AUDITORIA DE SISTEMAS

AULA 3

Prof. André Roberto Guerra

CONVERSA INICIAL

Nesta aula, serão apresentados e definidos os processos de planejamento de auditoria e pontos de controle, uma parte importante da gestão das auditorias de SI.

A primeira atividade é identificar um modelo, um conjunto de orientações para a definição de um planejamento das auditorias de SI. Serão apresentadas algumas visões sobre as fases que constituem uma auditoria de SI.

Os principais fatores a considerar na elaboração de um planejamento para as auditorias de SI estão contidos no seguinte comentário da Isaca (2005):

> For an internal audit function, a plan should be developed/updated, at least annually, for ongoing activities. The plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter. The new/updated plan should be approved by the Audit Committee…

Em tradução-livre, “Para uma função de auditoria interna, um plano deve ser desenvolvido/atualizado, pelo menos anualmente, para atividades em andamento. O plano deve servir de ‘*framework*’ (biblioteca de classes que suportam uma funcionalidade) para as atividades de auditoria e servir para abordar as responsabilidades definidas pela equipe de auditoria. O plano novo/atualizado deve ser aprovado pelo comitê de Auditoria”.

Essa passagem consta nos IS Standards, Guidelines and Procedures for Auditing and Control Professionals, nos quais existe uma norma (*standard*) relativa ao planeamento (*S5 – planning*).

Nela é definida a obrigatoriedade de um plano de auditoria de SI que cubra os objetivos da função e que esteja em conformidade com os regulamentos aplicáveis, incluindo os constantes das normas profissionais do auditor e da carta de auditoria. O plano deverá sintetizar a natureza, os objetivos, os recursos e o período relativos a cada auditoria, devendo ser aprovado pelo comitê de auditoria da organização. O plano da auditoria de SI deverá ser documentado e construído utilizando uma abordagem ao risco.

Para início das atividades de análise dentro do ambiente a ser auditado, é importante que o auditor de sistemas tenha pleno conhecimento do que se tratam os **pontos de controle**. Estes serão os principais meios de obtenção de evidências durante todo o processo de auditoria.

Ponto de controle é “a situação do ambiente computacional caracterizada pelo auditor como de interesse para validação e avaliação. Um ponto de controle

também pode ser caracterizado como uma combinação de rotinas e informações operacionais de controle" (Gil, 99).

TEMA 1 – O PLANEJAMENTO DE AUDITORIA DE SISTEMAS

Para o planejamento de uma auditoria de sistemas, a principal atividade de início é conhecer o ambiente a ser auditado. Trata-se de entender a estrutura de *hardware*, *software*, área de programação e análise, se há operações de TI, estrutura da TI e produtos obtidos através do sistema.

Para que o planejamento de auditoria ocorra de forma mais organizada, o auditor deve ter o entendimento de como proceder nas atividades de análise e considerações no ambiente que está auditando. Além disso, ele necessita fazer o registro das informações geradas nestas atividades, para que o programa de auditoria de sistemas possa ser dinâmico e contribua em futuras tarefas.

Como se percebe, o planejamento das auditorias de SI não serve apenas para indicar "o que" se vai auditar, mas é também um instrumento para determinar "quando" e com que "frequência" se deve auditar. Surge então um novo questionamento: o "por que" auditar?

A resposta está no risco. Na elaboração do planejamento devem se escolher para serem auditados os processos e os SI que maior risco trazem ou poderão vir a trazer para o negócio em determinado período.

No período de avaliação do sistema a ser auditado, existem alguns detalhes que o auditor deve observar. Para a compreensão do sistema a ser auditado, a documentação inicial de como está estruturado o ambiente do sistema deve seguir alguns pontos. Imoniana (2015) elenca os seguintes:

"a) identificação dos sistemas-chaves, neste caso o sistema ERP;
b) descrição do sistema;
c) descrição do perfil do sistema;
d) documentação da visão geral do processamento;
e) descrição de riscos dos sistemas aplicativos."

Após estar esclarecido sobre a estrutura inicial do ambiente a ser auditado, o auditor exerce a atividade de análise de riscos. Segundo Imoniana (2015), "sob o ponto de vista de auditoria de sistemas, trata-se de uma metodologia adotada por auditores de TI para saber, com antecedência, quais as ameaças puras ou prováveis existentes em um ambiente de TI de uma

organização". Esta análise de risco é efetuada por meio de investigações nos controles internos, quando se poderão identificar as possíveis fraquezas e seu correto cumprimento.

A ABNT (2006) que trata especificamente de gestão de riscos de segurança da informação apresenta uma série de atividades que fazem parte desta metodologia de análise de riscos. As etapas do roteiro proposto neste trabalho possuem atividades baseadas na ABNT de gestão de riscos. "Porém o roteiro não segue fielmente a metodologia, apenas procura adaptá-la a realidade de algumas de suas atividades" (ABNT, 2006).

Como elaborar, então, um planeamento de auditoria de SI que tenha em conta o negócio e os seus riscos? Essa abordagem ao risco é o instrumento-chave através do qual todo o plano deve ser desenvolvido.

O IIA (2006) tece um conjunto de considerações sobre o modo como as auditorias de SI devem ser definidas que são relevantes quando da elaboração do planeamento: "*The way in which IT audits are defined plays a large role in the overall effectiveness of the IT audit function*. (…) *Audit committee wants IT audit findings to be tied to the business issues*". Em tradução-livre, "A forma como as auditorias de TI são definidas desempenha um papel importante na eficácia global da função de auditoria de TI. (...) O comitê de auditoria quer que os resultados das auditorias de TI estejam ligados às questões de negócios"

Segundo essa perspectiva, o desafio está em encontrar o nível correto de granularidade da definição das auditorias de SI. Neste contexto, o IIA fornece algumas orientações a considerar, resumidas a seguir:

- Evitar o uso de definições/designações de Auditorias de SI muito abrangentes – É comum existir nos planejamentos da Auditoria de SI as chamadas "Auditorias de Controles Gerais". Estas podem tornar-se relativamente inúteis, sobretudo em grandes organizações, dado que, ou não cobrem todo o universo dos SI, ou para fazê-lo, tornam-se intermináveis no tempo. Por outro lado, há que ter muito cuidado na designação que se atribui às Auditorias pois podem induzir em erro a Gestão de Topo e a Gestão dos SI quanto à verdadeira abrangência do plano de Auditorias.
- O planejamento deve tocar todos os níveis de SI - O planejamento deve considerar a cada ano, pelo menos uma Auditoria em cada um dos níveis de controle dos SI: Governo, Gestão, Técnico. Caso não ocorra, existe sempre o risco de a organização considerar o planejamento omisso ou incompleto como um todo.
- O planejamento deve prever Auditorias que formem conjuntos lógicos de relatórios sobre determinados temas - As Auditorias devem ser planejadas de modo a fornecer um reporte eficaz e lógico dos resultados. Para ilustração, as Auditorias aplicacionais raramente são eficazes se forem divididas em Auditorias independentes (exemplo: auditar todos os módulos de SAP e não apenas o módulo financeiro). De modo semelhante, as Auditorias às tecnologias da rede

corporativa tendem a ser mais eficazes quando efetuadas ao nível de toda a organização (exemplo: não auditar a segurança da rede em uma só localização/instalação).

- O planejamento e respectivo orçamento devem cobrir os riscos de forma apropriada – O planejamento das Auditorias e o orçamento do departamento devem ser um resultado do processo de avaliação de riscos de SI, não devendo ser definidos antes de se proceder a essa avaliação. Esta deve ser efetuada no contexto da avaliação de riscos feita para toda a organização. Ao contrário do que acontece com outros tipos de Auditoria Interna com histórico mais longo nas organizações (exemplos: Auditoria Financeira, Auditoria de Qualidade, etc.), a estimativa de um orçamento para Auditoria de SI pode ser induzida em erro caso utilize técnicas de comparação com outras Auditorias ou se guie por ordens de grandeza. O orçamento da Auditoria de SI deve ser estimado em função da avaliação dos riscos de SI, deve possuir um processo de pré-planejamento robusto e deve contar com os contributos da Gestão dos SI (IIA, 2006)

TEMA 2 – OS DETALHES DO PLANEJAMENTO

A razão deste planejamento inicial é o direcionamento e a coordenação para a execução da auditoria. Este planejamento agrega todos os processos de auditoria elencados:

a. Conhecimento do ambiente.
b. Estabelecimento de estratégias.
c. Aplicação de técnicas.
d. Análise de etapas executadas.
e. Relatórios finais.

“Estes procedimentos serão evidenciados em documentos, principalmente no plano de auditoria. Neste plano que podem ser retratadas as áreas de risco e pontos de controle, prioridade de execução, tarefas, tempos de execução, equipe de auditoria e recursos metodológicos” (GIL, 99).

A norma da ABNT (2002) considera que “para o início dos trabalhos é importante o desenvolvimento de um plano de auditoria que contemple o maior número de detalhes possíveis”. A flexibilidade deve ser considerada, de modo que, conforme evoluam as atividades de auditoria, o plano possa sofrer modificações. A seguir, são elencados alguns itens considerados pela norma:

- Objetivos da auditoria.
- Escopo da auditoria.
- Datas e lugares onde as atividades de auditoria serão realizadas.
- Definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas.

- Principais pontos do relatório de auditoria.
- Quaisquer ações de acompanhamento de auditoria.

"Este plano deve passar por um fluxo de aprovação interno, para que seja validado junto aos principais envolvidos na auditoria. Suas revisões devem ser acordadas entre todas as partes, para o andamento do processo" (Brandalize, 2012).

A primeira atividade é interpretar esse modelo, definindo que o risco (*Recognition and Appreciation of Business Risks*) é o elo entre o lado do negócio e o lado da auditoria. No lado do negócio, constata-se que os objetivos de negócio determinam o plano estratégico (*Strategic Planning Process*), que, por sua vez, determina o plano anual de negócios (*Annual Business Plan*), o qual tem impacto nos processos e nas áreas de negócio (*Process or Work Unit Objectives*). Uma vez que a auditoria de SI deverá estar alinhada com as necessidades do negócio, então do lado da auditoria o planeamento deverá seguir um raciocínio semelhante. No lado da auditoria, partindo do universo da auditoria (*Audit Universe Process*), deverá ser elaborado um plano anual de auditorias (*Annual Audit Plan*) que determinará o âmbito de cada auditoria individual (*Individual Audit Scope*) e terá impacto no modo como as áreas de negócio avaliam e gerem os seus riscos (*Evaluate How Business Risks are Managed*).

O sucesso de um modelo de planeamento desse tipo passa pela necessária comunicação entre os dois lados. Assim, na prática, para a determinação do seu universo de atuação, a auditoria de SI deverá conhecer o plano estratégico dos SI. De igual modo, para a elaboração do planeamento anual, a auditoria de SI deverá conhecer o plano operacional do SI para esse mesmo ano. Ao contrário de outras abordagens mais tradicionais, em que os auditores de SI utilizavam os planos de SI para validar os planejamentos da auditoria de SI, este modelo defende que os planos dos processos de negócio, neste caso os planos dos SI, deverão ser determinantes ativos na elaboração do planejamento da auditoria.

Os riscos de negócio mais relevantes ao nível dos SI deverão ser os determinantes do âmbito anual da auditoria de SI. O modelo admite que as organizações usem cenários de risco na avaliação de risco anual, pois são mais apropriadas para setores de negócio em consolidação ou com ritmo de mudança elevado.

O modelo vai ainda mais longe quando afirma que as metodologias de avaliação de risco a utilizar (fatores de risco, modelos de risco etc.) podem ser derivadas diretamente da especificidade de cada processo de negócio (*Industry-Specific Scenarios Approaches Models*) em vez de serem determinadas unicamente pelos processos de auditoria. Ao nível das auditorias individuais, mais uma vez serão os riscos do processo ou do SI em causa que determinarão o planejamento dessa auditoria, incluindo quais são os testes a efetuar e o tipo de relatório mais adequado para emitir.

Esse modelo prevê dois órgãos de governo da organização (a Gestão de Topo e o Comité de Auditoria) que têm como responsabilidades contribuir para a elaboração e dar aprovação ao universo da auditoria e ao seu planeamento anual. É, no entanto, da responsabilidade do departamento de auditoria da organização transmitir a esses órgãos de governo cultura e percepção de risco, alinhadas com as restantes áreas da organização, e informá-los sobre as exposições aos riscos da organização.

Além da abordagem ao risco, é de grande destaque a relação com o negócio nas atividades de planejamento. Apenas uma nota para deixar claro que essa relação não é uma novidade nem uma necessidade exclusiva da auditoria de SI. Existem outras atividades de planejamento no domínio dos SI em que essa necessidade também é reconhecida.

> A atividade de planeamento de SI é desencadeada como parte integrante da atividade de planejamento estratégico da organização. (…) O planeamento de SI deverá estar integrado e alinhado com o planeamento do negócio, sendo extremamente importante ter a noção de que o mesmo é uma forma de planeamento da mudança organizacional… (Silva, 2007)

A função de auditoria de SI deve reportar ao responsável do departamento de Auditoria e Gestão de Risco. Por sua vez, este deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao responsável máximo da organização, que é o CEO (*Chief Executive Officer*). Note-se que o modelo de reporte aqui defendido difere ligeiramente face à maior parte das organizações em que a Auditoria e Gestão de Risco reporta ao CFO (*Chief Financial Officer*) ou, nalguns casos, diretamente ao CEO.

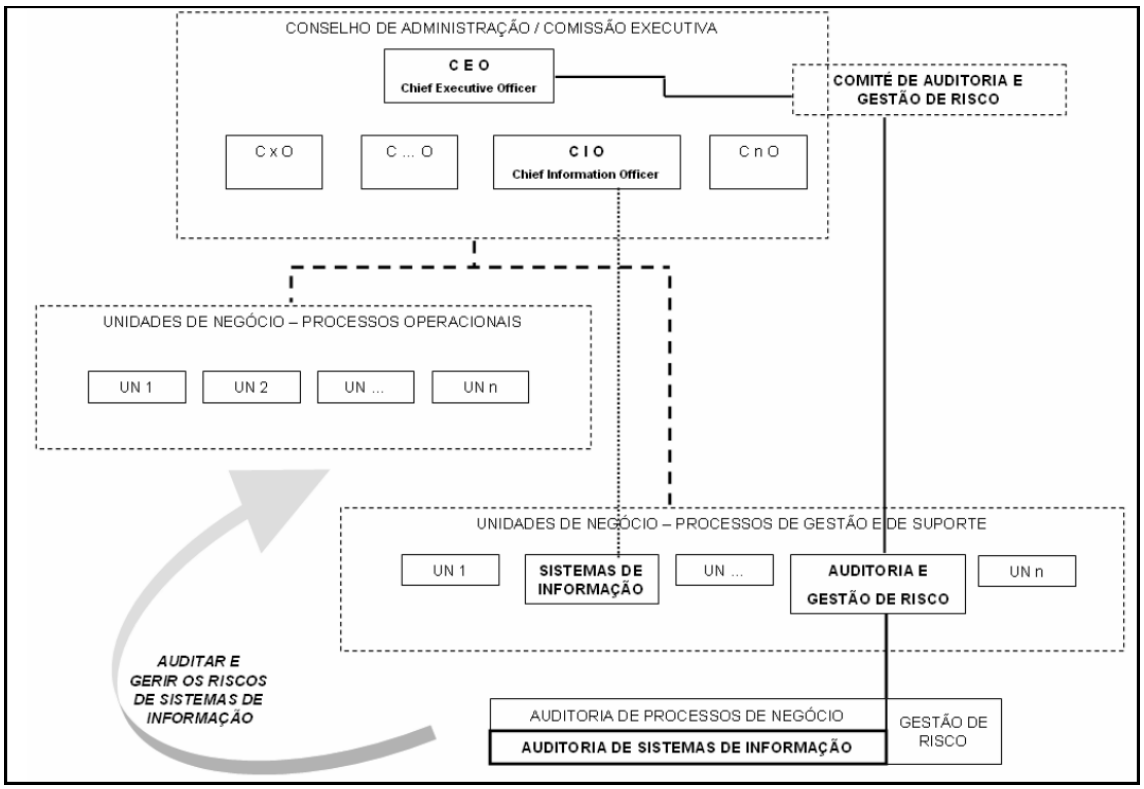
No sentido de garantir maior coerência com a abrangência das funções de Auditoria e Gestão de Risco, defende-se um reporte ao CEO, e não ao CIO.

> No sentido de garantir um maior grau de independência, defende-se que o reporte ao CEO seja no âmbito das suas

> responsabilidades de supervisão no Comité de Auditoria e Gestão de Risco e não diretamente no âmbito das suas funções executivas na Gestão de Topo da organização (Conselho de Administração / Comissão Executiva). Para além disso, o referido Comité pode ser entendido como uma última instância à qual o departamento de Auditoria e Gestão de Risco pode recorrer, em eventuais situações em que os gestores da organização não se mostram disponíveis para colaborar. (Silva, 2007)

Diferentemente, os responsáveis pelo departamento de SI deverão reportar diretamente à gestão de topo da organização, nomeadamente ao CIO (*Chief Information Officer*). Este papel (CIO) justifica-se com o fato de existir um processo de negócio responsável pela gestão dos recursos associados à informação, incluindo os SI e as TIC.

Figura 1 – Posicionamento e organização da função



Fonte: Silva, 2007.

TEMA 3 – A CRIAÇÃO DO PLANO DE AUDITORIA

No processo de criação de um programa de auditoria, é importante que os auditores conheçam o ambiente de ERP em que vão trabalhar. O escopo de uma auditoria pode ser delimitado através do conhecimento que se tem do ambiente de sistema a ser auditado. O conhecimento a ser adquirido pode ser através da compreensão do fluxo do sistema. A compreensão do fluxo aborda uma série de questões que Imoniana (2005) destaca.

Essas questões poderiam estar formatadas em um modelo, visando detalhamento do escopo de auditoria, e podem auxiliar na tomada de decisões futuras durante o andamento dos procedimentos de auditoria. As informações geradas a partir da análise dessas questões devem ser anexadas junto ao plano de auditoria. As técnicas que Imoniana (2005) cita “seriam por meio de visitas ou entrevistas junto a gestores ou analistas das áreas”. Na figura 2 é apresentado o modelo que contempla importantes questões, as quais podem ser discutidas internamente e que complementam demais artefatos utilizados no programa de auditoria.

Figura 2 – Questionário conhecimento de ambiente

	Questões	S/N	Documentos/Artefatos Referência
1	Há padrões de documentação para programas de sistema ERP que estão configurados para executar em modo *batch* ?		
2	Está sendo usado o padrão de documentação ?		
3	Há softwares de apoio à documentação do sistema ERP a ser auditado ?		
4	Existe trilha de auditoria do sistema ERP? (*logs*)		
5	Existem arquivos/relatórios/registros de controle no sistema ?		
6	As alterações de programas dos módulos do ERP, são controladas e registradas ?		
7	Existe grau de sigilo de arquivos e programas consoantes norma estabelecida ?		
8	Existe documentação referente ao sistema ERP, quanto a processos, manuntenções no sistema ?		
9	Existem procedimentos documentados descrevendo como os relatórios de saída são gerados e entregues aos usuários ? (acessos)		
10	Há monitoração via arquivos de *logs* enquanto ocorrem ciclos de processamento no sistema ?		
11	Há documentação de quem dá manutenção e suporte nas operações e funcionalidades do sistema ERP ?		

Fonte: Brandalise, 2012

Os resultados dessas atividades servirão como base para a montagem do plano de auditoria, o relacionamento e o início da análise dos pontos de controle.

3.1 Criação do plano de auditoria

A partir das definições feitas nesta fase de iniciação e planejamento de auditoria, é possível iniciar a elaboração do plano de auditoria. O plano de auditoria é um artefato elaborado durante toda a auditoria e deve ser preenchido conforme o roteiro determina, sendo geralmente no fim de cada uma das fases.

Seu principal objetivo é agregar informações e dados a respeito do programa de auditoria, de forma que seja simples de ser utilizado dentro de um

programa de auditoria e para consultas de gestores interessados nas informações contidas. O plano de auditoria é composto basicamente pelos tópicos que aparecem na figura 3.

Figura 3 – Tópicos básicos de um plano de auditoria

Tópicos
Objetivos da auditoria;
Critérios de auditoria e qualquer documento de referência;
O escopo da auditoria;
Definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas;
Pareceres do ambiente de sistema a ser verificado.
Os principais pontos do relatório de auditoria;
Quaisquer ações de acompanhamento de auditoria.

Fonte: ABNT, 2002.

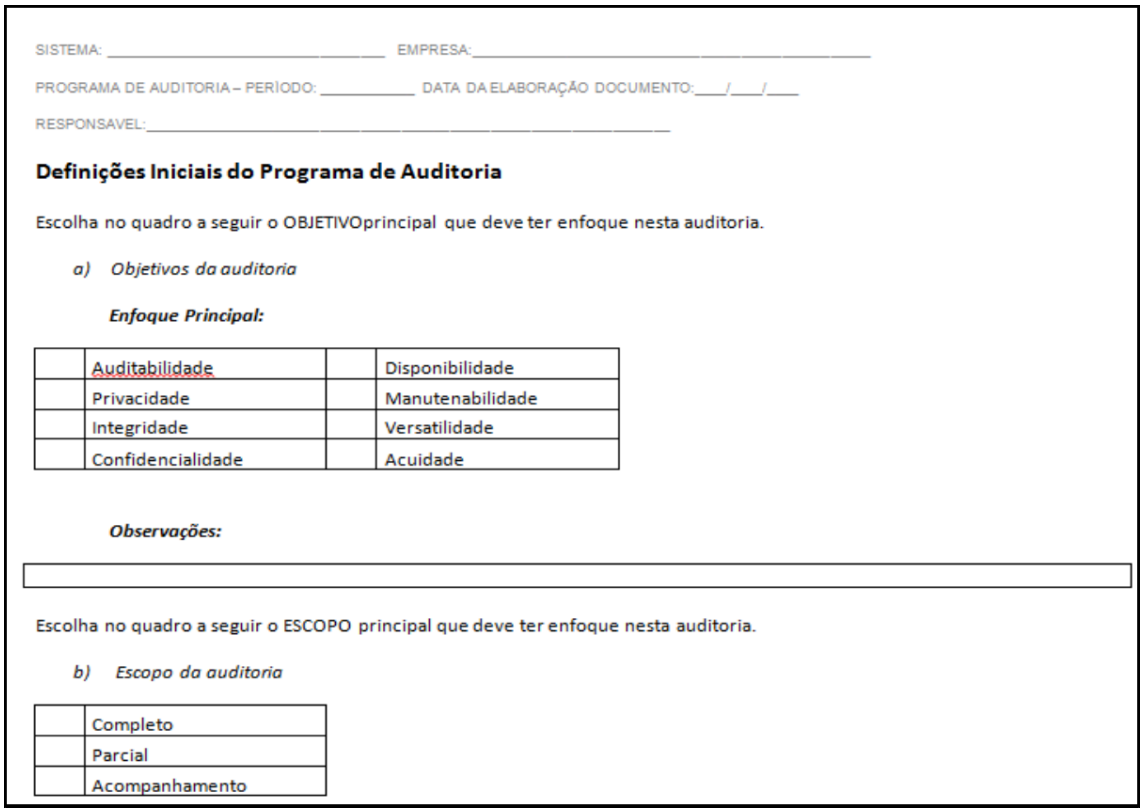
Planos de auditoria são flexíveis, sendo modificados durante o processo de auditoria. Essas modificações podem ser a agregação de mais detalhes nos tópicos ou mudanças nos existentes. Imoniana (2005) destaca que “a auditoria é um processo contínuo de avaliações de risco ao qual se adicionam experiências individuais dos profissionais e a evolução da prática e metodologias, com isso são inevitáveis que algumas mudanças mínimas acabem influenciando em pequenos ajustes no plano de auditoria”.

O plano de auditoria também é importante no processo de comunicação interna durante um programa de auditoria, pois elenca diversos tópicos de comum interesse aos auditores, auditados e comissão de auditoria. Na norma da ABNT (2002), afirma-se que “os envolvidos devem estar cientes de tudo que está contemplado no plano de auditoria, sendo este válido oficialmente dentro do programa de auditoria somente após o conhecimento de todas as partes interessadas”.

Com a criação do plano de auditoria, a fase atual pode ser dada como por encerrada. Algumas questões apenas são cabíveis, como pequenas revisões dos artefatos gerados, para um possível alinhamento com toda a equipe e para possíveis registros de considerações detectadas ou adequações para as próximas fases.

É demonstrado na Figura 4 um modelo de um plano de auditoria básico, que pode ser adaptado para auditorias de sistemas específicos.

Figura 4 – Modelo de um plano de auditoria básico



SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:___/___/___

RESPONSAVEL:_____

Definições Iniciais do Programa de Auditoria

Escolha no quadro a seguir o OBJETIVOprincipal que deve ter enfoque nesta auditoria.

a) Objetivos da auditoria

Enfoque Principal:

	Auditabilidade		Disponibilidade
	Privacidade		Manutenabilidade
	Integridade		Versatilidade
	Confidencialidade		Acuidade

Observações:

Escolha no quadro a seguir o ESCOPO principal que deve ter enfoque nesta auditoria.

b) Escopo da auditoria

	Completo
	Parcial
	Acompanhamento

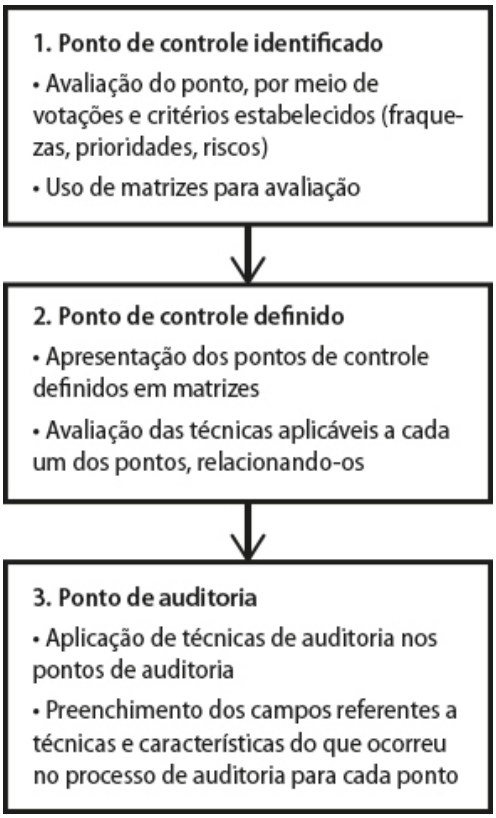
Fonte: Brandalise, 2012.

TEMA 4 – ANÁLISE E DEFINIÇÃO DOS PONTOS DE CONTROLE

Nesta fase, começam a ser trabalhados os pontos de controle do sistema. A fase está dividida em atividades que têm por objetivo tratar os pontos de controle, de modo que se tenham diversas etapas antes da definição de quais vão ser trabalhados, observando os objetivos estabelecidos no plano de auditoria para as etapas de identificação e definição dos pontos de controle a serem utilizados no programa de auditoria.

Na Figura 5 é apresentado o ciclo de definição de um ponto de controle, que ao fim se torna um ponto de auditoria e é utilizado como evidência de auditoria no processo.

Figura 5 – Ciclo de vida dos pontos de controle



Fonte: Brandalise, 2012.

Neste ciclo de vida dos pontos de controle, são exercidas as atividades de análise e definição dos pontos. Durante essas análises e definições, são gerados alguns artefatos, nos quais comissão de auditoria, auditores e demais envolvidos vão realizar os trabalhos de definições.

Os artefatos utilizados por comissão e gestores envolvidos estão ligados às análises feitas durante as atividades exercidas sob o ambiente do sistema na fase de iniciação do planejamento de auditoria. Eles serão úteis na identificação de todos os pontos de controle e também auxiliarão na análise e definição de quais pontos serão utilizados durante as atividades de auditoria.

4.1 Organização, identificação e definição dos pontos de controle

Para tratar todo o ciclo de vida dos pontos de controle, é proposta a elaboração de uma série de matrizes para a avaliação conjunta da equipe envolvida no programa de auditoria. O planejamento dessas matrizes pode contar com a presença de representantes das áreas de negócio, um representante da área de análise de sistemas, principais gestores e, caso

necessário, um profissional de consultoria externa com qualificações em auditoria e sistemas.

Na Figura 6, é apresentado recorte da atividade de organização, identificação e definição dos pontos de controle. Dentro dessa atividade, existem artefatos de entrada que apresentam matrizes, em que serão tratados os pontos de controle envolvidos, dividido por etapas para sua seleção.

Figura 6 – Atividades dos pontos de controle

Análise e definição dos pontos de controle	Organização, identificação e definição de pontos de controle	• Criação de arquivo que contém os pontos levantados e critérios estabelecidos • Reuniões com a comissão • Análise de auditorias passadas e pontos considerados importantes	Etapa 1 – Matriz de ponto de controle identificado Etapa 2 – Matriz ponto de controle identificado Etapa 3 – Matriz de ponto de controle definido	Modelo matriz pontos de controle identificados Matriz pontos de controle de auditoria	Equipe de auditoria, auditor líder, gestão

Fonte: Brandalise, 2012.

Esta atividade inicial da fase de análise e definição de pontos de controle contempla uma série de preenchimento de artefatos. Começa pela organização e identificação dos pontos, baseados no levantamento de informações e dados junto a gestores e usuários. Este artefato servirá para o registro do maior número de pontos de controle que a gestão e usuários-chave entenderem serem importantes para o bom funcionamento do sistema, já que todos podem ser passíveis de auditoria. Para que essas atividades ocorram, é necessária a formatação de um artefato que contenha as matrizes citadas e informações que complementem o artefato.

“O artefato inicial a ser utilizado será chamado Matriz Pontos de Controle Identificados e será composto por pontos de controle, seus detalhes específicos e os riscos de cada ponto apontado pelos participantes da seleção” (GIL, 99).

> O preenchimento do artefato Modelo Matriz Pontos de Controle Identificados ocorre durante reunião realizada entre a equipe de auditoria, gestores e principais usuários do sistema. Os gestores e usuários em conjunto com a equipe de auditoria preenchem o artefato de acordo com os pontos de controle existentes. Para cada um dos pontos de controle, os riscos são avaliados. (Brandalise, 2012)

A avaliação de riscos será baseada nas etapas existentes na identificação de riscos, que são:

- Identificação de pontos.
- Identificação de ameaças.
- Identificação de vulnerabilidades.
- Identificação de consequências.

> As identificações de vulnerabilidades e consequências de risco estarão relacionados ao conhecimento de negócio que o gestor e usuários envolvidos apontarão como sendo razões para o ponto elencado, e constarão na coluna de riscos do artefato Modelo Matriz Pontos de Controle Identificados.
> Após o artefato Modelo Matriz de Pontos de Controle Identificados estar preenchido, parte-se para a etapa de seleção de pontos de controle a serem trabalhados. O artefato que contempla estas informações é o de Matriz Pontos de Controle Definidos. Este artefato conta basicamente com os pontos de controle a serem analisados pela comissão e gestores, os riscos já identificados e uma coluna para o grau de importância a ser preenchido.
> A lógica de avaliação segue a importância que representa para a empresa o ponto de controle registrado. É importante que seja avaliado com cautela e baseado nos objetivos definidos no plano de auditoria.
> Através de reunião, o líder de equipe convoca gestores e usuários chave para o preenchimento individual do anexo e a definição dos pontos definidos. Durante a avaliação individual, o participante avalia os campos já preenchidos. Nesta avaliação existe a atividade de análise de risco agregada, onde cada participante deve considerar o risco do ponto elencado no momento de avaliar os graus de cada um deles.
> Após realizada a votação a partir do artefato Matriz Ponto de Controle Definidos, fica a critério da comissão ou dos auditores a formalização em um documento simples, sobre os pontos de controle selecionados para os trabalhos de auditoria. Para o andamento das atividades de programa de auditoria ocorrer, quando finalizado o processo de escolha dos pontos, deve ser criado um novo artefato. Este novo artefato chamado Modelo de Matriz Pontos de Controle Auditoria, trata basicamente da listagem dos pontos de controle definidos anteriormente e será usado também na fase de preparação e execução de atividades. Neste documento o auditor líder irá delegar as responsabilidades para a equipe de auditoria interna. Ele conterá registros dos auditores responsáveis por cada ponto, uma coluna para serem citadas as técnicas a serem aplicadas nos pontos, características, referências pesquisadas, considerações sobre a aplicação das técnicas e descrição de sugestões de melhoria para cada evidência relatada no ponto.
> Portanto, nesta fase de Análise e Definição dos Pontos, serão preenchidos os campos de ponto de controle e responsáveis, deixando os demais para a próxima fase, que contará com as informações geradas após a aplicação das técnicas de auditoria aqui elencadas. (Brandalise, 2012)

TEMA 5 – PREPARAÇÃO E EXECUÇÃO DE ATIVIDADES

Nesta fase, começa a acontecer a auditoria propriamente dita com o exame dos pontos de controle definidos.

O artefato Modelo de Matriz Pontos de Controle Auditoria possui a listagem de pontos de controle definidos. Esse documento deve vir com alguns campos preenchidos pela equipe de auditoria, como os próprios pontos de controle, as técnicas de auditoria e o responsável por cada ponto.

O ponto de controle passa a ser chamado de ponto de auditoria.

É na atual fase que serão aplicadas as principais técnicas de auditoria elencadas na fase anterior, para o levantamento de evidências e não conformidades de auditoria. O auditor pode complementar com mais técnicas caso seja necessário, e, após isso, inicia as execuções. “Dependendo das técnicas utilizadas, pode ser gerado um grande número de dados e informações, havendo a necessidade de o auditor filtrar esses resultados e compilá-los para posterior registro no artefato Modelo Matriz dos Pontos de Auditoria” (Brandalise, 2012).

Os dados e as informações resultantes da aplicação das técnicas devem ser utilizados para o preenchimento dos demais campos do documento Modelo Matriz Ponto de Controle Auditoria.

> A partir da próxima fase e com o Modelo de Matriz Ponto de Controle Auditoria preenchido é que serão formalizados os relatórios e demais artefatos onde constam parte das informações coletadas nesta fase e nas demais. A partir do trabalho de compilação e preparação dos dados gerados anteriormente, os auditores devem procurar distribuir essas informações nos artefatos finais que serão apresentados aos envolvidos na auditoria, principalmente a alta gestão. (Brandalise, 2012)

“Antes de emitir relatórios finais, é imprescindível solicitar a compreensão ou não dos auditados para dirimir as dúvidas que porventura tenham persistido durante o processo de auditoria” Imoniana (2005). Os artefatos usados neste momento são a carta-comentário e o rascunho preliminar do relatório final de auditoria.

A ABNT (2006) apresenta a etapa de comunicação de risco, “que no âmbito da auditoria pode ser associada a comunicação de evidências de auditoria. O objetivo é semelhante, fazer com que as partes envolvidas no processo de auditoria tenham conhecimento do que foi abordado e evidenciado ao longo dos trabalhos”.

> Para a pré-formalização do fechamento do programa de auditoria por parte dos auditores, pode ser utilizada a carta comentário. Ela é um artefato sucessor ao rascunho preliminar de auditoria, o qual estes apenas dependem da aprovação por parte dos destinatários, que

> podem ser os gestores responsáveis pelas áreas envolvidas. (Brandalise, 2012)

Para que a carta-comentário contenha uma base de informações consistente, a equipe de auditoria elabora o artefato chamado Rascunho Preliminar do Relatório de Auditoria. Esse artefato é um arquivo gerado e preenchido pela equipe de auditores com base na avaliação de artefatos gerados em outras fases do roteiro, principalmente dos resultados dos pontos de auditoria, e que será enviado anexo à carta-comentário, onde constarão os tópicos que seguem:

a. Objetivo do controle;
b. Considerações no ponto;
c. Descrição dos procedimentos executados;
d. Resultados;
e. Não conformidades e evidências achadas;
f. Recomendações;
g. Aval dos responsáveis internos.

> Dentro destes tópicos, o destinatário, que provavelmente será algum responsável pelo acompanhamento de auditoria ou um gestor, terá apenas de preencher o último tópico.
> Com a aprovação deste rascunho de relatório e o conhecimento de todas as partes interessadas, a próxima atividade é a criação do relatório final. Este relatório final é de responsabilidade do Líder da Equipe de Auditoria. Além de informações contidas no rascunho inicial, devem ser citados outros elementos que compõe o processo de auditoria, são eles:
> a) relação de normas, instruções, procedimentos e outros documentos utilizados como base (referência) para as avaliações;
> b) relação dos membros de equipe de auditoria;
> c) nomes de quaisquer outros observadores, participantes e de pessoas que foram contatadas em qualquer fase da auditoria;
> d) constatações finais, dando ênfase para deficiências detectadas.
> Devem ser fornecidos detalhes suficientes para permitirem avaliação, ação corretiva e providências complementares pela organização/setor auditado.
> O relatório pode ser distribuído aos gestores e responsáveis no momento da comunicação de encerramento do programa de auditoria, para que tenham o conhecimento dos resultados e pareceres finais extraídos do programa implantado. (Brandalise, 2012).

Conforme citado na norma da ABNT (2002), “as ações corretivas, preventivas ou de melhoria, que podem ser aplicáveis ao fim da apresentação dos resultados fica a critério do auditado e não são consideradas como parte da auditoria”. A norma também enfatiza que, para a verificação das ações, pode ser criado outro programa de auditoria, para que sejam verificadas as ações tomadas e a sua eficácia.

FINALIZANDO

Foram apresentados nesta aula o planejamento de auditoria e pontos de controle, como um roteiro para elaboração de auditoria em sistemas. No roteiro proposto foram apresentadas as fases, suas principais atividades, os responsáveis pela realização delas, os artefatos que devem ser utilizados como referência e, além disso, os artefatos gerados por cada atividade executada.

A utilização do roteiro pode ser feita por profissionais encarregados de implantar auditoria em ambientes internos de organizações. Esse roteiro pode ser alterado quando necessário, sendo acrescidas mais regras para verificações, atividades e artefatos. Esses critérios de mudança ficam sob a responsabilidade da comissão ou da equipe interna responsável pela elaboração de 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 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 – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2006. 65p.

BRANDALISE. M. M. T. **Roteiro para elaboração de programas de auditoria em sistema**. Universidade de Caxias do Sul, 2012.

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**. Disponível em: <http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx>. Acesso em: 1 dez. 2017.

_____. **CISA job practice areas**. Disponível em: <http://www.isaca.org>. Acesso em: 1 dez. 2017.

_____. **Glossary of terms**. Disponível em: <http://www.isaca.org>. Acesso em: 1 dez. 2017.

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

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.