linguagens de programação.
 - **Auditoria de Sistemas em Operação:** Familiaridade com legislação e normas administrativas relevantes, software de segurança, controle de acesso, contratos de software e técnicas de amostragem.

- **Auditoria do Data Center:** Conhecimento de normas administrativas e técnicas, procedimentos operacionais, funções desempenhadas nas áreas de Processamento Eletrônico de Dados (PED) e Data Center, contratos de software e hardware.
- Essas habilidades são essenciais para conduzir auditorias eficazes em ambientes informatizados e garantir a conformidade com as regulamentações e normas aplicáveis. Além disso, os auditores devem estar atualizados em relação às evoluções tecnológicas e legais no campo da auditoria de sistemas.

- O objetivo do auditor é proporcionar uma perspectiva abrangente do trabalho. O foco principal é estabelecer um método de auditoria para sistemas computadorizados, com ênfase na perspectiva dos auditores externos.
- Ao realizar a auditoria de um sistema informatizado, a primeira ação importante é distinguir entre duas situações essenciais: sistemas em fase de desenvolvimento e sistemas em operação.
- Para sistemas em desenvolvimento, o auditor deve identificar os ciclos envolvidos e determinar os processos e técnicas de auditoria a serem empregados.

- Levantamento.
 - Planejamento.
 - Revisão.
 - Negociação com os gestores.
-
- Para os sistemas em operação, o auditor deve definir quais os encadeamentos de tarefas que contemplam o planejamento, a execução, a análise e a auditoria do Data Center.

Auditoria em sistemas em desenvolvimento



Auditar um sistema em fase de desenvolvimento requer um profundo conhecimento de análise de sistemas por parte do auditor. Portanto, para realizar essa tarefa complexa com sucesso, é recomendável que o auditor possua conhecimentos sólidos em auditoria e Processamento Eletrônico de Dados (PED).



É crucial que o auditor de sistemas em desenvolvimento compreenda metodologias, técnicas, papéis de trabalho, além de entender as funções desempenhadas por analistas, programadores e profissionais de suporte e operação. Em qualquer auditoria, é essencial seguir uma metodologia que assegure a independência do trabalho do auditor.



A auditoria de sistemas em desenvolvimento, em essência, envolve a avaliação dos recursos que serão utilizados no processo futuro, incluindo o ciclo de desenvolvimento do sistema, seus procedimentos e técnicas de auditoria, negociação e a elaboração do relatório de auditoria.

• **Processos e técnicas de auditoria de sistemas em desenvolvimento**

- Em uma abordagem básica, esses processos e técnicas compreendem as seguintes etapas:
 - Levantamento de informações,
 - Análise de risco,
 - Planejamento da auditoria do projeto,
 - Revisão do projeto PED (Processamento Eletrônico de Dados) e
 - Técnicas de auditoria de sistemas.

- **Levantamento de informações**

- O levantamento de informações é a primeira fase da auditoria de um sistema em desenvolvimento. Sua finalidade é propiciar o conhecimento do projeto a ser auditado e das características organizacionais do ambiente em que será executado.

- **Análise de risco**

- A análise de risco tem como base o cuidado que o auditor deve ter ao selecionar e classificar os projetos, de acordo com os critérios de importância para garantir que todos os novos sistemas críticos e importantes sejam revisados.
- Compreende também a detecção e aferição das áreas suscetíveis a incidência de erro, com base nos controles internos propostos nos projetos.

- A identificação das áreas e o dimensionamento do risco envolvido permitirão ao auditor determinar a amplitude e o aprofundamento dos procedimentos a serem aplicados, a delimitação do escopo e análise da relação custo/benefício da auditoria.

- **Planejamento da auditoria do projeto**

- Ao desenvolver o planejamento é fundamental que o auditor esteja atento às oportunidades de execução da auditoria, pois a temporariedade é fator de maior relevância e se não for planejada com rigor, poderá torná-lo inviável.

- O planejamento é feito observando-se a sequência de atividades: conhecimento do ambiente computacional, determinação e definição dos objetivos de validação dos pontos de controle, análise de sensibilidade do nível de interesse da validação, avaliação e hierarquização dos pontos de controle e documentação de todo o processo de planejamento.
- O planejamento objetiva um modelo operacional que seja capaz de refletir a cultura da empresa. Nessa fase, devem ser definidos o grupo de talentos necessários à equipe, quais papéis de trabalho serão utilizados e como escolher os projetos para serem revisados.
- A metodologia recomendada consiste nas seguintes etapas:



Auditoria da metodologia de desenvolvimento de sistemas: documentação do sistema, técnicas de análise estruturada.



Auditoria das especificações do sistema.



Auditoria da administração do projeto.



Auditoria de pré-implantação do sistema.

• **Revisão do Projeto de Processamento Eletrônico de Dados (PED) e Técnicas de Auditoria de Sistemas**

- A revisão do projeto de Processamento Eletrônico de Dados (PED) e as técnicas de auditoria de sistemas desempenham um papel crucial na avaliação e garantia da eficácia, segurança e conformidade dos sistemas de informação.
- A revisão do projeto de PED envolve a análise minuciosa da documentação do projeto para identificar problemas e garantir que o sistema seja projetado de acordo com as necessidades e padrões.
- As técnicas de auditoria de sistemas, como revisão de políticas, testes de segurança e análise de registros, são usadas para avaliar a operação, segurança e conformidade dos sistemas. Esses processos ajudam a mitigar riscos, proteger ativos de informação e manter a confiança dos stakeholders.

• Revisão do projeto

- A revisão do projeto começa com o levantamento de informações, como datas, equipe, recursos, interfaces, volume, valor das transações, quantidade de usuários.
- Essas informações são básicas para o planejamento. Em função delas o Controle de Qualidade dos Sistemas em Desenvolvimento (CQSD) determina os objetivos da revisão, em que se pode analisar todo o projeto ou apenas parte dele.

- Na execução do trabalho de revisão pode-se conduzir as tarefas de auditoria por meio de entrevista com usuários, entrevista com a equipe, análise da documentação do projeto, participação em reuniões.
- Essas tarefas permitem ao auditor/revisor a detecção de problemas que devem ser colocados em um nível gerencial, qual o risco e custo do controle, se o usuário os aceita.

• Técnicas de auditoria de sistemas

- Dentro das técnicas de auditoria de sistemas em desenvolvimento, destacam-se várias abordagens, incluindo a validação do processo de geração das especificações em cada fase da metodologia, a análise e acompanhamento das técnicas aplicadas e dos procedimentos seguidos.
- Além disso, a validação dos resultados gerados em cada etapa da metodologia é essencial para garantir a conformidade com as normas e a qualidade das especificações.
- As técnicas de auditoria de sistemas em desenvolvimento devem fornecer a capacidade de testar as técnicas de aprimoramento desses sistemas, que podem ser categorizadas da seguinte maneira:

- **Técnicas no ciclo de desenvolvimento do sistema:** uma aplicação dessas técnicas exige pelo menos que se faça:
 - Análise da metodologia de desenvolvimento de sistemas.
 - Análise da documentação de desenvolvimento de sistema.
- **Técnicas complementares:** são utilizadas três técnicas complementares ao sistema PED durante seu desenvolvimento.

Avaliação do Sistema Base (Base Case System Evaluation): Esta técnica é desenvolvida e aplicada durante a implantação do sistema e durante sua operação para rastrear alterações que ocorrem (a correção de falhas é feita antecipadamente, melhorando assim a qualidade dos primeiros processamentos reais).

Teste Integrado (Integrated Test Facility): Esta técnica é criada para simplificar a realização de testes de integração durante o desenvolvimento do sistema e pode ser usada durante a operação do ciclo (envolve o desenvolvimento de rotinas dentro dos programas para selecionar dados de testes de auditoria).

- **Arquivo de Revisão de Controle do Sistema (System Control Audit Review File):** Esta técnica é criada durante o desenvolvimento do sistema e é usada para gerar rotinas de auditoria específicas dentro dos programas, a fim de selecionar transações reais. É amplamente aplicada em sistemas em tempo real e pode ser usada tanto no ciclo de desenvolvimento quanto no ciclo de operação.

Negociação e elaboração do relatório



Essa etapa do processo de auditoria ocorre ao final de cada tarefa, bem como antes da elaboração do relatório final, sendo aplicável em auditoria contábil, auditoria de sistemas em desenvolvimento e operação.



Nesse estágio, o auditor tem a oportunidade de discutir as situações encontradas durante as fases da auditoria com o cliente, gerentes de sistemas ou supervisores, a fim de validá-las ou ajustá-las conforme necessário.



O propósito dessa negociação é analisar as recomendações e/ou negociar suas soluções. Uma vez concluídas todas as negociações consideradas necessárias pelo auditor, ele pode dar por encerrada a tarefa ou o trabalho, procedendo à elaboração e apresentação de um relatório que seja claro, coeso e preciso.