Universidade Católica de Pelotas
Tecnólogo em Análise e Desenvolvimento de Sistemas
Disciplina de Qualidade de Software

AUDITORIA DE SOFTWARE

Prof. Luthiano Venecian
venecian@ucpel.tche.br
http://olaria.ucpel.tche.br/venecian

Agenda

- Conceitos Gerais
- Auditoria de Software
- Papel do Auditor
- Técnicas de Auditoria
- Tipos de Auditoria
- Processo de Auditoria
- Métricas de Auditoria
- Ferramentas
- Referência

Conceitos Gerais (1/2)

Auditoria = Audire = do latim "Saber ouvir"

- **Critério de Auditoria** – Conjunto de políticas, procedimentos e requisitos;
- **Evidências de auditoria** – Registros, fatos ou outras informações pertinentes aos critérios de auditoria;
- **Auditor** – Pessoa com a competência para realizar uma auditoria;

Conceitos Gerais (2/2)

- **Auditado** – Pessoa ou organização na qual passará pelo processo de auditoria;
- **Plano da Auditoria** – Descrição das atividades e arranjos para uma auditoria;
- **Escopo da auditoria** – Abrangência e limites de uma auditoria.

Auditoria de Software

- Um processo de auditoria exerce uma ação preventiva, reparadora e moralizadora.
- Ao realizar uma auditoria os principais objetivos são:

  1 - Verificar e constatar a eficácia do sistema;

  2 - Atestar a segurança física e lógica do sistema.

Auditoria de Software

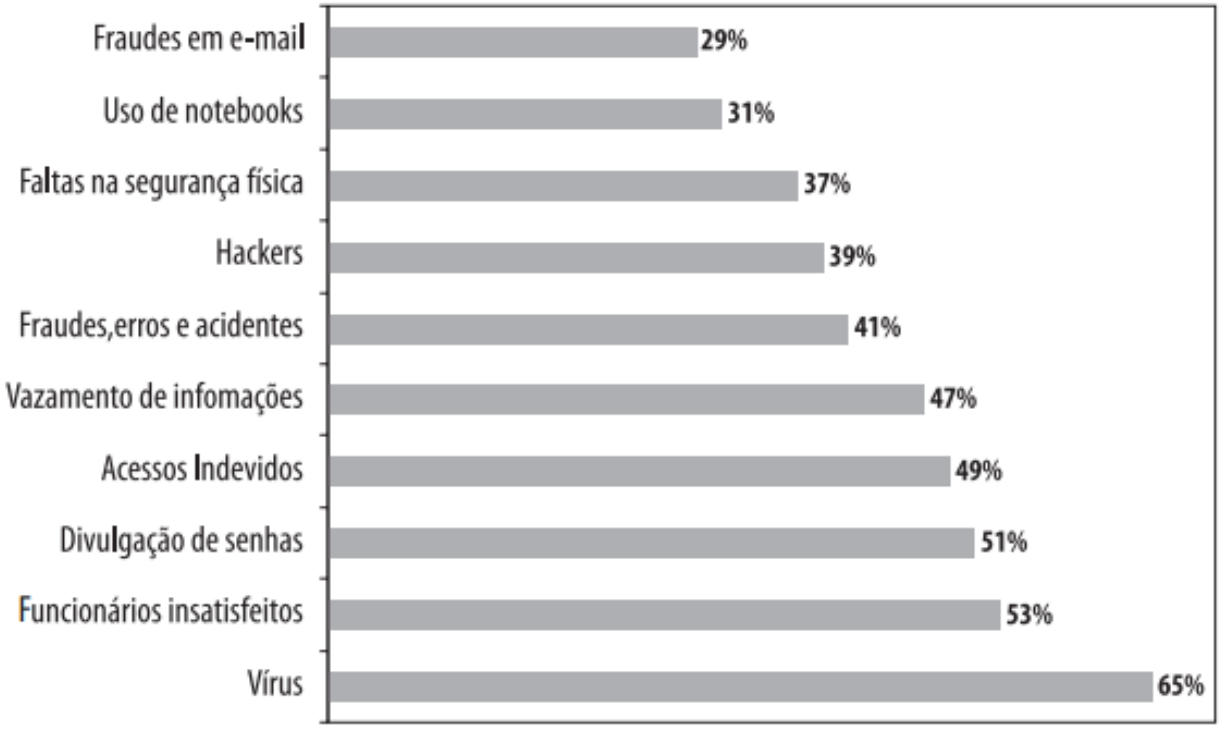

Figura: Pesquisa realizada pela Security Solutions

Papel do Auditor (1/5)

- Compreensão do ambiente;
- Análise do ambiente e determinação das situações mais sensíveis;
- Elaboração de uma massa de testes;
- Aplicação da massa de testes;
- Análise das simulações;
- Emissão da opinião quanto ao ambiente auditado;

Papel do Auditor (2/5)

- Debate com os profissionais da área auditada para discussão das alternativas recomendadas;
- Acompanhamento da implantação da solução proposta;
- Auditoria da solução implantada;
- Novas auditorias no ambiente.

Papel do Auditor (3/5)

- O auditor deve utilizar palavras de questionamentos como:
  - Como? (de que modo)
  - O que? (o fato)
  - Quando? (tempo)
  - Quem? (pessoas)
  - Onde? (lugar)
  - Por que? (motivos)
  - Mostre-me (Evidência)

Papel do Auditor (4/5)

- Estar bem preparado para realizar a auditoria
- Tentar prever o máximo de situações possíveis
- Evitar surpresas ao auditado
- Esclarecer todas as dúvidas sobre uma não-conformidade
- Buscar objetividade e fatos concretos (Evidências)

Papel do Auditor (5/5)

- Não atacar pessoas e sim fatos concretos
- Motivar a identificação de melhorias
- Persuadir, não impor
- O auditor não deve relacionar pessoas à não-conformidades ou deficiências
- Ser flexível quando necessário
- Ser imparcial e objetivo para obtenção dos fatos

Técnicas de Auditoria

- Questionários
- Simulação de dados
- Visita in loco
- Entrevista
- Análise de Log
- Análise do programa fonte
- Etc.

Tipos de Auditoria

- **Primeira parte:** realizada por uma organização sobre si mesma;
- **Segunda parte:** conduzida por uma organização sobre uma outra para fins da organização condutora da auditoria;
- **Terceira parte:** realizadas por uma terceira independente sem interesses nos resultados da auditoria.

Processo de Auditoria

- Pode variar de organização para organização, porém não deve deixar de alcançar o objetivo da auditoria.
- CMM KPA N2 – SQA
- CMMI PA N2 - PPQA
- Etapas
  - Planejamento
  - Auditoria
  - Finalização

Processo de Auditoria: Planejamento (1/2)

- Identificação do objetivo de cada auditoria
- Identificação do escopo da auditoria, ou seja, onde se quer verificar a existência de não-conformidades
- **Auditoria no produto ou no processo**
- Definição da estratégia da auditoria, ou seja, como ela será realizada
- Definição de um cronograma de auditoria

Processo de Auditoria: Planejamento (2/2)

- Auditorias devem ter um cronograma atualizado e sendo executadas com freqüência.
  - Ex: mensal: Cada mês focar em uma área especifica
- A freqüência pode variar por projeto ou organização
- Utilizar uma análise de risco para poder atualizar o cronograma
- Um cronograma de auditoria é conhecido pelos membros do projeto

Processo de Auditoria: Auditoria (1/2)

- Pode ser conduzida por um ou mais auditores;
- O auditor identifica os critérios de auditoria (processo, templates e informações pertinentes);
- Realiza uma preparação no material;
- Cria ou seleciona um checklist para que sirva de guia durante a execução da auditoria;
- Identifica possíveis auditados (Verificar com o líder da equipe);
- Apresenta-se formalmente ao auditados, descrevendo os objetivos da auditoria;

Processo de Auditoria: Auditoria (2/2)

- Na reunião de auditoria:
  - O auditor usa o checklist para guiar na identificação das informações necessárias;
  - O auditor deve questionar o entrevistado com base no que foi estudado e no checklist;
  - O auditor anota todas as informações pertinentes à auditoria que posteriormente vai utilizar para identificar não-conformidades;
  - Pedir sugestões aos auditados.

Processo de Auditoria: Finalização(1/3)

- Com base nas informações coletadas na auditoria, bem como evidências coletadas, o auditor deve verificar junto aos processos, procedimentos e padrões da organização, se são caracterizadas não-conformidades;
- As oportunidades de melhoria são identificadas;
- As boas práticas são identificadas;

Processo de Auditoria: Finalização(2/3)

- Tendo relacionado as não-conformidades, oportunidades de melhoria e boas práticas, o auditor deve verificar sua coerência com os auditados;
- O auditor deve criar um relatório contendo as informações da auditoria e para cada não-conformidade deve ser apresentada:
  - Uma ação de correção
  - Data para conclusão
  - Responsável pela ação

Processo de Auditoria: Finalização(3/3)

- Após o relatório finalizado, o mesmo deve ser apresentado, para que todos fiquem cientes do resultado da auditoria
- As não-conformidades devem ser acompanhadas até o seu fechamento
- Caso as datas não sejam cumpridas, deve ser um utilizado um critério de escalação, até que a não-conformidade seja finalizada
- O relatório de auditoria deve estar em um repositório com controle de versão

Métricas de Auditoria

- # de não-conformidades por projeto
- # de Auditorias Planejadas X # de Auditorias Realizadas
- # de não-conformidades fechadas por mês

Ferramentas de auditoria (1/3)

- Ferramentas generalistas:

  São softwares que podem processar, simular, analisar amostras, gerar dados estatísticos, sumarizar, apontas duplicidade, e outras funções.

  Ferramentas:

  - Audit Command Language (ACL)
  - Interactive Data Extraction & Analisys (IDEA)
  - IDEA / Audimation
  - Galileo
  - Pentana

Ferramentas de auditoria (2/3)

- Ferramentas especialistas

  São softwares desenvolvidos especialmente para executar certas tarefas em circunstâncias definidas.

  O Software pode ser desenvolvido pelo próprio auditor, pelos especialistas da empresa auditada ou terceiros contratados pelo auditor.

  Desvantagens:

  - Pode ser muito caro, pois seu uso é limitado e restrito apenas a um cliente.

Ferramentas de auditoria (2/3)

- Ferramentas de utilidade geral

  São softwares não específicos para atividade de auditoria, é possível citar como exemplos as planilhas eletrônicas, softwares de gerenciamento de banco de dados, ferramentas de Business Intelligence, software estatísticos.

  Ferramentas:

  - Suíte Trauma Zer0
  - MailDetective
  - Velop Escudo
  - MailMarshal Exchange e IQ.Suite for Domino

Referências

- CMM in Practice Processes for Executing Software Projects at Infosys
- CMMI Guidelines for Process Integration and Product Improvement
- NBR ISO 19011 – Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental