

ULBRA – Universidade Luterana do Brasil
Faculdade de Informática
Prof. Luís Fernando Garcia
Disciplina de Qualidade e Auditoria de Software

Auditoria de TIC – aula 2

Controle Interno

- Função administrativa exercida pelo auditor de TIC que valida as demais funções administrativas
- Auditoria nos processos administrativos e na administração da TIC
- Auditar a qualidade dos sistemas e processos

- **Tipos de auditoria**
 - Confronto
 - Contestação do ambiente
 - Busca de otimização, eficiência, segurança
 - Exceção
 - Pesquisa e Definição dos pontos de atuação
 - Ponto de controle
 - Subconjunto submetido a auditoria

- **Pontos de controle**

- Abordagem da fraqueza buscada
 - Erro
 - Falta
 - Omissão
 - Falha de procedimentos
- Rotinas e informações operacionais e de controle
- Recursos humanos, materiais e tecnológicos

- **Forma de atuação**
- **Através de TIC**
 - Sistemas de informações
 - Centro de computação
 - Processos
- **Analisando**
 - Rotinas operacionais
 - Informações operacionais
 - Rotinas de controle
 - Informação de controle
- **PROCESSO**
- Compreensão do ambiente – levantamento e documentação
- Análise do ambiente – situações sensíveis/análise de risco
- Elaboração da massa de testes – escopo/dados/resultados esperados
- Aplicação do teste
- Análise do teste e julgamento dos resultados
- Emissão de opinião sobre o ambiente – recomendações/sugestões
- Discussão – alternativas de solução/ajustes/substituições
- Acompanhamento da implantação da solução
- Auditoria da funcionalidade da solução implementada
- Novas auditorias futuras
- **Ponto de Controle**
- Situação do ambiente computacional de interesse para a auditoria
- Sistema → módulo → banco dados → tabela → coluna → linha
- **Ciclo de vida do Ponto de Controle**
- Início
- Ponto de controle identificado
- Avaliar (sim/não?)
 - Se sim
 - Fraquezas (sim/não?)

- Se sim → ponto de auditoria → banco de dados da auditoria

- **Análise de Risco**

- Conhecer o ambiente a ser auditado
 - Levantamento de dados
 - Estudo da documentação do ambiente
 - Complementação das informações
 - Visita ao ambiente de TIC
 - Entrevistas no ambiente de TIC
- Planejamento da auditoria
 - Determinação dos pontos de controle
 - Estabelecimento dos objetivos
 - Técnicas
 - Prazos
 - Custos
 - Nível de conhecimento de TIC exigido
 - Analise da sensibilidade de cada PC
 - Hierarquização dos PC
 - Documentação do processo de auditoria
- Produtos Gerados
 - Relatório de Fraquezas
 - Objetivos da auditoria
 - PC auditados
 - Conclusões sobre cada PC
 - Alternativas de solução propostas
 - Certificado de auditoria

- **Técnicas de Auditoria de TIC**

- Condicionadas ao ambiente computacional auditado
- Uso combinado de várias técnicas
- Uso da técnica reflete plano de auditoria

- Questionário
- Simulações de dados
- Visita in loco
- Mapeamento estatístico
- Rastreamento
- Entrevista
- Análise de relatório/tela
- Simulação paralela
- Análise de Log
- Análise de programa fonte
- Snapshot

- Questionário

- Conjunto de perguntas com objetivo de verificar PC
- Preferencialmente dados quantitativos
- E-mail, pessoalmente, etc...
- Processo:
 - Analisar PC
 - Definir população e amostra
 - Instruções de preenchimento/resposta
 - Distribuição
 - Recebimento
 - Análise das respostas

- Simulação

- Conjunto de dados de teste submetido ao sistema
- Simular situações corretas/incorretas
- Foco na preparação do ambiente de teste

- Visita in Loco

- Atuação pessoal do auditor no ambiente de TIC

- Elemento surpresa x horário marcado
 - Registros formais – data, hora, participantes, avaliação
 - Análise das respostas
- Mapeamento estatístico
 - Inserção de rotinas específicas no processo normal/sistema
 - Situações de rotinas fraudulentas/freqüência de execução
- Rastreamento
 - Seguir o caminho de transação durante a execução do sistema
 - Tracing – debug
- Entrevistas
 - Reunião entre auditor e auditado
 - Uso conjunto com questionário e visita in loco
- Análise de relatórios e telas
 - Avaliação do resultado produzido
 - Verificação da aderência as regras de negócio
- Simulação Paralela
 - Inverso da simulação
 - Usa dados reais em sistemas simulados
 - Confronta resultados
- Análise de Log
 - Verificação dos arquivos de log gerados por servidores e aplicações
 - Indicadores de qualidade/ de status
- Análise de programa fonte
 - Análise visual (ou automática) do programa fonte
 - Aderência a padrões/normas/estilos
- Snapshot
 - Análise do Dump de memória produzido pelo sistema