

Auditoria de Sistemas de Informação



Everson Santos Araujo
<everson@por.com.br>

Abordagens

- * Ao redor do computador
- * Através do computador
- * Com o computador

2

Ao redor do computador

- * Auditoria de documento-fonte com as funções de entrada
- * Análise das funções de saída

3

Ao redor do computador

- | | |
|--------------------------------|--|
| * Vantagens | * Desvantagens |
| * Não exige conhecimento de TI | * Restrição operacional |
| * Custos baixos e diretos | * Sem parâmetros claros e padronizados |
| | * Número maior de riscos |

4

Através do computador

- * Auditoria do manuseio e fluxo dos dados
- * Aprovação e registro das informações

5

Através do computador

- | | |
|---|--|
| * Vantagens | * Desvantagens |
| * Simulação de transações | * Possibilidade de perdas de dados |
| * Capacitação do auditor | * Técnica manual como complemento |
| * Verificação constante de pontos específicos | * Risco de contaminação do Software de Auditoria |

6

Com o computador

- * Utilização de capacidades do computador para auxiliar a Auditoria, tais como:
 - * Lógica
 - * Aritmética
 - * Estatística para geração de amostras
 - * Edição e classificação

7

Com o computador

- * Utilização de Técnicas de Auditoria Assistida por Computador (TAAC)
- * Criação de programas genéricos
- * Melhor utilização do tempo do Auditor e menor tempo de resposta da Auditoria

8

Controles Internos

Controles Internos

- * "Planos organizacionais e coordenação de um conjunto de métodos e medidas adotado numa empresa, a fim de salvaguardar o ativo, verificar a exatidão e a veracidade de registros contábeis, promover a efetividade de sistemas de informação contábil e eficiência operacional, assim como fomentar uma grande adesão às políticas da organização." (Instituto americano de contadores públicos)

10

Tipos de controle

- * Administrativos e gerências
- * Segurança e privacidade
- * Preparação e captação de dados
- * Entrada de dados
- * Processamento
- * Saída e emissão de relatórios
- * Gravação e recuperação de dados

11

Técnicas

Dados de teste

- * Conjunto de entrada de dados
- * Testar os controles programados e os controles do sistema
- * Pode-se usar um software gerador de dados aleatórios
- * Difícil planejamento e antecipação de todas as combinações de transações

13

Facilidade de teste integrado

- * Para ambientes *on line* e *realtime*
- * Os dados são integrados aos ambientes reais de processamento utilizando a versão de produção
- * Aplicação de entidades fictícias
- * Usa o ambiente normal da empresa
- * Cuidado no estorno das transações e seus efeitos no sistema

14

Simulação paralela

- * Uso de um programa que atenda as lógicas necessárias
- * Sistema para processar transações executadas numa rotina normal e operacional
- * O sistema opera em ambiente real
- * Maior volume de dados e teste mais detalhado
- * Custo muito alto

15

Auditoria embutida nos sistemas

- * Depende do desenvolvedor do sistema
- * Relatórios periódicos para revisão e acompanhamento constante
- * Pode ser usado com sistemas *on line*
- * Não apresenta restrições de dados inseridos
- * Custo adicional de utilização das máquinas

16

Análise da lógica de programação

- * Verificação da lógica da programação
- * Manualmente através de leitura do código fonte de amostras dos programas
- * Utilizando *softwares* especializados

17

Auditoria Assistida por Computador

Auditoria de Controles

Auditoria de controles organizacionais

- * Controles administrativos instalados nos processos de fluxo das transações econômicas e financeiras dos sistemas de informação, com a função de auxiliar nos objetivos dos negócios

20

Tarefas

- * delineamento das responsabilidades
- * coordenação de orçamento
- * desenvolvimento e implementação das políticas
- * comunicação com terceiros
- * gerenciamento de suprimentos
- * desenvolvimento de plano de capacitação

21

Políticas de responsabilidade

- * Definir a responsabilidade da gerência e de todos a respeito de manipulação e salvaguarda dos ativos da organização
- * Identificar e proteger os ativos críticos para as operações

22

Responsabilidades

- * Identificação de ativos críticos
- * Implementação de sistemas seguros
- * Desenvolver procedimento de conscientização
- * Promover a revisão dos procedimentos
- * Relatar abusos e transgressões em tempo hábil para punição

23

Continuidade dos negócios

- * Identificar informações críticas, níveis de serviços necessários e o maior tempo permitido de queda do sistema
- * Assinalar prioridades aos sistemas de informação para determinar as necessidades de *backup* e periodicidade
- * Geração de um plano de continuidade documentado e atualizado

24

Cargos de TI

Supervisão de infra-estrutura

- * Garantir o patamar adequado da infra-estrutura
- * Definir e buscar recursos para crescimento e ampliação do ambiente
- * Coordenar implantação de projetos e metas
- * Garantir integração das equipes técnicas e de suporte
- * Manter e garantir sigilo das informações de infra

26

Administração de redes

- * Administrar e supervisionar as instalações de rede
- * Instalar e administrar os servidores de rede
- * Administrar as contas de usuários e permissões
- * Garantir privacidade, integridade e confiabilidade
- * Monitorar e gerar documentação da rede
- * Avaliar a adoção de novas tecnologias

27

Administração de Banco de Dados

- * Planejar e implementar estratégias de utilização
- * Manter ativo e em operação os sistemas elaborados com Banco de Dados
- * Administrar as contas de usuários e permissões
- * Manter sigilo sobre as informações da empresa
- * Planejar e executar backup dos servidores

28

Administração de segurança

- * Implementar políticas de segurança
- * Detectar invasões e ameaças
- * Testar e determinar pontos de vulnerabilidade
- * Customizar a segurança de acordo com a política
- * Pesquisar novas falhas
- * Disseminar a cultura da segurança

29

Análise, programação e manutenção de Sistemas

- * Projetar e desenvolver os sistemas necessários
- * Realizar o trabalho de análise e elaboração de especificações técnicas
- * Serviço permanente de acompanhamento e verificação
- * Suporte aos usuários
- * Definir o projeto e a arquitetura dos sistemas

30

Operador de console

- * Responsáveis pelo processo dos dados, conforme manual de operações e mensagens recebidas dos sistemas

31

Suporte técnico

- * Manutenção preventiva e corretiva
- * Realizar inventário de Hardware e Software
- * Instalar e remanejar estrutura e equipamentos
- * Instalar e configurar sistema operacional e aplicativos, bem como controlar licenças
- * Realizar suporte técnico aos usuários
- * Acompanhar chamados abertos até sua solução

32