Auditoria de Sistemas

Prof. Luiz Antonio Ferraro Mathias

Aula 02

Conceitos Básicos da Auditoria

Conceitos básicos da Auditoria

Alguns conceitos básicos relacionados com a auditoria são: campo, âmbito e área de verificação.

a) O **campo** compõe-se de aspectos como: objeto, período e natureza da auditoria.

b) O **objeto** é definido como o "alvo" da auditoria, pode ser uma entidade completa (corporações públicas ou privadas, por exemplo).

c) **Período** a ser fiscalizado pode ser um mês, um ano ou, em alguns casos, poderá corresponder ao período de gestão do administrador da instituição.

d) A **natureza** da auditoria poderá ser operacional, financeira ou de legalidade, por exemplo.

Conceitos básicos da Auditoria

e) O **âmbito da auditoria** pode ser definido como a amplitude e exaustão dos processos de auditoria, ou seja, define o limite de aprofundamento dos trabalhos e o seu grau de abrangência.

f) A **área de verificação** pode ser conceituada como sendo o conjunto formado pelo campo e âmbito da auditoria

Conceitos básicos da Auditoria

Os procedimentos de auditoria formam um conjunto de verificações e averiguações que permite obter e analisar as informações necessárias à formulação da opinião do auditor. O processo de auditoria é baseado em controles, que representam a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos ou sobre produtos, para que estes não se desviem das normas ou objetivos previamente estabelecidos. Existe m três tipos de controles:

Controle	Descrição
Preventivos	usados para prevenir fraudes, erros ou vulnerabilidades. (senhas de acesso a algum sistema informatizado, por exemplo.
Detectivos	usados para detectar fraudes, erros, vulnerabilidades (por exemplo: Log de eventos de tentativas de acesso a um determinado recurso informatizado).
Corretivos	usados para corrigir erros ou reduzir impactos causados por algum sinistro (planos de contingência, por exemplo).

Conceitos básicos da Auditoria

Um dos objetivos desses controles é, primeiramente, a manutenção do investimento feito pela corporação em sistemas informatizados, tendo em vista que os sistemas de informação interconectados de hoje desempenham um papel vital no sucesso empresarial de um empreendimento. Esses controles também têm como objetivo evitar que algum sinistro venha a ocorrer; não conseguindo evitar, tentar fazer com que o impacto seja pequeno e, se mesmo assim, o impacto for grande, ter em mãos processos que auxiliem a reconstrução do ambiente

O resultado da análise dos controles durante o processo de auditoria se materializa através dos chamados “achados” de auditoria que são fatos importantes observados pelo auditor durante a execução dos trabalhos. Apesar de que geralmente são associados a falhas ou vulnerabilidades, os “achados” podem indicar pontos fortes da corporação auditada. Para que eles façam parte do relatório final de auditoria, estes devem ser relevantes e baseados em fatos e evidências incontestáveis.

Esses registros podem estar em forma de documentos, tabelas, listas de verificações, planilhas, arquivos, entre outros. Estes documentos são a base para o relatório de auditoria, pois contêm registro da metodologia utilizada, procedimentos, fontes de informação, enfim, todas as informações relacionadas ao trabalho de auditoria.

Conceitos básicos da Auditoria

Elas são medidas corretivas possíveis, sugeridas pela pelo auditor em seu relatório, para corrigir as deficiências detectadas durante o trabalho de verificação de vulnerabilidades ou deficiências. Dependendo da competência ou posição hierárquica do órgão fiscalizador, essas recomendações podem se transformar em determinações a serem cumpridas (DIAS, 2000)

Vários autores fazem uma classificação ou denominação formal sobre a natureza ou sobre os diversos tipos de auditorias existentes. Os tipos mais comuns são classificados quanto: à forma de abordagem, ao órgão fiscalizador e à área envolvida. Acompanhe, a seguir, quais são elas:

Quanto à forma de abordagem:

Controle	Descrição
Auditoria horizontal	auditoria com tema específico, realizada em várias entidades ou serviços paralelamente.
Auditoria orientada	focaliza uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.

Classificação das Auditorias

Quanto ao órgão fiscalizador:

Controle	Descrição
Auditoria interna	auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Este serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.
Auditoria externa	auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.
Auditoria articulada	trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

Classificação das Auditorias

Quanto à área envolvida:

Controle	Descrição
Auditoria de programas de governo	Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico – verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.
Auditoria administrativa	engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.
Auditoria contábil	é relativa à fidedignidade das contas da instituição. Esta auditoria, consequentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.

Classificação das Auditorias

Auditoria financeira	**conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade – conhecida como auditoria de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.**
Auditoria operacional	incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.
Auditoria de sistemas informatizados	tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

Classificação das Auditorias

Dependendo da área de verificação escolhida, este tipo de auditoria pode abranger: todo o ambiente de informática ou a organização do departamento de tecnologia. Além disso, pode ainda contemplar: os controles sobre banco de dados, redes de comunicação e de computadores e controles sobre os aplicativos.

Deste modo, sob o ponto de vista dos tipos de controles citados, a auditoria pode ser separada em duas grandes áreas:

a) Auditoria de segurança de informações - este tipo de auditoria em ambientes informatizados determina a postura ou situação da corporação em relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança, enfim, controles que influenciam o bom funcionamento dos sistemas de toda a organização. São estes:

I. Avaliação da política de segurança;

II. Controles de acesso lógico;

Classificação das Auditorias

i. Controles de acesso físico;
ii. Controles ambientais;
iii. Plano de contingência e continuidade de serviços;
iv. Controles organizacionais;
v. Controles de mudanças;
vi. De operação dos sistemas;
vii. Controles sobre o banco de dados;
viii. Controles sobre computadores;
ix. Controles sobre ambiente cliente-servidor

Classificação das Auditorias

a) Auditoria de aplicativos - este tipo de auditoria está voltado para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende, como: orçamento, contabilidade, estoque, marketing, RH etc. A auditoria de aplicativos compreende:

i. Controles sobre o desenvolvimento de sistemas aplicativos;
ii. ii. Controles de entrada, processamento e saída de dados;
iii. iii. Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida

Motivação das Auditorias

Um ditado popular diz “que nenhuma corrente é mais forte que seu elo mais fraco”; da mesma forma, “nenhuma parede é mais forte que a sua porta ou janela mais fraca, de modo que você precisa colocar as trancas mais resistentes possíveis nas portas e janelas”. De forma similar é o que acontece quando você implementa segurança em um ambiente de informações. Na realidade, o que se procura fazer é eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível para estes.

Acima de tudo, o bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com este bem de consumo ou serviço. Ao longo da história, o ser humano sempre buscou o controle das informações que lhe eram importantes de alguma forma; isto é verdadeiro mesmo na mais remota antiguidade. O que mudou desde então foram as formas de registros e armazenamento das informações; se na pré-história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento e registro de informações era a memória humana, com o advento dos primeiros alfabetos isto começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

Motivação das Auditorias

Atualmente , não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou- se muito em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação. Independente do setor da economia em que a empresa atue, as informações estão relacionadas com seu processo de produção e de negócios, políticas estratégicas, de marketing, cadastro de clientes etc. Não importa o meio físico em que as informações estão armazenadas, elas são de valor inestimável não só para a empresa que as gerou, como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas com atividades diárias da empresa que, sem elas, poderia ter dificuldades.

Motivação das Auditorias

Tradicionalmente, as empresas dedicam grande atenção de seus ativos físicos e financeiros, mas pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem; esta proteção tradicional pode nem mesmo visar um bem valioso. Da mesma forma que seus ativos tangíveis, as informações envolvem 3 (três) fatores de produção tradicionais: capital, mão-de-obra e processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento fisco-contábil que os outros ativos, do ponto de vista do negócio, elas são um ativo da empresa e, portanto, devem ser protegidas. Isto vale tanto para as informações como para seus meios de suporte, ou seja, para todo o ambiente de informações (O`BRIEN, 2002).

Numa instituição financeira, o ambiente de informações não está apenas restrito à área de informática, ele chega a mais longínqua localização geográfica onde haja uma agência ou representação de qualquer tipo. Enquanto na área de informática os ativos de informação estão armazenados, em sua maior parte, em meios magnéticos, nas áreas fora deste ambiente eles ainda estão representados em grande parte por papéis, sendo muito tangíveis e de entendimento mais fácil por parte de seres humanos

Motivação das Auditorias

E, dada à característica de tais empreendimentos, que no caso de bancos é essencialmente uma relação de confiança, é fácil prever que isto acarretaria completo descontrole sobre os negócios e até uma corrida ao caixa. A atual dependência das instituições financeiras em relação à informática está se estendendo por toda a economia, tornando aos poucos todas as empresas altamente dependentes dos computadores e, consequentemente, cada vez mais sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle gerencial.

Os riscos são agravados em progressão geométrica à medida que informações essenciais ao gerenciamento dos negócios são centralizadas e, principalmente, com o aumento do grau de centralização. Ainda que estes riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob aspectos econômicos, quanto sob aspectos de agilização de processos de tomada de decisão em todos os níveis. Esta agilização é tanto mais necessária, quanto maior for o uso de facilidades de processamento de informação pelos concorrentes

Motivação das Auditorias

É preciso, antes de qualquer coisa, cercar o ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável, pois é impossível obter-se segurança total já que, a partir de um determinado nível, os custos envolvidos tornam-se cada vez mais onerosos e superam os benefícios obtidos. Estas medidas devem estar claramente descritas na política global de segurança da l organização, delineando as responsabilidades de cada grau da hierarquia e o grau de delegação de autoridade e, muito importante, estarem claramente sustentadas pela alta direção.

A segurança, mais que estrutura hierárquica, os homens e os equipamentos envolvem uma postura gerencial, que ultrapassa a tradicional abordagem da maioria das empresas.