T2 AUDITORIA DE SISTEMAS – GRUPO 3

MATERIAL DE APOIO – PROVINHAS

ERP - Um breve Histórico

Link 1: http://www.empari.com.br/a-historia-do-erp-e-sua-importancia-nas-empresas.html

Link 2: Auditoria de sistema passa por processo de auditoria?

Auditoria de Sistemas

O que é? Validação e avaliação do controle interno de sistemas de informação.

Objetivo: Verificar se as informações armazenadas em meio eletrônico atendem aos requisitos de confiança e segurança e se os controles internos foram implementados e também se são efetivos.

Importância: As organizações realizam altos investimentos em sistemas computadorizados e, consequentemente precisam garantir a segurança de seus computadores. É necessário possuir garantia do alcance da qualidade dos sistemas computadorizados e também auxiliar a organização a avaliar e validar o ciclo administrativo.

Funções: A auditoria de sistema promove adequação (avaliação e recomendações para aprimoramento) dos controles internos nos sistemas de informação da empresa. Além de utilização de recursos humanos, materiais e tecnológicos envolvidos no processo dos mesmos.

Dificuldades da auditoria: Defasagem tecnológica, falta de bons profissionais, falta de cultura da empresa, tecnologia variada e abrangente.

Boa empresa de auditoria: deve ser eficiente e oferecer serviços de qualidade, estar preparada para ser a melhor do mercado (ou uma das melhores do mercado). Deve ainda oferecer treinamento de pessoal e superação de resistência à tecnologia; avaliar, escolher e implementar software de auditoria; gerenciar arquivos eletrônicos, dispositivos de segurança e bkp; disponibilizar equipamentos para que sua equipe de auditores possa trabalhar em rede; instalar e manter uma boa malha de comunicação; permitir maior transferência de conhecimento entre os membros da equipe e entre equipes diferentes; ser independente das limitações impostas por documentos de auditoria em papel; economizar tempo em documentação, obter maior rapidez no fluxo de informação, obter maior produtividade.

Tipos de abordagem da auditoria:

Ao redor do computador: trabalha a partir de documentos de E/S; não envolve muita T.I.; Não se preocupa muito com funções de processamento; Apropriada para pequenas empresas; Vantagens: Não exige muito conhecimento de TI, baixo custo. Desvantagens: Incompleta, poucos parâmetros de auditoria, documentos ficam desatualizados, decisões são baseadas em relatórios e documentos podem ser distorcidos.

Através do computador: Além de envolver a confrontação de documentos, alerta quanto ao manuseio do dos dados, aprovação e registro de transações comerciais, mas não constrói controles de programas junto aos sistemas. Utiliza técnicas de verificação, como os dados são

processados e os resultados intermediários através de simulações. Vantagens: Capacita melhor o adutor a respeito de habilidade profissional no que tange ao conhecimento de processamento eletrônico de dados. Desvantagens: Necessidade de treinamento de auditores, aquisição e manutenção de pacotes de software; há risco de que os programas de teste estejam incorretos ou "viciados". Ignora as tarefas executadas manualmente.

O papel do auditor: Validação do fluxo administrativo (planejamento, execução e controle); ênfase nos processos computacionais; comprovação da efetividade dos sistemas computadorizados; garantia da segurança lógica e física e da confidencialidade dos sistemas.

Auditor Interno: É empregado da empresa auditada, possui menor grau de independência, executa auditoria contábil, operacional, de gestão, de qualidade, de processos, de produtos e outros.

Os principais objetivos dele: Verificar a existência, a suficiência e aplicação dos controles internos, bem como contribuir para o seu aprimoramento; verificar se as normas internas estão sendo seguidas; verificar a necessidade de monitoramento das normas internas vigentes. Seu trabalho apresenta como característica um maior volume de testes em função da maior disponibilidade de tempo na empresa para executar os serviços de auditoria.

Auditor Externo: Não tem vínculo empregatício com a empresa auditada, possui maior grau de independência; Seu trabalho tem como principal objetivo emitir um parecer ou opinião sobre os processos de negócio, no sentido de verificar se estes refletem adequadamente a as regas da empresa e normas legais; apresenta como característica um menor volume de testes, já que o auditor externo está interessado em erros que individualmente ou cumulativamente possam alterar de maneira substancial as informações dos processos da empresa.

Treinamento do auditor: Conceituação de auditoria de sistemas; controle interno; momentos de atuação do auditor de sistemas, produtos finais da auditoria de sistemas; mecânica de implantação das recomendações de auditoria; postura do auditado durante a atuação da auditoria de sistemas;

Padroes e Código de Ética: Auditoria de sistemas de informações e considerada uma parte da auditoria geral de uma organização; as normas de auditoria geralmente não tratam isoladamente a auditoria de sistemas; nunca foi vista como uma profissão isolada, mas sim um avanço na auditoria geral para acompanhar a tecnologia da informação nas organizações.
Padrões: Responsabilidade, autoridade, prestação de contas, independência profissional, ética profissional, competência, planejamento, emissão de relatório.

Ética: Código de ética para auditoria de sistemas de acordo com a ISACA EUA: Apioar a implementação e encorajar o cumprimento dos padrões sugeridos para controles de SI; exercer suas funções com objetividade, diligência e zelo profissional de acordo com as melhores práticas; servir aos interesses de alta administração de forma legal e honesta com alto padrão de conduta e caráter profissional; manter privacidade e confidencialidade das informações obtidas no decurso de suas funções; atuar smente nas atividades para as quais estiver capacitado, informar as partes envolvidas sobre o andamento dos atrabalhos, auxiliar a alta administração na compreensão dos sistemas de informação, segurança e controle;

Auditoria de Sistemas Informatizados

Compreende o exame e a avaliação dos processos de planejamento, desenvolvimento, teste e implantação dos sistemas informatizados da empresa. Também visa ao exame e à avaliação:

• de estruturas lógicas, físicas e ambientais;

• de sistemas de controle, segurança e proteção de determinados ativos;

• de aplicativos desenvolvidos pela empresa ou adquiridos no mercado; e

• das informações, visando à qualidade de controles internos sistêmicos e de sua observância em todos os níveis gerenciais.

Enfoque em processo x Auditoria de Sistemas Informatizados

Na verdade, a Auditoria de Sistemas Informatizados não representa uma modalidade de Auditoria diferenciada da Auditoria de Processo. Com um melhor conhecimento técnico dos processos informatizados da empresa, a Auditoria de Sistemas Informatizados pode muito bem atuar com um enfoque de processo ou ser utilizada como um suporte ao auditor de processo.

O processo de Certificação

Atualmente a certificação CISA – Certified Information Systems Auditor, oferecida pela ISACA – Information Systems and Control Association é uma das mais reconhecidas e avaliadas por organismos internacionais, já que o processo de seleção consta de uma prova extensa que requer conhecimentos avançados, além de experiência profissional e a necessidade de manter-se sempre atualizado, através de uma política de educação continuada (CPE) na qual o portador da certificação deve acumular carga horária de treinamento por período estabelecido.

Link 1: http://www.auditsafe.com.br/pag.asp?p=1&cod=265

Link 2: http://www.isaca.org/chapters9/Brasilia/Certification/Pages/Page1.aspx

CISA – destinado a avaliar o grau de proficiência e excelência nas disciplinas de auditoria, controle e segurança em TI. Este exame tem sido considerado um dos mais eficazes instrumentos de certificação em âmbito global.

Passar em um exame específico, demonstrar experiência e qualificações proffionais requeridas, fornecendo evidências de prática conforme o tipo de certificação. Aderir formalmente ao código de ética da ISACA, aderir à política de eduação profissional continuada da isaca (que envolve uma quantidade mínima de horas anuais em treinamentos e qatividades de contribuição à profissão).[

Para manutenção do certificado, o postulante deve evidenciar 120h de CPE ao longo de três anos (sendo no mínimo 20 h CPE a cada ano). Isso é demonstrado pela participação em atividades educacionais das quais participa e atividades que demonstrem as contribuição para a profissão, como ministrar cursos no tema, participar em pesquisas da ISACA, etc.

Auditoria da Tecnologia da Informação (TI)

As implicações da Tecnologia da Informação (TI) Principais riscos

• Ineficácia da estrutura organizacional da área de TI: Quando a empresa não possui uma estrutura da área de Tecnologia de Comunicação, capaz de atender a todas as suas necessidades, existe a grande possibilidade de pendências de atendimento serem acumuladas, permitindo o atraso de ações voltadas para a própria manutenção da rentabilidade da atividade de negócio exercida.

• Recursos materiais e humanos de TI insuficientes e/ou ineficientes: A falta de equipamentos ou de técnicos especializados coloca em risco a qualidade do serviço de TI prestado junto à empresa, possibilitando falta de segurança sobre a eficácia de todos os processos que envolvam sistemas informatizados.

• Fraudes e problemas operacionais: A utilização de sistemas informatizados gera a oportunidade de que, na falta de controles de acessos e de segurança adequados, pessoas não bem intencionadas possam criar fraudes ou problemas para a empresa, acessando, manipulando ou deteriorando os dados registrados em seus bancos de dados.

Atribuições básicas e perfil ideal do Auditor de Sistemas

• formular, aprimorar e verificar o cumprimento das normas e políticas de TI da organização;

• avaliar a estrutura organizacional e a sua gestão da TI (eficácia e eficiência);

• auditar o processo de desenvolvimento de sistemas;

• auditar os sistemas aplicativos; e

• apurar fraudes.

Perfil ideal do Auditor de Sistemas

• ético;

• sólida formação em tecnologia;

• conhecimentos profundos em Auditoria e Negócios/Atualizado tecnicamente;

• capacidade de negociação/Relacionamento pessoal;

• raciocínio lógico acurado/Criatividade; e

• domínio dos idiomas Português e Inglês. Áreas de atuação da Auditoria de Sistemas

• Gerenciamento e Organização de TI: · planejamento estratégico de TI; · terceirizações; · orçamento;

· planejamento de capacidade e crescimento; · padrões de documentação; e · processos de TI.

• Disponibilidade, Confidencialidade e Integridade dos Sistemas de Informação:

· controle de acesso lógico; · senhas; · criptografia; · controle de acesso físico; · controle de ambiente; e · plano de continuidade de negócios.

• Desenvolvimento, Aquisição e Manutenção dos Sistemas de Informação.

· SDLC – Ciclo de Vida de Desenvolvimento de Sistemas; · metodologias de desenvolvimento; · o papel do auditor:

a) determinar os riscos e as exposições que o sistema pode inserir;

b) identificar controles que eliminem ou reduzam os riscos e exposições; e

c) monitorar o desenvolvimento do sistema de forma a garantir que os controles estejam sendo implementados.

COBIT – Control Objectives for Information & Related Technology

• é publicado pelo ISACA (Information Systems Audit and Control Association);

• representa um guia de “melhores práticas” para Gestão, Controle e Audi-toria de TI;

• consiste em quatro domínios, que são constituídos por 34 processos de TI; • pode balizar o Plano Anual de Auditoria; e

• é de grande valia na elaboração de programas de trabalho. Internet Oportunidades

• Para o Auditor de Sistemas:

a) fonte de pesquisas e conhecimento;

b) permanente atualização profissional;

c) contato direto com seus pares no mundo inteiro; e d) benchmarking com outras empresas e auditorias.

• Para os negócios da empresa:

a) recrutamento e seleção de pessoal;

b) prestação e obtenção de serviços;

c) fonte de pesquisas e conhecimento;

d) benchmarking;

e) globalização do seu mercado potencial;

f) globalização dos seus fornecedores em potencial; g) marketing individualizado/disponibilidade.

Riscos

• Divulgação de informações sigilosas: A Internet facilita o acesso a informações pertinentes apenas à Empresa. Isto ocorre quando não existem atividades de controle sobre os acessos aos bancos de dados e cadastros de seus processos.

• Interrupção das comunicações/operações: O acesso ou invasão pode chegar ao cúmulo de interromper a atividade de negócio exercida pela empresa, proporcionando, além da perda financeira, prejuízo a sua imagem perante o mercado e seus clientes.

• Pagamentos indevidos a fornecedores fictícios: Casos de distorções ou manipulações nos sistemas financeiros estão cada dia mais corriqueiros e, no caso da inexistência de controles adequados, proporcionam prejuízos imensos às empresas.

• Desvio de recursos financeiros: Sem controle, desvios financeiros podem nem ser percebidos.

• Corrupção dos sistemas de compras e vendas. A informatização da área de compras deve ser totalmente monitorada e documentada, visando minimizar o risco de corrupção ou fraudes. Pontos de Auditoria com enfoque em TI

• Agregar valor aos acionistas, identificando se o ambiente de TI contempla os seguintes aspectos:

a) atendimento às necessidades da empresa e dos usuários;

b) processamento e controles corretos, adequados e no tempo ideal;

c) segurança física e lógica;

d) vida útil/atualização tecnológica;

e) documentação; e

f) segregação de funções.

Fonte: **http://webserver.crcrj.org.br/APOSTILAS/A1039P0147.pdf**