AUDITORIA DE SISTEMAS

AULA 4

Prof. André Roberto Guerra

CONVERSA INICIAL

A partir das décadas de 1940 e 1950, o conceito de auditoria interna começa a afirmar-se, passando o controle interno a ter um papel-chave na auditoria das grandes organizações.

> A origem dos controles internos está relacionada as necessidades crescentes de informações sobre a *performance* empresarial. Para gerar essas informações passou-se a exigir controle interno eficiente, a fim de permitir um acompanhamento eficaz dessa *performance* pela Gestão e público em geral.
> O controle interno compreende o plano de organização e o conjunto coordenado dos métodos e medidas adotados pela empresa para salvaguardar seu patrimônio, conferir exatidão e fidedignidade dos dados, promover a eficiência operacional e encorajar a obediência as diretrizes traçadas pela administração da companhia. (Costa, 2017)

A auditoria pode ser considerada como infraestrutura de controle interno, orientada para fomentar a viabilidade da organização, na medida em que as operações (áreas auditadas) se beneficiam do fato da auditoria lhes disponibilizar recomendações de como operar de um modo mais eficiente. No entanto, a função de controle interno de SI distingue-se por ser executada por profissionais internos à organização, que reportam à gestão dos SI e que se dedicam à análise de um conjunto definido de controles no cotidiano.

TEMA 1 – FUNDAMENTOS DE CONTROLES INTERNOS EM SISTEMAS DE INFORMAÇÕES

O conceito de controle interno em um sistema de informação, conforme declaração do Instituto Americano de Contadores Públicos (AICPA, 2017) significa

> [...] planos organizacionais e coordenação de um conjunto de métodos e medidas adotado numa empresa, a fim de salvaguardar o ativo, verificar a exatidão e veracidade de registros contábeis, promover a efetividade de sistema de informação contábil e eficiência operacional, assim como fomentar uma grande adesão às políticas da organização. (AICPA, 2017)

O uso do computador de forma alguma altera os conceitos básicos de um sistema de controle interno. O que muda são as abordagens diferentes, usadas em ambiente de tecnologia de informação, distintas das do ambiente manual. Dessa forma, com o aumento do uso de tecnologia de informações nos negócios, o auditor incorpora a nova tarefa, inclui revisão de controles em sua cobertura

de riscos empresariais, assim como enfatiza o texto de anuência às características essenciais de controle.

A auditoria de sistema de controle interno de uma organização inclui verificações dos processos e confirmação quanto à sua efetividade, e é por isso que é regida pela lei da variedade de requisitos. Entretanto, esta última característica deveria ser observada se a organização, devido a seu sistema dinâmico operacional claramente definido, tem que manter fidelidade e/ou integridade de informação, eficiente e eficaz.

A eficácia de um sistema tem sido visualizada quanto à consecução da missão de tecnologia de informação. Vejam: se o objetivo do sistema for reduzir *headcount* ou agilizar o processo de tomada de decisão, este tem que ser atingido, ou o sistema não virá ao encontro da sua expectativa e poderá ser julgado a partir da função de fornecer informação necessária ao processo de tomada de decisão da gerência.

A responsabilidade total sobre o sistema de controle interno de uma organização pertence à gerência e, mais particularmente, àqueles cuja autoridade foi delegada no que diz respeito a responsabilidades funcionais.

1.1 A importância dos controles internos

Segundo Attie (1995),

> Os problemas de controles internos estão em todas as áreas da empresa: vendas, fabricação, compras, tesouraria etc. O exercício de um adequado controle sobre cada uma dessas funções assume fundamental importância para alcançar resultados mais favoráveis com menores desperdícios. Informações distorcidas podem levar a conclusões erradas e danosas para a empresa. (Attie, 1995)

Confiar nos subordinados não deixa de ser correto, porém é necessário admitir-se que esta confiança pode dar lugar a toda espécie de fraudes. Grande parte das irregularidades nos negócios, segundo se tem verificado, deve-se a funcionários que se consideravam de confiança. Além disso, onde não existem procedimentos de controle interno, são frequentes os erros involuntários e desperdícios. A estrutura relata que os controles internos são “pilares” em que a administração se apoia para medir o alcance dos objetivos fixados pela organização.

A importância do controle interno pode ser resumida, segundo Attie (1992, p. 61), considerando-se os seguintes fatores:

- quanto maior a empresa, mais complexa é a sua organização estrutural. Para controlar as operações eficientemente, a administração necessita de relatórios e análises concisos, que reflitam a situação da companhia;
- um sistema de controle interno que funcione adequadamente constitui a melhor proteção para a companhia contra as fraquezas humanas. As rotinas de verificação e revisão são características de um bom controle interno, que reduzem a possibilidade de que erros ou tentativas fraudulentas permaneçam por muito tempo e permitem à administração possuir maior confiança na adequação dos dados. (Attie1992)

1.2 Princípios fundamentais de controles internos

A natureza da estrutura de controles internos é variável entre as empresas devido às particularidades do segmento econômico de cada uma.

Isso porém não invalida o reconhecimento da existência de princípios fundamentais que devem estar presentes em qualquer estrutura de controle eficiente.
Os princípios fundamentais de controle interno são:

- é necessário fixar as responsabilidades – para ter clara delimitação de responsabilidade em um sistema bem planejado. Caso contrário não haverá eficiência;
- os registros devem estar separados das operações – as funções de operações e registro são incompatíveis entre si e, por conseguinte, não devem ser executadas pela mesma pessoa;
- o ciclo completo de uma transação não deve ser executado apenas por uma única pessoa – nenhuma pessoa deve ter a seu cargo a realização de todas as fases de uma transação comercial. Qualquer pessoa, seja funcionário ou administrador, comete erros, deliberados ou não, porém é muito provável que o erro seja descoberto quando a transação, para sua completa concretização, necessariamente envolva duas ou mais pessoas;
- o pessoal envolvido com funções de controle deve ser criteriosamente selecionado, bem treinado – antes de contratar qualquer funcionário com vista ao preenchimento de cargos que tem funções de controle, é necessário que o seu passado seja investigado e suas referências conferidas. O treinamento é imprescindível para familiarizar o novo empregado com suas tarefas;
- sempre que possível, promover o rodízio de funcionários – periodicamente deve ser promovido um rodízio de funcionários, de modo que cada um possa ser capaz de executar outras tarefas. Isso aumenta a segurança do sistema, ao eliminar os chamados funcionários imprescindíveis, além de estimular a criatividade de cada um, mediante os desafios implícitos que as novas funções trazem. Todos necessitam de férias regulares, o que resulta em maior produtividade operacional e reduz a possibilidade de ocultação de fraudes;
- as tarefas devem estar previstas no manual da organização – preferencialmente todas as instruções necessárias ao desempenho funcional dentro do sistema devem ser escritas e catalogadas em um manual de organização. Aqui também se espera conseguir aumento de eficiência operacional, juntamente com a diminuição do risco de erros;
- os responsáveis pela custódia de numerários e outros ativos devem ter seguro-fidelidade – além de proteger o patrimônio da entidade em caso de desvio, o seguro-fidelidade é um freio psicológico para as tentativas de desfalques, pois os funcionários sabem que a

companhia seguradora somente indenizará prejuízo quando houver comunicação da ocorrência à autoridade policial, e assim as responsabilidades serão apuradas;

- devem ser utilizados equipamentos informatizados para registro automático de operações – sua utilização evita erros e aumenta consideravelmente a eficiência do sistema de controle, permitindo a realização simultânea de vários procedimentos de registro. (CEAD, 2017)

TEMA 2 – CONTROLES INTERNOS EM TI, PRINCÍPIOS, FINALIDADES E OBJETIVOS

A natureza e a extensão de controles necessários em ambiente de tecnologia de informação variam paulatinamente de acordo com a complexidade da tecnologia de informação em operação. Para aquele(a) que acompanha o sistema de controle em um ambiente particular, é imperativo determinar e padronizar os tipos de equipamentos em operação, a natureza dos dados que são processados e os procedimentos metodológicos existentes.

Num ambiente de sistema computadorizado básico, que processe seus dados mais manualmente do que computacionalmente, pode haver uma necessidade de procedimentos, tais como:

- Identificação;
- Autorização;
- Autenticação;
- Classificação de dados que sejam realizados manualmente.

Evidentemente, o sistema necessitará mais de controles convencionais do que de controles modernos e computadorizados, que são bastante direcionados para ambientes de tecnologia de informação mais complexos.

Para isso, vários tipos de controles são estabelecidos pela gerência de uma organização para manter uma administração própria de um sistema computadorizado. Eles envolvem:

- Controles organizacionais;
- Controles de segurança e privacidade;
- Controles de preparação;
- Controles de entrada;
- Controles de processamento;
- Controles de recuperação e armazenamento de dados;
- Controles de saída.

2.1 Finalidades dos controles internos

Existem interpretações distintas atribuídas ao conceito de proteção de ativos de uma entidade. A mais abrangente entende que os ativos devem ser resguardados de qualquer situação indesejável. Nesse caso, compreende-se que a proteção dos ativos atuais e futuros se constitui numa das funções principais da administração da companhia.

> A segunda interpretação do conceito de proteção de ativos, menos abrangente, leva em consideração que tal conceito refere-se à proteção contra erros involuntários (não intencionais) ou irregularidades intencionais. Citam-se exemplos, tais como: erros provenientes de cálculos incorretos, realização de procedimentos indevidos ou sua omissão. (CEAD, 2017)

As interpretações do conceito de proteção entendem que a proteção dos ativos se referem tão somente aos erros intencionais (fraude).

2.2 Objetivos dos controles internos

Os objetivos do controle interno são, entre outros, assegurar que as várias fases do processo decisório, o fluxo de informações e a implementação das decisões se revistam da necessária confiabilidade.

Os principais objetivos de um sistema geral de controle interno são:

- Proteger os ativos de uma organização;
- Manter a integridade;
- Corrigir e garantir a confiabilidade dos registros;
- Promover a eficiência operacional;
- Encorajar o cumprimento dos procedimentos e das políticas da gerência.

Esses objetivos não apresentam diferenças nos procedimentos de controles internos em ambientes de tecnologia de informações.

Princípios de controles internos geralmente aceitos em ambiente de tecnologia de informação constituem a parte integral dos objetivos e princípios de controles internos em âmbito global, mesmo ainda não tendo aceitação universal. Contudo, alguns desses princípios estão em operação dentro dos ambientes computadorizados e são aceitos.

Segundo Imoniana (2015) eles são:

> **Supervisão** – A gerência, por objetivos, procedimentos e tomada de decisões, deve manter um controle que a capacite a uma supervisão efetiva dentro do ambiente de tecnologia de informação.

Registro e comunicação – A gerência da empresa deve estabelecer critérios para criação, processamento e disseminação de informação de dados, através de autorização e registro de responsabilidades.
Segregação das funções – As responsabilidades e ocupações incompatíveis devem estar segregadas de maneira a minimizar as possibilidades de perpetuação de fraudes e até de suprimir erro e irregularidade na operação normal.
Classificação de informação – A gerência deve estabelecer um plano para classificação de informação que melhor sirva às necessidades da organização, em conformidade com os princípios de contabilidade geralmente aceitos e também padrões de auditoria geralmente aceitos.
Tempestividade – A gerência deve delinear procedimentos, monitorar os registros corretos das transações econômicas, financeiras e contábeis das empresas, processando-as e comunicando os resultados às pessoas necessárias em tempo hábil.
Auditoriabilidade – Os procedimentos operacionais devem permitir a programação e verificação periódica no que concerne à precisão do processo de processamento de dados e de geração de relatório, de acordo com as políticas.
Controle independente – Os sistemas em funcionamento devem ter procedimentos adequados para identificação e correções de erros no fluxo de processamento, inclusive nos processos executados concomitantemente.
Monitoramento – A gerência deve possuir acesso *master* ao sistema e controle de uso, que lhe permita fazer o acompanhamento *pari-passu* das transações.
Implantação – A gerência deve planejar a aquisição, o desenvolvimento, a manutenção e a documentação de sistema, de forma a coincidir com as metas empresariais.
Contingência – A gerência deve implementar um plano adequado e procedimentos para prevenir-se contra as falhas de controles que podem surgir durante especificações de sistema, desenho, programação, testes e documentação de sistemas e nas fases pós-implantações.
Custo efetivo – Investimentos em tecnologia de informação devem ser propriamente planejados, a fim de coincidirem com o custo efetivo. Imoniana (2015)

TEMA 3 – TIPOS DE CONTROLES INTERNOS

Existem vários tipos de controles em sistemas computadorizados, desde formais até informais, dependendo da sofisticação do sistema em operação.

Um sistema de informação, sob o ponto de vista de auditoria, segundo Imoniana (2015), está dividido pela gerência em diversos controles. Os controles internos são

> [...] os planos organizacionais e coordenação de um conjunto de métodos e medidas adotado numa empresa, a fim de manter o ativo, verificar a exatidão e a veracidade de registros, promover a efetividade de sistema de informação e fomentar uma grande adesão às políticas da organização. Estes controles internos dividem-se em organizacionais, controles de segurança e privacidade, controles de preparação, controles de entrada, controles de processamento, controles de recuperação, de armazenamento de dados e de saída. Imoniana (2015)

3.1 Controles administrativos e gerenciais

O Autor Imoniana (2015) descreve:

> A gerência de uma organização é responsável pelos controles administrativos e gerenciais de um sistema de informação. Esses controles incluem a separação convencional de funções ou responsabilidades, o estabelecimento de objetivos e metas de segurança de informação, planos orçamentários, seleção de pessoal, designação de autoridades e treinamento de pessoal, além de desenvolvimento e implementação de medidas corretivas para os desvios de políticas e padrões estipulados para o processo de gerenciamento. Imoniana (2015)

Em organizações cujas responsabilidades são impropriamente delineadas, a fraude é perpetrada facilmente, devido ao conhecimento de que ninguém será responsabilizado. Assim, o trabalho dos desenhistas de controles administrativos e gerenciais é segregar adequadamente as tarefas e/ou atividades incompatíveis: quem prepara a entrada de dados, quem processa os dados, quem os gerencia e quem são os usuários finais. Mais da metade dos casos recentes de fraude no computador envolveu conivência. Esse é um incidente muito maior do que uma fraude manual e pode significar que a fraude em computador requer mais habilidade, acesso e conhecimento do que simples conhecimentos gerais.

Em um sistema computadorizado, existem duas funções distintas bastante afins, assim como acontece em todas as atividades de processamento eletrônico de dados. A primeira diz respeito à elaboração de programas, e a segunda está relacionada às operações diárias do sistema.

Com os princípios fundamentais de controles internos, as responsabilidades dos desenhos e o detalhamento de programas em um ambiente de tecnologia de informação devem ser atribuídos a pessoas que não têm nenhum acesso às operações do computador. Assim, também os usuários finais não devem ter qualquer acesso aos documentos detalhados dos programas.

3.2 Controles de segurança e privacidade

Conceitua-se privacidade em termos genéricos, para uma fácil compreensão. É uma conotação ambígua de segurança de informações. Mostra um estado oculto e fora do alcance de algum grupo particular em um ambiente de computação, programas, aplicativos, dados e/ou equipamentos e informação

pertencentes a pessoas restritas a certas funções. A proteção e/ou o acesso livre à informação sempre trouxeram conflitos de interesses entre gerentes, departamentos operacionais ou organizações do mesmo conglomerado e até países em nível internacional. As preocupações de privacidade, quando são intensificadas internacionalmente, buscam reduzir atos como os de espionagem.

Com o aumento crescente da necessidade de segurança, os usuários de informações são conscientizados, e os controles que restringem o acesso às informações são aceitos com maior naturalidade. Os controles de segurança de dados em sistema de informações computadorizados são referentes à proteção de informação, evitando-se atos de destruição intencionais, ou não intencionais, acidentes e outros atos de sabotagem. Outros são referentes a furtos, manipulação fraudulenta ou divulgação de informações sigilosas para competidores a fim de obter vantagens próprias. Esses atos, se desprezados, podem mostrar efeitos devastadores na organização. Qualquer organização que opere com tecnologia de informação necessita de segurança, que varia proporcionalmente de acordo com a complexidade de seu ambiente operacional. Os controles de segurança mudam de tempos em tempos, dependendo da evolução da tecnologia do computador.

A segurança em sistema computadorizado é muito importante, não somente em termos de proteção física de dados, mas também para prevenir ocorrências de incidentes fatais, que podem causar estragos irreparáveis em documentos e programas vitais. Geralmente, a decisão sobre a implementação de controles de segurança de informações é tomada em conjunto com a alta administração.

Os controles de segurança em detrimento do funcionamento normal do sistema são também concernentes às provisões de facilidades de *backup.* Esses controles podem também incluir a programação de tarefas de forma ordenada, evitando conflitos de ciclos operacionais que congestionam os sistemas, planos de contingência e de recuperação de desastres.

Segundo Imoniana (2015), as propriedades dos controles de segurança de sistemas são:

> **SIGILO**: fornecer uma privacidade ou situação estritamente confidencial aos dados. Um pequeno deslize nesta propriedade conduz a uma derrocada de assuntos restritos.
> **INTEGRIDADE**: fornecer um requisito de informação completa, correta e válida, e confiabilidade a dados autorizados, guardando-os das distribuições e modificações não usuais. Qualquer sistema que

preencha tais requisitos estará manifestando as propriedades de integridade.

DISPONIBILIDADE: tornar os dados disponíveis a quem quer que esteja autorizado a usar tais dados. Apesar de ser dada proteção total aos dados, os requisitos para usá-los não devem ser prejudiciais. No entanto, poderão ser extraídas informações com um mínimo esforço ou interferência.

CONTABILIDADE: registrar todas as transações ocorridas nos sistemas, a fim de permitir o relato correto do conteúdo dos dados alimentados no sistema e, sobretudo, permitir, quando for necessário, rastrear a verdade e reportar a visão justa das informações armazenadas.

AUDITORIABILIDADE: em qualquer sistema de segurança, os dados devem ser auditados. Isso possibilita à gerência relatórios de acompanhamento, para que se saiba se estão sendo efetivos os controles implementados. O sistema também deve fornecer facilidade necessária para exames e averiguação de responsabilidades. Imoniana (2015)

3.3 Controles de preparação e captação de dados

Este é um controle exercido no começo de cada atividade de processamento de dados. Envolve o recebimento de documentos (dados-fonte), pré-numerando e preparando o *input,* o qual vem a constituir-se no processo de conversão dentro de uma linguagem de máquina.

Esses documentos, quando recebidos, são agrupados em *batches* (lotes), preferivelmente aquelas transações que possuem sequência de processamento comum, através dos comandos de leitura do lote. Isso facilitará o acesso, quando for necessário, nas atividades de processamento normal.

Como esses *batches* são controlados? São controlados pelo uso dos totais de controle. Isso assegura que os lotes pretendidos estão completos. Normalmente, é aconselhável minimizar o tamanho do lote, de maneira que facilite a investigação dos erros. Os lotes muito grandes dificultam a descoberta dos erros de processamentos.

3.4 Controles de entrada de dados

Os controles de entrada visam assegurar que os dados de entrada sejam validados, editados e consistentes com o tempo e com dados-fontes. A validação de dados de entrada identifica erros de dados, dados incompletos ou faltantes e inconsistências.

As entradas erradas conduzem a saídas erradas, e isso pode ser prejudicial para o ambiente econômico, social e humano de qualquer

organização. Pode causar aumento de custo, trazendo desmoralização e falta de credibilidade, e pode também causar medo quanto ao uso do sistema.

Assim, esse controle é responsável pela redução de dúvidas que possam existir no ponto de entrada dos dados do sistema de informação computadorizado.

Esses controles são embutidos nos próprios sistemas, que ajudam a indagar quanto à veracidade das transações que estão sendo efetivadas. Quaisquer inconsistências são negadas. Ou, quando acontece uma transação incomum, geralmente há intervenção da gerência para liberar tal lançamento.

Os controles de entradas podem ser a autorização de entrada que verifica se todas as operações foram autorizadas e aprovadas pela administração e incluem assinaturas nos formulários de lote ou documentos de origem, controles de acessos *on-line*, senhas exclusivas para iniciar as transações, identificação do terminal ou estação de trabalho, principalmente para transações sensíveis, documentos de origem e numerações, controles de lote e balanceamento, controles de lote e as operações de entrada por grupo para fornecer os totais de controle.

3.5 Registro de erros e manipulação

Os processamentos de entradas exigem que os controles sejam identificados para verificar se os dados são aceitos no sistema corretamente e se os erros de entrada são reconhecidos e corrigidos. A entrada de manipulação de erro pode ser processada das seguintes formas:

- Rejeitando operações com erros;
- Rejeitando todo o lote de transações;
- Segurando o lote em suspense;
- Aceitando o lote e as operações com erros sinalizados.

3.6 Controles de processamento

Com o pressuposto de que os dados corretos entraram no computador de forma segura, os controles de processamento são aqueles responsáveis pelo lançamento do relatório pretendido. Os controles de processamento são programados ou construídos dentro do computador e executam vários tipos de operações quando acionados nos ciclos transacionais.

Algumas das atividades são checagens da sequência dos arquivos-mestres e arquivos de transações e checagem dos campos dos arquivos, para detectar superposição de dados. Isso assegura que os registros de transações disponíveis no computador sejam processados antes que o arquivo-mestre seja fechado.

Esse controle faz uso do limite lógico, dos testes de racionalidade e de total cruzados. O limite lógico e a racionalidade verificam a extensão para a qual o processamento foi executado, se está no limite predeterminado e, então, checam sua racionalidade e fazem o *cross-footing.*

O *cross-footing* é aquele controle similar às técnicas manuais para comparar totais independentes de itens individuais com o derivado do total geral, o qual é executado nos formatos programados. Frequentemente utilizados, são controles de balanceamento, nos quais os registros processados são reconciliados a fim de assegurar a integridade do *log* de transação.

3.7 Controles de saída e de emissão de relatórios

Os controles de saída visam garantir que as informações entregues aos usuários sejam apresentadas em formatos corretos, completas, para atender às necessidades desses usuários, e, ainda, consistentes com modelos preestabelecidos e de forma segura.

Para que a distribuição de relatórios seja satisfatória, os procedimentos de manuseio de *output* devem ser administrados, a fim de assegurar que os relatórios solicitados sejam impressos ou transmitidos e que somente pessoas autorizadas devam recebê-los.

Os controles de saída incluem:

- Registro e armazenamento de documentos sensíveis e críticos em local seguro;
- Geração pelos computadores de instrumentos negociáveis, formulários e assinaturas e distribuição de relatórios;
- Equilíbrio e conciliação;
- Tratamento de erros de saída;
- Retenção de relatório de saída; e
- Verificação de recebimento de relatórios.

3.8 Controles de gravação e recuperação de dados

A biblioteca de dados controla a liberação de dados para o processamento e seu armazenamento subsequente. Esse controle certifica a integridade de dados recebidos dentro da *data-base*, e qualquer indivíduo autorizado pode acessá-lo com o mínimo esforço.

Normalmente, os arquivos de programas e transação são estocados em fitas magnéticas, CDs, entre outros dispositivos periféricos e unidades de memória auxiliar de computador. O bibliotecário não tem acesso à unidade de leitura e gravação desses dispositivos, uma vez que poderia violar os princípios de segurança de informações.

Para se obter acesso ao banco de dados, os controles relacionados ao uso de *passwords* e códigos de acessos são muito importantes. Envolvem um diálogo simples entre o usuário em interface com o próprio computador, e, a partir do momento em que as respostas forem favoráveis, com a validação e identificação dos usuários, a tal usuário será permitido o acesso, dando-lhe uma chance de responsabilizar-se com certo grau de risco, no limite de acesso, e este será plenamente responsável pelos recursos do computador que está sendo usado. O uso lógico dessas senhas reduz conflitos ou intervenções no processamento.

A manutenção e a atualização periódicas de arquivo são ideais em qualquer banco de dados. Isso assegura a eficácia dos controles que isolam a existência de arquivos obsoletos ou inativos. O monitoramento de arquivos críticos conceitua-se em um controle maior para manter a integridade de tais arquivos. Por exemplo: os arquivos de registros de pessoal devem ser atualizados de acordo com suas promoções, seja horizontal ou vertical, que, por sua vez, afetam os salários e, consequentemente, a folha de pagamento.

Falar sobre controles de gravação de dados lembra-nos da probabilidade de incidentes ou desastres que podem ocorrer no ambiente do computador. No caso de tipos não triviais, as facilidades de *backup* são aplicadas para manter o sistema em funcionamento.

No que se refere a tipos mais desastrosos, os planos desastre, contingência e recuperação de dados são usados a fim de abranger todas as prováveis ameaças. Os planos são revisados e testados de tempos em tempos, à medida que nova tecnologia ofereça novos riscos.

TEMA 4 – AVALIAÇÃO DOS PROCEDIMENTOS DE CONTROLES INTERNOS DE SI

O processo de avaliação implica naquele utilizado pelo auditor para confirmar as assertivas em relação à transação ou aos processos de uma entidade, seja ele de controles internos sistêmicos ou de transações sobre os documentos, com a finalidade de apoiar a formação de uma opinião e proporcionar uma informação sobre o grau em que as assertivas estão em conformidade com um conjunto de padrões identificados.

Exame da configuração de sistemas de segurança de informação atende às políticas e do processo de *compliance* que fornece o mais alto nível de garantia sobre a afirmação de que um auditor pode proporcionar. São exemplos de teste:

- Teste de controles: efetuar o *walk-through* do processo de movimentação;
- Testes substantivos: recalcular totais de inventários e custos de produtos vendidos.

Testes de resiliência podem não ter sido contemplados nos testes relacionados aos monitoramentos efetuados pela administração de segurança de informações. Neste caso, deve-se selecionar a política de segurança de informações para averiguar os testes estabelecidos a respeito de riscos cibernéticos.

Geralmente, as assertivas podem ser estabelecidas pelos auditores em nível de transação:

- **Integridade** – as operações registradas e tratadas não foram processadas corretamente, considerando todos os comandos, e estão incompletas, considerando todos os dados necessários a partir do banco de dados para concluir a operação.
- **Válido** – todos os dados que resultaram em débito das contas devem representar as operações que realmente ocorreram e que estão relacionadas com os ativos existentes.
- **Registro** – todos os dados registrados em uma rotina devem ser resumidos em um valor que não está acima do que é apropriado para o período. *Cut-off* – crédito antecipado ou postecipado/débito devem refletir uma operação que ocorreu em um período em curso e não posterior.

A avaliação dos procedimentos de controles internos em ambiente de sistemas de informações de uma organização é um trabalho executado pelo auditor que tem habilidade em tecnologia de informações.

Quanto mais fortes forem os reflexos de controle interno dentro de uma organização, menor será a intensidade dos trabalhos de avaliação dos controles internos e também a relação com a integridade de dados e vice-versa. Crê-se que os sistemas computadorizados, ao inverso dos sistemas manuais, têm maior consistência, mas estes não fazem teste de anuência.

Alguém pode sempre pegar alguns dados e traçá-los corretamente a partir do *input*, direcionando-os através do processamento até o output, para ver se houve adequado procedimento de processamento e em conformidade com as políticas de gerenciamento.

Em qualquer sistema de informação complexo ou moderado, não importa, sua avaliação pelos auditores internos se processa através do uso de ferramentas adequadas de auditoria.

Para os trabalhos de auditoria interna, devem-se testar os controles internos, conforme o planejamento dos trabalhos, à medida que surjam as necessidades gerenciais. Outrossim, para que esses testes sejam mais direcionados, os auditores de sistemas devem partir de algumas premissas que são apresentadas em formas de assertivas sobre todos os procedimentos de controles listados para serem avaliados.

TEMA 5 – ANÁLISE DE RISCO NA AVALIAÇÃO DE SISTEMA DE CONTROLE INTERNO

Segundo Imoniana (2015),

> A análise de risco é uma metodologia adotada pelos auditores de TI para saber com antecedência quais as ameaças puras ou prováveis em um ambiente de tecnologia de informação de uma organização. Essas ameaças constituem eventos futuros não desejáveis e incertos, cuja ocorrência resulta em perdas. (Imoniana, 2015)

O auditor, dessa forma, estando alinhado com as necessidades da gerência e visando à busca de eficácia dos sistemas de controles internos e suas possíveis rupturas, verifica risco de integridade na implementação das políticas gerenciais.

Apesar da identificação de risco em um sistema computadorizado ser provavelmente a tarefa mais dificultosa no processo de auditoria de sistemas,

pode ser muito desastrosa ainda; se quaisquer ameaças não forem detectadas em tempo e se tais brechas forem aproveitadas, podem acarretar um prejuízo financeiro para a organização.

Geralmente, os estágios de operação de sistemas que envolvem captação de dados, entrada, processamento, emissão de relatórios, documentação e guarda de dados oferecem riscos aparentes pela própria natureza de tarefas envolvidas. Nesse processo são compreendidas modificação das estratégias predeterminadas e interrupção das operações normais e das funções não autorizadas.

Quando há modificações não autorizadas, evidentemente se identifica uma ruptura de controles na manutenção da integridade dos registros. Em outra visão, quando há uma interrupção, remoção ou destruição de dados, há uma ruptura de controles na disponibilidade da informação.

E, finalmente, quando houver divulgações não autorizadas, haverá também brechas nos controles organizacionais. Nesses casos, o auditor estabelece sua preocupação em relação aos riscos aparentes do ambiente a ser auditado.

O *backup* de dados também poderia apresentar alguma preocupação para o auditor. Se as rotinas de gravação de dados e guarda de cópias foram politicamente determinadas, cabe verificar se o ambiente de controle propicia a implementação dessas políticas. No entanto, o auditor analisa os riscos combinando-os com as técnicas de controle, atentando para a confirmação de sua efetividade.

Hipoteticamente, pode presumir que o sistema de contingência e de recuperação de dados que foi avaliado está perfeito e dentro da atmosfera de observância e presume-se ainda que os comentários hipotéticos estão satisfatórios. Nesse fato, pode não haver necessidade para testes posteriores, uma vez constatado que os riscos são mínimos.

Pode ocorrer que outro sistema, que esteja sob a custódia de auditoria, seja aparentemente inadequado e insatisfatório. Isso pode ser processado e podem ser analisados o risco e a combinação própria dos controles existentes efetuados.

Assim, o auditor necessita continuar a ter mais testes substantivos após os levantamentos e testes de controles internos neste ambiente, usando normalmente as ferramentas de auditoria e técnicas mais apropriadas, tais como

dados de teste, listas de checagem e mapeamento. Isso facilitará a auditoria detalhada, que será capaz de apontar a evidência corroborativa que deve marcar a base do julgamento final do auditor.

FINALIZANDO

Foram apresentados nesta aula os principais conceitos de Controle Interno na Auditoria de Sistemas de Informação.

“A filosofia de auditoria em tecnologia de informação está calcada em confiança e em controles internos. Estes visam confirmar se os controles internos foram implementados e se existem; caso afirmativo, se são efetivos”. (Dutra, 2017)

A ABNT (2005) cita alguns procedimentos de revisão dos controles internos.

> Na categoria A.12.2 - O Processamento correto de aplicações, é explicada a importância da presença de controles dentro de um sistema. Os controles podem ser, por exemplo, funções que monitorem o a manutenção geral dos dados, mantendo os mesmos íntegros. A norma exemplifica que os dados sofrem este monitoramento no momento de sua entrada no sistema, processamento e suas saídas. ABNT (2005)

A auditoria de sistemas une-se a infraestrutura de controle interno, orientada para fomentar a viabilidade da organização, na medida em que as operações (áreas auditadas) se beneficiam do fato de a auditoria lhes disponibilizar recomendações de como operar de um modo mais eficiente.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14598: **Tecnologia da Informação – Avaliação de produto de *software*:** parte 1: visão geral. Rio de Janeiro: ABNT, 2001.

_____. NBR ISO 19011: **Diretrizes para auditoria de gestão da qualidade e/ou ambiental**. Rio de Janeiro: ABNT, 2002.

_____. NBR ISO 27005: **Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação**. Rio de Janeiro: ABNT, 2006. 65p.

AICPA – American Institute of Certified Public Accountants – Instituto Americano de Contadores Públicos Certificados. Disponível em: <http:// www.aicpa.org>. Acesso em: 4 dez. 2017.

ATTIE, W. **Auditoria interna**. São Paulo: Atlas, 1992.

_____. **Auditoria Conceitos e Aplicações**. São Paulo: Atlas, 1995.

BRANDALISE. M. M. T. **Roteiro para elaboração de programas de auditoria em sistema**. 102 f. Trabalho de conclusão de curso (Bacharelado em Sistema de Informação) – Universidade de Caxias do Sul. Caxias do Sul, 2012. Disponível em: <https://repositorio.ucs.br/xmlui/bitstream/handle/11338/1228/TCC%20Mauricio%20Modesto%20Toscan%20Brandalise.pdf?sequence=1&isAllowed=y>. Acesso em: 22 jan. 2018.

TESTES de auditoria e controles internos. CEAD Virtual, 3 set. 2015. Disponível em: <https://issuu.com/materiaisceadvirtual/docs/aula03_8fe93f3a081057>. Acesso em: 4 dez. 2017.

COSTA, J. C. B. **Controle Interno**: sugestão de implantação em uma empresa de corretagem de seguros. Disponível em: <http://brasilesco.la/m14692>. Acesso em: 4 dez. 2017.

DUTRA, E. C. **Auditoria de sistemas de informação**: introdução, controles organizacionais e operacionais. Disponível em: <https://jus.com.br/artigos/56084/auditoria-de-sistemas-de-informacao-introducao-controles-organizacionais-e-operacionais>. Acesso em: 4 dez. 2017.

GIL, A. L. **Auditoria de computadores**. São Paulo: Atlas, 1999.

IIA – The Institute of Internal Auditors. **GTAG – Global Technology Audit Guide**: Management of IT Auditing. The Institute of Internal Auditors. Florida, USA, 2006.

IMONIANA, J. O. **Auditoria de sistemas de informação**. 3. ed. São Paulo: Atlas, 2015.

ISACA – Information Systems Audit and Control Association. **COBIT 5**. Estados Unidos, 2015. Disponível em: <http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx>. Acesso em: 4 dez. 2017.

_____. **CISA Job Practice Areas**. Disponível em: <http://www.isaca.org>. Acesso em: 4 dez. 2017.

_____. **Glossary of Terms**. Disponível em: <http://www.isaca.org>. Acesso em: 4 dez. 2017.

MICHAELIS. **Dicionário *online***. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 4 dez. 2017.

SILVA, P. M. G. **A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências**. 193 f. Dissertação (Mestrado em Tecnologias e Sistemas de Informação) – Universidade do Minho. Braga, 2007. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/8058/1/Pedro%20Gomes%20Silva_A%20Funcao%20Auditoria%20de%20SI.pdf>. Disponível em: 22 jan. 2018.