



**Auditoria de
TI**

Módulo II

**Teoria e
Exercícios**



www.provasdeti.com.br
<http://www.itnerante.com.br/group/contratos-e-auditoria-de-ti>
www.twitter.com/gabrielpacheco

 www.facebook.com/professorgabrielpacheco

Quem sou eu?

- ❧ PPC, PMP, CSM, MPS.BR e MBA.
- ❧ Bacharel em Ciências da Computação.
- ❧ Consultor de Projetos / EProj.
- ❧ Professor em cursos profissionalizantes e preparatórios para concursos na área de TI.
- ❧ Responsável pela publicação de materiais em PDF, artigos e comentários de questões on-line com foco em TI para Concursos.
- ❧ Fundador e coordenador pedagógico dos sites www.tiparaconcursos.net e www.metodoconcursos.com.br
- ❧ Coordenador de cursos presenciais.
- ❧ Empregado Público.
- ❧ **CONCURSEIRO DE PLANTÃO. 😊**



Links de Interesse

-  www.tcu.gov.br
-  www.cgu.gov.br
-  www.isaca.org
-  www.instosai.org
-  www.coso.org
-  www.provasdeti.com.br
-  www.itnerante.com.br
-  www.metodoconcursos.com.br
-  www.tiparaconcursos.net

Programação?

- ❧ Características do curso.
- ❧ Conteúdo programático deste módulo.
- ❧ Teoria.
- ❧ Exercícios.



Características do Curso.

- 🌀 Curso em Videoaulas.
- 🌀 Dividido em módulos de 4 a 8 horas aproximadamente.
- 🌀 Direito aos slides utilizados em todos os módulos anotados e não anotados.
- 🌀 Material de apoio. (lista de exercícios, mapa mental)
- 🌀 Módulos divididos de acordo com os atuais editais publicados e futuros editais previstos.
- 🌀 Módulos teóricos com resolução de exercícios comentados.
- 🌀 Posteriormente, módulos voltados somente à resolução de Exercícios das principais bancas (ESAF, CESPE, FCC, Cesgranrio, FGV).

Características do Curso.

Auditoria de Sistemas de Informação

- 1 Fontes de Estudo
- 2 História e Origem da Auditoria e do Controle no Brasil e no Mundo
- 3 Conceitos Aplicáveis à Auditoria de TI
 - Diferenças entre Fiscalização, Controle e Auditoria
 - Órgãos de Fiscalização, Auditoria e Controle na Administração Pública Federal
 - Tipos de Auditoria
 - Auditoria de TI
- 4 Código de Ética e Padrões
- 5 Abordagens de Auditoria de Sistemas de Informação
- 6 Procedimentos de Auditoria de Sistemas Aplicativos
- 7 Abordagem Técnica da Auditoria de TI

Fontes de Estudo.

- TCU:
 - www.tcu.gov.br.
 - Glossário de Termos de Controle.
 - Normas de Auditoria do TCU – NATs.
- CGU:
 - www.cgu.gov.br.
 - Manual de Auditoria – IN SFC 01/2001.
- Livros:
 - Auditoria de Sistemas de Informação – Joshua Imoniana – 2ª edição – 2011.
 - Auditoria e Controle de Sistemas de Informação – 2009.
 - Princípios de Sistemas de Informação – Star Reinolds - 2002.
 - Implantando a Governança de TI da Estratégia à Gestão de Processos – 4ª Edição.

Fontes de Estudo.



Fontes de Estudo.

- Site da ISACA:
 - www.isaca.org/portuguese/pages/default.aspx.
 - Cobit 5.
 - Certificações da ISACA.
 - Normas de Auditoria e Garantia de Sistemas de Informação.
- Site do COSO:
 - www.coso.org.
 - Principal modelo norteador da estruturação de sistemas de controles internos e de gestão de risco.
- www.cespe.unb.br
- www.fcc.org.br
- www.cesgranrio.org.br
- www.esaf.fazenda.gov.br

Características do Curso.

Auditoria de Sistemas de Informação

- 1 Fontes de Estudo
- 2 História e Origem da Auditoria e do Controle no Brasil e no Mundo
- 3 Conceitos Aplicáveis à Auditoria de TI
 - Diferenças entre Fiscalização, Controle e Auditoria
 - Órgãos de Fiscalização, Auditoria e Controle na Administração Pública Federal
 - Tipos de Auditoria
 - Auditoria de TI
- 4 Código de Ética e Padrões
- 5 Abordagens de Auditoria de Sistemas de Informação
- 6 Procedimentos de Auditoria de Sistemas Aplicativos
- 7 Abordagem Técnica da Auditoria de TI

Procedimentos de Auditoria de Sistemas Aplicativos.

- Referem-se àqueles executados para averiguar se os sistemas que constituem o cerne de negócio de uma empresa registram as transações rotineiras adequadamente.
- Possuem como objetivos globais:
 - Integridade
 - Confidencialidade
 - Privacidade
 - Acuidade
 - Disponibilidade
 - Auditabilidade
 - Versatibilidade
 - Manutenibilidade

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[48] Os objetivos globais referentes à auditoria de sistemas aplicativos NÃO incluem

- a) integridade e privacidade
- b) confidencialidade e disponibilidade.
- c) acuidade e auditabilidade.
- d) versatilidade e manutenibilidade.
- e) irreversibilidade e retratabilidade.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[48] Os objetivos globais referentes à auditoria de sistemas aplicativos NÃO incluem

- a) integridade e privacidade
- b) confidencialidade e disponibilidade.
- c) acuidade e auditabilidade.
- d) versatilidade e manutenibilidade.
- e) irreversibilidade e retratabilidade.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.

- ☞ Sistema Geral de Controle Interno:

- ☞ Principais Objetivos:

- ☞ Salvar o ativo de uma organização.
 - ☞ Manter a Integridade, correção e confiabilidade dos registros contábeis.
 - ☞ Promover a eficiência operacional.
 - ☞ Encorajar o cumprimento dos procedimentos e políticas da gerência.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.

🌀 Princípios de Controle Interno:



🌀 Supervisão, Registro e Comunicação, Segregação das funções, Classificação de informação, Tempestividade, Auditoriabilidade, Controle Independente, Monitoramento, Implantação, Contingência, Custo-Efetivo.



Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.



Princípios de Controle Interno:

-  **Supervisão:** A gerência por objetivos, procedimentos e tomada de decisões deve manter um controle que a capacite a uma supervisão efetiva dentro do ambiente de TI.
-  **Registro e Comunicação:** A gerência da empresa deve estabelecer critérios para criação, processamento e disseminação de informação de dados, através de autorização e registro de responsabilidades.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.



Princípios de Controle Interno:

-  Segregação das funções: As responsabilidades e ocupações incompatíveis devem estar segregadas de maneira a minimizar as possibilidades de perpetuação de fraudes e até de suprimir erro e irregularidade na operação normal.
-  Classificação de informação: A gerência deve estabelecer um plano de classificação de informação que melhor sirva às necessidades da organização, em conformidade com os princípios de contabilidade geralmente aceitos e também padrões de auditoria geralmente aceitos.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.



Princípios de Controle Interno:

-  **Tempestividade:** A gerência deve delinear procedimentos, monitorar os registros corretos das transações econômicas, financeiras e contábeis das empresas, processando-as e comunicando os resultados às pessoas necessárias em tempo hábil.
-  **Auditoriabilidade:** Os procedimentos operacionais devem permitir a programação e verificação periódica no que concerne à precisão do processo de processamento de dados e de geração de relatório, de acordo com as políticas.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.



Princípios de Controle Interno:

-  Controle Independente: Os sistemas em funcionamento devem ter procedimentos adequados para identificação e correções de erros no fluxo de processamento, inclusive nos processos executados concomitantemente.
-  Monitoramento: A gerência deve possuir acesso máster ao sistema e controle de uso que lhe permita fazer o acompanhamento pari passu das transações.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.


Princípios de Controle Interno:

-  Implantação: A gerência deve planejar a aquisição, o desenvolvimento, a manutenção e a documentação de sistema, de forma a coincidir com as metas empresariais.
-  Contingência: A gerência deve implementar um plano adequado e procedimentos de implantação para prevenir-se contra as falhas de controles que podem surgir durante especificações de sistema, desenho, programação, testes e documentação de sistemas e nas fases pós-implementações.

Procedimentos de Auditoria de Sistemas Aplicativos.

Controle Interno em Sistemas de Informação.

 **Princípios de Controle Interno:**

 **Custo-Efetivo:** Investimentos em tecnologia da informação devem ser propriamente planejados, a fim de coincidirem com o custo efetivo.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

☞ Controles Administrativos e Gerenciais:

☞ São de responsabilidade da gerência.

☞ Incluem:




- ☞ Separação convencional de funções ou responsabilidades (segregação de funções).
- ☞ Estabelecimento de objetivos e metas de segurança da informação.
- ☞ Planos orçamentários.
- ☞ Seleção de pessoal.
- ☞ Designação de autoridades e treinamento de pessoal.
- ☞ Desenvolvimento de implementação de medidas corretivas para os desvios de políticas e padrões estipulados para o processo de gerenciamento.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

Controles de Segurança e Privacidade:

Privacidade:



-  Mostra um estado oculto e fora do alcance de algum grupo particular em um ambiente de computação, programas, aplicativos, dados e/ou equipamentos e informação pertencentes a pessoas restritas e certas funções.
-  Acaba gerando frequentes mudanças de regras de tempos em tempos.
-  Trata desde a proteção física até a prevenção de incidentes fatais que podem causar danos irreversíveis em documentos e aplicações da organização.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

Controles de Segurança e Privacidade:

Propriedades:



-  Sigilo: fornecer uma privacidade ou situação estritamente confidencial aos dados. Um pequeno deslize nesta propriedade conduz a uma derrocada de assuntos restritos.
-  Integridade: fornecer um requisito de informação completa, correta e válida e confiabilidade a dados autorizados, guardando-os das distribuições e modificações não usuais. Qualquer sistema que preencha tais requisitos estará manifestando as propriedades de integridade.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

Controles de Segurança e Privacidade:

Propriedades:


-  Disponibilidade: tornar os dados disponíveis a quem quer que esteja autorizado a usar tais dados. Apesar de ser dada proteção total aos dados, os requisitos para usá-los não devem ser prejudiciais. No entanto, poderão ser extraídas informações com um mínimo esforço ou interferência.
-  Contabilidade: registrar todas as transações ocorridas nos sistemas, a fim de permitir o relato correto do conteúdo dos dados alimentados no sistema e, sobretudo, permitir, quando for necessário, rastrear a verdade e reportar a visão justa das informações armazenadas.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

Controles de Segurança e Privacidade:

Propriedades:

-  Auditoriabilidade: em qualquer sistema de segurança os dados devem ser auditados. Isso possibilita à gerência relatórios de acompanhamento, para que se saiba se estão sendo efetivos os controles implementados. O sistema também deve fornecer facilidade necessária para exames e averiguação de responsabilidades.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

☞ Controles de preparação e captação de dados:

- ☞ Realizado no início de cada atividade de processamento de dados.
- ☞ Envolve o recebimento de documentos, a pré-numeração e preparação de input.
- ☞ Documentos são convertidos em lote
 - ☞ Precisaremos controlar estes arquivos de lote (chamados de batches) e neste caso eles são controlados pelo uso dos totais de controle, garantindo assim que os lotes pretendidos estejam completos.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.






☞ Controles de entrada de dados.

- ☞ Dados que entram errados em um sistema irão produzir fatalmente saídas erradas.
- ☞ Recursos a serem utilizados no controle da entrada de dados.
 - ☞ Criação de documentos de leituras óticas.
 - ☞ Uso de documentos pré-numerados sequencialmente.
 - ☞ Autorização própria para inputs de dados.
 - ☞ Uso de Control Totals (CRT).
 - ☞ Uso de dígitos de checagem completa.
 - ☞ Controles embutidos nos próprios sistemas.
 - ☞ Controladores de linha e modem loop-back.
 - ☞ Backup de discagem automática para garantir a continuidade das operações.
 - ☞ Etiquetas de arquivos.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.


Controles de processamento:

-  Atuam no momento que os dados já estão no computador e precisam ser processados.
-  Trabalha com:
 -  Checagens da sequência dos arquivos mestres e arquivos de transações.
 -  Checagem dos campos dos arquivos para detecção de superposição de dados.
 -  Limite lógico, testes de racionalidade e totais cruzados.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.



Controles de saída e de emissão de relatórios:

-  Os procedimentos de manuseio de output devem ser administrados, a fim de assegurar que os relatórios solicitados sejam impressos ou transmitidos e que somente pessoas autorizadas devem recebê-los.

Procedimentos de Auditoria de Sistemas Aplicativos.

Tipos de Controles em Sistemas de Informação.

Controles de gravação e recuperação de dados:

-  Certifica a integridade de dados recebidos dentro da base de dados e qualquer indivíduo autorizado pode acessá-lo com o mínimo esforço.
-  Necessidade da utilização de senhas e códigos de acessos como fatores primordiais.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[45] No tocante a auditoria de TI, principalmente aos fundamentos de controles internos, considere:

- I. Os principais objetivos de um sistema geral de controle, entre outros, são salvaguardar o ativo de uma organização, manter a integridade, correção e confiabilidade dos registros contábeis.
- II. A gerência por objetivos, procedimentos e tomada de decisões deve manter um controle que a capacite a uma supervisão efetiva dentro do ambiente de tecnologia da informação.
- III. As responsabilidades e ocupações compatíveis devem estar segregadas de maneira a minimizar as possibilidades de perpetuação de fraudes e até de suprimir erro e irregularidade na operação normal.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[45] No tocante a auditoria de TI, principalmente aos fundamentos de controles internos, considere:

Está correto o que consta em

- a) III, apenas.
- b) I e III, apenas.
- c) I e II, apenas.
- d) II e III, apenas.
- e) I, II e III.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[45] No tocante a auditoria de TI, principalmente aos fundamentos de controles internos, considere:

Está correto o que consta em

- a) III, apenas.
- b) I e III, apenas.
- c) I e II, apenas.
- d) II e III, apenas.
- e) I, II e III.

Exercícios.

(INMETRO – Analista em Métricas e Qualidade – Ciências da Computação – 2007 – CESPE)

Julgue os próximos itens, relativos a conceitos de auditoria e controle de riscos em tecnologia da informação (TI).

[118] Após uma auditoria, as recomendações para a separação de técnicos de uma organização de desenvolvimento de sistemas em duas equipes: de desenvolvimento e de teste, podem ser diretamente embasadas no princípio da segregação de responsabilidades.

Exercícios.

(INMETRO – Analista em Métricas e Qualidade – Ciências da Computação – 2007 – CESPE)

Julgue os próximos itens, relativos a conceitos de auditoria e controle de riscos em tecnologia da informação (TI).

[118] Após uma auditoria, as recomendações para a separação de técnicos de uma organização de desenvolvimento de sistemas em duas equipes: de desenvolvimento e de teste, podem ser diretamente embasadas no princípio da segregação de responsabilidades.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[72] Em uma auditoria, se os controles se apresentam estabelecidos

- a) adequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência limitada.
- b) inadequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência significativa.
- c) adequadamente e forem aplicados consistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência limitada.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[72] Em uma auditoria, se os controles se apresentam estabelecidos

d) inadequadamente e forem aplicados consistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência significativa.

e) inadequadamente ou forem aplicados inconsistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência significativa.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[72] Em uma auditoria, se os controles se apresentam estabelecidos

- a) **adequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência limitada.**
- b) inadequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência significativa.
- c) adequadamente e forem aplicados consistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência limitada.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[74] No processo de Avaliação de Riscos, no qual são executadas as análises da relevância dos riscos identificados nas entidades do setor público, NÃO se inclui

- a) a forma de como serão gerenciados.
- b) a avaliação das probabilidades de suas ocorrências.
- c) a resposta aos riscos, indicando a decisão gerencial para mitigá-los, considerando as hipóteses de eliminação, redução, aceitação ou compartilhamento.
- d) a definição das ações para prevenir ocorrências ou para minimizar os seus efeitos.
- e) o acompanhamento dos pressupostos do controle interno.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[74] No processo de Avaliação de Riscos, no qual são executadas as análises da relevância dos riscos identificados nas entidades do setor público, NÃO se inclui

- a) a forma de como serão gerenciados.
- b) a avaliação das probabilidades de suas ocorrências.
- c) a resposta aos riscos, indicando a decisão gerencial para mitigá-los, considerando as hipóteses de eliminação, redução, aceitação ou compartilhamento.
- d) a definição das ações para prevenir ocorrências ou para minimizar os seus efeitos.
- e) o acompanhamento dos pressupostos do controle interno.

Características do Curso.

Auditoria de Sistemas de Informação

- 1 Fontes de Estudo
- 2 História e Origem da Auditoria e do Controle no Brasil e no Mundo
- 3 Conceitos Aplicáveis à Auditoria de TI
 - Diferenças entre Fiscalização, Controle e Auditoria
 - Órgãos de Fiscalização, Auditoria e Controle na Administração Pública Federal
 - Tipos de Auditoria
 - Auditoria de TI
- 4 Código de Ética e Padrões
- 5 Abordagens de Auditoria de Sistemas de Informação
- 6 Procedimentos de Auditoria de Sistemas Aplicativos
- 7 Abordagem Técnica da Auditoria de TI

Abordagem Técnica da Auditoria de TI.

Ferramentas e Técnicas de Auditoria de TI.

- Chamadas de TAAC - Técnicas de Auditoria Asssistida por Computadores.
- Possuem como principal objetivo auxiliar o auditor a auditar 100% a população da área ou transação revisada.
- Podem ser aplicadas em diferentes situações:
 - Testes de controles gerais: como de configuração de um Sistema Operacional ou para confirmação de versões aprovadas em um ambiente de produção.
 - Testes de detalhes de transações: exemplos clássicos seriam o recalcule dos saldos ou a geração de juros sobre uma conta cliente
 - Analítico e substantivo: para identificação de inconsistências ou flutuações anormais nas contas e grupos de contas contábeis.
 - Amostragem: para gerar amostras para alimentação dos programas de auditoria.

Abordagem Técnica da Auditoria de TI.

Ferramentas e Técnicas de Auditoria de TI.

- 🌀 A aplicação de TAACs seguem os seguintes passos
 - 🌀 Estabelecer os objetivos da aplicação de TAAC.
 - 🌀 Determinar os dados a serem utilizados para as técnicas, inclusive a forma de acesso.
 - 🌀 Identificar os arquivos e bancos de dados a serem testados.
 - 🌀 Entender as entidades de relacionamentos das tabelas de dados onde a base de dados será examinada.
 - 🌀 Definir testes e procedimentos de testes, inclusive as transações e contras e grupos de contas afetadas.
 - 🌀 Definir os relatórios esperados.
 - 🌀 (...)

Abordagem Técnica da Auditoria de TI.

Ferramentas e Técnicas de Auditoria de TI.

- 🌀 A aplicação de TAACs seguem os seguintes passos
 - 🌀 (...)
 - 🌀 Programar junto aos clientes e sua área de informática cópias de arquivos ou bases de dados que devem ser gerados com cut-off de data e tempo adequados.
 - 🌀 Identificar o técnico que irá processar a aplicação de TAAC.
 - 🌀 Estimar os custos de TAAC.
 - 🌀 Certificar que os processos de TAAC foram adequadamente executados e os papéis de trabalhos documentados.
 - 🌀 Avaliar resultados.

Abordagem Técnica da Auditoria de TI. Softwares e Aplicativos.

- 🌀 Software Generalista de Auditoria de TI.
 - 🌀 Série de software em ambiente batch.
 - 🌀 Suas funções são:
 - 🌀 Extração de dados de amostra.
 - 🌀 Testes globais.
 - 🌀 Geração de dados estatísticos para análise.
 - 🌀 Sumarização.
 - 🌀 Composição de outro arquivo a partir de um arquivo mestre de dados.
 - 🌀 Apontamento de duplicidade de registros ou sequência incorreta.

Abordagem Técnica da Auditoria de TI. Softwares e Aplicativos.

🌀 Software Generalista de Auditoria de TI.

🌀 Os principais softwares generalistas encontrados são:

🌀 ACL - Audit Command Language

🌀 Utilizado na extração e análise de dados.

🌀 Desenvolvido no Canadá.

🌀 IDEA - Interactive Data Extration e Analysis

🌀 Utilizado na extração e análise de dados.

🌀 Desenvolvido no Canadá.

🌀 Animation

🌀 Versão norte-americana do IDEA.

Abordagem Técnica da Auditoria de TI. Softwares e Aplicativos.

- Software Generalista de Auditoria de TI.

- Os principais softwares generalistas encontrados são:

- Galileo

- Software integrado de gestão de auditoria.

- Principais funções

- Riscos de auditoria

- Documentação

- Emissão de relatório

- Pentana

- Software de planejamento estratégico de auditoria

- Principais recursos

- Planejamento e monitoramento de recursos.

- Controle de horas.

- Registro de checklists e programas de auditoria.

- Desenho e gerenciamento de plano de ação.

Abordagem Técnica da Auditoria de TI. Softwares e Aplicativos.

- Softwares Especializados.
 - Desenvolvido especificamente para executar certas tarefas em um circunstância pré-definida.
 - Pode ser desenvolvido pelo próprio Auditor.
- Programas Utilitários.
 - Utilizados pelos Auditores em atividades do dia a dia.
 - Podem ser encontrados até mesmo em SGBDs.

Abordagem Técnica da Auditoria de TI.






Técnicas

- ⌚ Abordagem está para um jogo assim como a Técnica está para a regra do jogo.
- ⌚ Vantagens esperadas:
 - ⌚ Produtividade.
 - ⌚ Custo.
 - ⌚ Qualidade assegurada.
 - ⌚ Valor agregado.
 - ⌚ Benefícios corporativos.
 - ⌚ Benefícios para o auditor.

Abordagem Técnica da Auditoria de TI.

Técnicas

Dados de Teste.

-  Test Data ou Test Deck
-  Aplicado em ambientes de processamento batch.
-  Possui um conjunto de dados de entrada pré-formatados especialmente com o objetivo de testar os controles programados e os controles de sistemas aplicativos.
-  Realiza diversas transações para que se possa no final ter como comparar os resultados obtidos com os predeterminados.
-  Trata-se de uma simulação de dados para que sejam realizados testes nos processos computacionais.

Abordagem Técnica da Auditoria de TI. Técnicas





🌀 Dados de Teste.

🌀 Fases:

- 🌀 Selecionar o módulo de sistema
- 🌀 Escolher o parâmetro de controle
- 🌀 Elaborar a simulação dos dados de teste
- 🌀 Preparar os formulários de controle
- 🌀 Transcrever os dados para o sistema
- 🌀 Criar as condições do teste
- 🌀 Processar os dados
- 🌀 Avaliar os resultados
- 🌀 Redigir o relatório sobre o ponto de controle

Abordagem Técnica da Auditoria de TI. Técnicas



Facilidade de teste integrado

-  Integrated Test Facility (ITF).
-  Executada somente em ambientes on-line e realtime, visto que faz uso das versões em produção.
-  Faz uso de entidades fictícias no sistema.
-  Após os resultados obtidos com a entidades fictícias, eles são confrontados com os resultados esperados.



Abordagem Técnica da Auditoria de TI.

Técnicas

Simulação Paralela:







-  O programa aqui é desenvolvido pelo próprio Auditor para fazer a execução paralela.
-  Trabalha com um programa específico para atender a todas as lógicas necessárias para um aplicativo devidamente testado de forma que seus resultados possam ser comparados com dados de transações executadas anteriormente

Lógica de Auditoria embutida nos sistemas:

-  Inclusão direta nos sistemas em seu momento de desenvolvimento de lógicas de auditoria.
-  Gera a emissão de relatórios periódicos.

Abordagem Técnica da Auditoria de TI. Técnicas




Rastreamento e mapeamento

-  Trabalha com o desenvolvimento de uma trilha de auditoria (audit trail) para acompanhar certos pontos da lógica do processamento de algumas transações
 -  Trilha de auditoria é um meio
-  Seus apontamentos trabalham com dados estatísticos baseados em funções não executadas, como
 -  Tempo de máquinas utilizado
 -  Funções executadas
 -  Quantas vezes essas funções foram executadas

Abordagem Técnica da Auditoria de TI.

Técnicas

Análise da lógica de programação

-  Comparação entre lógica de programação e os documentos dos sistemas aplicativos
-  Avalia se as instruções dadas ao computador são as mesmas já identificadas nos respectivos documentos
-  Pode ser feita manualmente ou com o uso de software

Exercícios.

(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)

[72] A técnica de auditoria denominada test-deck trata-se de

- a) uma tabulação de um arquivo log para verificar a utilização de um recurso computacional.
- b) um rastreamento do processamento para avaliar o caminho de uma transação.
- c) um mapeamento do processamento para identificar rotinas não utilizadas.
- d) uma simulação de dados para testar processos computacionais.
- e) uma análise de dados para avaliar a integridade das informações.

Exercícios.

(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)

[72] A técnica de auditoria denominada test-deck trata-se de

- a) uma tabulação de um arquivo log para verificar a utilização de um recurso computacional.
- b) um rastreamento do processamento para avaliar o caminho de uma transação.
- c) um mapeamento do processamento para identificar rotinas não utilizadas.
- d) uma simulação de dados para testar processos computacionais.
- e) uma análise de dados para avaliar a integridade das informações.

Exercícios.

(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)

Para assegurar que as medidas de controle estabelecidas estejam funcionando como prescrito de maneira consistente e contínua e para concluir sobre a adequação do ambiente de controle, os passos de auditoria são estabelecidos, em uma guia de auditoria, na etapa

- a) obtendo um entendimento.
- b) avaliando os controles.
- c) elaborando o relatório.
- d) avaliando a conformidade.
- e) evidenciando o risco.

Exercícios.

(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)

Para assegurar que as medidas de controle estabelecidas estejam funcionando como prescrito de maneira consistente e contínua e para concluir sobre a adequação do ambiente de controle, os passos de auditoria são estabelecidos, em uma guia de auditoria, na etapa

- a) obtendo um entendimento.
- b) avaliando os controles.
- c) elaborando o relatório.
- d) avaliando a conformidade.
- e) evidenciando o risco.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[21] Sobre Auditoria de TI, analise:

I. Nos projetos de TI a auditoria tem ênfase na análise do passado e não na avaliação atual dos processos da empresa para definir ações futuras.

II. Todos os processos de auditoria são reativos, ou seja, buscam culpados por determinadas ocorrências geradas, as quais tenham ou não trazido determinados riscos operacionais ou mesmo de imagem à corporação.

III. O CobiT pode ampliar a visão da auditoria interna possibilitando uma melhor identificação dos riscos relacionados com a TI e a apresentação de resultados consistentes, com baixo grau de refutação por parte dos auditados.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[21] Sobre Auditoria de TI, analise:

IV. Os resultados das auditorias podem provocar discussões internas e a identificação da necessidade de evolução da maturidade dos processos e do modelo de governança de TI, que deve estar sustentada pela Governança Corporativa.

Está correto o que consta em

- a) III, apenas.
- b) II e IV, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) I, II, III e IV.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[21] Sobre Auditoria de TI, analise:

IV. Os resultados das auditorias podem provocar discussões internas e a identificação da necessidade de evolução da maturidade dos processos e do modelo de governança de TI, que deve estar sustentada pela Governança Corporativa.

Está correto o que consta em

- a) III, apenas.
- b) II e IV, apenas.
- c) **III e IV, apenas.**
- d) I, II e III, apenas.
- e) I, II, III e IV.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[22] Sobre as etapas do processo de auditoria interna de TI é correto afirmar:

- a) Possui 6 etapas: Planejamento, Análise, Projeto, Execução, Relatório e Plano de Ação.
- b) A identificação e apresentação dos Pontos de Auditoria ocorrem apenas em duas fases do processo de auditoria: no Planejamento da Auditoria e no Relatório de Auditoria.
- c) Os documentos resultantes da Auditoria de TI são apresentados apenas à área de TI, pois mostra a direção a ser tomada e os investimentos prioritários e necessários apenas nessa área.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[22] Sobre as etapas do processo de auditoria interna de TI é correto afirmar:

- d) Tem como resultado alguns documentos que geralmente contêm informações sobre os riscos encontrados e a avaliação desses riscos, os controles em conformidade ou não com normas, e recomendações de melhoria.
- e) Apesar do relatório de auditoria funcionar como um mapa que mostra a direção a ser tomada pela área de TI, ele não serve como um guia para auxiliar a administração no planejamento estratégico e na priorização de investimentos, pois apresenta informações técnicas de interesse exclusivo da área de TI.

Exercícios.

(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

[22] Sobre as etapas do processo de auditoria interna de TI é correto afirmar:

d) Tem como resultado alguns documentos que geralmente contêm informações sobre os riscos encontrados e a avaliação desses riscos, os controles em conformidade ou não com normas, e recomendações de melhoria.

e) Apesar do relatório de auditoria funcionar como um mapa que mostra a direção a ser tomada pela área de TI, ele não serve como um guia para auxiliar a administração no planejamento estratégico e na priorização de investimentos, pois apresenta informações técnicas de interesse exclusivo da área de TI.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[73] Sobre a documentação de auditoria, considere:

- I. O conteúdo da documentação deve ser registrado apenas em papel para facilitar a apresentação de evidências.
- II. Resumos ou cópias de registros da entidade podem ser incluídos na documentação.
- III. Versões superadas de papéis de trabalho e de demonstrações financeiras não precisam ser incluídas na documentação.
- IV. A existência de plano de auditoria demonstra que o auditor planejou a auditoria.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[73] Sobre a documentação de auditoria, considere:

Está correto o que se afirma em

- a) I, II, III e IV.
- b) II, III e IV, apenas.
- c) I e III, apenas.
- d) II e IV, apenas.
- e) II, apenas.

Exercícios.

(TCE-SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

[73] Sobre a documentação de auditoria, considere:

Está correto o que se afirma em

- a) I, II, III e IV.
- b) II, III e IV, apenas.
- c) I e III, apenas.
- d) II e IV, apenas.
- e) II, apenas.

Exercícios.

(SEBRAE II – AN07 – Analista Técnico II – 2010 - Cespe)

A respeito das ferramentas de extração de dados, julgue os seguintes itens.

[57] A utilização de software generalista de auditoria de tecnologia de informação envolve o uso de programa específico, o que inibe a extração de dados de vários ambientes distintos para a realização da auditoria.

Exercícios.

(SEBRAE II – AN07 – Analista Técnico II – 2010 - Cespe)

A respeito das ferramentas de extração de dados, julgue os seguintes itens.

[57] A utilização de software generalista de auditoria de tecnologia de informação envolve o uso de programa específico, o que inibe a extração de dados de vários ambientes distintos para a realização da auditoria.

Exercícios.

(SEF-SC – Tecnologia da Informação – 2010 – CESPE)

[56] Com relação à auditoria de segurança de sistemas, assinale a alternativa correta.

- a) Em um processo de auditoria de sistema, o auditor deve necessariamente ser um colaborador da organização auditada, preferencialmente, deve pertencer ao setor analisado na auditoria.
- b) Achados de auditoria são fatos significativos observados pelo auditor durante a execução da auditoria. Geralmente, são associados a falhas e irregularidades, porém podem também indicar pontos fortes da instituição auditada. O achado deve ser relevante e baseado em fatos e evidências irrefutáveis.

Exercícios.

(SEF-SC – Tecnologia da Informação – 2010 – CESPE)

[56] Com relação à auditoria de segurança de sistemas, assinale a alternativa correta.

c) A auditoria da segurança de informação tem como principal objetivo implantar a política de segurança e o plano de continuidade de negócios (PCN) de uma organização.

d) O processo de auditoria está dividido em três fases: planejamento, execução e relatório. Na fase de planejamento, todas as evidências das falhas e irregularidades encontradas devem ser coletadas para que durante a fase de execução as devidas correções nos controles sejam realizadas.

e) Devido à falta de confiabilidade dos dados processados por computador, ferramentas computacionais de apoio, tais como mapping, tracing e snapshot, não podem ser empregadas em auditorias de segurança.

Exercícios.

(SEF-SC – Tecnologia da Informação – 2010 – CESPE)

[56] Com relação à auditoria de segurança de sistemas, assinale a alternativa correta.

a) Em um processo de auditoria de sistema, o auditor deve necessariamente ser um colaborador da organização auditada, preferencialmente, deve pertencer ao setor analisado na auditoria.

b) Achados de auditoria são fatos significativos observados pelo auditor durante a execução da auditoria. Geralmente, são associados a falhas e irregularidades, porém podem também indicar pontos fortes da instituição auditada. O achado deve ser relevante e baseado em fatos e evidências irrefutáveis.

Exercícios.

(TJ-PE – Analista Judiciário – Analista de Suporte – 2007 – FCC)

[29] Em auditoria de sistemas, para verificar se os controles estão funcionando conforme prescrito, consistentemente e continuamente, utiliza-se:

- a) documentação dos requisitos de negócio.
- b) documentação das evidências.
- c) teste de conformidade.
- d) teste substantivo.
- e) identificação dos pontos de controle.

Exercícios.

(TJ-PE – Analista Judiciário – Analista de Suporte – 2007 – FCC)

[29] Em auditoria de sistemas, para verificar se os controles estão funcionando conforme prescrito, consistentemente e continuamente, utiliza-se:

- a) documentação dos requisitos de negócio.
- b) documentação das evidências.
- c) teste de conformidade.
- d) teste substantivo.
- e) identificação dos pontos de controle.

Exercícios.

(TJ-PE – Analista Judiciário – Analista de Suporte – 2007 – FCC)

[30] Para uma avaliação de auditoria nas funcionalidades das transações de negócio realizadas por um sistema em operação normal, deve-se utilizar a técnica

- a) test-deck.
- b) teste beta.
- c) teste de desempenho.
- d) análise de dados.
- e) verificação in-loco.

Exercícios.

(TJ-PE – Analista Judiciário – Analista de Suporte – 2007 – FCC)

[30] Para uma avaliação de auditoria nas funcionalidades das transações de negócio realizadas por um sistema em operação normal, deve-se utilizar a técnica

- a) test-deck.
- b) teste beta.
- c) teste de desempenho.
- d) análise de dados.
- e) verificação in-loco.

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 🌀 Metodologia adotada pelos auditores de TI para saberem quais as ameaças puras ou prováveis em um ambiente de TI de um organização, claramente são as ameaças que vão representar eventos futuros não desejáveis e incertos para a organização e que gerarão perdas, caso ocorram.

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 🌀 Resolução CFC nº 981/2003 – Conselho Federal de Contabilidade.
- 🌀 *11.6.1.7 - O auditor independente deve considerar a possibilidade de distorções de valores, relativamente, não-relevantes que, ao serem acumulados, possam, no conjunto, produzir distorção relevante nas demonstrações contábeis. Por exemplo, um erro na aplicação de um procedimento de encerramento mensal pode ser um indicativo de uma distorção relevante durante o exercício social, caso tal erro se repita em cada um dos meses.*
- 🌀 *Indícios de erros repetitivos, mesmo não-relevantes, individualmente, podem indicar deficiência nos controles internos, requerendo do auditor independente o aprofundamento dos exames.*

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 11.6.1.8 - O auditor independente deve avaliar a questão da relevância tanto em relação às demonstrações contábeis tomadas em conjunto como em relação a saldos individuais de contas, classes de transações e divulgações (notas explicativas). A avaliação da relevância pode ser influenciada por requisitos regulatórios e aspectos particulares de rubricas específicas das demonstrações. Tal avaliação pode resultar em diferentes níveis de relevância.

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 🌀 11.6.1.9 - A relevância definida, quantificada e documentada nos papéis de trabalho que evidenciam o planejamento deve ser considerada pelo auditor independente ao:
- 🌀 a) determinar a natureza, época e extensão dos procedimentos de auditoria; e
- 🌀 b) avaliar o efeito de distorções identificadas.

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 🌀 11.6.2 - *Relacionamento entre a relevância e os riscos de auditoria*
- 🌀 11.6.2.1 - *Ao definir seu plano de auditoria, o auditor independente deve levar em conta quais fatores poderiam resultar em distorções relevantes nas demonstrações contábeis sob exame. A avaliação do auditor independente, quanto à relevância de rubricas específicas e classes de transações ou divulgações necessárias, ajuda-o a decidir sobre assuntos de planejamento de auditoria, como por exemplo:*
 - 🌀 a) *quais itens a examinar;*
 - 🌀 b) *onde aplicar, ou não, amostragem e procedimentos analíticos.*
 - 🌀 *Isso permite ao auditor independente selecionar procedimentos de auditoria que, combinados, possam reduzir o risco de auditoria a um nível aceitável.*

Abordagem Técnica da Auditoria de TI.

Risco de Auditoria.

- 🌀 11.6.2.2 - *Existe uma relação inversa entre o risco de auditoria e o nível estabelecido de relevância, isto é, quanto menor for o risco de auditoria, maior será o valor estabelecido como nível de relevância e vice-versa. O auditor independente toma essa relação inversa em conta ao determinar a natureza, época e extensão dos procedimentos de auditoria. Por exemplo, se na execução de procedimentos específicos de auditoria, o auditor independente determinar que o nível de risco é maior que o previsto na fase de planejamento, o nível de relevância, preliminarmente estabelecido, deve ser reduzido. O auditor independente deve atenuar tal ocorrência por:*
- 🌀 a) *reduzir o nível de risco de controle, onde praticável, e suportar tal redução por meio de ampliação dos testes de controles; ou*
- 🌀 b) *reduzir o risco de detecção via modificação da natureza, época e extensão dos testes substantivos planejados.*

Exercícios.

(TCE-GO – Analista de Controle Externo - TI– 2009 – FCC)

[94] Na relação entre risco de auditoria e relevância,

- I. quanto maior o risco, maior será o valor estabelecido como nível de relevância.
- II. quanto maior a relevância de um item, menor é a possibilidade de ele não ser selecionado para teste.
- III. o auditor deve selecionar o item que será examinado para diminuir o risco.

Está correto o que se afirma em

- a) I, II e III.
- b) I, apenas.
- c) I e II, apenas.
- d) I e III, apenas.
- e) II e III, apenas.

Exercícios.

(TCE-GO – Analista de Controle Externo - TI– 2009 – FCC)

[94] Na relação entre risco de auditoria e relevância,

- I. quanto maior o risco, maior será o valor estabelecido como nível de relevância.
- II. quanto maior a relevância de um item, menor é a possibilidade de ele não ser selecionado para teste.
- III. o auditor deve selecionar o item que será examinado para diminuir o risco.

Está correto o que se afirma em

- a) I, II e III.
- b) I, apenas.
- c) I e II, apenas.
- d) I e III, apenas.
- e) II e III, apenas.

Características do Curso.

Auditoria de Sistemas de Informação

- 1 Fontes de Estudo
- 2 História e Origem da Auditoria e do Controle no Brasil e no Mundo
- 3 Conceitos Aplicáveis à Auditoria de TI
 - Diferenças entre Fiscalização, Controle e Auditoria
 - Órgãos de Fiscalização, Auditoria e Controle na Administração Pública Federal
 - Tipos de Auditoria
 - Auditoria de TI
- 4 Código de Ética e Padrões
- 5 Abordagens de Auditoria de Sistemas de Informação
- 6 Procedimentos de Auditoria de Sistemas Aplicativos
- 7 Abordagem Técnica da Auditoria de TI

E por hoje é só pessoal.



<http://www.itnerante.com.br/group/contratos-e-auditoria-de-ti>

<http://www.itnerante.com.br/profile/ProfGabrielPacheco>

<http://www.facebook.com/professorgabrielpacheco>

<http://www.facebook.com/groups/tiparaconcursos>

<http://www.twitter.com/gabrielpacheco>

www.provasdeti.com.br