Escola Técnica Pandiá Calógeras
Centro de Computação & Segurança de Informação

Trabalho de CPD

Centro de Computação & Segurança de Informação

Grupo C

Autores

Grupo C – Componentes

Aline Rodrigues de Souza
Carlos Eduardo Guimarães de Salles
Carlos Eduardo Martins de Oliveira (CaEd)
Cristiane Barbosa da Cruz
Fabio dos Santos Moreira
José Osvaldo Amaral Tepedino
Maurício Domingues da Silva
Nívea Gonçalves da Silva
Paula Tabajaras
Rodrigo Otávio Guimarães Haydt
Simone de Miranda Milani
Sylvia Maria da Silva Seito

Auditoria em Informática

Introdução

O crescente uso dos computadores nas empresas bem como a sua importância estratégica, vem fazendo com que as empresas se preocupem em aumentar o controle sobre os departamentos de processamento de dados, já que estes controlam informações vitais à empresa.

Este controle é feito através de um processo de Auditoria, que visa descobrir as irregularidades em tais departamentos (caso seja feito em microcomputadores) ou nos centros de processamento da empresa. A Auditoria também identifica os pontos que irão desagradar a alta administração para que estes possam ser corrigidos.

Como no passado, a base da investigação era restrita ao setor da finanças, as empresas não viam o porquê de manter um departamento somente de auditores, preferindo contratar empresas prestadoras deste serviço. Atualmente com a proliferação do comutador, já é necessário manter um departamento de auditoria interna.

A prática deste tipo de auditoria iniciou-se nos Estados Unidos e na Europa na década de 80. Como as técnicas de processamentos e as maneiras de burlar os controles vêem evoluindo de maneira rápida, os auditores devem estar sempre atentos a tais mudanças.

A Auditoria de processamento de dados deve abranger todas as áreas de um departamento de processamento de dados:

- Coordenação de Problemas;
- Coordenação de Mudanças;
- Sistemas em Processamento “Batch” (em série);
- Recuperação de desastre;
- Capacidade dos Sistemas;
- Desempenho dos Sistemas;
- Desenvolvimento de Sistemas;
- Sistemas em Processamento On-Line (linha por linha);
- Sistemas Financeiros
- Rede de Telecomunicações
- Segurança de informação
- Centro de computação
- Microcomputador
- Distribuição dos Custos.

Perfil do Profissional Auditor em Informática

O auditor é aquela pessoa, ou departamento, que foi designado pela alta administração da empresa para avaliar, examinar e descobrir os pontos falhos e a devida eficácia dos departamentos por ela vistoriados. Logicamente auditado é aquela pessoas ou setor que sofre a investigação da auditoria.

O auditor deve ser um profissional de grande conhecimento da área de processamento de dados e todas as suas fases. Deve ter objetividade, discrição, raciocínio lógico e principalmente um sentimento real de independência, ou seja, em seus relatórios sejam eles intermediários ou finais, devem possuir personalidade e até mesmo os fatos incorretos na administração do auditado.

Posicionamento da Auditoria dentro da organização

Este setor deve ser totalmente independente dos outros setores a fim de que não tenha influências no seu desempenho. Deve estar ligado diretamente à alta administração da empresa.

Outro ponto importante é a existência de um planejamento prévio, a nível de datas, de quando e como irão ocorrer as auditorias. O sigilo deste planejamento é importante para que não hajam acertos de última hora que irão resultar em relatórios não condizentes com a realidade, prejudicando o desempenho da organização.

Importância da Auditoria e suas fases

Como já foi dito a auditoria dentro de um departamento, principalmente na área de processamento de dados, é de vital importância para empresa, já que através desta a alta administração deverá ditar os rumos da empresa, além de evitar fraudes e garantir o bom desempenho dos setores aditados.

Este processo é composto de: Pré-Auditoria, Auditoria e Pós-Auditoria.

- **Pré-Auditoria:**

Nesta fase é enviado ao departamento a ser auditado um anúncio, através de um notificação formal do setor de auditoria ou pelo setor de Controle Interno da empresa. Este anúncio deve ser feito com até duas semanas de antecedência e deverá especificar quais serão as áreas a ser auditadas, com seus respectivos planos de trabalho.

Ainda destro desta fase, serão feitas as primeiras reuniões da alta administração com os auditores visando esclarecer os pontos e planos de trabalho.

Nesta fase o grupo Auditor deve preparar as atividades administrativas necessárias para a realização da auditoria, definir as áreas a auditar, orientar o grupo de auditores quanto a estratégia a ser adotada, preparar o documento de anúncio e anunciar o setor da Auditoria.

O setor a ser auditado deve preparar as atividades administrativas de apoio ao Grupo Auditor, educar o pessoal do setor quanto ao processo que será utilizado, deliberar (resolver após a exanimação) quais informações são necessárias ao processo e fazer uma revisão final no setor.

- **Auditoria:**

Terminadas as reuniões iniciais e após definir as ações que serão tomadas, inicia-se a auditoria. O Auditor-chefe fará as solicitações por escrito e com data de retorno do representante do setor auditado.

De acordo com as datas preestabelecidas (na pré-auditoria) serão feitas reuniões onde os fatos identificados serão expostos e é entregue um relatório destes fatos ao representante do setor auditado para que este emita, por meio de outro relatório as razões de estar em desacordo.

Se tais razões não forem aceitas pelo grupo Auditor, elas farão parte do relatório denominado Sumário Executivo, que é apresentado à alta diretoria da empresa. Dentro deste mesmo relatório constará uma Avaliação Global da situação da área de informática que está sendo auditada.

Geralmente a auditoria dura cerca de seis semanas.

Nesta fase, o Grupo Auditor deve avaliar os Controles(ou seja, como a área auditada funciona); documentar os desvios encontrados (falhas); validar as soluções, preparar o relatório final e apresentá-lo para a Presidência.

O Setor Auditado deve prover as informações necessárias ao trabalho da auditoria, analisar a exposição dos desvios encontrados, entender os desvios encontrados, desenvolver planos de ação que solucionarão os desvios encontrados, corrigir as exposições e revisar o Sumário Executivo.

- **Pós-Auditoria:**

Terminada a auditoria, o grupo auditor emite um relatório final detalhando as suas atividades. Este relatório conterá o objetivo da Auditoria, as áreas cobertas por ela, os fatos identificados, as ações corretivas recomendadas e a avaliação global do ambiente auditado.

Este relatório é enviado a todas as linhas administrativas, começando pela presidência e terminando no representante do setor auditado.

Nesta fase, o Setor Auditado deve solucionar os desvios encontrados pela auditoria, preparar resposta ao Relatório Final e apresentar para a Presidência, administrar conclusão dos desvios e manter o controle para que os erros não se repitam e a eficácia seja mantida.

O Grupo Auditor deve distribuir o Relatório Final, revisar resposta recebida(soluções e justificativas apresentadas), assegurar o cumprimento do compromissado e analisar a tendência de correção.

Inter-Relação entre auditoria e segurança em informática

Resumindo, podemos dizer que a segurança e a auditoria são interdependentes, ou seja, uma depende da outra para produzirem os efeitos desejáveis à alta administração.

Enquanto a segurança tem a função de garantir a integridade dos dados, a auditoria vem garantir que estes dados estejam realmente íntegros propiciando um perfeito processamento, obtendo os resultados esperados.

Com isso, concluímos que para que uma empresa continue competitiva no mercado, ela deve manter um controle efetivo sobre as suas áreas e isso é feito através do processo de auditoria

Segurança da Informação

Introdução

Segurança da informação é o processo responsável pela proteção dos bens da informação (dados, imagem, texto e voz no computador), e contra uso indevidos e perdas de bens de informação.

Hoje em dia, a segurança de informação é o tópico mais importante em uma empresa, pois dá garantia ao que chamamos de proteção das informações da empresa em todos os aspectos.

Para se ter um ótimo controle de acesso as informações em uma grande empresa é indispensável o uso de um software específico para manter esse controle, devido ao grande número de dados manipulados. O RACF20 é um exemplo deste tipo de software, que é um produto da IBM Corporation.

A atividade de auditoria em segurança de informação

A auditoria tem como verificar se os requisitos para segurança da informação estão implementados satisfatoriamente, mantendo a segurança nos dados da empresa e verificando se os seus bens estão sendo protegidos adequadamente.

Inicialmente o auditor deve revisar o plano aprovado, ou seja, verificar se o método utilizado para proteção de informações é o melhor ou se precisa sofrer alguma atualização, sempre relacionado com o esquema de trabalho a seguir dentro da área que está sendo auditada.

Depois de terminado o estudo do plano, o auditor solicita os procedimentos necessários para descrever as diversas atividades que exige uma Segurança em Informática. Esses procedimentos serão confrontados com a realidade do dia-a-dia dentro do departamento, ou seja, verificando se todos os procedimentos necessários à Segurança em Informática são corretamente utilizados no departamento que está sendo auditado.

Na investigação o Auditor deverá revisar os seguintes itens, verificando se:

- O proprietário (aquele que tem permissão para acessar um certo conjunto de informações), periodicamente faz uma revisão em todos os dados que ele possui acesso para verificar se houver perdas, alterações, ou outras problemas de qualquer natureza. O Centro de Computação deve ser avisado sobre os resultados obtidos através da revisão tanto quando eles forem favoráveis (os dados estão corretos) ou quando for encontrado alguma irregularidade.

- Todos os proprietários estão identificados, ou seja, os que possuem acesso a um conjunto de informações específicas;

- Os inventários são realizados conforme requerido, padronizados e periodicamente;

- Os dados possuem a proteção necessária para garantir sua integridade, protegendo-os contra acessos e alterações indevidas;

- As documentações necessárias devem ser avaliadas pelas áreas competentes, garantindo que estas demonstrem o que realmente ocorre dentro da área a que se está referindo as documentações;

- Quando ocorrem desastres desde um erro de digitação até a perda total dos dados de um banco de dados, existe um plano de recuperação em caso de desastre que são testados conforme requerido. Por exemplo, existem os sistemas de backup e recovery, isto é, os dados mais importantes devem possuir cópias evitando transtorno em caso de acontecimentos inesperados, verificando sempre se essas cópias estão seguras evitando problemas;

- Os programas críticos, ou seja, os programas de sobrevivência da empresa mais importantes, são seguros o suficiente que qualquer tentativa de fraude não consiga alterar o sistema;

- Um terminal tem acesso somente as informações inerente àqueles que irão manipulá-lo, ou seja, um terminal no setor de Finanças só proverá informações ligadas a este setor e seus processos, não terá acesso às informações relacionadas ao setor de Recurso Humanos. Por sua vez, estes terminais podem possuir senhas próprias, podendo ser acessado somente pelos envolvidos a este setor que estejam autorizados a possuírem tais informações, estando protegido assim, contra acessos não autorizados, ou utilizado outros métodos, pois depende de que área encara como segurança da informação;

- As senhas devem possuir suas trocas automáticas garantidas, pois é muito arriscado para uma empresa, principalmente empresas de grande porte, manter uma mesma senha por um grande período;

- O processo de auto-avaliação desta área foi feito e concluído com sucesso;

- Todos os usuários estão autorizados para o uso do computador, isto é, qualquer pessoa não autorizada a manipular dados dentro do sistema possa obter informações sem influenciar o sistema. Ex.: alterações.