

ENGENHARIA DE SOFTWARE

Auditoria de sistemas

Ma. Vanessa Matias Leite

1

Unidade de Ensino: 04

Competência da Unidade: Conhecer e os fundamentos de auditoria de sistemas, bem como a manutenção e evolução de software

Resumo: Analisar e avaliar o contexto de aplicação da auditoria de sistemas de informação e manutenção e evolução de software

Palavras-chave: auditoria; sistemas de informação; manutenção de software; reengenharia; sistemas legados

Título da Teleaula: Auditoria de sistemas

Teleaula nº: 04

2

Na aula de hoje

- Auditoria de sistemas de informação;
- Sistemas legados;
- Mudanças e manutenções em software;
- Reengenharia de software;

3

Fundamentos de auditoria de sistemas

4

Auditoria

Principal função analisar parcial ou globalmente os processos, resultados e, em alguns casos, sugerir ações corretivas ou melhorias. Elas podem ser aplicadas por diversos métodos (questionário, teste de uso prático, análise documental, entre outras formas), porém os resultados obtidos não devem gerar dúvidas.

5

Auditoria

- Uma auditoria aponta falhas, erros, pontos de atenção, no entanto não obriga a empresa a tomar outros rumos.
- As atividades de auditoria de software são pautadas por testes, análises, avaliações e outras formas que possam provar que algo de inconformidade está ocorrendo ou sendo executado;

6

Auditoria

- Processos;
- Desenvolvimento;
- Testes;
- Segurança e proteção dos dados;
- Estrutura de desenvolvimento;

7

Auditoria de Sistemas de Informação

Verificação de toda a estrutura computacional da empresa. Entre os principais objetivos dessa inspeção estão analisar a eficiência dos processos, garantir a segurança dos dados e assegurar o cumprimento das leis e demais normas que permeiam as ações;

8

Abordagem ao redor do computador

- Baseado em confrontar documentos fontes com os resultados esperados;
- Utiliza-se rotinas manuais;
- Sua aplicação envolve custos baixos e diretos.
- Não se exige conhecimento extenso de tecnologia de informação;

9

Abordagem através do computador

- Capacita o auditor a verificar com maior frequência as áreas que necessitam de verificação constante.
- Faz aprovação dos registros [logs] armazenados.
- Esta abordagem não deixa evidências documentais através dos controles dos programas.
- Se for realizada incorretamente pode levar a grande perdas;

10

Abordagem com o computador

- Mais completa e mais utilizada;
- Utiliza as capacidade lógicas e aritméticas do computador.
- Possibilita a maior perfeição possível, fazendo uma compilação dos processos automatizados e manuais.
- Possibilidades de desenvolver programas específicos para serem usados pelo auditor.

11

Auditor

Auditor é o profissional que tem conhecimentos técnicos, gerenciais, operacionais e analíticos para conduzir as atividades relacionadas ao desenvolvimento de auditorias em sistemas da informação.

12

TIPOS	ATRIBUIÇÃO
Inspeção	<ul style="list-style-type: none"> Efetuar inspeção dos processos e dos desenvolvimentos. Verificar onde ocorrem inconformidades e apresentar provas convincentes.
Controle	<ul style="list-style-type: none"> Efetuar a análise de controle dos processos, podendo ser operacionais, de desenvolvimento ou gerenciais.
Risco	<ul style="list-style-type: none"> Verificar quais riscos podem afetar o projeto, a fim de se indicar a equipe na qual existe um risco. Isso permite que o gerente de projetos possa tomar medidas corretivas/preventivas. Analisar de forma mais abrangente os riscos, apresentando consequências externas que possam ocorrer.
Contínua	<ul style="list-style-type: none"> Elaborar relatórios das análises em espaços curtos de tempo. Utilizar sistemas de verificação constantes para que se faça uma análise de diversos momentos. Contratar especialistas da área em que é necessária uma análise mais profunda, a fim de se permitir o aumento do detalhamento dos processos.

Fonte: Livro texto

13

Ciclo de vida da auditoria

14

Ciclo de Vida



Fonte: Livro texto

15

Planejamento do cronograma

- As atividades de elaboração do cronograma mostram o nível de organização da equipe que aplicará a auditoria. Além disso, é possível compreender como o ciclo todo será organizado. Ao divulgar o cronograma da auditoria, a empresa/equipe que será auditada pode ajustar alguns pontos de melhorias.
- Deve ser validado com o contratante;

16

Planejamento do cronograma

Início	Atividade	Final	Auditor
05/01/2020	Planejamento da auditoria	20/01/2020	Fulano de Tal
21/01/2020	Condução da auditoria	05/02/2020	Fulano de Tal
06/02/2020	Reporte da auditoria	01/03/2020	Fulano de Tal

Fonte: Livro texto

17

Planejamento da auditoria

Entre as atividades do planejamento da auditoria, deve-se estar claro qual o objetivo de determinada auditoria, de forma que a empresa de desenvolvimento de software que receberá os auditores possa se adequar às necessidades do cliente.

18

Planejamento da auditoria

O planejamento é um documento que deve ser elaborado pelos auditores de forma que três pontos fiquem claros para equipe de auditores e para a organização/equipe a ser auditada:

- Quem será auditado?
- O que será auditado?
- Quando ocorrerá a auditoria?

19

Condução da auditoria

Quando o planejamento da auditoria está pronto e aprovado, dá-se seu início, no qual são aplicadas as atividades de coleta de informações tais como: revisão documental, conversas e entrevistas, análise de dados de processos, observações, entre outras técnicas.

20

Condução da auditoria

Data	Hora	Atividade	Local	Processo	Auditor	Auditado
05/01/2020	08:00	Reunião de abertura	Sala de reunião	----	Todos	Todos
21/01/2020	09:00	Análise documental	Sala de reunião	Questionário de UX	Fulano	Developer
06/02/2020	10:00	Entrevista	Café	Utilização do framework	Fulano	Developer

Fonte: Livro texto

21

Reporte da auditoria

- Encerramento da Auditoria;
- Podem ser feitas reuniões, relatórios, apresentações, entre diversos outros recursos que fornecem a devolutiva do que foi auditado;
- Dependendo do acordado na contratação desse serviço, podem-se propor melhorias e ajustes. Porém, não cabe à empresa/equipe de auditoria promover as mudanças descritas no reporte.

22

Auditoria de sistemas de informação

23

Auditoria de Controles Organizacionais e Operacionais

- Delineamento das responsabilidades operacionais;
- Coordenação de orçamento de capital de informática e bases;
- Desenvolvimento e implementação das políticas globais de informática;
- Intermediação com terceiros (*networking*);
- Gerenciamento de suprimentos;
- Desenvolvimento de plano de capacitação.

24

Auditoria de Controles Organizacionais e Operacionais

Cargos:

- Supervisão da infraestrutura de TI
- Administração de redes
- Administração de banco de dados
- Administração de dados
- Administração de segurança
- Análise, programação e manutenção de sistemas
- Design para web
- Suporte técnico

25

Auditoria de Controles de Hardware

- Objetivo de implantar os procedimentos de segurança física sobre os equipamentos instalados em ambiente de informática – *Data Center* de uma organização.
- Os controles podem ser físicos e automatizados.
- Fazer inventários de hardwares.

26

Auditoria de Controles de Hardware

- BIOS;
- processadores (*chips*);
- sistema operacional e a linguagem;
- fabricante/modelo e séries;
- monitor e a resolução;
- placas de *modem*, som, vídeo etc.

27

Auditoria de Controles de Hardware

Recursos para amenizar os riscos:

- Extintores de incêndio;
- *Sprinklers*;
- *Firewalls*:
 - a. detecção de intrusos;
 - b. controle de aplicativos;
 - c. controle de privacidade.

28

Procedimentos de Auditoria de Sistemas Aplicativos

Objetivos:

- Integridade;
- Confidencialidade;
- Privacidade;
- Acuidade;
- Disponibilidade;
- Versatilidade;
- Manutenibilidade.

29

Procedimentos de Auditoria de Sistemas Aplicativos

Compreensão do fluxo de sistemas de aplicativos:

- Identificação de sistemas-chaves;
- Descrição do sistema;
- Descrição do perfil do sistema;
- Documentação da visão geral do processamento;
- Descrição de riscos dos sistemas aplicativos.

30

Auditoria de Redes de Computadores

- Planejamento da concepção da rede com visão estratégica ao integrar o plano diretor de informática;
- Desenho das arquiteturas e da topologia da rede;
- Implementação dos projetos físicos e lógicos;
- Monitoramento dos desempenhos e possíveis interceptações nas redes;
- Replanejamento de capacidade;
- Levantamento dos problemas operacionais e sua resolução.

31

Auditoria de Redes de Computadores

Objetivo da auditoria:

- Segurança física;
- Segurança lógica;
- Segurança de enlace;
- Segurança de aplicação;

32

Auditoria de plano de contingência e de recuperação de desastres

- Há planos desenvolvidos que contemplem todas as necessidades de contingências;
- A equipe de contingência está preparada para as eventualidades;
- Os *backups* são atualizados e podem ser recuperados com pouca ou nenhuma dificuldade;
- Há relatórios gerenciais (confiáveis) que facilitam o acompanhamento dos procedimentos;

33

Plano de Contingência

- Classificação das aplicações críticas;
- Análise de riscos potenciais;
- Contingências em relação aos recursos tecnológicos;

34

Mudança e Manutenção de Software

35

Categorias de Softwares

- Software de Sistema;
- Software de Aplicação;
- Software científico e de Engenharia;
- Software embutido;
- Software para linhas de produto;
- Aplicação web;
- Software para Inteligência Artificial;

36

Software Legado

Programas antigos e que precisam ser modificados para satisfazer mudanças nos requisitos de negócios e de plataforma de computação.

37

A Qualidade de Software Legado

- Sistemas legados podem ter uma má qualidade:
 - ✓ Projetos não-extensíveis;
 - ✓ Código complicado;
 - ✓ Pouca ou documentação inexistente;
 - ✓ Histórico de modificação mal gerido;

38

A Qualidade de Software Legado

- Evolução do sistema legado:
 - ✓ Adaptação do software para atender novas necessidades do ambiente;
 - ✓ O software precisa ser aperfeiçoado para implementar novos requisitos de negócios;
 - ✓ Necessidade de extensão para torná-lo interoperável;
 - ✓ Necessidade de modificação para o sistema se tornar viável em um ambiente de rede.

39

Gestão de Modificação

- Modificações são inevitáveis;
- Gestão de Modificação:
 - ✓ Identificar modificações;
 - ✓ Controlar modificações;
 - ✓ Garantir que as modificações sejam implementadas corretamente;
 - ✓ Relatar/Documentar as modificações;

40

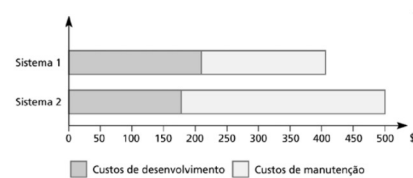
Manutenção de Software



Fonte: Sommerville (2007)

41

Manutenção de Software



Fonte: Sommerville (2007)

42

Manutenção de Software

- Estabilidade da equipe;
- Responsabilidade contratual;
- Habilidade pessoal;
- Idade e estrutura do programa;

43

Previsão de Manutenção

- Previsão de facilidade da manutenção;
- Previsão de mudanças do sistema;
- Previsão do custo da mudança;

44

Manutenção de Software

- Manutenção Corretiva;
- Manutenção Adaptativa;
- Manutenção perfectiva;
- Manutenção preventiva (reengenharia);

"Quanto mais difícil de entender um programa, mais difícil de mantê-lo" (Gerald Berns);

45

Reengenharia de Software

- Busca examinar os sistemas com a finalidade de reestruturá-los para atender aos novos requisitos e tenham uma maior qualidade.
- Ter que criar um produto com funcionalidades adicionais, melhor confiança, desempenho e modo de manutenção aperfeiçoada.

46

Motivações

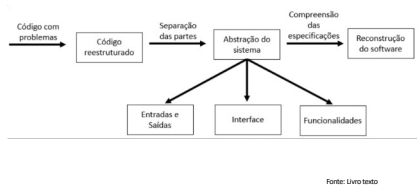
- O sistema não atende mais as necessidades;
- Não possui documentação;
- Modernizar os sistemas legados;
- Custo alto para manter o sistema;
- Código confuso e com erros;

47



48

Reengenharia de Software



49

Recapitulando

50

Recapitulando

- Auditoria de sistemas de informação;
- Sistemas legados;
- Mudanças e manutenções em software;
- Reengenharia de software;

51



52