

Aula 1

Auditoria de Sistemas

Prof. André Roberto Guerra

Conversa Inicial

Organização da disciplina

- **Aula 1 - Conceitos básicos de auditoria de sistemas**
- **Aula 2 - Equipe de auditoria e as competências do auditor de SI**
- **Aula 3 - Planejamento de auditoria e pontos de controle**
- **Aula 4 - Controles internos**

- **Aula 5 - *Compliance*, normas, guias e procedimentos para auditoria**
- **Aula 6 - Ferramentas e *softwares* de auditoria de sistemas**
- **Aulas 7 a 10 - Aulas práticas - 1 a 4: resolução de exercícios propostos**

Aula 1 - Conceitos básicos de auditoria de sistemas

- **Definições de auditoria de sistemas**
- **Os objetivos**
- **As competências do(a) auditor(a)**
- **Roteiro e planejamento para elaboração**
- **Procedimentos - etapas da auditoria**

- **A evolução dos sistemas e dos processos de auditoria**
- **Identificação de atividades específicas de auditoria de sistemas de informação**
- **CobiT, ITIL e Normas ISO 17799/27002**

Definições de auditoria de sistema

- **Definição inicial e elementar - Auditoria:** exame analítico, minucioso, de investigação e validação de um sistema, atividade ou informação (Michaelis, 2017)
- **Auditar**, do latim de *auditu* - saber por ouvir

- **Auditoria é muito mais do que ouvir**, é um "retrato técnico" da organização e dos sistemas como um todo
- **Maior eficácia e eficiência**, seguindo princípios e normas com aplicações próprias e direcionando a entidade a melhores resultados

- **Sistema:** conjunto de elementos programados, inter-relacionados e interatuantes, que, quando processados, auxiliam na consecução dos objetivos dos negócios
- **Processo** que transforma dados de entrada, agregados aos comandos gerenciais, em saídas

- **Sistemas abertos** podem receber dados controlados e não controlados, pois recebem influência do ambiente interno e externo em que operam
- **Sistemas fechados**, devido à sua natureza, não têm interferência do ambiente e somente poderiam receber os dados controlados

Os objetivos

Objetivos globais de auditoria

- **Além dos objetivos listados**, a auditoria de sistemas possui alguns objetivos globais que identificam os controles e avaliam os riscos dos sistemas, permitindo ao auditor obter conclusões (Imoniana, 2016).

▪ **Integridade**

- ABNT (2005) cita alguns procedimentos de revisão dos controles internos. Na categoria A.12.2 - O processamento correto de aplicações

▪ **Confidencialidade**

- No COBIT, são descritos, pelo objetivo PO2.3 - Esquema de classificação de dados
- ABNT (2005) - item 12.4.3 - Controle de acesso ao código-fonte do programa

▪ **Privacidade**

- ABNT (2005) - item 11.5.1 - Procedimentos seguros para entrada no sistema

▪ **Acuidade**

- ABNT (2005) - item 12.2 que trata do processamento correto das aplicações

▪ **Disponibilidade**

- COBIT - Processo DS4 - Assegurar a continuidade dos serviços
- ITIL - Processo de gerenciamento de disponibilidade

▪ **Auditabilidade**

- As trilhas de auditoria - *audit trails* - podem ser aplicadas nesse contexto
- COBIT - objetivo AI2 - Adquirir e manter *software* aplicativo e AI2. 3 - Controle e auditabilidade do aplicativo

- ABNT (2005) - item A.15.1 - Conformidade com requisitos legais *compliance*

• Alguns dos subitens desse item são:

- ✓ a) proteção de dados e privacidade da informação pessoal;
- ✓ b) prevenção de mau uso de recursos de processamento da informação.

- Versatilidade
 - Usabilidade do sistema
- Manutenibilidade
 - COBIT - objetivo AI 2.2 - Projeto detalhado - dentro do objetivo AI2 – Adquirir e manter *software* aplicativo. AI6 - Gerenciar mudanças - e AI7 – Instalar e homologar soluções e mudanças

As competências do(a) auditor(a)

- A composição da equipe deve ser feita por auditores selecionados e recrutados conforme conhecimentos e habilidades nas áreas de sistemas e de negócios
- Etapas básicas para a aplicação do programa de auditoria
- Tabela 1 – Competência e perfis do auditor de sistemas

Roteiro e planejamento para elaboração

- CobiT (Control Objectives for Information and related Technology) - ponto de partida para a identificação das atividades
- ITIL (Information Technology Infrastructure Library) e ISO 17799/27002 - aspectos ligados a sistemas de gestão
- Norma ABNT 19011 - Diretrizes para auditoria de gestão de sistemas.

- A organização dos trabalhos de auditoria segue a norma de execução de trabalhos do auditor, o principal componente das normas de auditoria geralmente aceitas.

- Contempla, entre outros: planejamento de auditoria, avaliação de riscos de auditoria, supervisão e controle de qualidade, documentação da auditoria, avaliação da continuidade normal dos negócios da entidade, aplicação de amostragem estatística.

- Para simplificar, adotam-se as seguintes estruturas didáticas: planejamento; escolha da equipe, programação da equipe; execução e documentação de trabalho; supervisão em campo; revisão dos papéis de trabalho, conclusão e emissão (*follow-up*) de relatórios; atualização do conhecimento permanente e avaliação da equipe.

Planejamento

- Apoiada em níveis de riscos aparentes, é imprescindível para melhor orientar o desenvolvimento dos trabalhos
- Matriz de risco: desde os primeiros trabalhos e permanentemente atualizada
- Exemplo: memorando de planejamento de auditoria de sistemas

Procedimentos: etapas da auditoria

- Os procedimentos de auditoria de sistemas devem ser entendidos como um conjunto de etapas e atividades bem distribuídas, que são planejadas, executadas e avaliadas por diversas partes interessadas, ocorrendo antes, durante e depois de uma auditoria.

- É possível pensar em aplicar uma metodologia de trabalho flexível e aderente a todas as modalidades da auditoria em sistemas de informação e que não se distancie de melhores práticas.

▪ A metodologia pode ser composta pelas seguintes etapas:

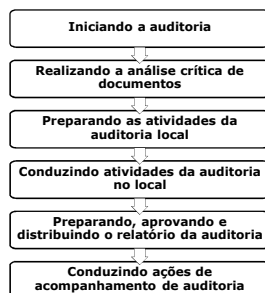
- a) planejamento e controle do projeto de auditoria de sistemas;
- b) levantamento do sistema de informação a ser auditado;

- c) identificação e inventário dos pontos de controle;
- d) priorização e seleção dos pontos de controle do sistema auditado;
- e) avaliação dos pontos de controle;
- f) conclusão da auditoria;
- g) acompanhamento da auditoria.


▪ O desenvolvimento de um roteiro baseado na organização sugerida, onde os procedimentos ficam bem distribuídos no roteiro, assim com as atividades de revisões e avaliações dos processos e rotinas de auditoria (Lyra, 2015).

- Os procedimentos de auditoria devem contemplar a avaliação de:
- a) dados e informações que compõe os resultados do sistema;
 - b) as rotinas de processos do sistema.

▪ ABNT (2002)



Finalizando

- 
- Apesar de autores considerarem diferentes etapas de auditoria, elas podem ser resumidas em planejamento de auditoria, execução de procedimentos de auditoria e as conclusões de auditoria
 - Com base nessas etapas citadas, o roteiro de auditoria começa a ser formado