

ARTHUR LEONE

AUDITORIA

para Concursos

TEORIA E QUESTÕES COMENTADAS

Esta obra contém:

- Auditoria independente
- Auditoria interna

8^a

EDIÇÃO

Revista, atualizada
e ampliada

2026

 **EDITORA**
*Jus*PODIVM
www.editorajuspodivm.com.br

AMBIENTE PED

1. NOÇÕES GERAIS

Até o final de 2009, vigorou a Resolução 1.029/05 do CFC, que tratava especificamente do ambiente de processamento eletrônico de dados, denominado ambiente PED. Isso faz com que o tema seja incluído, com essa exata nomenclatura, em alguns editais. A partir de 2010, por ocasião da convergência, o assunto passou a ser tratado em diversas normas, de forma esparsa, mas concentrado especialmente na NBC TA 315. Há, contudo, uma série de referenciais sobre o assunto na doutrina, bem como de organizações como COSO e COBIT, especialmente com foco nos controles.

Modernamente, o ambiente PED é referenciado como ambiente de TI. Convém lembrar, para evitar confusões, que TI, nesse caso, significa tecnologia da informação e não há qualquer relação com as normas de auditoria interna designadas como NBC TI.

O tema não está entre os mais cobrados em provas e concursos e há poucas questões disponíveis sobre o assunto. Ainda assim, esporadicamente é contemplado em editais de alguns concursos.

Para delimitar nossa área de estudo, saibamos que estamos no campo da auditoria contábil, e não no da auditoria de sistemas informatizados. Interessa-nos, portanto, o ambiente eletrônico em que os dados são processados, e não o conhecimento especializado de TI.

Avaliemos, então, de que forma um ambiente PED (ou ambiente de TI) se relaciona a uma auditoria contábil: diante do estágio tecnológico avançado de nossos dias, um ambiente de TI influencia até mesmo

as atividades mais rotineiras de nossa vida particular e doméstica. Realizamos operações bancárias pela Internet, assinamos contratos digitalmente, mantemos dados em dispositivos eletrônicos diversos.

Nesse ambiente, apesar de ganho de eficiência, somos submetidos a uma série de riscos novos, antes inexistentes. Por exemplo: nossas senhas podem ser roubadas resultando em acessos não autorizados, transações não autorizadas podem ser processadas, nossos bancos de dados podem ser acessados por terceiros, os registros podem ser perdidos, uma linha de programa mal definida pode resultar em saída de dados irreais etc.

Uma entidade empresarial está sujeita a riscos semelhantes. Transações podem ser simuladas, manipuladas, não capturadas pelo sistema de registro, em razão da ação de terceiros, funcionários, administração ou por falhas de sistema.

NBC TA 315, 12

Riscos oriundos do uso de TI é a susceptibilidade dos controles de processamento de informações ao desenho ou à operação ineficiente, ou os riscos à integridade das informações (ou seja, a integridade, a precisão e a validade das transações e outras informações) no sistema de informação da entidade, devido ao desenho ou à operação ineficiente de controles nos processos de TI da entidade.

NBC TA 315, 12

Ambiente de TI são aplicativos de TI e a infraestrutura de suporte de TI, assim como os processos de TI e o pessoal envolvido nesses processos, que uma entidade utiliza para suportar as operações comerciais e alcançar estratégias de negócios.

Podemos perceber que um ambiente PED cria cenários diferentes que merecem a atenção do auditor, mas não modifica a essência da auditoria. A auditoria continua sendo um exame para assegurar a fidedignidade das demonstrações contábeis, como exposto no capítulo 2 deste livro. Porém, submetidos a esse novo cenário, os dados contábeis são gerados a partir de um ambiente PED.

2. CONCEITO

Afinal, o que é um ambiente PED? A resposta é simples. Existe um ambiente PED quando a entidade processa informações que tenham relevância para a auditoria se utilizando de um computador. Observe que a denominação PED caracteriza não apenas ambientes de alta

tecnologia e informatização. Se há pelo menos um computador envolvido nos processos da auditada que seja relevante para a auditoria, já temos um ambiente PED. Um questionamento plausível seria:

Existe entidade sem ambiente PED?

Inimaginável pensar em uma organização nos dias de hoje sem o uso massivo da TI para processar volumosas informações. Ambientes de TI são inerentes a praticamente qualquer organização moderna e mudaram a forma tradicional de comprar e vender mercadorias e serviços e a forma de controlar e manter informações.

3. AMBIENTE PED E OS OBJETIVOS DO AUDITOR

Sabendo que a auditoria consiste em emitir uma opinião sobre as demonstrações contábeis, e que para alcançar esse objetivo o auditor precisa planejar os trabalhos, executar testes de controle e procedimentos substantivos, um questionamento pertinente seria:

Um ambiente PED modificará esses objetivos?

A resposta é não! Se o auditor vai executar uma auditoria em entidade que utiliza um ambiente PED, esse fato não modifica os objetivos dele, isto é, o objetivo da auditoria continua sendo emitir a opinião sobre as demonstrações contábeis e, em busca desse objetivo, o auditor desenvolverá seu trabalho. Muda-se, porém, o ambiente envolvido no trato dos registros contábeis e administrativos, já que a forma de armazenamento e processamento das informações é realizada mediante utilização de recursos PED.

Então, de que forma o ambiente PED interfere no trabalho do auditor?

O uso de PED pode afetar a organização de modo positivo ou negativo. O auditor, quando se prepara para efetuar uma auditoria, preliminarmente avalia os riscos envolvidos e analisa o controle interno da entidade.

Nesses termos, ao iniciar os trabalhos de avaliação de riscos e obtenção do entendimento da entidade, ele deve considerar se a entidade faz uso de TI e de que forma a TI interfere nos registros contábeis.

Nesse processo de conhecimento da entidade, o auditor deve obter entendimento sobre o sistema de informação, inclusive dos processos de negócio relacionados, relevantes para as demonstrações contábeis, compreendendo como os procedimentos de TI iniciam, registram, processam, corrigem e transferem para os registros contábeis as operações.

Observação:

A depender da complexidade envolvida, o auditor poderá determinar, na fase de planejamento, a necessidade da utilização de especialista em TI. O auditor é um contador, e não um especialista na área tecnológica, porém este é um julgamento que cabe a ele.

Ao tempo que processamos muitas informações eletronicamente, fruto de toda essa incorporação tecnológica às empresas, são implantados pelas organizações sistemas de controle interno, que serão providos, também, e conseqüentemente, em um ambiente de TI.

3.1. Influência do ambiente PED na auditoria contábil

Uma transação, ao chegar às demonstrações contábeis, percorreu um longo caminho, que envolve a captura, o controle interno até o efetivo registro. É fácil concluir que nessa “viagem” até chegar às demonstrações contábeis, efetuada eletronicamente, a informação está sujeita a uma série de riscos de manipulação ou adulteração, ainda que não intencional, ou até mesmo ao risco de não captura da transação, além de outras falhas de sistema.

Um ambiente de TI traz mais riscos para o auditor?

Não podemos generalizar. De modo geral, a TI beneficia o controle interno da entidade, permitindo a esta:

- aplicar consistentemente regras de negócio predefinidas e executar cálculos complexos no processamento de grandes volumes de transações ou dados;
- aprimorar a tempestividade, a disponibilidade e a exatidão das informações;
- facilitar a análise adicional das informações;

- aprimorar a capacidade de monitorar o desempenho das atividades da entidade e de suas políticas e procedimentos;
- reduzir o risco de que os controles sejam transgredidos; e
- aprimorar a capacidade de conseguir segregação eficaz de funções por meio da implementação de controles de segurança em aplicativos, bases de dados e sistemas operacionais.

4. CONTROLE INTERNO E AMBIENTE PED

Qualquer sistema de controle interno tem limitações. Um sistema de controle baseado em TI também pode introduzir riscos relacionados a:

- confiança em sistemas ou programas que estejam processando dados imprecisamente, processando dados incorretos ou ambas as coisas;
- acesso não autorizado a dados, que pode resultar em destruição ou modificações inadequadas de dados, incluindo o registro de transações não autorizadas ou inexistentes ou o registro incorreto de transações. Podem surgir riscos específicos quando múltiplos usuários têm acesso à base de dados comum;
- possibilidade de que os empregados de TI consigam acesso privilegiado além dos necessários para executar os deveres a eles atribuídos, rompendo assim a segregação de funções;
- modificações não autorizadas de dados nos arquivos-mestre;
- modificações não autorizadas de sistemas ou programas;
- falha na realização de modificações necessárias em sistemas ou programas;
- intervenção manual inadequada;
- perda potencial de dados ou incapacidade de acessar dados como exigido.

Na essência, quando nos debruçamos sobre os riscos que são gerados por controles de TI, observamos que, didaticamente, não diferem dos riscos gerados por controles fora de um ambiente de TI. Os riscos são genuinamente os mesmos, apenas são expostos de modo diferente. Em geral, em vez de uma pessoa, temos uma operação eletrônica.

Observe: para testar os controles de uma entidade sem ambiente PED, o auditor poderia desejar saber, por exemplo, quem tem a chave

do cofre onde é guardado o numerário para fazer os pagamentos, e assim conhecer os riscos de controle e a possibilidade de desfalques.

Por sua vez, em um ambiente PED, o auditor desejaria saber quem tem as senhas do sistema que executa os pagamentos. Perceba que, na essência, os fatos e critérios são similares, distinguem-se apenas em seu formato, afinal chave equivale à senha. Então, muda-se o cenário, não os fins.

O auditor, ao avaliar o controle interno da entidade, deve avaliar se o sistema mantém a integridade das informações e a segurança dos dados que processam, assim como incluem controles gerais de TI e controles efetivos sobre os aplicativos.

E é dessa forma que o COSO e a NBC TA 315, definem os dois grupos de controle em ambiente TI: controles gerais de TI e controles de processamento de informações (controle dos aplicativos).

Controles gerais

Estão representados pelas políticas e procedimentos que se relacionam com diversos aplicativos e sustentam o funcionamento efetivo dos controles do aplicativo.

NBC TA 315, 12, d

Controles gerais de tecnologia da informação (TI) são os controles sobre os processos de TI da entidade que suportam a operação adequada contínua do ambiente de TI, incluindo o funcionamento efetivo continuado dos controles de processamento de informações e a integridade das informações (ou seja, a integridade, a precisão e a validade das informações) no sistema de informações da entidade.

Controles de processamento de informações

São procedimentos manuais ou automatizados que geralmente operam em nível de processo de negócio e são utilizados no processamento de transações por aplicativos individuais.

NBC TA 315, 12, (e

Controles de processamento de informação são os controles relacionados com o processamento das informações em aplicativos de TI ou processos manuais de informações no sistema de informação da entidade que abordam diretamente os riscos à integridade das informações (ou seja, a integridade, a precisão e a validade das transações e outras informações).