Auditoria e Qualidade de Software

Profª. Maria Joseane de Araújo

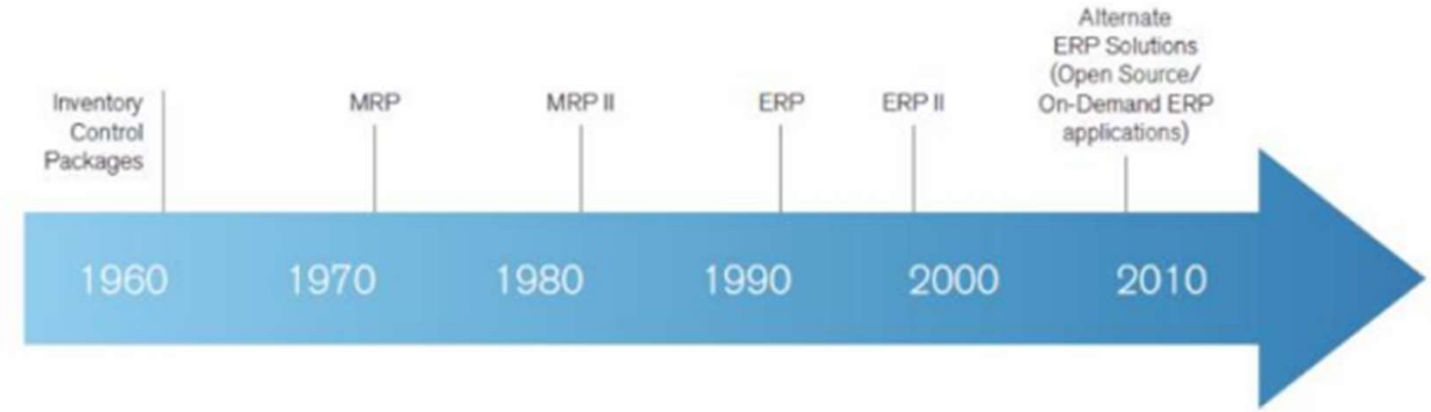
Email: mariajoseane@prof.unipar.br


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE

ENTERPRISE RESOURCE PLANNING - ERP

- Mainframes para controles de estoque (1950);
- MRP - Material Requirement Planning (1960 e 1970): permite a gestão e o controle dos inventários;
- ERP - Enterprise Resource Planning (década de 90): foi possível integrar as áreas de recursos humanos, vendas, marketing, finanças, faturamento, contabilidade, entre outros.



ENTERPRISE RESOURCE PLANNING - ERP

- Mostram dados em Tempo Real através de relatórios
- Informações que se interagem e se alimentam
- Auxiliam na tomada de de Decisão
- *Supplychain* (Cadeia de mantimentos)

ENTERPRISE RESOURCE PLANNING - ERP

- Elimina Uso de Interfaces Manuais
- Elimina retrabalho
- Aprimoramento dos processos internos
- Informação de qualidade em tempo real
- Otimiza tomada de decisão
- Melhor gestão dos resultados

ENTERPRISE RESOURCE PLANNING - ERP

- Altos custos de implementação
- Dependência do fornecedor
- Dependência da Tecnologia
- Mão-de-obra capacitada
- Padronização entre as empresas do segmento

AUDITORIA DE SISTEMAS

“É a avaliação e a validação do controle interno de sistemas de informação”

AUDITORIA DE SISTEMAS

Histórico

> Utilização crescente de Sistemas de Gestão

> Necessidade de melhor gerenciamento e criação de controles

Objetivos

> Validar e avaliar os controles internos de Sistemas

> Validar a eficácia do sistema

> Reunir, agrupar e validar evidências

> Garantir a segurança (física e lógica) da Informação e sistema

Segurança da Informação

> Integridade

> Disponibilidade

> Confidencialidade

AUDITORIA DE SISTEMAS

- Pode detectar problemas em:

  - Fraudes em e-mail;
  - Uso inadequado de hardwares;
  - Fraudes, erros e acidentes;
  - Vazamento de informações;
  - Falta de segurança física (acessos indevidos)

Auditoria de TI ≠ Auditoria de Controles por meio de TI

Auditoria de TI	Auditoria de controles por meio de ferramentas de TI
Exemplo de teste de auditoria: Verificação controles de acesso para alteração da base de dados de um ERP (alto risco)	Exemplo de teste de auditoria: Verificação de acessos para testes de segregação de função
Mais realizados por externas e auditorias especializadas	Mais realizado por auditorias internas (externas com foco nas DC's)

Tipos de abordagem de auditorias de sistemas

Ao redor do computador:

- Trabalha com documentos de entrada e saída;
- Não necessita profundo conhecimento em TI;

➢ Vantagens: baixo custo

➢ Desvantagens: Incompleta, poucos parâmetros

Através do computador:

. Envolve aprovação e registro de transações;

. Utiliza técnicas de verificação;

➢ Vantagens: aprofundado validação e apontamentos;

➢ Desvantagens: alto custo

Principais tipos de auditorias de sistemas

- Pesquise quais tipos existem e como são utilizados...

- Interna e Externa

Principais tipos de auditorias de sistemas

- **Auditoria Legal ou Regulatória:**
  - Atendimento a regulamentações locais e internacionais (Lei Sarbanes-Oxley, Basileia II, Comissão de Valores Mobiliários, etc).

- **Auditoria de Integridade de Dados:**
  - Classificação dos dados, atualização, bancos de dados, aplicativos, acessos, estudo dos fluxos (entradas e saídas) de transmissão, controles de verificação qualidade e confiabilidade das informações. (exemplo anexo)

- **Auditoria em Segurança da Informação:**
  - Métodos de autenticação, autorização, criptografia, gestão de certificados digitais, segurança de redes, gestão dos usuários, configuração de antivírus, atualizações, políticas, normas, manuais operacionais.

- **Auditoria de Segurança Física:**
  - Avaliação de localidades e riscos ambientais: vidas (capital intelectual), furto/roubo, acesso, umidade, temperatura, acidentes, desastres, etc. e as proteções: perímetros de segurança, câmeras, sensores, guardas, dispositivos, proteções do ambiente.

- **Auditoria de Desenvolvimento de Sistemas:**
  - Validação dos processos de gestão de projetos, cumprimento de metodologia de qualidade, orçamentos previstos e realizados e avaliação de desvios.

Por que ter uma auditoria de sistemas?

- Para ter transparência na área de TI e processos da empresa

- SOX (30/07/2002)
  - gerou mudanças que afetam a forma como as empresas realizam seus controles internos, auditoria e *compliance*, além de sua responsabilidade perante os órgãos reguladores.
  - referencia
    - https://www.soxlaw.com/

O processo de certificação do auditor de sistemas

- CISA – Certified Information Systems Auditor
- Oferecida pelo ISACA
- Uma das mais reconhecidas e eficazes em âmbito global
  - https://www.isaca.org/credentialing/cisa

O processo de certificação do auditor de sistemas

- **Para passar no exame:**
  - Demonstrar experiência e qualificações profissionais, fornecer evidência de práticas; aderir formalmente ao código de ética do ISACA, etc.

- **Para manutenção do certificado:**
  - Participar de atividades educacionais e comprovar que contribuiu para a profissão de auditoria de maneira “correta”

O CIO (Chief Information Officer)

- Profissão que contempla o papel principal de fomentar a capacitação da organização necessária para extrair um maior valor dos investimentos em TI.

- O CIO é um participante crítico, considerando a crescente importância de TI na ativação do desempenho e da competitividade dos negócios.
- Passou de gerente funcional para gerente geral com escopo e responsabilidades de toda a empresa.

QOS – Quality Of Service

- Imposição de requisitos de qualidade no momento da aquisição do serviço, em:
  - Sistema de manufaturas;
  - Sistema de compensação bancária;
  - Plataformas de telecomunicação, etc.

- O objetivo é reduzir custos, simplificar a manutenção e facilitar a interoperabilidade do sistema.

EDP – Electronic Data Processing

- Processamento de dados que é realizado através de dispositivos eletrônicos, que, segundo a norma NPC T 11:
- modifica a forma de processamento e armazenamento de informações, afetando a organização e os procedimentos adotados pela entidade na consecução de adequados controles internos;
- julga importante conhecer suficientemente o sistema de contabilidade e controle interno afetado pelo ambiente de PED; deve determinar o efeito que o ambiente de PED possa ter sobre a avaliação de risco global da entidade em nível de saldos de contas;
- estabelecer e supervisionar o nível de provas de controle e de procedimentos substantivos capaz de assegurar a confiabilidade necessária para conclusão dos controles internos e das demonstrações contábeis.

Resumo ...

- **Conceito de Auditoria de Software:**
  - processo sistemático e independente que tem como objetivo avaliar a conformidade, eficácia e eficiência dos processos de desenvolvimento, manutenção e gestão de software.

  - **Objetivos da Auditoria de Software:**
    - Assegurar a Conformidade
    - Identificar Problemas e Riscos
    - Avaliar a Eficácia dos Processos
    - Garantir a Qualidade do Software
    - Promover a Transparência e Confiança
    - Prevenir Problemas Futuros

Tipos de Auditoria: Interna e Externa

- **Auditoria Interna:** Realizada por profissionais pertencentes à própria organização, focando na **avaliação dos processos internos, controles e conformidade com políticas e procedimentos** estabelecidos pela empresa.

- **Auditoria Externa:** Conduzida por **auditores independentes**, externos à organização, com o objetivo de avaliar as **demonstrações financeiras, conformidade legal, eficácia dos controles internos e a transparência** das informações para stakeholders externos.

Papel e responsabilidades dos auditores

- **Auditores Internos:** São responsáveis por **avaliar e melhorar** os processos internos da organização, identificar riscos, garantir conformidade com políticas e procedimentos, e fornecer recomendações para aprimoramento.

- **Auditores Externos:** Atuam de forma independente para garantir a precisão e confiabilidade das informações financeiras da empresa, assegurando que as demonstrações contábeis estejam em conformidade com os **princípios contábeis geralmente aceitos e normas vigentes.**

Segundo Benedetti(2015)

- As áreas de auditoria de sistemas são basicamente as seguintes: ***segurança da informação, TI e Aplicativos***.

- Não há uma **regra fixa** para determinar como as organizações devem classificar sua área de auditoria; isto fica a critério da própria organização.

Segurança da informação:

- **confidencialidade**: controles de acesso (físico e lógico);
- **integridade:** gravação e atualização autorizadas (mantém-se um responsável pela informação);
- **disponibilidade:** sistema disponível sempre que necessário;
- **consistência:** sistema funcionando dentro dos requisitos especificados;
- **confiabilidade:** sistema atua conforme esperado.

Tecnologia da informação:

Mudanças organizacionais, operações de sistemas, hardware, computação em nuvem (Cloud Computing), sistemas ERP (Enterprise Resource Planning), data warehousing, entre outras.

É desejável também que o auditor desta área tenha certificações (ITIL, Cobit, entre outras)

Certifications in ITIL 4

https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1

COBIT 5 Foundation

Aplicativos:

controla o desenvolvimento de software, a entrada, o processamento e a saída dos dados, o conteúdo e o funcionamento.

Exercícios:

1 - O que é ITIL e o COBIT? Discorra sobre cada uma.

Padrões e código de ética

O comitê de padrões da Associação de Controle e Auditoria de Tecnologia de Informação dos Estados Unidos define os seguintes padrões:

- responsabilidade, autoridade e prestação de contas;
- independência profissional;
- ética profissional e padrões;
- competência;
- planejamento;
- emissão de relatório;
- atividades de follow-up (acompanhamento).

Associação de Auditores de Sistemas & Controles (ISACA) define o código de ética profissional contendo os seguintes itens:

1. apoiar a implementação de padrões sugeridos para procedimentos e controles dos sistemas de informação e encorajar seu cumprimento;

2. exercer suas funções com objetividade e zelo profissional, seguindo padrões profissionais e melhores práticas;

3. servir aos interesses dos stakeholders de forma legal e honesta, com alto padrão de conduta e caráter profissional e desencorajar atos de descrédito à profissão;

4. manter a privacidade e a confidencialidade das informações obtidas, exceto quando exigido legalmente. Estas informações não devem ser utilizadas em benefício próprio ou compartilhadas com pessoas não autorizadas;

5. manter competência na sua especialidade e assegurar que somente atua nas atividades em que tem habilidade suficiente;

6. informar os stakeholders sobre os resultados de seus trabalhos, expondo os fatos significativos desde que em seu alcance;

7. apoiar a conscientização profissional das partes envolvidas para auxiliar sua compreensão dos sistemas de informação, segurança e controle.

Planos de contingência

- Uma contingência é um evento que **pode ou não** acontecer

  - **por exemplo:**
  - um equipamento que para de funcionar;
  - um funcionário que adoece;
  - um incêndio;
  - a indisponibilidade de sistema;
  - queda de energia elétrica, entre outros.

O que é plano de contingência?

- Sequência de ações predeterminadas que devem ser seguidas na ocorrência de uma emergência, a fim de estabelecer a continuidade do serviço
- O plano não contempla apenas os serviços de informática e sua disponibilidade.
  - Os impactos que a emergência pode causar para a segurança das pessoas, danos ambientais e até mesmo o desgaste da imagem da organização em relação aos clientes e fornecedores devem ser considerados no momento da elaboração do plano de contingência, para que os danos causados com a ocorrência sejam os menores possíveis.

Riscos e Ameaças

- A ameaça é um evento ou uma atitude indesejável que pode danificar um recurso

- roubo;
- incêndio;
- vírus;
- queda de energia elétrica...


UNIPAR
UNIVERSIDADE PARANAENSE

- A auditoria de sistemas é de vital importância para o bom andamento dos processos organizacionais. Alguns tipos de empresas podem ter perdas financeiras significativas na ocorrência de ameaças que parecem não ser tão graves. Defina qual a importância da disponibilidade de serviços de TI em uma empresa de vendas pela internet. Dê um exemplo de ameaça com alto escore de risco para empresas deste tipo.

Possível resposta:

- Um ataque de negação de serviço distribuído (DDoS).
- Nesse tipo de ataque, os servidores da empresa são sobrecarregados com um grande volume de tráfego falso, tornando os serviços inacessíveis para os usuários legítimos.
- Pode resultar em tempo de **inatividade prolongado, perda de vendas e danos à reputação da empresa.**

O Funcionamento, os Controles Internos e as Ferramentas da Auditoria

- Compreensão do dia a dia do auditor de sistemas;
- Mostrar o que são e quais são os controles internos utilizados em auditoria de sistemas;
- Apresentar a sequência lógica das fases da auditoria de sistemas e suas ações;
- Apresentar as ferramentas de software que auxiliam na auditoria.

O funcionamento da auditoria de sistemas

- planejamento;
- execução;
- emissão de relatórios;
- acompanhamento das mudanças geradas como resultado da auditoria;

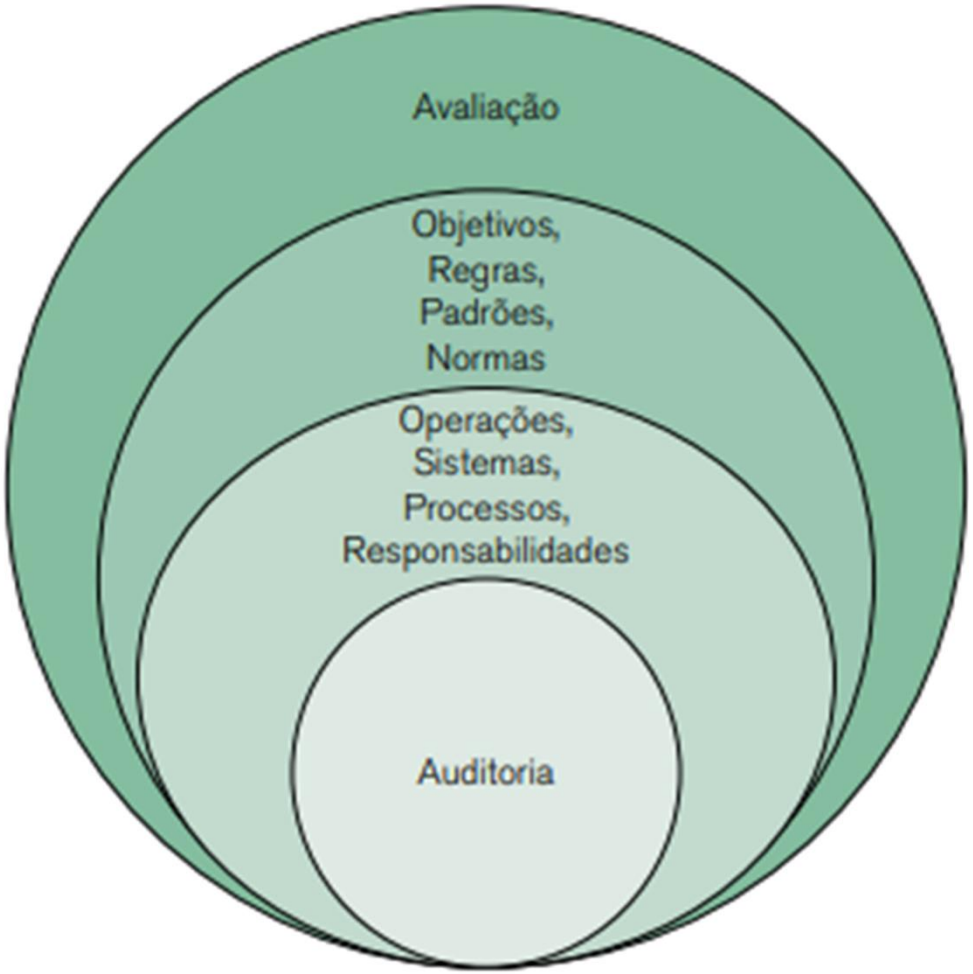


Figura 2.1 – Relação entre as funções de uma auditoria de sistemas.

Ferramentas de auditoria

- **sistemas que estão em desenvolvimento**
  - foca sua atenção no planejamento dos controles internos, processos e controles de negócio.

- **sistemas em operação.**
  - verificada a existência de pontos de controle e são executados testes para verificação destes pontos.
  - têm-se:
    - ***softwares generalistas;*** ***softwares especializados;*** ***softwares utilitários.***

Softwares generalistas

São programas em ambiente batch (offline).
Carecem de personalização, softwares conhecidos como “de prateleira”

Segundo Imoniana (2008), podem ter funções como:

- extração de dados de amostra;
- geração de dados estatísticos;
- gravação de arquivos auxiliares;
- testes globais;
- detecção de duplicidades;
- apontamento de duplicidade de registros;
- apontamento de sequência incorreta;

Exemplos deste tipo de softwares:

- ACL (Audit Command Language): extração e análise de dados;
- IDEA (Interactive Data Extraction & Analysis): extração e análise de dados;
- Galileo: softwares integrado de gestão de auditoria, incluindo gestão de riscos, documentação, relatórios;
- Pentana: softwares para planejamento estratégico de auditoria, diversos controles, entre outras funcionalidades.

Segundo Imoniana (2008), entre vantagens, pode-se citar:

- poder de processamento de vários arquivos ao mesmo tempo;
- poder de integração com outros softwares e hardwares;
- não é necessário que o auditor seja especialista em informática para que desenvolva aplicativos de testes de dados, apenas utiliza-se do aplicativo já desenvolvido.

Como desvantagens, tem-se (IMONIANA, 2008):

- não se pode fazer aplicações online, pois os softwares utilizam-se de arquivos que são analisados separadamente;
- impossibilidade de rodar cálculos complexos e específicos devido ao seu caráter generalista.

Softwares especializados

- atende melhor o usuário na especialidade para qual foi desenvolvido.
- geralmente são desenvolvidos pelos auditores, a fim de resolver problemas pontuais e específicos da área ou sistema auditado.

Vantagens:

- inclusão de testes e verificadores de controles internos específicos do sistema auditado;
- desenvolvimento de soluções para auditar áreas mais complexas e específicas, podendo se utilizar disto como vantagem competitiva.

Desvantagens:

- o auditor deve estar **familiarizado com desenvolvimento** de software;
- o **custo** do desenvolvimento de softwares especializados pode não compensar.

Softwares utilitários

- Funções básicas
- Apoio
- Auxiliar em tarefas comuns
  - Os sistemas operacionais e os sistemas gerenciadores de bancos de dados possuem softwares que podem ser utilizados como auxílio a auditoria, como, por exemplo, para efetuar cálculos, geração de relatórios, entre outras funcionalidades auxiliares.

Vantagem apontada por Imoniana (2008) no uso deste tipo de software é que, na **falta de outros recursos**, **pode-se atingir bons resultados** utilizando softwares de apoio.

Como desvantagem, é citado que sempre necessitará do **auxílio do auditado para o uso da ferramenta.**

Técnicas de auditoria

- software para auditoria;
- questionários;
- visita in loco;
- entrevista;
- teste de observância;
- teste substantivo;
- dados de teste;
- teste integrado;
- simulação paralela;
- lógica de auditoria embutida nos sistemas;
- mapeamento estatístico dos programas;
- rastreamento dos programas;
- análise da lógica de programação;
- análise de log.

Importante!!!

- *Os **logs** são arquivos que armazenam **informações de acesso e uso de um servidor, sistema ou aplicação.** Geralmente têm **data, hora, descrição do evento, informações do usuário e/ou da máquina.***

- *Um **sistema em produção**, diferentemente do que pode parecer, é um sistema que **está sendo utilizado**, **um sistema pronto**, e não um sistema que está sendo produzido (neste caso, diz-se que o sistema está em desenvolvimento).*

Auditoria baseada em **software** deve-se verificar se os *atributos estão corretos*.

No caso de a auditoria encontrar atributo incorreto, **deve-se** exibir de alguma forma o erro, seja listando ou gravando a tela na qual **evidencie** a incorreção do atributo, entre outras formas.

A listagem de código-fonte pelo auditor deve-se ater a alguns requisitos, estes são eles:

- quando não há movimento (utilização) há mais de um ano;
- quando a quantidade em estoque registrada no software for abaixo da quantidade real;
- quando a quantidade em estoque registrada for zero ou negativa.

Para a execução de teste em um sistema, o auditor pode fazê-lo de duas maneiras:

- desenvolvendo programas e os rodando com massa de dados real;
- preparando a massa de dados artificial e rodando com programas em produção.

Questionário

- Um questionário contém perguntas e um espaço necessário para que o auditor possa assinalar se o sistema satisfaz ou não o ponto de controle em questão. Caso o sistema não o satisfaça, o auditor deve então registrar a solicitação de correção. (GIL,2000)

- Há uma série de pontos de controle específicos para os quais se pode direcionar os questionários, como segurança da informação e a eficiência no uso de recursos de tecnologia da informação.

Em segurança da informação, podem-se citar:

- a segurança física dos equipamentos computacionais;
- a segurança lógica do tráfego de informações pela rede;
- o controle de acesso físico às instalações da área de tecnologia da informação;
- a segurança ambiental (combate a incêndios, invasões, atentados, sabotagens, situações de greve, inundações, entre outras).

- uso eficiente dos recursos de TI
  - o tempo médio de disponibilidade do sistema que está sendo auditado no momento;
  - o tempo de uso dos equipamentos;
  - a verificação do SLA.
    - Acordo de Nível de Serviço entre o provedor de serviços de TI e o cliente.

Visita in loco

- obtenção de dados por observação;
- obtenção de dados por teste;
- obtenção de dados por documentação;
- anotação de informações para posterior documentação

  - Caso o auditor identifique falhas, *o auditado é informado instantaneamente, pessoalmente e informalmente.* Porém, posteriormente, o auditor também notifica o auditado sobre falha por escrito.

Entrevista

- Podem ser feitas pessoalmente, por telefone e também por videoconferência.
- No planejamento da auditoria, é feito um **roteiro para a execução** das entrevistas. Este roteiro serve como um **guia, definindo a abordagem e quem serão os entrevistados.**

- De acordo com o manual de técnica de entrevista para auditorias do Tribunal de Contas da União (TÉCNICA DE ENTREVISTA PARA AUDITORIAS, 2010), existem três tipos de entrevistas de campo:
- ***estruturada; não estruturada; semiestruturada.***

- **entrevista estruturada**, o auditor utiliza formulários para a coleta de informações e dados.

- **não estruturada** é mais flexível, podendo o auditor adaptar as perguntas e o rumo da entrevista de acordo com as informações que forem adquiridas durante o processo.

- **semiestruturada** segue um roteiro prédefinido com algumas perguntas fechadas, porém, há a possibilidade do auditor estender a entrevista para abordagens diferentes conforme haja necessidade (perguntas abertas)

Teste de observância

- O **teste de aderência**, o objetivo do uso desta técnica é determinar se os procedimentos internos (controles internos) da organização estão sendo cumpridos por meio de observação por parte do auditor (LINDNER, 2015).

- Uma das particularidades do teste de observância é que o auditado não pode perceber que está sendo observado.

Teste substantivo

Objetivo de **obtenção de provas convincentes** sobre as operações, para que possa determinar sua opinião com embasamento.

Cordeiro (2015) define como **objetivos fundamentais** do teste substantivo:

- verificar a **existência real de que as transações registradas** realmente tenham acontecido;
- verificar a **integridade das informações e se permanecem inalteradas** desde sua gravação;
- verificar se **os interessados recebem as informações em sua totalidade**;
- verificar se os **itens foram avaliados e aferidos de forma correta**;
- verificar se as **transações e os registros têm sido divulgados corretamente**.

Dados de teste

- ***test data*** ou ***test deck*** e consiste em o auditor preparar um conjunto de dados que são utilizados para testar os controles do sistema auditado.

- a massa de dados deve ser preparada com o objetivo de testar uma ***grande quantidade de possibilidades e combinações de possíveis transações***, a fim de que se **possa simular o ambiente real de uso** do sistema.

Teste integrado

- Conhecida como ITF *(Integrated Test Facility),* é utilizada em ambiente **on-line**, isto é, com o sistema rodando em produção.
- Sua execução consiste na aplicação de **entidades fictícias** no sistema, para que se possa ***testar as funcionalidades sem precisar manipular os dados reais da aplicação.***
- O confronto dos dados reais com os dados de teste é o trabalho do auditor ao executar esta técnica, que acontece **sem o consentimento do operador do computador.**
- Esta técnica ***não atualiza as bases de dados reais da organização***, pois são criados arquivos separados para os dados fictícios (IMONIANA, 2008).

Simulação paralela

- Nesta técnica o programa é simulado e executado com a massa de dados real (IMONIANA, 2008).
- Focando nos pontos de controle.

Lógica de auditoria embutida nos sistemas

Inclusão da lógica de auditoria nos sistemas informatizados consiste em *desenvolver funcionalidades* que permitam ***o próprio sistema emitir*** relatórios de auditoria.

Vantagem do uso desta técnica pode-se citar o monitoramento permanente das atividades do sistema.

Como desvantagens, há o custo adicional de desenvolvimento do sistema e perda no desempenho (IMONIANA, 2008).

Mapeamento estatístico dos programas

- rotinas obsoletas ou não utilizadas;
- frequência de utilização de rotinas;
- rotinas existentes em programas já desativados ou de uso esporádico;
- rotinas mais utilizadas, normalmente a cada processamento do programa;
- rotinas fraudulentas e de uso em situações irregulares;
- rotinas de controle acionadas a cada processamento;

- pré-requisitos, como a necessidade de utilização de software de apoio e a necessidade de inclusão de instruções especiais junto aos programas em produção, acarretando em custo e perda de desempenho do programa.

Rastreamento dos programas

- transações durante o seu processamento (caminho)

Análise da lógica de programação

- determinar se a lógica das funcionalidades do sistema está em conformidade com a documentação e a efetividade dos controles programados

Análise de log

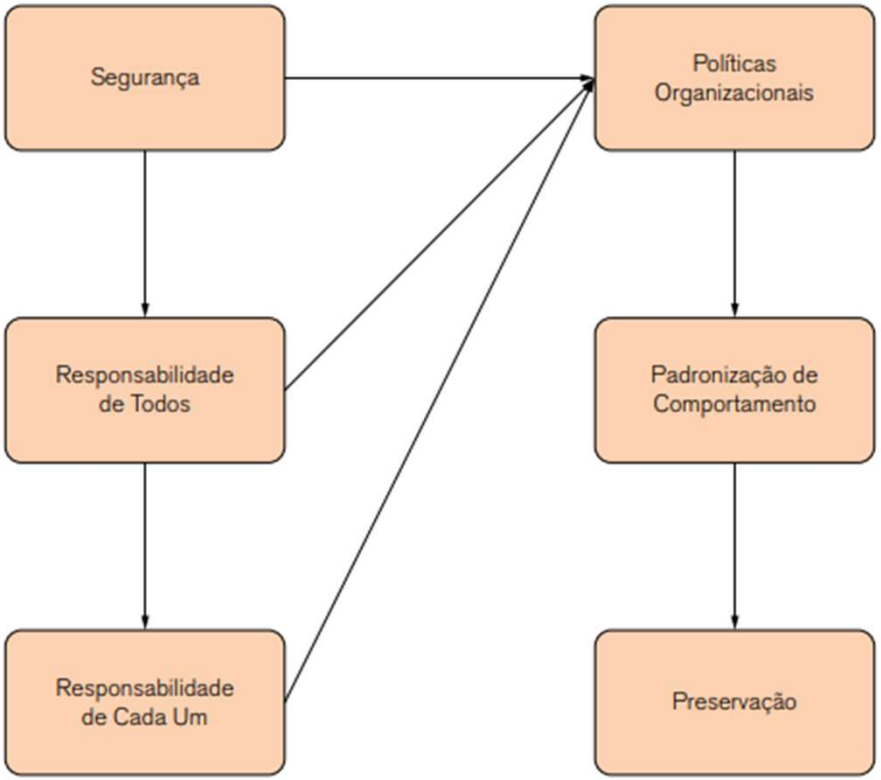
determinar erros de programas;

- flagrar o uso de programas fraudulentos;
- captar tentativas de acesso indevido a arquivos;
- monitorar a rede. Esta análise, segundo Gil (2000), pode gerar:
- indicadores de qualidade;
- indicadores para estudo e planejamento da capacidade da tecnologia da informação, buscando maior rendimento e segurança;

Auditoria de controles organizacionais e operacionais

- Políticas organizacionais
- Violação de políticas organizacionais
- Descrição de cargos em tecnologia da informação

O papel das políticas organizacionais de segurança



- Um exemplo de política de segurança de uma organização pode ser a proibição da contratação de pessoal que tenha parentesco com algum outro colaborador, evitando assim protecionismo e fraudes.

Violação de políticas organizacionais

- É necessário que se investigue a causa da violação da política para identificar se ela ocorreu por *negligência, erro, acidente, desconhecimento, problema no plano de sistemas de informação, ação deliberada, entre outros possíveis fatores causadores*.

- A política de segurança engloba ***a ação que deve ser tomada em cada tipo de violação,*** incluindo as correções sobre vulnerabilidades e a punição dos infratores.

Descrição de Cargos na TI

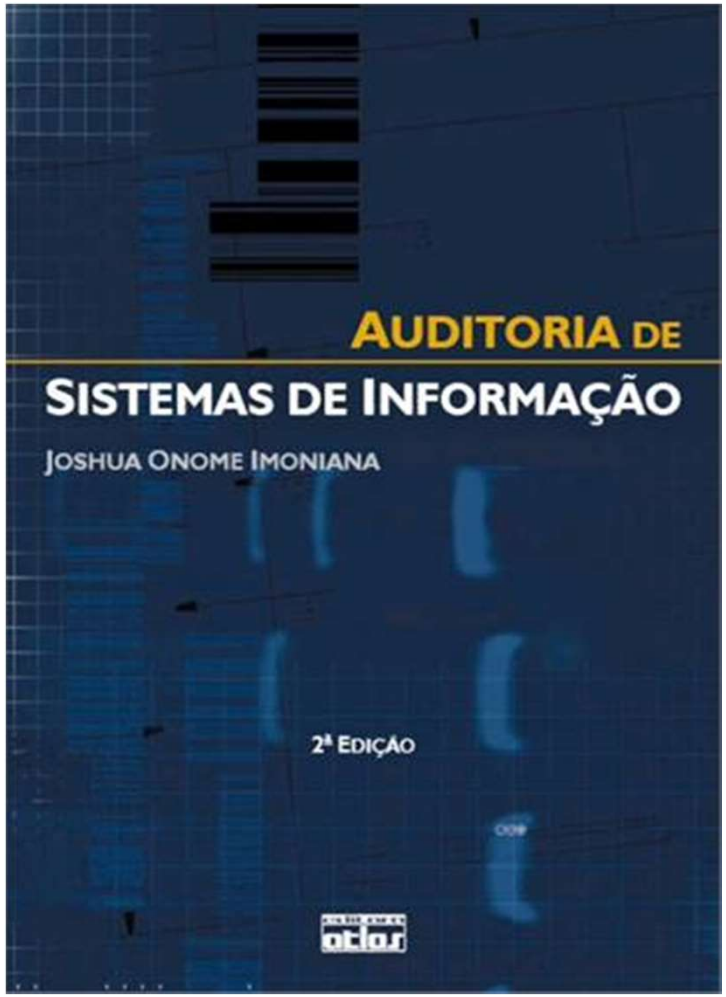
- supervisor de infraestrutura de TI;
- administrador de redes;
- administrador de bancos de dados;
- administrador de segurança;
- analista de sistemas;
- web designer;
- suporte técnico;
- supervisor de service desk;
- supervisor de restart/recovery;

Exercícios:

- 01. Quais as técnicas de auditoria que podem necessitar do desenvolvimento de programas por parte do auditor?
- 02. Quais as técnicas de auditoria que necessitam da presença física do auditor na organização auditada?
- 03. Qual o profissional de TI responsável por programar o backup dos bancos de dados?
- 04. O que pode ser alterado após uma política organizacional ter sido implantada definitivamente?

Auditoria Direcionada

- Auditoria de rede
- Auditoria de hardware
- Auditoria de controles de acesso
- Auditoria de aquisição, desenvolvimento, documentação e manutenção de sistemas
- Auditoria de operação
- Auditoria de suporte técnico



- Auditoria de Sistemas de Informação - Joshua Onome Imoniana


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE


UNIPAR
UNIVERSIDADE PARANAENSE