Auditoria de Sistemas

Prof. Luiz Antonio Ferraro Mathias

Aula 05

Auditoria em Sistemas de Informação

Auditoria em Sistemas de Informação

Uma auditoria de sistemas de informação pode abranger desde o exame de dados registrados em sistemas informatizados, até a avaliação do próprio sistema informático – aplicativos, sistemas operacionais etc.; a avaliação do ambiente de desenvolvimento, do ambiente de operação, do ambiente de gerenciamento da rede e todos os demais elementos associados a um ou mais sistemas de informação corporativos.

Técnicas de auditoria de Sistemas de Informação

Existem inúmeras técnicas de auditoria de sistemas de informação. É durante a fase de planejamento da auditoria, dependendo dos objetivos, do escopo e das limitações inerentes ao trabalho, que a equipe de auditoria seleciona as técnicas de auditoria mais adequadas para se chegar às conclusões esperadas do trabalho.

Algumas técnicas usadas em auditorias de sistemas são comuns a outros tipos de auditoria, como:

- entrevista (reunião realizada com os envolvidos com o ponto auditado, que deve ser documentada);
- questionário (conjunto de perguntas que podem ser aplicadas a muitas pessoas simultaneamente, sem a presença do auditor);
- verificação in loco (observação direta de instalações, atividades ou produtos auditados).

Técnicas de auditoria de Sistemas de Informação

Outras técnicas são específicas para a avaliação de operações, transações, rotinas e sistemas em operação ou desenvolvimento. A seguir, acompanhe quais são elas:

Método	Características
Test-deck	consiste na aplicação do conceito de "massa de teste" para sistemas em operação, envolvendo testes normais e corretos, com campos inválidos, com valores incompatíveis, com dados incompletos etc.
Simulação paralela	consiste na elaboração de programas de computador para simular as funções da rotina do sistema em operação que está sendo auditado. Utiliza-se os mesmos dados da rotina em produção como input do programa de simulação.

Técnicas de auditoria de Sistemas de Informação

Teste de recuperação	avaliação de um sistema em operação quanto aos procedimentos manuais e/ou automáticos para a recuperação e retomada do processamento em situações de falhas. Um exemplo típico é testar para ver se o backup funciona.
Teste de desempenho	Verificação de um sistema em operação quanto ao consumo de recursos computacionais e ao tempo de resposta de suas operações (exige instrumentos de monitoração para hardware e software).
Teste de estresse	Avaliação do comportamento de um sistema em operação quando submetido a condições de funcionamento envolvendo quantidades, volumes e frequências acima do normal.

Técnicas de auditoria de Sistemas de Informação

Teste de segurança	Avaliação dos mecanismos de segurança preventivos, detectáveis e corretivos presentes no sistema.
Teste de caixa preta	Método que se concentra nos requisitos funcionais dos programas em operação. Os casos de testes, normalmente derivados de diferentes condições de entrada, avaliam funções, interfaces, acessos a bancos de dados, inicialização e término do processamento.

Técnicas de auditoria de Sistemas de Informação

Mapping, tracing e snapshot	**Métodos que preveem a inserção de rotinas especiais nos programas em operação, usadas para depurá-los (debug) após serem executados. São estes:** **Mapping: lista as instruções não utilizadas que determina a frequência daquelas executadas.** **Tracing: possibilita seguir o caminho do processamento dentro de um programa, isto é, visualizar quais instruções de uma transação foram executadas e em que ordem.** **Snapshot: fornece o conteúdo de determinadas variáveis do programa durante sua execução, de acordo com condições preestabelecidas.**
Teste de caixa branca	Concentra-se nas estruturas internas de programas em desenvolvimento. Os casos de testes avaliam decisões lógicas, loops, estruturas internas de dados e caminhos dentro dos módulos.

Controles Gerais

Controles gerais consistem na estrutura, políticas e procedimentos que se aplicam às operações do sistema computacional de uma organização como um todo. Eles criam o ambiente em que os sistemas aplicativos e os controles irão operar.

Durante uma auditoria em que seja necessário avaliar algum sistema informatizado, seja ele financeiro, contábil, de pagamento de pessoal etc., é preciso inicialmente avaliar os controles gerais que atuam sobre o sistema computacional da organização.

Controles gerais deficientes acarretam uma diminuição da confiabilidade a ser atribuída aos controles das aplicações individuais. Por esta razão, os controles gerais são normalmente avaliados separadamente e antes da avaliação dos controles dos aplicativos que venham a ser examinados em uma auditoria de sistemas informatizados.

Controles Gerais

São identificadas 5 (cinco) categorias de controles gerais que podem ser consideradas em auditoria:

a) Controles organizacionais - políticas, procedimentos e estrutura organizacional estabelecidos para organizar as responsabilidades de todos os envolvidos nas atividades relacionadas à área da informática;

b) Programa geral de segurança - oferece estrutura para: (1) gerência do risco, (2) desenvolvimento de políticas de segurança, (3) atribuição das responsabilidades de segurança, e (3) supervisão da adequação dos controles gerais da entidade;

c) Plano de continuidade do negócio - controles que garantam que, na ocorrência de eventos inesperados, as operações críticas não serão interrompidas., Elas devem ser imediatamente retomadas e os dados críticos protegidos;

Controles Gerais

d) Controle de software de sistema - limita e supervisiona o acesso aos programas e arquivos críticos para o sistema que controla o hardware e protege as aplicações presentes. O controle sobre o acesso e a alteração do software de sistema é essencial para oferecer uma garantia razoável de que os controles de segurança baseados no sistema operacional não estão comprometidos, prejudicando o bom funcionamento do sistema computacional como um todo;

e) Controles de acesso - limitam ou detectam o acesso a recursos computacionais (dados, programas, equipamentos e instalações), protegendo estes recursos contra modificação não-autorizada, perda e divulgação de informações confidenciais. Os controles de acesso têm o propósito de oferecer uma garantia razoável de que os recursos computacionais (arquivos de dados, programas aplicativos, instalações e equipamentos relacionados aos computadores) estão protegidos contra modificação ou divulgação não-autorizada, perda ou danos. Eles incluem controles físicos, tais como manutenção dos computadores em salas trancadas para limitar o acesso físico, e controles lógicos (softwares de segurança projetados para prevenir ou detectar acesso não autorizado a arquivos críticos).

Tipos de Auditoria de Sistema de Informação

Dentre as auditorias de sistemas de informação, destacam-se: auditoria de software aplicativo, auditoria do desenvolvimento de sistemas, auditoria de banco de dados, auditoria de redes e de equipamentos.

Auditoria de software aplicativo

Os softwares aplicativos são aqueles projetados para executar determinado tipo de operação, a exemplo do cálculo da folha de pagamento ou de controle de estoque. São exemplos de controles que podem ser auditados: controles de aplicativos; controles de entrada de dados; a autorização para entrada de dados; controles do processamento de dados e controles da saída de dados.

Tipos de Auditoria de Sistema de Informação

Auditoria de Desenvolvimento de Sistemas

A auditoria do desenvolvimento de sistemas objetiva avaliar a adequação das metodologias e procedimentos de projeto, desenvolvimento, implantação e revisão pós-implantação dos sistemas produzidos dentro da organização auditada.

Esta avaliação pode abranger apenas o ambiente de desenvolvimento da organização ou prever também a análise do processo de desenvolvimento de um sistema específico, ainda na fase de planejamento, já em andamento ou após sua conclusão.

Tipos de Auditoria de Sistema de Informação

Todos os projetos de desenvolvimento de sistemas precisam ter sido avaliados em profundidade, devendo ser precedidos de análises de custo/benefício, capacidade de satisfação dos usuários e de atendimento aos objetivos da organização, custos de desenvolvimento, medidas de desempenho, planos de implementação, previsão de recursos humanos etc. São necessários, também, mecanismos gerenciais que auxiliem a definição de prioridade dos projetos e permitam sua avaliação e controle durante todo o processo de desenvolvimento.

Tipos de Auditoria de Sistema de Informação

Auditoria de Banco de Dados

Tradicionalmente, o termo banco de dados foi usado para descrever um arquivo contendo dados acessíveis por um ou mais programas ou usuários. Os arquivos de dados eram designados para aplicações específicas e o programa era projetado para acessá-los de uma forma predeterminada.

Auditoria de redes de computadores

Atualmente, é bastante comum que os usuários de um sistema estejam em um local diferente de onde se encontram os recursos computacionais da organização. Isto torna necessário o uso de mecanismos de transporte de informações entre diferentes computadores e entre computadores e seus periféricos. Para o bom funcionamento da comunicação de dados são usados:

Tipos de Auditoria de Sistema de Informação

a) Arquivo log de comunicações, onde ficam registrados todos os blocos transmitidos correta e incorretamente para efeito estatístico e para tentativas de recuperação de dados transmitidos;

b) Software de comunicação de dados para verificação de protocolo de transmissão, gravação do arquivo log de transações e para codificação de sinais de comunicação;

c) Protocolo de transmissão que garante a recepção correta do bloco de informações transmitidas;

d) Software ou hardware para a realização de codificação e decodifcação das informações transmitidas.

Tipos de Auditoria de Sistema de Informação

O principal risco oferecido pelas redes é o de acesso não autorizado a dados e programas da organização, que pode resultar em danos ou prejuízos intencionais ou acidentais.

Auditoria de equipamentos

Normalmente são chamados microcomputadores os computadores de mesa que compreendem um processador, disco rígido e flexível, monitor e teclado. Os microcomputadores podem ser utilizados isoladamente ou estar conectados a uma rede, com o propósito de compartilhar dados ou periféricos.

Tipos de Auditoria de Sistema de Informação

Para que possa proteger-se contra diversos tipos de riscos, a organização precisa adotar políticas e procedimentos específicos quanto ao uso de microcomputadores pelos seus funcionários, compreendendo padrões de hardware, software, aquisição, treinamento e suporte, além dos controles gerais e de aplicativos.

Os microcomputadores precisam de controles específicos destinados a protegê-los de furto ou acidente, que podem ocasionar a perda de dados e programas. Isto pode ser evitado através de restrições físicas de acesso às máquinas, controles de software, tais como: senhas de acesso e realização periódica de cópias de segurança. O furto de equipamentos pode ser evitado por meio de mecanismos adequados de segurança no local de trabalho.