AUDITORIA DE SISTEMAS

AULA 1

Prof. André Roberto Guerra

CONVERSA INICIAL

A auditoria e os sistemas estão em constante atualização em busca de melhores resultados, preocupando-se atualmente com os processos de negócio e com os sistemas de informação que os suportam, baseando-se numa abordagem ao risco. Como consequência dessa evolução, deve-se verificar também uma indissociável evolução no modelo de competências dos profissionais de auditoria, “além da identificação de atividades específicas de Auditoria de Sistemas de Informação prevista em três referenciais de Sistemas de Informação (CobiT, ITIL e ISO 17799/27002) e a utilização dos conceitos de Gestão de Projetos aplicados na Gestão das Auditorias de Sistemas de Informação”. (Silva, 2007).

Os conteúdos previstos para disciplina de Auditoria de Sistemas contemplam essas demandas citadas e serão ministrados em 6 (seis) aulas teóricas e 4 (quatro) práticas, e, em cada uma delas, os temas serão individualmente descritos/apresentados. O roteiro proposto contempla na aula inicial as definições e os conceitos básicos da auditoria de sistemas, seguido pelas diversas abordagens da auditoria de sistemas, planejamento e técnicas de auditoria de sistemas. Nos temas seguintes, ferramentas computacionais para auditoria, relatório de auditoria de sistemas, para no final apresentar aplicações e estudos de casos (boas práticas) de auditoria de sistemas de informações.

Objetivos de acordo com a taxonomia de Bloom revisada:

- Definições preliminares
- Objetivos específicos

TEMA 1 – DEFINIÇÕES DE AUDITORIA DE SISTEMAS

O tema inicial remete a definições e conceitos básicos da auditoria de sistemas, termos mais utilizados e importância em seguir as regras e normas, além da aderência à legislação. Serão apresentadas as diversas abordagens da auditoria de sistemas.

A primeira e elementar definição é a de auditoria: “Exame analítico, minucioso, de investigação e validação de um sistema, atividade ou informação” (Michaelis, 2017).

A palavra auditar é originária do latim *de auditu*, ou seja, saber por ouvir. Contudo, o processo de auditoria é muito mais do que ouvir, é um "retrato

técnico" da organização, dos sistemas como um todo. Atualmente, auditoria define-se como "um ramo de estudo das ciências de negócios, que avalia determinadas informações com o objetivo de trazer maior eficácia e eficiência, seguindo princípios e normas com aplicações próprias e direcionando a entidade a melhores resultados" (Oliveira, 2015).

Imoniana (2016) define o sistema como

> [...] um conjunto de elementos programados, inter-relacionados e interatuantes, que, quando processados, auxiliam na consecução dos objetivos dos negócios por meio de sistemas de informação; por exemplo, os sistemas de informações contábeis que orientam as transações econômicas e financeiras, produzindo relatórios que nortearão a tomada de decisões gerenciais. (Imoniana, 2016)

Neste percurso, pode-se identificar o processo que transforma dados de entrada, agregados aos comandos gerenciais, em saídas. Assim, o *feedback* do sistema faz com que, no meio da manutenção do ciclo operacional, sejam ativadas novas estratégias empresariais visando à geração de informações qualitativas ou quantitativas para suportar o alcance do sucesso absoluto.

Os sistemas são **abertos** ou **fechados**. Os sistemas **abertos** podem receber dados controlados e não controlados, uma vez que recebem influência do ambiente interno e externo onde operam. Os sistemas **fechados**, devido à sua natureza, não têm interferência do ambiente e somente poderiam receber os dados controlados.

As delimitações dos sistemas são feitas propositadamente durante seu desenho apenas para fomentar a segregação das funções dos sistemas incompatíveis agrupados nos sistemas de ERPs atuais. Podem ser tanto adaptáveis, quando implantados para produzir um resultado desejado em um ambiente de grandes mudanças rotineiras, como também corretivos, implantados para produzir um resultado específico e não rotineiro.

Stair e Reynolds (2017) afirmam que “os sistemas desempenham diversos papéis: coletam, processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, análises e o gerenciamento de organizações”. Porém, com o passar dos anos, os sistemas e os processos acabaram tornando-se mais complexos. Isso afetou diretamente os sistemas de informação e criou necessidades de verificações e adequações por conta de customizações às regras de negócio e à complexidade de alterações.

Imoniana (2016) descreve os conceitos de auditoria de sistemas de informação: “A auditoria em ambiente de tecnologia de informação (TI), ora

chamada de auditoria de sistemas de informação (SI), não muda a formação exigida para a profissão de auditor". Apenas percebe que as informações até então disponíveis em forma de papel são agora guardadas em forma eletrônica e que o enfoque de auditoria teria que mudar para se assegurar de que essas informações em forma eletrônica sejam confiáveis antes de emitir sua opinião.

Segundo Lyra (2015), "a função de auditoria de sistemas está ligada a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informação da empresa".

> A auditoria de sistemas impõe senso crítico dentro de um ambiente de sistemas de informação. Ela busca inovações, otimizações de processos empresariais, potenciais relações custo versus benefício, avaliação de riscos, maior eficiência, eficácia e segurança. É importante que uma organização possa ter um meio de medir se seus resultados estão coerentes ou se podem ser melhorados. (Lyra, 2015)

Segundo Gil (1999), "a eficácia dos resultados gerados e a eficiência dos processos concluídos necessitam ser validadas e avaliadas, e a auditoria de sistemas computadorizados pode ser o campo de ação para a certeza do alcance da qualidade de computação necessária". Em empresas onde a TI (Tecnologia da Informação) é considerada parte do mapa estratégico, é importante que seus sistemas de informação estejam bem alinhados com os processos da organização.

TEMA 2 – OS OBJETIVOS

As atividades de auditoria de tecnologia de informações, além de tentar utilizar os recursos de informática para auditar o próprio computador, também visam automatizar todos os processos de auditoria. Como em qualquer outra atividade, as empresas de auditoria também buscam um diferencial competitivo.

Entre outros objetivos, consideram-se:

- Melhorar a eficiência e reduzir os custos;
- Melhorar a qualidade do trabalho de auditoria, reduzindo, assim, os níveis de risco de auditoria;
- Atender às expectativas dos clientes, que esperam de seus auditores o mesmo grau de automatização que utilizam em seu próprio negócio;
- Preparar-se para a globalização dos negócios, que vem exigindo uma globalização dos auditores;
- Manter-se entre as maiores e mais reconhecidas pelo mercado;

- Criar valor agregado para seus clientes, ajudando-os a reduzir os riscos nos processos operacionais.

Os benefícios da automação que incluem também os processos de auditoria compreendem, entre outros:

- Treinamento de pessoal e superação de resistências à tecnologia;
- Melhoria na decisão de quais tarefas devem ser automatizadas em termos prioritários;
- Avaliação, escolha e implantação de *softwares* e *hardwares*;
- Gerenciamento dos recursos eletrônicos: dispositivos de segurança e *backup*;
- Disponibilização de equipamentos para toda a equipe de auditores, podendo trabalhar em redes;
- Instalação e manutenção de uma malha de comunicações;
- Maior transferência de conhecimento entre os membros da equipe e entre trabalhos de equipes diferentes;
- Independência das limitações impostas pelos arquivos de auditoria em papel;
- Produtividade e economia de tempo das atualizações;
- Melhor qualidade na apresentação;
- Liberação de funcionários mais experientes para que se dediquem a áreas mais técnicas e de maior risco;
- Agregação de valor ao trabalho de auditoria;
- Formação de equipes virtuais (*groupware*), maximizando a especialização;
- Fluxo de informações mais rápido;
- Maior satisfação profissional;
- Maior respeito pelo auditado;
- Maior produtividade;
- Conectividade com os parceiros de negócios;
- Realização das tarefas sem a automatização pelos profissionais menos experientes, que antes somente poderiam ser executadas por profissionais mais experientes.

Além dos objetivos listados, a auditoria dos sistemas aplicativos, segundo Imoniana (2016):

> Possui alguns objetivos globais que identificam os controles e avaliam os riscos de confidencialidade, integridade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenabilidade dos sistemas, permitindo ao auditor, a partir da auditoria, obter conclusões a respeito do sistema aplicativo e suas respectivas funções, se este atende às missões empresariais. (Imoniana, 2016)

Lyra (2015) destaca os objetivos globais da auditoria de sistemas de informação: “integridade, confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenabilidade”.

A seguir, são conceituados os objetivos globais, segundo Lyra (2015):

> **1) Integridade**: “dentro deste conceito, o auditor verifica se as transações são confiáveis ao serem processadas. Podem verificar se o sistema evidencia claramente a completa e correta exibição dos dados sem que os usuários tenham de se preocupar com a veracidade dos mesmos”.
> **2) Confidencialidade:** “Confidencialidade de um sistema consiste em existir mecanismos que barrem pessoas não autorizadas, a terem acesso a informações restritas, de forma acidental ou intencional. Para maior controle, devem existir procedimentos que autorizem o acesso. O auditor pode se basear em como a empresa se preocupa com a organização das informações dentro do sistema.
> Outra verificação que pode ser feita para medir a confidencialidade de um sistema ERP é através de questionários. Estes questionários devem ser bem elaborados pela equipe de TI, abrangendo as diversas formas de contornar possíveis informações falsas. Eles podem denunciar se os usuários estão com acessos indevidos a informações que não condizem às suas funções.
> No COBIT, são descritos, pelo objetivo PO2.3 - Esquema de Classificação de Dados, os detalhes sobre o grau de importância que a informação pode ter (pública, confidencial, altamente secreta). Essa diretriz pode ajudar a organização a manter um controle sobre seus dados e informações, criando mecanismos de controles de acesso a informações, arquivamentos e criptografias.”
> Já o item 12.4.3 Controle de acesso ao código-fonte do programa, da Norma ABNT (2005), frisa a importância restrita aos códigos fonte, evitando riscos de alterações não solicitadas.
> **3) Privacidade:** “o auditor deverá certificar-se de que os dados do sistema estão seguros por algum tipo de controle. Este controle visa a liberação de usuários a terem acesso a determinados programas, telas ou rotinas no sistema ERP, que realmente sejam necessários para exercer suas funções na empresa. Procedimento para acesso ao sistema é um exemplo de controle de privacidade”.
> O item 11.5.1 - Procedimentos Seguros para entrada no sistema da Norma ABNT (2005), foca mais precisamente o login no sistema. O auditor deve discutir a política de usuários do sistema ERP, se existe algum controle para as senhas e qual a periodicidade de trocas.
> **4) Acuidade:** “o sistema ERP deve possuir procedimentos internos de controle de entrada de dados, não permitindo a inserção de dados que invalidem as informações resultantes nos relatórios emitidos”.
> O item 12.2 que trata do Processamento Correto das Aplicações. Este item da Norma ABNT (2005) tem por objetivo garantir que não haja perdas, erros, modificações não autorizadas ou mal-uso de informações em aplicações. (Lyra, 2015)

Para isso, o sistema deve possuir, da mesma forma que existe no objetivo global de Integridade, alguns meios de validações, que são:

- Validações dos dados de entrada;
- Controle do processamento interno;
- Integridade de mensagens;
- Validação de dados de saída.

Estes meios de validação asseguram para o corpo de auditores que o processamento atual está falho ou condizendo ao que se propõe.

> **5) Disponibilidade:** "de alguma forma, o sistema deve estar online na maior parte do tempo para não comprometer transações. Na empresa deve existir algum modo em que seja medida a disponibilidade do sistema, para que usuários possam se precaver e para que a própria equipe de infraestrutura de TI possa ter documentado em um repositório em comum junto a analistas de sistemas e analistas de negócios".
> Dentro dos domínios do COBIT, existe um processo que trata sobre continuidade de serviços. Este processo chama-se Assegurar a continuidade dos serviços – DS4, o qual tem por objetivo assegurar que as informações estejam disponíveis para usuários e processos autorizados.
> O ITIL, também faz referência à disponibilidade dos serviços, neste caso disponibilidade do sistema, chamando o processo de Gerenciamento de Disponibilidade.
> **6) Auditabilidade:** "o auditor verifica a existência de registros referentes ao sistema. O custo pode ser elevado para o armazenamento de registros, dependendo o tamanho do sistema ERP a ser verificado, e também por causa do número de transações diárias. As trilhas de auditoria podem ser aplicadas neste contexto, também chamadas de *audit trails* por alguns autores".
> A auditabilidade de um sistema, segundo o COBIT, pode ser descrita pelo objetivo AI2 Adquirir e Manter software Aplicativo, e detalhado através do item AI2. 3 - Controle e Auditabilidade do aplicativo. Este item explica a importância em assegurar que os controles de negócio sejam expressos adequadamente nos controles dos aplicativos. Estes controles garantem que o processamento ocorra no prazo correto e seja exato, completo, autorizado e auditável.

O controle de aplicação e de auditabilidade é responsável por diversos mecanismos, e para um sistema ERP podem ser citados:

- Mecanismos de autorização;
- Integridade da informação;
- Controle de acessos ao sistema;
- Esquemas de rastreamento de auditorias.

No item A.15.1, que trata de conformidade com requisitos legais da ABNT (2005), "são destacados os objetivos de evitar violações no sistema que estejam relacionadas com crimes que afetem estatutos regulamentações ou obrigações".

Alguns dos subitens deste item que são aplicáveis a sistemas ERP em produção são:

- Proteção de dados e privacidade da informação pessoal, neste caso do sistema ERP e do usuário;
- Prevenção de mau uso de recursos de processamento da informação, em que os usuários devem estar conscientes de que o uso inadequado dos dados extraídos do sistema pode acarretar sérios problemas.

Como foi citada pelo COBIT e pela ABNT, a auditabilidade aborda diversos controles dentro de um sistema para poder ser considerada um objetivo alcançável em uma auditoria de sistema ERP. Para um sistema ser considerado auditável, existe certa complexidade devido ao alto nível de conhecimento que exigirá de auditores e sua experiência em poder adequar ferramentas para levantamento de evidências capazes de relacionar pontos de auditoria e serem tratados posteriormente.

> **7) Versatilidade**: "a versatilidade está ligada a usabilidade do sistema. Deve ser dada a atenção para disposição dos elementos que compõem o software. Através de questionários aplicados aos usuários podem ser levantadas possíveis melhorias. Além disso, deve ser feita uma análise se novos workflows operacionais de negócio da empresa podem ser adaptados ao software ERP".
> Outro importante ponto que LYRA (2015) "pondera é que deve ser observada se a sincronia de aplicativos independentes é fácil de ser feita com o sistema ERP".
> **8) Manutenabilidade:** "durante a manutenção dos sistemas é importante a existência de documentos que descrevam os passos de como proceder em atualização do sistema. Nestes documentos é importante que sejam destacados os responsáveis pelas atualizações, testes que devem ser feitos para certificar a atualização, análise de módulos impactados, formas de restauração de dados caso ocorra algo inesperado e meio de divulgação para as áreas interessadas".
> O COBIT trata dentro do domínio de Adquirir e Implementar, o objetivo AI 2.2 - Projeto Detalhado, que visa a prática de revisão de se sistemas estão tendo relevantes discrepâncias técnicas e lógicas. O objetivo apresenta ações que podem ser tomadas para que sejam verificadas falhas que ocorrem em momentos de atualizações de versões de módulos, troca de procedimentos etc.

Além disso, dentro do objetivo AI2 – Adquirir e Manter Software Aplicativo, no COBIT é encontrado um item que sugere às empresas estratégia e planos de manutenção do *software* aplicativo ou *software* ERP. Isso é importante, pois, no momento em que há atualizações de estrutura do *software* e de base de dados, a organização pode seguir um passo a passo de como efetuar as atualizações de forma mais organizada.

Outros itens deste mesmo objetivo seriam AI6 - Gerenciar Mudanças e AI7 – Instalar e Homologar Soluções e Mudanças, em que o primeiro visa controlar as alterações em ambiente de produção de sistemas aplicativos, de forma adequada e com um gerenciamento controlado. Já o segundo processo prevê um ambiente de homologação para testes e análise de impactos.

Na questão de manutenabilidade, no item 12.5.3 - Restrições em atualização de software da norma ABNT (2005), é explicado que mudanças em pacotes de *software* devem ser limitadas.

A partir dos objetivos citados, o auditor deve começar a montar o escopo e o planejamento da auditoria do sistema ERP, baseado nos objetivos da auditoria e observando critérios estabelecidos por ele e sua equipe no início dos trabalhos.

TEMA 3 – AS COMPETÊNCIAS DO AUDITOR

Para que uma organização, a qual deseja criar um programa de auditoria interna em sistemas, possa suprir os requisitos desejados em seus controles internos, é importante que ela conte com profissionais capacitados para a condução do programa. Esses profissionais farão parte da equipe de auditoria, que será organizada por gestores do programa de auditoria interna.

A composição da equipe deve ser feita por auditores selecionados e recrutados conforme conhecimentos e habilidades nas áreas de sistemas e de negócios. Um auditor, tendo o conhecimento do ambiente e de seus controles internos, pode ter um desempenho melhor em suas responsabilidades dentro de um programa de auditoria.

Estas são etapas básicas para a aplicação do programa de auditoria, que por consequência afetarão demais atividades do roteiro. O programa de auditoria precisa ter um planejamento adequado e com os objetivos definidos, assim o auditor pode executar seus trabalhos em controles específicos, agregando técnicas de auditoria para auxílio em suas análises e constatações.

A tabela a seguir apresenta o que compete ao auditor de sistemas de informações em termos de responsabilidades na equipe de auditoria e confronta com o *know-how* do perfil de desenvolvimento profissional que precisa conhecer, a fim de somar com contento.

Tabela 1 – Competência e perfis do auditor de sistemas

Tarefas do auditor de sistemas de informação	Conhecimentos de tecnologia e sistemas de informações	Conhecimentos de auditoria
Planejar a auditoria de sistemas documentando nível de risco aparente do ambiente.	Definir escopo de auditoria de sistemas e limitações para atender a ISAs, ITGC etc.	Definir escopo e apontamento de *engagement charter* para atender a ISAs e NBC-TAs.
Compreender os negócios, o setor, as unidades, os comitês, os executivos, a gerência, o organograma operacional e as partes interessadas, além do plano de valor agregado.	Conhecer a governança de TI como adicional de valor e também para definir riscos de controles internos, atentando para alinhamento com os objetivos dos negócios. Conhecer COBIT, COSO.	Conhecer a governança corporativa e definir o nível de riscos inerentes, controles e detecção de seu impacto nas demonstrações contábeis.
Compreender e certificar-se dos processos-chave e dos procedimentos operacionais para mitigar os riscos.	Conhecer os sistemas ERP e suas redes de operações e a relação de infraestruturas que suportam as atividades.	Conhecer as aplicações dos negócios e comparar sua função com padrões exigidos pelos organismos reguladores.
Compreender e certificar-se da integridade da comunicação de dados interinstituição e intrainstituição e certificar-se do controle.	Conhecer o ICT e redes; conectividades e seus funcionamentos. Deve-se incluir roteadores e *switches* de operabilidade de internet.	Conhecer os controles e como podem afetar os testes substantivos de auditoria, tomando como base os conceitos de riscos e materialidade.
Compreender e certificar-se da classificação de informações, de pessoas, dados conforme aplicações essenciais para negócios.	Conhecer a estrutura de dados da empresa, os bancos de dados em uso como *Big Data* e sua manutenção.	Compreender os procedimentos de controles internos referentes ao funcionamento e às operações, tomando como base as assertivas de controles internos.
Verificar a proteção de dados, informações, pessoas e ativos em geral em TI e certificar-se do controle, de SLAs, da disponibilidade e das políticas.	Conhecer a segurança de informações físicas, lógicas e os requisitos de implementação de políticas de segurança de informações e monitoramento.	Compreender os princípios e as práticas contábeis, os processos de *compliance das regulamentações* de auditoria, além de atenuar os riscos de certificação das contas constantes no *Lead schedule.*
Compreender e verificar o suporte para usuários, para atender às funções críticas aos negócios.	Conhecer a operação do computador, o planejamento de capacidade e processamentos, a manutenção de sistemas operacionais e utilitários.	Obter conhecimento de geração de relatórios para comparação com dados originais, a fim de testar a integridade dos cálculos e confirmação de saldos, além de outros procedimentos substantivos.
Verificar a consistência e a confiabilidade da evolução de sistemas aplicativos em pró-tendências dos negócios e seus funcionamentos.	Conhecer o processo de aquisição, desenvolvimento, manutenção e documentação de sistemas; em suma, o *SDLC– Systems Development Life Cycle.* Saber como rodar CAAT e *Data Analytics.*	Obter a confiabilidade das transações processadas em relação às contas contábeis ou aos grupos de contas com ajuda de testes substantivos e procedimentos analíticos, tendo como base as assertivas de integridade (correto e completo), validade, classificação, direito e obrigação*, cut-off,* existência, valorização e *disclosure.*
Certificar-se da continuidade em caso de contingências nas operações gerais dos negócios.	Conhecer os processos de elaboração de implementação de *Business Continuity Planning* e também de *Disaster Recovery Planning.*	Conhecer o processo de garantia dos funcionamentos essenciais das operações econômicas, financeiras e contábeis em casos de interrupções parciais e prolongadas de TI, a fim de cumprir necessidades de regulamentos, *compliance*, entre outros.
Certificar-se dos contratos de disponibilidades de operações com *outsourcing* e *cloud computing.*	Conhecer o processo de elaboração de contratos de serviços de TI, SLAs e o monitoramento.	

Fonte: Adaptado de Imoniana, 2015.

TEMA 4 – ROTEIRO E PLANEJAMENTO PARA ELABORAÇÃO

Para montar um roteiro de auditoria interna de sistemas, deve ser destacado o uso de referências consolidadas como normas e guias aplicáveis a sistemas de gestão. Silva (2007) cita o CobiT (*Control Objectives for Information and related Technology*) como “ponto de partida para a identificação das atividades de Auditoria de Sistemas de Informação”. Aborda também referenciais ITIL (*Information Technology Infrastructure Library*) e ISO 17799/27002 para a identificação de atividades, uma vez que estes referenciais são mais específicos em alguns aspectos ligados a sistemas de gestão. A norma ABNT 19011 - Diretrizes para auditoria de gestão de sistemas - também é um referencial para a condução de auditoria.

Dutra (2017) apresenta

> o processo de organização dos trabalhos de auditoria de sistemas de informações segue a norma de execução de trabalhos do auditor, o principal componente das normas de auditoria geralmente aceitas. Vale recapitular que essa norma contempla: planejamento de auditoria, avaliação de riscos de auditoria, supervisão e controle de qualidade. (Dutra, 2017)

Outros são: estudo e avaliação do sistema contábil e de controles internos e aplicação dos procedimentos de auditoria, documentação da auditoria, avaliação da continuidade normal dos negócios da entidade, aplicação de amostragem estatística etc.

Para simplificar, adotam-se as seguintes estruturas didáticas: planejamento; escolha da equipe, programação da equipe; execução e documentação de trabalho; supervisão em campo; revisão dos papéis de trabalho, conclusão e emissão (*follow-up*) de relatórios; atualização do conhecimento permanente e avaliação da equipe (Dutra, 2017).

Ressalta-se que o mesmo processo efetuado convencionalmente se adapta à auditoria de tecnologia de informações. A única diferença é que cada uma dessas etapas pode ser automatizada por meio de ferramentas de produtividade para o controle dos trabalhos do auditor.

4.1 Planejamento

A atividade de planejamento em auditoria de sistemas de informações é apoiada em níveis de riscos aparentes, e essa ação é imprescindível para melhor

orientar o desenvolvimento dos trabalhos. Como o trabalho de auditoria global representa um processo contínuo de avaliação de risco ao qual se adicionam as experiências individuais dos profissionais e a evolução da prática e metodologias, esses são aliados aos resultados dos trabalhos e processos de negócios anteriores, objetos de avaliação dos auditores.

"O planejamento é caracterizado para evitar quaisquer surpresas que possam acontecer tanto nas atividades empresariais, objetivo de auditoria, como também na relação auditor-cliente, definindo as responsabilidades dos auditores" (Dutra, 2017). Desde os primeiros trabalhos deve ser desenhada uma "matriz de risco" que seja permanentemente atualizada a partir dos resultados obtidos nos testes e nas avaliações dos auditores.

Dutra (2017) cita que, assim,

> devem-se contemplar os impactos das mudanças ocorridas nos negócios resultantes de alterações de estratégias empresariais, evoluções tecnológicas, concorrência, mudanças estatutárias, sociais e econômicas, mudanças nas legislações, nas leis ambientais, ou em qualquer outro fator que tenha reflexo nas demonstrações financeiras, além da continuidade operacional, qualidade dos controles e, sobretudo, nos processos operacionais. (Dutra, 2017)

A título de exemplo, é apresentado a seguir um memorando de planejamento de auditoria de sistemas:

(Nome do cliente)

MEMORANDO DE PLANEJAMENTO DE AUDITORIA DE SISTEMAS DE INFORMAÇÕES

Introdução

Este memorando descreve os objetivos, o escopo (abrangências) dos procedimentos a serem avaliados e as abordagens que devem ser adotadas pela equipe de auditoria de sistemas de informações como suporte aos trabalhos de auditoria das demonstrações financeiras do (nome do cliente) para o ano findo em 31 de dezembro de 2015.

Conforme o memorando de planejamento de auditoria geral para o cliente, a extensão do uso de informática pelo (nome do cliente) foi classificada como (classificação que pode ser significante, moderada ou pequena). A equipe de auditoria das demonstrações financeiras adotou a estratégia de confiança nos controles internos de todos os sistemas de informações computadorizados, exceto o sistema (nome do sistema), descrito nas seções de riscos específicos identificados (documentar uma seção para riscos identificados quando for necessário).

Escopo

Conforme acordado na reunião de planejamento, o escopo do trabalho de auditoria de sistemas obedecerá ao seguinte:

Entendimento global e atualização das seguintes informações: (1) processo e *workflow* das transações contábeis; (2) ambiente de sistemas de informações; e (3) estrutura de controles computadorizados:

•identificar e atualizar a compreensão dos controles de sistemas aplicativos e os controles gerais do computador;

•programar testes nos controles que minimizam os riscos identificados para o sistema aplicativo de (nome do sistema);

•utilizar de ferramenta ACL (*Audit Command Language*) para extração de dados do sistema de (nome do sistema) para análises substantivas.

Administração de considerações especiais

Data para realização dos trabalhos; formalização do nº do serviço para controle de horas; endereço da empresa e pessoa-chave para contato; data limite para entregas do relatório final; formato do relatório (padrão específico); destinatário do relatório final e comentários da gerência.

Estimativa de horas

De acordo com o tempo de execução das tarefas e os profissionais envolvidos, estimamos o trabalho em **9.999** horas.

De acordo:

Gerente de Auditoria de Sistemas

Gerente de Auditoria Financeira

Sócio Responsável

TEMA 5 – PROCEDIMENTOS: ETAPAS DA AUDITORIA

Os procedimentos de auditoria de sistemas devem ser entendidos como um conjunto de etapas e atividades bem distribuídas, que são planejadas, executadas e avaliadas por diversas partes interessadas, ocorrendo antes, durante e depois de uma auditoria. Imoniana (2016) explica que “os procedimentos de auditoria de sistemas aplicativos referem-se àqueles executados para averiguar se os sistemas que constituem o cerne do negócio de uma empresa estão acontecendo de forma adequada, executando suas atividades rotineiras adequadamente”.

A organização dos procedimentos de auditoria deve estar de forma que os trabalhos sejam feitos adequadamente dentro do processo de auditoria. Lyra (2015) afirma que “é possível pensar em aplicar uma metodologia de trabalho que seja flexível e aderente a todas as modalidades da auditoria em sistemas de informação e que não se distancie de melhores práticas”.

A metodologia pode ser composta pelas seguintes etapas:

a. Planejamento e controle do projeto de auditoria de sistemas;
b. Levantamento do sistema de informação a ser auditado;
c. Identificação e inventário dos pontos de controle;
d. Priorização e seleção dos pontos de controle do sistema auditado;
e. Avaliação dos pontos de controle;
f. Conclusão da auditoria;
g. Acompanhamento da auditoria.

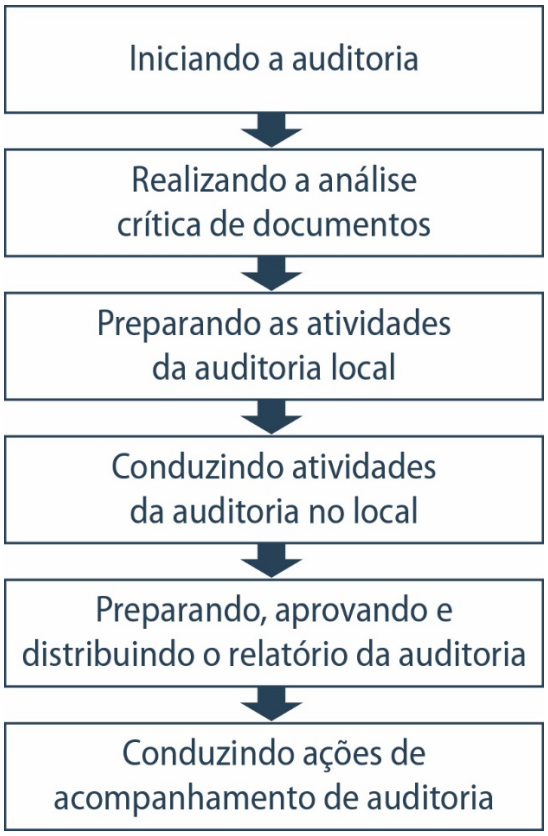
O desenvolvimento de um roteiro para a auditoria de sistemas pode estar baseado na “organização sugerida, onde os procedimentos ficam bem distribuídos no roteiro, assim com as atividades de revisões e avaliações dos processos e rotinas de auditoria” (Lyra, 2015).

Os procedimentos de auditoria devem contemplar a avaliação de:

- Dados e informações, que compõe os resultados do sistema, e
- Rotinas de processos do sistema.

A norma da ABNT (2002) considera que os procedimentos de auditoria dentro de um programa a ser aplicado podem ser baseados conforme apresentado na figura a seguir:

Figura 1 – Procedimentos de auditoria



Fonte: Adaptado de ABNT, 2002.

Essas etapas e atividades são aplicáveis a auditorias de sistemas e sua abrangência, na qual esses procedimentos podem ser aplicados, depende do escopo, da complexidade da auditoria específica e do uso para as conclusões de auditoria.

Estas etapas são resultado de variadas fontes pesquisa a respeito de auditorias e normas e procedimentos que se aplicam a sistemas de informação. A partir destas etapas, haverá conclusões e definições para uma posterior aplicação em um programa de auditoria.

FINALIZANDO

Na aula inicial, foram apresentadas as definições e conceitos básicos da auditoria de sistemas. Para um sistema em produção, podem ser realizadas auditorias internas com diferentes objetivos, tais como: integridade, manutenabilidade, auditabilidade, disponibilidade, integridade, confidencialidade, privacidade, acuidade e versatilidade.

As técnicas de auditoria contribuem para o levantamento de evidências. Sua escolha e sua execução podem ser programadas de acordo com os pontos de auditoria a serem selecionados para a posterior aplicação da técnica compatível. As técnicas também podem ser pré-selecionadas de acordo com os objetivos que a auditoria se propõe a atingir.

A capacitação de profissionais é importante para que sejam conduzidos os trabalhos que envolvem a criação de um programa de auditoria. Por meio de pré-requisitos estabelecidos por uma comissão interna, o desenvolvimento de uma equipe de auditoria acaba por selecionar os profissionais mais capacitados a exercerem a condução e a delegação de atividades que compõem uma auditoria interna, registrando e extraindo resultados ao fim dos trabalhos.

Apesar de autores considerarem diferentes etapas de auditoria, elas podem ser resumidas em planejamento de auditoria, execução de procedimentos de auditoria e conclusões de auditoria. Com base nestas etapas citadas, o roteiro de auditoria começa a ser formado. Além disso, apresenta também as atividades e os produtos gerados que podem ser os artefatos de saída e entrada, onde ficam registradas informações e dados relevantes de uma auditoria interna.

REFERÊNCIAS

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 17799: **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 132p.

_____. NBR 27002: **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 140p.

_____. NBR ISO 19011. **Diretrizes para auditoria de gestão da qualidade e/ou ambiental**. Rio de Janeiro: ABNT, 2002. 25p.

_____. NBR ISO 27005: **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2006. 65p.

ATTIE, W. **Auditoria conceitos e aplicações**. São Paulo: Atlas, 2010.

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: 1 dez. 2017.

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

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: 1 dez. 2017.

IT SERVICE MANAGEMENT FORUM. **An Introductory Overview of ITIL**. Version 1.0.a itSMF: United Kingdom, 2004.

LYRA, M. R., **Governança da Segurança da Informação.** Edição do Autor – Brasília, 2015.

MICHAELIS. **Dicionário *on-line***. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 1 dez. 2017.

SILVA, P. M. G. **A função auditoria de sistemas de informação**: modelo funcional e de competências. Braga: Escola de Engenharia – Universidade do Minho, 2007

STAIR, R. M.; REYNOLDS, G. W. **Princípios de sistemas de informação**. São Paulo: Cengage Learning, 2015.