Aula 3

Auditoria de Sistemas

Prof. André Roberto Guerra

Conversa Inicial

Aula 3: Planejamento de auditoria e Pontos de Controle

- **O planejamento de auditoria de sistemas**
- **Os detalhes do planejamento**
- **A criação do plano de auditoria**
- **Análise e definição dos pontos de controle**
- **Preparação e execução de atividades**

- **A primeira atividade é a de identificar um modelo, um conjunto de orientações para a definição de um planejamento das auditorias de SI.**
- **O plano deverá sintetizar a natureza, os objetivos, os recursos e o período de tempo relativos a cada auditoria, devendo ser aprovado pelo comitê de auditoria da organização.**

- **Para início das atividades o auditor deve possuir pleno conhecimento dos pontos de controle. Serão os principais meios de obtenção de evidências durante toda a auditoria.**

- **Ponto de controle é a situação do ambiente computacional caracterizada pelo auditor como de interesse para validação e avaliação. Também caracterizado como uma combinação de rotinas e informações operacionais de controle (Gil, 99).**

O planejamento de auditoria de sistemas

- A principal atividade de início é conhecer o ambiente a ser auditado. (hardware, software, área de programação e análise, se há operações de TI, estrutura da TI e produtos obtidos por meio do sistema.

- Mais do que indicar "o que" auditar, é também um instrumento para determinar "quando" e com que "frequência" se deve auditar.
- Surge então o questionamento: por que auditar?

- A resposta está no risco.
  - No planejamento devem ser escolhidos os processos e os SI de maior risco para o negócio.

- Detalhes a observar, a documentação inicial deve seguir alguns pontos:
  - a) identificação dos sistemas-chaves;
  - b) descrição do sistema;

  - c) descrição do perfil do sistema;
  - d) documentação da visão geral;
  - e) descrição de riscos dos aplicativos.

- Como elaborar um planejamento de Auditoria que leve em conta o negócio e os seus riscos? A abordagem ao risco é o instrumento chave - todo o plano deve seguir.
- O (IIA, 2006) tece um conjunto de considerações sobre elaboração do planeamento de Auditorias de SI

- Evitar o uso de definições / designações de Auditorias muito abrangentes
- O planejamento deve tocar todos os níveis de SI
- O planejamento deve prever Auditorias que formem conjuntos lógicos de relatórios sobre determinados temas
- O planejamento e respectivo orçamento devem cobrir os riscos de forma apropriada

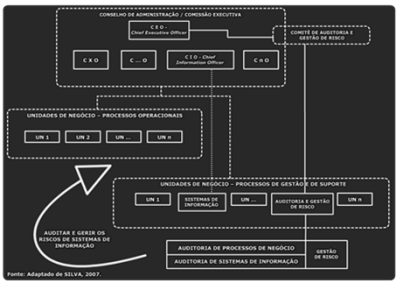
Os detalhes do planejamento

- Planejamento inicial é um direcionamento e coordenação para a execução da auditoria. Agrega todos os processos de auditoria elencados:

  a) conhecimento do ambiente;
  b) estabelecimento de estratégias;
  c) aplicação de técnicas;
  d) análise de etapas executadas;
  e) relatórios finais.

- A norma ABNT considera alguns itens:
  - a) objetivos da auditoria;
  - b) o escopo da auditoria;
  - c) as datas e lugares nas quais as atividades de auditoria serão realizadas;

- d) definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas;
- e) os principais pontos do relatório de auditoria;
- f) quaisquer ações de acompanhamento de auditoria.



A criação do plano de auditoria

- **O escopo da auditoria delimitado por meio do conhecimento do ambiente adquirido pela compreensão do fluxo do sistema.**
- **É apresentado o modelo que contempla importantes questões.**

	QUESTÕES	S/N	DOCUMENTOS/ ARTEFATOS REFERÊNCIA
1	Há padrões de documentação para programas de sistema ERP que estão configurados para executar em modo batch?		
2	Está sendo usado o padrão de documentação?		
3	Há softwares de apoio à documentação do sistema ERP a serem auditados?		
4	Existe trilha de auditoria do sistema ERP? (logs)		
5	Existem arquivos/relatórios/registros de controle no sistema?		
6	As alterações de programas dos módulos do ERP, são controladas e registradas?		
7	Existe grau de sigilo de arquivos e programas consoantes norma estabelecida?		
8	Existe documentação referente ao sistema ERP, quanto a processos, manutenções no sistema?		
9	Existem procedimentos documentados descrevendo como os relatórios de saída são gerados e entregues aos usuários? (acessos)		
10	Há monitoração via arquivos de logs enquanto ocorrem ciclos de processamento no sistema?		
11	Há documentação de quem dá manutenção e suporte nas operações e funcionalidades do sistema ERP?		

Fonte: BIANCHI,ISO, 2012.

- **O plano de auditoria é composto basicamente pelos tópicos:**

TÓPICOS
Objetivos da auditoria
Critérios de auditoria e qualquer documento de referência
O escopo da auditoria
Definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas
Pareceres do ambiente de sistema a ser verificado
Os principais pontos do relatório de auditoria
Quaisquer ações de acompanhamento de auditoria

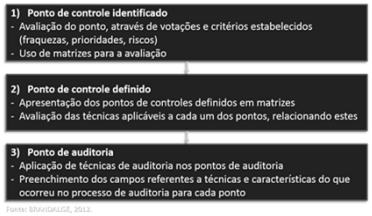
Fonte: ABNT, 2002.

- **É demonstrado na figura um modelo de um plano de auditoria básico que pode ser adaptado para auditorias de sistemas específicos**


SISTEMA: _____ EMPRESA: _____
PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO: ___/___/___
RESPONSÁVEL: _____
Definições Iniciais do Programa de Auditoria
Escolha na questão a seguir o OBJETIVO principal que deve ter enfoque nesta auditoria.
a) Objetivos da auditoria
Enfoque principal:
Auditabilidade | Disponibilidade
Privacidade | Manutenabilidade
Integridade | Formalidade
Confiabilidade | Acurácia
Observações:
Escolha na questão a seguir o ESCOPO principal que deve ter enfoque nesta auditoria.
b) Escopo da auditoria
Completo
Parcial
Acompanhamento
Fonte: MAGNALDO, 2012

Análise e definição dos pontos de controle

- **No esquema, é apresentado o ciclo de definição de ponto de controle**



Fonte: BRANDALISE, 2012.

Organização, identificação e definição dos pontos de controle

- **Na figura, é apresentado recorte da atividade**

Análise e definição dos pontos de controle	Organização, identificação e definição de pontos de controle	- Criação de arquivo que contém os pontos levantados de critérios estabelecidos - Reuniões com a comissão - Análise de auditorias passadas e pontos considerados importantes	Etapa 1: Matriz de ponto de controle identificado Etapa 2: Matriz ponto de controle identificado Etapa 3: Matriz de ponto de controle definido	- Modelo matriz de pontos de controle identificados - Matriz pontos de controle auditoria	*Equipe de auditoria, auditor líder, gestão*

Fonte: BRANDALISE, 2012.

- **A matriz Pontos de Controle Identificados será composta por pontos de controle, seus detalhes específicos e os riscos de cada ponto indicado pelos participantes da seleção.**

- **A avaliação de riscos será baseada nas etapas existentes na identificação de riscos, que são:**
  - **identificação de pontos;**
  - **identificação de ameaças;**
  - **identificação de vulnerabilidades;**
  - **identificação de consequências.**

Preparação e execução de atividades

- **Nesta fase, começa a acontecer a auditoria propriamente dita, com o exame dos pontos de controle definidos.**
- **O ponto de controle passa a ser chamado de ponto de auditoria.**
- **A ABNT (2006) apresenta a etapa de comunicação de risco, a comunicação de evidências de auditoria.**

- **Carta-comentário com os tópicos:**
  - **objetivo do controle;**
  - **considerações no ponto;**
  - **descrição dos procedimentos executados;**

- resultados;
- não conformidades e evidências achadas;
- recomendações;
- aval dos responsáveis internos.

- No relatório final, devem ser citados:
  - relação de normas, instruções, procedimentos e outros documentos utilizados como base (referência) para as avaliações;
  - relação dos membros da equipe de auditoria;

- Nomes de quaisquer outros observadores, participantes e de pessoas que foram contatadas em qualquer fase da auditoria.
- Constatações finais, dando ênfase para deficiências detectadas. Devem ser fornecidos detalhes suficientes para permitirem avaliação, ação corretiva e providências complementares pela organização/setor auditado.

Finalizando

- Apresentados o planejamento de auditoria e pontos de controle, um roteiro para elaboração de auditoria em sistemas.
- Foram apresentadas as fases, suas principais atividades, os responsáveis, os artefatos utilizados e, além disso, os artefatos gerados por cada atividade executada.

- A utilização do roteiro é feita por profissionais encarregados de implantar auditoria.
- Este roteiro pode ser alterado, sendo acrescidas mais regras para verificações, atividades e artefatos.
- Sob a responsabilidade da comissão ou equipe interna responsável pela elaboração de auditoria interna.