Diretrizes para auditoria de sistemas de gestão

1) Este Projeto de Revisão foi elaborado pela Comissão de Estudo de Tecnologia de Suporte (CE-25:000.03) do Comitê Brasileiro da Qualidade (ABNT/CB-25), nas reuniões de:

09.09.2011	03.01.2012	17.01.2012

2) Este Projeto de Revisão/Emenda é previsto para cancelar e substituir a edição anterior (ABNT NBR 19011:2002), quando aprovado, sendo que nesse ínterim a referida norma continua em vigor;

3) Previsto para ser equivalente à ISO 19011:2011;

4) Não tem valor normativo;

5) Aqueles que tiverem conhecimento de qualquer direito de patente devem apresentar esta informação em seus comentários, com documentação comprobatória;

6) Este Projeto de Norma será diagramado conforme as regras de editoração da ABNT quando de sua publicação como Norma Brasileira.

7) Tomaram parte na elaboração deste Projeto:

Participante	Representante
CQSI	Ariosto Farias Jr.
ELETROBRAS	Roberto Gomes de Almeida
INMETRO	Ana Julia Ramos
INMETRO	Ana Carolina Faria
IFRJ	Fernando Sepulveda
Particular	Basílio Vasconcellos Dagnino
Particular	Soyla Oleika Moraes

PETROBRAS	Carlos Leonam Mendes dos Reis
PETROBRAS	Renato Pedroso Lee
PETROBRAS	Sergio Pinto Amaral

Diretrizes para auditoria de sistemas de gestão

Guidelines for auditing management systems

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretiva ABNT, Parte 2.

A ISO 19011 foi preparada pelo Comitê Técnico ISO/TC 176, Quality Management and quality assurance, Subcommittee SC3, Suporting Technologies.

Esta segunda edição cancela e substitui a primeira edição ABNT NBR ISO 19011:2002, que foi tecnicamente revisada.

As principais diferenças comparadas com a primeira edição são as seguintes:

— o escopo foi ampliado de auditoria de sistemas de gestão da qualidade e meio ambiente para auditoria de sistemas de gestão de qualquer natureza;

— a relação entre a ISO 19011 e a ISO/IEC 17021 foi esclarecida;

— métodos de auditoria remota e o conceito de risco foram introduzidos;

— confidencialidade foi acrescentada como um novo princípio de auditoria;

— as seções 5,6 e 7 foram reorganizadas;

— informações adicionais foram incluídas em um novo anexo B, resultando na remoção das caixas de textos

— o processo de avaliação e de determinação de competência tornou-se mais rígido;

— exemplos ilustrativos de habilidades e conhecimentos de disciplina específicos foram incluídos em um novo Anexo A;

— diretrizes adicionais estão disponíveis no seguinte site:www.iso.org/19011auditing.

O Escopo desta Norma Brasileira em inglês é o seguinte:

Scope

This Standard provides provides guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process, including the person managing the audit programme, auditors and audit teams.

It is applicable to all organizations that need to conduct internal or external audits of management systems or manage an audit programme.

The application of this Satandard to other types of audits is possible, provided that special consideration is given to the specific competence needed.

Introdução

Desde que a primeira edição desta Norma foi publicada em 2002, um número de novas normas de sistemas de gestão foi publicado. Como resultado, há, agora, a necessidade de se considerar um escopo mais abrangente de auditoria de sistema de gestao, como também fornecer diretrizes que sejam mais genéricas.

Em 2006, o comitê ISO para avaliação de conformidade (CASCO) desenvolveu a ISO/IEC 17021, que estabelece requisitos para sistemas de gestao de certificação de terceira parte e que se baseou parcialmente nas diretrizes contidas na primeira edição desta Norma.

A segunda edição da ISO/IEC 17021 publicada em 2011, foi ampliada para transformar as diretrizes descritas na norma de 2006 em requisitos para auditorias de certificação de sistemas de gestão. É, neste contexto, que a segunda edição desta Norma fornece diretrizes para todos os usuários, incluindo pequenas e medias organizações, e concentra-se naquilo que é comumente denominado de auditorias internas (primeira parte) e auditorias conduzidas por clientes em seus fornecedores (segunda parte). Enquanto aqueles os envolvidos com em auditorias de certificação de sistemas de gestão seguem os requisitos da ISO/IEC 17021:2011, eles podem, também, considerar úteis as diretrizes contidas nesta Norma.

A relação entre esta segunda edição da Norma e a ABNT NBR ISO/IEC 17021:2011 é mostrada na Tabela 1.

Tabela 1 — Escopo desta Norma e sua relação com a ABNT NBR ISO/IEC 17021:2011

Auditoria interna	**Auditoria externa**	
	Auditoria no fornecedor	**Auditoria de terceira parte**
Algumas vezes chamada de auditoria de primeira parte	Algumas vezes chamada auditoria de segunda parte	Para propósitos legais, regulatórios e similares Para fins de certificação (ver também os requisitos da ABNT NBR ISSO/IEC 17021)

Esta Norma não estabelece requisitos, mas fornece diretrizes sobre a gestão de um programa de auditoria, sobre o planejamento e a realização de uma auditoria de sistema de gestão, bem como sobre a competência e avaliação de um auditor e de uma equipe auditora.

Organizações podem operar mais de um sistema de gestão formal. Para simplificar a leitura desta Norma o termo “sistema de gestão” é o preferido, porém o leitor pode adaptar a implementação das diretrizes para sua própria situação em particular. Isto também se aplica ao uso de “pessoa” e “pessoas”, “auditor” e “auditores”.

Pretende-se que esta Norma seja aplicada a uma ampla gama de potencial usuários, incluindo auditores, organizações que implementam sistemas de gestão e organizações que necessitam realizar auditorias de sistemas de gestão por razões contratuais ou regulatórios. Os usuários desta norma podem, entretanto, utilizar estas diretrizes no desenvolvimento dos seus próprios requisitos relacionados à auditoria.

As diretrizes desta Norma podem, também, ser usadas com a finalidade de auto-declaração, e podem ser úteis às organizações envolvidas no treinamento de auditor ou certificação pessoal.

As diretrizes desta Norma procuram ser flexíveis. Conforme indicado em vários pontos no texto, o uso destas diretrizes pode variar dependendo do tamanho e do nível de maturidade do sistema de gestão de uma organização e da natureza e complexidade da organização a ser auditada, como também com os objetivos e escopo das auditorias a serem executadas.

Esta Norma introduz o conceito de risco para auditoria de sistemas de gestão. O enfoque adotado se relaciona com o risco do processo de auditoria em não atingir seus objetivos e com a possibilidade da auditoria interferir com os processos e atividades da organização auditada. Ela não fornece diretrizes específicas sobre o processo de gestão de risco da organização, mas reconhece que as organizações podem focar o esforço da auditoria em assuntos de importancia para o sistema de gestão.

Esta Norma adota o enfoque que quando dois ou mais sistemas de gestão de diferentes disciplinas são auditados em conjunto, isto é chamado de uma “auditoria combinada”. Quando esses sistemas são integrados em um sistema de gestão único, os princípios e processos de auditoria são os mesmos que para uma auditoria combinada.

A Seção 3 estabelece os termos chave e definições usados nesta Norma.Todo um esforço foi feito para assegurar que estas definições não conflitem com as definições usadas em outras normas.

A Seção 4 descreve os princípios nos quais a auditoria está baseada. Estes princípios ajudam o usuário a entender a natureza essencial da auditoria e são importantes no entendimento das diretrizes estabelecidas nas Seções 5 a 7.

A Seção 5 fornece orientação sobre como estabelecer e gerenciar um programa de auditoria, estabelecer os objetivos do programa de auditoria e coordenar as atividades de auditoria.

A Seção 6 fornece orientação sobre como planejar e realizar uma auditoria de um sistema de gestão.

A Seção 7 fornece orientação relacionadas com a competência e avaliação de auditores de sistemas de gestão e das equipes de auditoria.

O Anexo A ilustra a aplicação das diretrizes na Seção 7 para diferentes disciplinas.

O Anexo B fornece orientação adicional para auditores sobre o planejamento e realização de auditorias.

1 Escopo

Esta Norma fornece orientação sobre auditoria de sistemas de gestão, incluindo os princípios de auditoria, a gestão de um programa de auditoria e a realização de auditorias de sistema de gestão, como também orientação sobre a avaliação da competência de pessoas envolvidas no processo da auditoria, incluindo a pessoa que gerencia o programa de auditoria, os auditores e a equipes auditora.

Ela é aplicável a todas as organizações que necessitam realizar auditorias internas ou externas de sistemas de gestão ou gerenciar um programa de auditoria.

A aplicação desta Norma para outros tipos de auditorias é possível, desde que seja dada consideração especial para a necessidade de competência específica.

2 Referências normativas

Não são citadas referências normativas. Esta seção é incluída a fim de que se mantenha a numeração idêntica da seção com outras normas da ISO de sistema de gestão.

3 Termos e definições

Para os efeitos desta norma aplicam-se os seguintes termos e definições

3.1
auditoria
processo sistemático, documentado e independente para obter **evidência de auditoria** (3.3) e avaliá-las, objetivamente, para determinar a extensão na qual os **critérios da auditoria** (3.2) são atendidos.

NOTA 1 Auditorias internas, algumas vezes chamadas de auditorias de primeira parte, são conduzidas pela própria organização, ou em seu nome, para análise crítica pela direção e outros propósitos internos (por exemplo, para confirmar a eficácia do sistema de gestão ou para obter informações para a melhoria do sistema de gestão). Auditorias internas podem formar a base para uma autodeclaraçao de conformidade da organização. Em muitos casos, particularmente em pequenas organizações, a independência pode ser demonstrada através da isenção de responsabilidade pela atividade sendo auditada ou isenção de tendenciosidade e conflito de interesse por parte do auditor.

NOTA 2 Auditorias externas incluem auditorias de segunda e terceira parte. Auditorias de segunda parte são realizadas por partes que têm um interesse na organização, tais como clientes, ou por outras pessoas em seu nome. Auditorias de terceira parte são realizadas por organizações de auditoria independentes, tais como organismos de regulamentação ou organismos de certificação.

NOTA 3 Quando dois ou mais sistemas de gestão de disciplinas diferentes (por exemplo, qualidade, meio ambiente, segurança e saúde ocupacional) são auditados juntos, isto é chamado de auditoria combinada.

NOTA 4 Quando duas ou mais organizações de auditoria cooperam para auditar um único auditado (3.7), isto é chamado de auditoria conjunta.

NOTA 5 Adaptado da ABNT NBR ISO 9000:2005, definição 3.9.1

3.2
critério de auditoria
conjunto de políticas, procedimentos ou requisitos usados como uma referência na qual a **evidência de auditoria** (3.3) é comparada.

NOTA 1 Adaptada da NBR ISO 9000:2005, definição 3.9.3

NOTA 2 Se os critérios de auditoria são requisitos legais (incluindo estatutário ou regulatório), os termos "conformidade" ou "não conformidade" são sempre usados nas constatações de auditoria (3.4).

3.3
evidência de auditoria
registros, apresentação de fatos ou outras informações, pertinentes aos **critérios de auditoria** (3.2) e verificáveis.

NOTA Evidência de auditoria pode ser qualitativa ou quantitativa.

[ABNT NBR ISO 9000:2005, definição 3.9.4]

3.4
constatações de auditoria
resultados da avaliação da **evidência de auditoria** (3.3) coletada, comparada com os **critérios de auditoria** (3.2)

NOTA 1 Constatações de auditoria indicam conformidade ou não-conformidade.

NOTA 2 Constatações de auditoria podem conduzir à identificação de oportunidades para melhoria ou registros de boas práticas.

NOTA 3 Se os critérios de auditoria forem selecionados de requisitos legais ou outros requisitos, a constatação da auditoria é denominada de conformidade ou não conformidade.

NOTA 4 Adaptado da ABNT NBR ISO 9000:2005, definição 3.9.5

3.5
conclusão de auditoria
Resultado de uma **auditoria** (3.1), após levar em consideração os objetivos da auditoria e todas as **constatações de auditoria** (3.4)

NOTA Adaptado da ABNT NBR ISO 9000:2005, definição 3.9.6

3.6
cliente de auditoria
organização ou pessoa que solicita uma **auditoria** (3.1)

NOTA 1 No caso de auditoria interna o cliente da auditoria pode também ser o **auditado** (3.7) ou o gestor do programa de auditoria. Solicitações para auditorias externas podem ser oriundas de fontes tais como, organismos de regulamentação, partes contratantes ou clientes potenciais.

NOTA 2 Adaptado da ABNT NBR ISO 9000:2005, definição 3.9.7

3.7
auditado
organização que está sendo auditada
[ABNT NBR ISO 9000:2005, definição 3.9.8]

3.8
auditor
pessoa que realiza uma **auditoria** (3.1)

3.9
equipe de auditoria
um ou mais **auditores** (3.8) que realizam uma **auditoria** (3.1), apoiados, se necessário, por **especialistas** (3.10)

NOTA 1 Um auditor da equipe de auditoria é indicado como o líder da equipe.

NOTA 2 A equipe de auditoria pode incluir auditores em treinamento.

[ABNT NBR ISO 9000:2005, definição 3.9.10]

3.10
especialista
pessoa que provê conhecimento ou experiência específicos para a equipe de auditoria (3.9)

NOTA 1 Conhecimento ou experiência específicos são relativos ao processo ou atividade auditada ou idioma ou cultura para a organização.

NOTA 2 Um especialista não atua como um **auditor** (3.8) na equipe de auditoria.

[ABNT NBR ISO 9000:2005, definição 3.9.11]

3.11
observador
pessoa que acompanha a **equipe de auditoria** (3.9), mais não audita.

NOTA 1 Um observador não faz parte da **equipe de auditoria** (3.9) e não influencia ou interfere com a realização da **auditoria** (3.1).

NOTA 2 Um observador pode ser do **auditado** (3.7), de um organismo regulatório ou outra parte interessada que testemunhe a **auditoria** (3.1).

3.12
guia
pessoa indicada pelo **auditado** (3.7) para apoiar a **equipe de auditoria** (3.9).

3.13
programa de auditoria
conjunto de uma ou mais **auditorias** (3.1) planejado para um período de tempo especifico e direcionado a propósito especifico.

NOTA Adaptado da ABNT NBR ISO 9000:2005, definição 3.9.2

3.14
escopo de auditoria
abrangência e limites de uma **auditoria** (3.1)

NOTA O escopo de auditoria geralmente inclui uma descrição das localizações físicas, unidades organizacionais, atividades e processos, bem como o período de tempo coberto.

[ABNT NBR ISO 9000:2005, definição 3.9.13]

3.15
plano de auditoria
descrição das atividades e arranjos para uma **auditoria** (3.1).

[ABNT NBR ISO 9000:2005, definição 3.9.12]

3.16
risco
efeito da incerteza nos objetivos
NOTA Adaptado da ABNT NBR ISO Guia 73:2009, definição 1.1

3.17
competência
capacidade para aplicar conhecimentos e habilidades para atingir resultados pretendidos.

NOTA Capacidade implica na aplicação apropriada do comportamento pessoal durante o processo de auditoria

3.18
conformidade
atendimento a um requisito

[ABNT NBR ISO 9000:2005, definição 3.6.1]

3.19
não-conformidade
não atendimento a um requisito.

[ABNT NBR ISO 9000:2005, definição 3.6.2]

3.20
sistema de gestão
sistema para estabelecer política e objetivos, e para atingir estes objetivos.

NOTA Um sistema de gestão de uma organização pode incluir diferentes sistemas de gestão, tais como um sistema de gestão da qualidade, um sistema de gestão financeira ou um sistema de gestão ambiental.

[ABNT NBR ISO 9000:2005, definição 3.2.2].

4 Princípios de auditoria

A auditoria é caracterizada pela confiança em alguns princípios. Convém que estes princípios ajudem a tornar a auditoria uma ferramenta eficaz e confiável em apoio às políticas de gestão e controles, fornecendo informações sobre as quais uma organização pode agir para melhorar seu desempenho. A

aderência a estes princípios é um pré-requisito para se fornecer conclusões de auditoria que são pertinentes e suficientes, e para permitir que auditores que trabalhem independentemente entre si, cheguem a conclusões semelhantes em circunstâncias semelhantes.

As orientações dadas nas Seções 5 a 7 estão baseadas nos seis princípios apresentados abaixo:

a) **Integridade**: o fundamento do profissionalismo.

Convém que os auditores e a pessoa que gerencia um programa de auditoria:

— realize o seu trabalho com honestidade, diligência e responsabilidade;

— observe e esteja em conformidade com quaisquer requisitos legais aplicáveis;

— demonstre sua competência enquanto realiza o seu trabalho;

— desempenhe o seu trabalho de forma imparcial, isto é, mantendo–se justo e sem tendenciosidade em todas as situações;

— esteja sensível a quaisquer influências que possam ser exercidas sobre seu julgamento enquanto realizando uma auditoria.

b) **Apresentação justa**: a obrigação de reportar com veracidade e exatidão.

Convém que as constatações de auditoria, conclusões de auditoria e relatórios de auditoria reflitam com veracidade e com precisão as atividades de auditoria. Convém que os problemas significativos encontrados durante a auditoria e não resolvidos por divergência de opiniões entre a equipe de auditoria e o auditado, sejam relatados. Convém que a comunicação seja verdadeira precisa objetiva, (em tempo oportuno), clara e completa.

c) **Devido cuidado profissional**: a aplicação de diligência e julgamento na auditoria.

Convém que os auditores exerçam com o devido cuidado de acordo com a importância da tarefa que eles executam e a confiança neles depositada pelo cliente da auditoria e por outras partes interessadas. Um fator importante na realização do seu trabalho com o devido cuidado profissional é ter a capacidade de fazer julgamentos ponderados em todas as situações da auditoria.

d) **Confidencialidade**: segurança da informação

Convém que os auditores tenham discrição no uso e proteção das informações obtidas no curso das suas obrigações. Convém que as informações da auditoria não sejam usadas de forma inapropriada para ganhos pessoais pelo auditor ou pelo cliente da auditoria, ou de maneira prejudicial para o legítimo interesse do auditado. Este conceito inclui o manuseio apropriado de informações confidenciais ou sensíveis.

e) **Independência**: a base para imparcialidade da auditoria e objetividade das conclusões da auditoria.

Convém que os auditores sejam independentes da atividade que está sendo auditada, quando for possível, e convém que em todas as situações hajam de tal modo que estejam livres de tendenciosidade e conflitos de interesse. Para auditorias internas, convém que os auditores sejam independentes das operações gerenciais da função que está sendo auditada. Convém que os auditores

mantenham objetividade ao longo de todo o processo de auditoria para assegurar que as conclusões e constatações da auditoria estejam baseadas somente nas evidências de auditoria.

Para pequenas organizações, pode não ser possível para os auditores internos terem total independência da atividade que está sendo auditada, porém convém que seja feito todo esforço para remover a tendenciosidade e encorajar a objetividade.

f) **Abordagem baseada em evidência**: o método racional para alcançar conclusões de auditoria confiáveis e reproduzíveis em um processo sistemático de auditoria.

Convém que a evidência da auditoria seja verificável. Ela geralmente é baseada em amostras das informações disponíveis, uma vez que uma auditoria é realizada durante um período de tempo finito e com recursos limitados. Convém que o uso apropriado de amostras seja aplicado, uma vez que esta situação esta intimamente relacionada com a confiança que pode ser depositada nas conclusões da auditoria.

5 Gerenciando um programa de auditoria

5.1 Geral

Convém que uma organização que necessita realizar auditorias estabeleça um programa de auditoria que contribua para a determinação da eficácia do sistema de gestão do auditado. O programa de auditoria pode incluir considerações de auditorias de uma ou mais normas de sistema de gestão, conduzidas de forma separada ou em conjunto.

Convém que a alta direção assegure que os objetivos do programa de auditoria sejam estabelecidos e atribuídos a uma ou mais pessoas competentes para gerenciar o programa da auditoria. Convém que a abrangência de um programa de auditoria esteja baseada na natureza e tamanho da organização que esta sendo auditada, como também na natureza, funcionalidade, complexidade e nível de maturidade do sistema de gestão a ser auditado. Convém que seja dada prioridade para alocar recursos ao programa de auditoria, para auditar aquelas questões de grande importância dentro do sistema de gestão. Isto pode incluir características chave da qualidade do produto ou dos perigos relativos à saúde e segurança, ou aspectos ambientais significativos e seus controles.

NOTA Este conceito é normalmente conhecido como auditoria baseada em risco. Esta Norma não fornece diretrizes adicionais de auditorias baseada em risco.

Convém que o programa da auditoria inclua informações e recursos necessários para organizar e realizar suas auditorias de forma eficaz e eficiente dentro de um período de tempo específico e que pode também incluir o seguinte:

— objetivos para o programa de auditoria e auditorias individuais;

— abrangência/ número/ tipos/ duração/ localizações/ programação de auditorias;

— procedimentos do programa de auditoria;

— critérios de auditoria;

— métodos de auditoria;

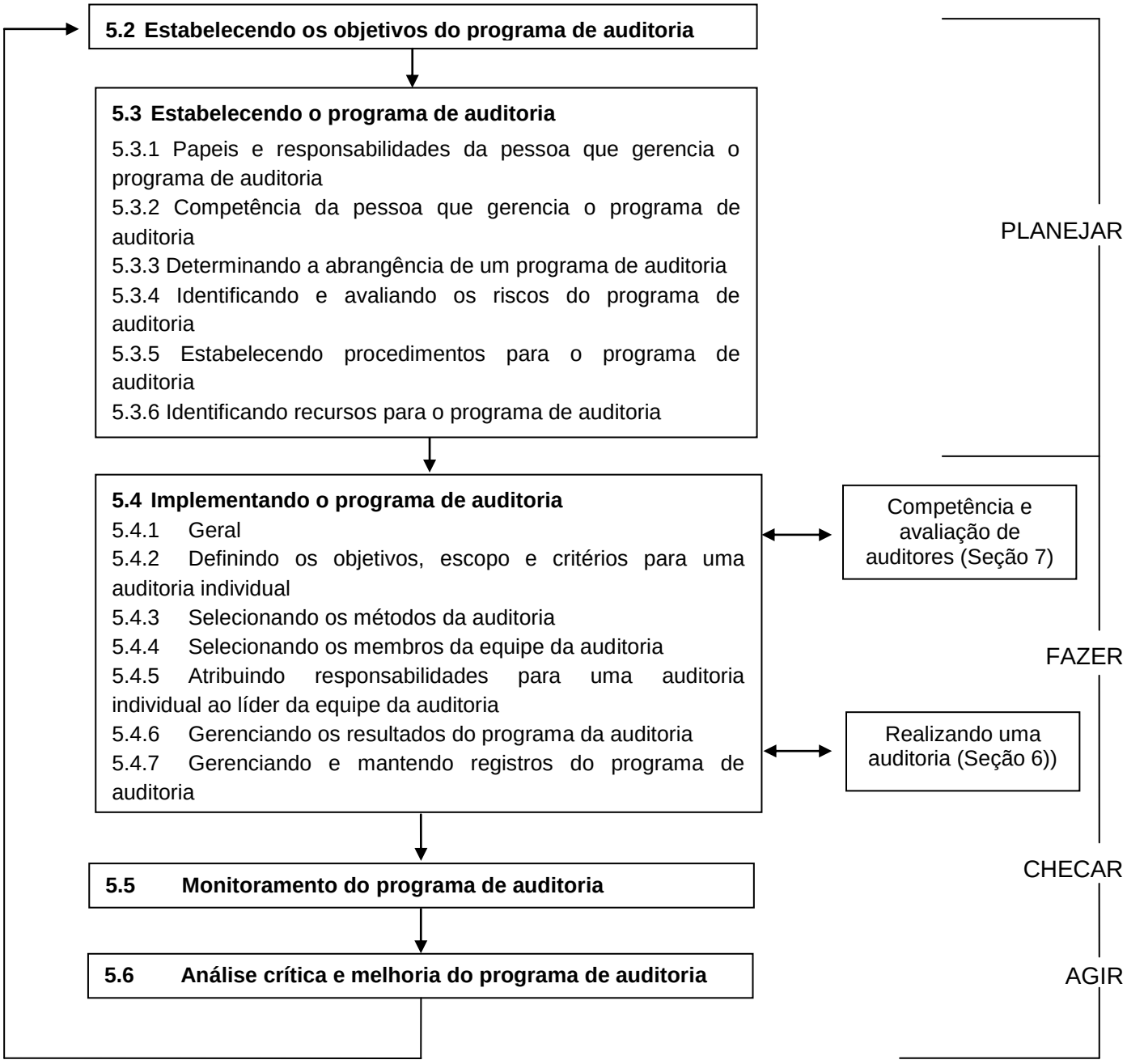
— seleção da equipe de auditoria;

— recursos necessários, incluindo viagem e acomodação;

— processos para tratamento da confidencialidade, segurança da informação, saúde e segurança, e outros assuntos similares.

Convém que a implementação do programa de auditoria seja monitorada e medida para assegurar que seus objetivos foram alcançados. Convém que o programa de auditoria seja analisado criticamente para identificar possíveis melhorias.

A Figura 1 Ilustra o fluxo do processo para a gestão de um programa de auditoria.



NOTA 1 Esta figura ilustra a aplicação do ciclo PDCA a esta norma.

NOTA 2 Numeração de Seções/ Subseções refere-se as Seções/Subseções pertinentes desta norma.

Figura 1 — Fluxograma do processo para gerenciamento de um programa de auditoria

5.2 Estabelecendo os objetivos do programa de auditoria

Convém que a alta direção assegure que os objetivos do programa de auditoria sejam estabelecidos para direcionar o planejamento e a realização de auditorias e assegurar que o programa de auditoria

seja implementado eficazmente. Convém que os objetivos do programa de auditoria sejam consistentes com, e apóiem, os objetivos e a política do sistema de gestão.

Estes objetivos podem ser baseados nos seguintes pontos:

a) prioridades da direção;

b) intenções comerciais e outros negócios;

c) características de processos, produtos e projetos e quaisquer mudanças a estes;

d) requisitos do sistema de gestão;

e) requisitos legais e contratuais e outros requisitos com os quais a organização esteja comprometida;

f) necessidade para avaliação de fornecedor;

g) necessidades e expectativas das partes interessadas, incluindo os clientes;

h) nível de desempenho do auditado, como mostrado na ocorrência de falhas, incidentes ou reclamações de clientes;

i) riscos para o auditado;

j) resultados de auditorias anteriores;

k) nível de maturidade do sistema de gestão que está sendo auditado.

Exemplos de objetivos do programa de auditoria incluem:

— contribuir para melhoria de um sistema de gestão e o seu desempenho;

— atender a requisitos externos, por exemplo, certificação de acordo com uma norma de sistema de gestão;

— verificar a conformidade com requisitos contratuais;

— obter e manter confiança na capacidade de um fornecedor;

— determinar a eficácia do sistema de gestão;

— avaliar a compatibilidade e o alinhamento dos objetivos do sistema de gestão com a política do sistema de gestão e os objetivos gerais da organização.

5.3 Estabelecendo programa de auditoria

5.3.1 Papeis e responsabilidades da pessoa que gerencia o programa de auditoria

Convém que a pessoa que gerencia o programa de auditoria:

— estabeleça a abrangência do programa de auditoria;

— identifique e avalie os riscos para o programa de auditoria;

— estabeleça as responsabilidades de auditoria;

— estabeleça os procedimentos para os programas de auditoria;

— determine os recursos necessários;

— assegure a implementação do programa de auditoria, incluindo o estabelecimento dos objetivos da auditoria, escopo e critérios das auditorias individuais, determinando os métodos da auditoria, selecionando a equipe auditora e avaliando os auditores;

— assegurar que os registros apropriados do programa de auditoria sejam gerenciados e mantidos;

— monitorar, analisar criticamente e melhorar o programa de auditoria.

Convém que a pessoa que gerencia um programa de auditoria informe à alta direção sobre o conteúdo do programa de auditoria e, se necessário, solicite sua aprovação.

5.3.2 Competência da pessoa que gerencia o programa de auditoria

Convém que a pessoa que gerencia o programa de auditoria tenha a necessária competência para gerenciar o programa e seus riscos associados, de forma eficiente e eficaz, como também conhecimento e habilidades nas seguintes áreas:

— princípios da auditoria, procedimentos e métodos;

— normas de sistema de gestão e documentos de referência;

— atividades, produtos e processos do auditado;

— requisitos legais aplicáveis e outros requisitos pertinentes para as atividades e produtos do auditado;

— clientes, fornecedores e outras partes interessadas do auditado, quando aplicável.

Convém que a pessoa que gerencia o programa de auditoria esteja envolvida em atividades apropriadas de desenvolvimento profissional continuo, para manter o necessário conhecimento e habilidades para gerenciar o programa de auditoria.

5.3.3 Determinando a abrangência de um programa de auditoria

Convém que a pessoa que gerencia um programa de auditoria determine a abrangência do programa de auditoria o qual pode variar dependendo do tamanho e natureza da organização auditada, como também da natureza, funcionalidade, complexidade e nível de maturidade do sistema de gestão, e temas de importância para o sistema de gestão a ser auditado.

NOTA Em certos casos, dependendo da estrutura da organização auditada ou das suas atividades, o programa de auditoria pode consistir apenas de uma única auditoria (p.ex. atividade de um pequeno projeto)

Outros fatores que impactam a abrangência de um programa de auditoria incluem o seguinte:

— o objetivo, escopo e duração de cada auditoria e o número de auditorias a serem realizadas incluindo auditorias de acompanhamento, quando pertinente;

— o número, importância, complexidade, similaridade e localizações das atividades a serem auditadas;

— fatores que influenciam a eficácia do sistema de gestão;

— critérios de auditoria aplicáveis, tais como preparativos planejados para as normas de gestão pertinentes, requisitos legais e contratuais outros requisitos com os quais a organização esteja comprometida;

— conclusões de auditorias anteriores, internas ou externas;

— resultados de análise crítica de programas de auditorias anteriores;

— questões social, cultural e de idioma;

— questões relativas às partes interessadas, tais como reclamações de clientes ou não-conformidades com requisitos legais;

— mudanças significativas para o auditado ou suas operações;

— disponibilidade da tecnologia da informação e comunicação para apoiar as atividades da auditoria, em particular o uso de métodos de auditoria remota (ver Seção B.1);

— a ocorrência de eventos internos e externos, tais como falhas de produtos, vazamento de segurança da informação, incidentes com saúde e segurança ocupacional, atos criminosos ou incidentes ambientais.

5.3.4 Identificando e avaliando os riscos do programa de auditoria

Existem muitos riscos diferentes associados com o estabelecimento, implementação, monitoramento, análise crítica e melhoria de um programa de auditoria que pode afetar o alcance dos seus objetivos. Convém que a pessoa que gerencia o programa de auditoria considere esses riscos no seu desenvolvimento. Esses riscos podem estar associados com o seguinte:

— planejamento, por exemplo, falha para estabelecer os objetivos pertinentes da auditoria e determinar a abrangência do programa de auditoria;

— recursos, por exemplo, permitindo tempo insuficiente para desenvolver o programa da auditoria ou realizar uma auditoria;

— seleção da equipe de auditoria, por exemplo, a equipe não tem a competência coletiva para realizar auditorias de forma eficaz;

— implementação, por exemplo, comunicação ineficaz do programa de auditoria;

— registros e seus controles, por exemplo, falha para proteger de forma adequada os registros de auditoria para demonstrar a eficácia do programa de auditoria;

— monitoramento, análise crítica e melhoria do programa de auditoria, por exemplo, monitoramento ineficaz dos resultados do programa de auditoria.

5.3.5 Estabelecendo procedimentos para o programa de auditoria

Convém que a pessoa que gerencia um programa de auditoria estabeleça um ou mais procedimentos contemplando os seguintes pontos, quando aplicáveis:

— planejamento e programação das auditorias considerando os riscos do programa da auditoria;

— assegurar a confidencialidade e segurança da informação;

— garantia da competência dos auditores e dos líderes da equipe de auditoria;

— seleção apropriada das equipes de auditoria e atribuições de seus papéis e responsabilidades;

— realização de auditorias, incluindo o uso apropriado de métodos de amostragem;

— realização de auditoria de acompanhamento, se aplicável;

— relato para a alta direção sobre os resultados globais do programa de auditoria;

— manutenção dos registros do programa de auditoria;

— monitoramento e análise crítica do desempenho e riscos, e das melhorias da eficácia do programa de auditoria.

5.3.6 Identificando recursos para o programa de auditoria

Quando da identificação dos recursos para o programa de auditoria, convém que a pessoa que gerencia o programa de auditoria considere:

— os recursos financeiros necessários para desenvolver, implementar, gerenciar e melhorar as atividades de auditoria;

— métodos de auditoria;

— a disponibilidade de auditores e especialistas que tenham a competência apropriada para os objetivos do programa de auditoria em particular;

— abrangência do programa de auditoria e dos riscos do programa de auditoria;

— tempo de viagem e custos, acomodações e outras necessidades de auditoria;

— a disponibilidade das tecnologias da informação e comunicação.

5.4 Implementando o programa de auditoria

5.4.1 Geral

Convém que a pessoa que gerencia o programa de auditoria implemente o este programa através dos seguintes meios:

— comunicação às partes pertinentes do programa de auditoria e as informe periodicamente do seu progresso;

— definição dos objetivos, escopo e critérios para cada auditoria individual;

— coordenar e programar as auditorias e outras atividades pertinentes ao programa de auditoria;

— assegurar a seleção de equipes de auditoria com a necessária competência;

— fornecer os recursos necessários para as equipes de auditoria;

— assegurar a realização de auditorias de acordo com o programa de auditoria e dentro do período de tempo acordado;

— assegurar que as atividades de auditoria são registradas e estes registros são adequadamente gerenciados e mantidos.

5.4.2 Definindo os objetivos, escopo e critérios para uma auditoria individual

Convém que cada auditoria individual seja baseada nos objetivos, escopos e critérios de auditoria documentados. Convém que estes sejam definidos pela pessoa que gerencia o programa de auditoria e seja consistente com os objetivos globais do programa de auditoria.

Os objetivos de auditoria definem o que deve ser acompanhado por uma auditoria individual e pode ainda incluir o seguinte:

— determinação da abrangência de conformidade do sistema de gestão a ser auditado, ou parte dele, com os critérios de auditoria;

— determinação da abrangência de conformidade das atividades, processos e produtos com os requisitos e procedimentos do sistema de gestão;

— avaliação da capacidade do sistema de gestão para assegurar a conformidade com requisitos legais e contratuais e outros requisitos com os quais a organização esteja comprometida;

— avaliação da eficácia do sistema de gestão para atender aos seus objetivos especificados;

— identificação de áreas para potencial de melhoria do sistema de gestão.

Convém que o escopo da auditoria seja consistente com o programa e os objetivos da auditoria. Isto inclui fatores tais como localização física, unidades organizacionais, atividades e processos a serem auditados, bem como o período de tempo coberto pela auditoria.

Os critérios de auditoria são usados como uma referência contra a qual a conformidade é determinada e pode incluir políticas, procedimentos, normas, requisitos legais, requisitos de sistema de gestão, requisitos contratuais, códigos de conduta setoriais ou outros arranjos planejados aplicáveis.

No caso de quaisquer mudanças nos objetivos de auditoria, no escopo ou nos critérios convém que o programa de auditoria seja modificado, se necessário.

Quando dois ou mais sistemas de gestão de diferentes disciplinas são auditados juntos (uma auditoria combinada), é importante que os objetivos, escopo e critérios da auditoria sejam consistentes com os objetivos dos programas de auditoria pertinentes.

5.4.3 Selecionando os métodos da auditoria

Convém que a pessoa que gerencia o programa de auditoria selecione e determine os métodos para realizar de forma eficaz uma auditoria, dependendo dos objetivos, escopo e critérios definidos da auditoria.

NOTA Diretrizes sobre como determinar os métodos de auditoria, são dadas no anexo B.

Quando duas ou mais organizações auditoras realizam uma auditoria conjunta do mesmo auditado, convém que as pessoas que gerenciam os diferentes programas de auditoria, concordem com o método de auditoria e considerem as implicações dos recursos e planejamento de auditoria. Se uma organização auditada opera dois ou mais sistemas de gestão de diferentes disciplinas, auditorias combinadas podem ser incluídas no programa da auditoria.

5.4.4 Selecionando os membros da equipe da auditoria

Convém que a pessoa que gerencia o programa de auditoria indique os membros da equipe de auditoria incluindo o auditor líder e quaisquer especialistas necessários para a auditoria específica.

Convém que uma equipe de auditoria seja selecionada levando em consideração a competência necessária para atingir os objetivos de uma auditoria individual dentro do escopo definido. Se existe apenas um único auditor, convém que o auditor desempenhe todas as responsabilidades de um auditor líder aplicáveis.

NOTA A Seção 7 contém diretrizes sobre a determinação da competência requerida para os membros da equipe de auditoria e descreve os processos para avaliação de auditores.

Ao decidir o tamanho e composição da equipe de auditoria para uma auditoria especifica, convém que sejam considerado o seguinte:

a) a competência global da equipe de auditoria necessária para atingir os objetivos de auditoria, levando em consideração o critério e escopo de auditoria;

b) complexidade da auditoria e se ela é uma auditoria combinada ou conjunta;

c) os métodos da auditoria que foram selecionados;

d) requisitos legais e contratuais e outros requisitos com os quais a organização esteja comprometida;

e) a necessidade de assegurar a independência dos membros da equipe de auditoria das atividades a serem auditadas e evitar qualquer conflito de interesse [ver princípio e) da Seção 4];

f) capacidade dos membros da equipe de auditoria para interagir de forma eficaz com os representantes do auditado e para trabalharem em conjunto;

g) o idioma da auditoria, e as características culturais e sociais do auditado. Estes tópicos podem ser considerados ou pelas habilidades próprias do auditor ou através do apoio de um especialista.

Para assegurar uma competência global da equipe de auditoria, convém que os seguintes passos sejam realizados:

— identificação do conhecimento e habilidades necessários para atingir os objetivos da auditoria;

— seleção dos membros da equipe de auditoria de tal modo que a equipe de auditora tenha todo o conhecimento e habilidades necessários.

Caso toda a competência necessária não seja coberta pelos auditores da equipe de auditoria, convém que os especialistas com competências individuais sejam incluídos na equipe. Convém que os especialistas operem sob a orientação de um auditor, porém não podem atuar como auditores.

Auditores em treinamento podem ser incluídos na equipe de auditoria, porém convém que ele participe sob a orientação e diretrizes de um auditor.

Ajustes ao tamanho e composição da equipe de auditoria podem ser necessários durante a auditoria, por exemplo, se surgir conflito de interesses ou questões de competências Em tal situação surgir, convém que ela seja discutida com as partes apropriadas (por exemplo, o líder da equipe de auditoria, a pessoa que gerencia o programa de auditoria, o cliente da auditoria ou o auditado) antes que quaisquer ajustes sejam feitos.

5.4.5 Atribuindo responsabilidades para uma auditoria individual ao líder da equipe da auditoria

Convém que a pessoa que gerencia o programa de auditoria atribua a responsabilidade para conduzir a auditoria individual, a um auditor líder.

Convém que esta atribuição seja feita com uma antecedência suficiente da data programada para a auditoria a fim de assegurar um planejamento eficaz da auditoria.

Para assegurar a realização eficaz de auditorias individuais, convém que as seguintes informações sejam fornecidas ao auditor líder:

a) objetivos da auditoria;

b) critérios da auditoria e quaisquer documentos de referencia;

c) escopo da auditoria incluindo identificação das unidades organizacionais e funcionais e dos processos a serem auditados;

d) procedimentos e métodos de auditoria;

e) composição da equipe auditora;

f) detalhes dos contatos do auditado, as localizações, as datas e a duração das atividades da auditoria a ser realizada;

g) alocação de recursos apropriados para realizar a auditoria;

h) informações necessárias para a avaliação e consideração dos riscos identificados para atingir os objetivos de auditoria.

Convém que as informações de atribuição também considerem o seguinte, conforme apropriado:

— idioma do relatório e do trabalho da auditoria, quando existir diferença do idioma do auditor ou do auditado, ou ambos;

— conteúdo do relatório da auditoria e a sua distribuição requerida pelo programa de auditoria;

— assuntos relativos a confidencialidade e segurança da informação, quando requeridos pelo programa de auditoria;

— quaisquer requisitos de saúde e segurança pessoal para os auditores;

— quaisquer requisitos de autorização e segurança;

— quaisquer ações de acompanhamento, por exemplo, de auditorias anteriores, se aplicável;

— coordenação com outras atividades de auditoria, no caso de auditoria conjunta.

Quando uma auditoria conjunta é realizada, é importante obter um acordo, antes da auditoria iniciar, entre as organizações que vão realizar a auditoria, sobre as responsabilidades especificas de cada parte, especialmente com relação à autoridade do auditor líder indicado para auditoria.

5.4.6 Gerenciando os resultados do programa da auditoria

Convém que a pessoa que gerencia o programa de auditoria assegure que as seguintes atividades são desempenhadas:

— análise critica e aprovação dos relatórios de auditoria, incluindo avaliação da adequação e pertinência das constatações da auditoria;

— análise critica da causa raiz e a eficácia de ações corretivas e ações preventivas;

— distribuição dos relatórios de auditoria para alta direção e outras partes pertinentes;

— determinação da necessidade para qualquer auditoria de acompanhamento.

5.4.7 Gerenciando e mantendo registros do programa de auditoria

Convém que a pessoa que gerencia o programa de auditoria assegure que os registros de auditoria são criados, gerenciados, e mantidos para demonstrar a implementação do programa de auditoria. Convém que os processos sejam estabelecidos para assegurar que quaisquer necessidades de confidencialidade associadas com os registros de auditoria, sejam consideradas.

Convém que os registros incluam o seguinte:

a) registros relacionados ~~com~~ ao programa de auditoria, tais como:

— abrangência e objetivos do programa de auditoria documentados;

— aqueles voltados para os riscos do programa de auditoria;

— analises criticas da eficácia do programa de auditoria;

b) registros relativos a cada auditoria individual, tais como:

— planos de auditoria e relatórios de auditoria;

— relatórios de não-conformidade;

— relatórios de ações corretivas e preventivas;

— relatórios de auditoria de acompanhamento, se aplicável;

c) registros relativos ao pessoal da auditoria cobrindo tópicos, tais como:

— avaliação da competência e desempenho dos membros da equipe auditora;

— seleção das equipes auditoras e dos membros da equipe;

— manutenção e melhoria da competência.

Convém que a forma e o nível de detalhes dos registros demonstrem que os objetivos do programa de auditoria foram atingidos.

5.5 Monitorando o programa de auditoria

Convém que a pessoa que gerencia o programa de auditoria monitore a sua implementação considerando a necessidade de:

a) avaliar a conformidade com programas de auditoria, planejamentos e objetivos da auditoria;

b) avaliar o desempenho dos membros da equipe auditora;

c) avaliar a capacidade das equipes auditoras para implementar o plano de auditoria;

d) avaliar a retroalimentação da alta direção, auditados, auditores e outras partes interessadas.

Alguns fatores podem determinar a necessidade de modificar o programa de auditoria, tais como

— constatações da auditoria;

— nível demonstrado de eficácia do sistema de gestão;

— mudanças do sistema de gestão do auditado ou do cliente;

— mudanças com relação aos requisitos das normas, requisitos legais e contratuais e outros requisitos aos com os quais a organização esteja comprometida;

— mudança de fornecedor.

5.6 Analisando criticamente e melhorando o programa de auditoria

Convém que a pessoa que gerencia um programa de auditoria analise criticamente o programa de auditoria para verificar se seus objetivos foram atendidos. Convém que lições aprendidas da analise critica do programa de auditoria sejam usadas como dados de entrada para o processo de melhoria continua do programa.

Convém que a analise critica do programa de auditoria considere o seguinte:

a) resultados e tendências do monitoramento do programa de auditoria;

b) conformidade com os procedimentos do programa de auditoria;

c) evolução de necessidades e expectativas de partes interessadas;

d) registros do programa de auditoria;

e) alternativas ou novos métodos de auditoria;

f) eficácia de medidas para considerar os riscos associados com o programa de auditoria;

g) questões de confidencialidade e segurança da informação relativos ao programa de auditoria

Convém que a pessoa que gerencia o programa de auditoria analise criticamente a implementação global do programa de auditoria, identifique áreas de melhorias, altere o programa se necessário e também considere:

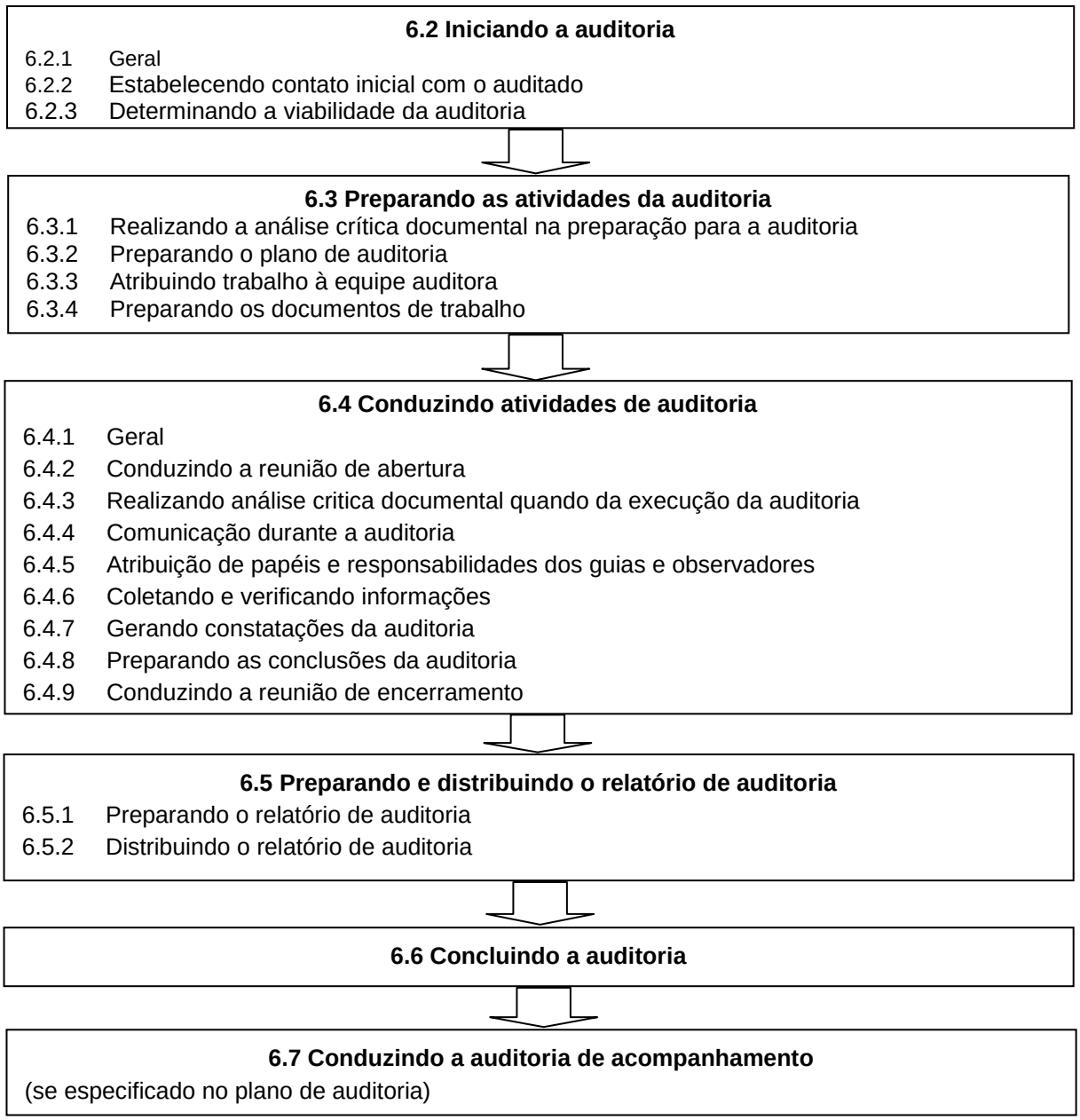
— análise crítica do contínuo desenvolvimento profissional dos auditores,de acordo com 7.4, 7.5 e 7.6;

— relato da análise crítica dos resultados do programa de auditoria para a alta direção.

6 Executando uma auditoria

6.1 Geral

Esta seção contém orientações sobre como planejar e realizar as atividades de auditoria como parte de um programa de auditoria. A figura 2 fornece uma visão geral das atividades típicas de auditoria. A abrangência na qual as disposições desta seção são aplicáveis depende dos objetivos e escopo da auditoria específica.



NOTA: A numeração dos subseções refere-se às subseções pertinentes desta norma.

Figura 2 — Atividades típicas de auditoria

6.2 Iniciando a auditoria

6.2.1 Geral

Quando uma auditoria é iniciada, a responsabilidade para conduzir a auditoria é do auditor líder da equipe designado (ver 5.4.5), até que auditoria esteja concluída (ver 6.6).

Para iniciar uma auditoria convém que os passos da figura 2 sejam considerados; entretanto, a seqüência pode variar dependendo do auditado, do processos e das circunstâncias especificas da auditoria.

6.2.2 Estabelecendo contato inicial com o auditado

O contato inicial com o auditado para a realização da auditoria pode ser formal ou informal e convém que seja feito pelo auditor líder. São os seguintes os propósitos do contato inicial:

— estabelecer a comunicação com os representantes do auditado;

— confirmar a autoridade que vai conduzir a auditoria;

— prover informações sobre os objetivos da auditoria, escopo, métodos e composição da equipe auditora, incluindo os especialistas;

— solicitar acesso a registros e documentos pertinentes para fins de planejamento;

— determinar os requisitos contratuais e legais aplicáveis e outros requisitos pertinentes às atividades e produtos do auditado;

— confirmar o acordo com o auditado quanto à abrangência da divulgação e tratamento das informações confidenciais;

— fazer arranjos para a auditoria incluindo a programação de datas;

— determinar quaisquer requisitos específicos para acesso aos locais, segurança, saúde, segurança pessoal ou outros;

— acordar sobre a participação de observadores e a necessidade de guias para a equipe de auditoria;

— determinar quaisquer áreas de interesse ou preocupação para o auditado em relação à auditoria especifica.

6.2.3 Determinando a viabilidade da auditoria

Convém que a viabilidade da auditoria seja determinada para fornecer confiança razoável de que os objetivos da auditoria podem ser atingidos.

Convém que a determinação da viabilidade leve em consideração a disponibilidade dos seguintes fatores:

— informações suficientes e apropriadas para o planejamento e realização da auditoria;

— cooperação adequada do auditado;

— tempo e recursos adequados para a realização da auditoria.

Quando a auditoria não é viável, convém que seja proposta uma alternativa ao cliente da auditoria, em acordo com o auditado.

6.3 Preparando as atividades da auditoria

6.3.1 Realizando a análise crítica documental na preparação para a auditoria

Convém que a documentação pertinente do sistema de gestão do auditado seja analisada criticamente para:

— obter informações para preparar as atividades da auditoria e os documentos de trabalho aplicáveis (ver 6.3.4), por exemplo, sobre processos, funções;

— estabelecer uma visão da abrangência da documentação do sistema para detectar possíveis lacunas.

NOTA Diretriz sobre como realizar uma análise crítica documental é fornecida na Seção B.2

Convém que a documentação inclua, quando aplicável, registros e documentos do sistema de gestão, bem como relatórios de auditorias anteriores. Convém que a análise crítica documental leve em conta o tamanho, natureza e complexidade da organização e do sistema de gestão do auditado, bem como o escopo e objetivos da auditoria.

6.3.2 Preparando o plano de auditoria

6.3.2.1 Convém que o líder de equipe da auditoria prepare um plano de auditoria baseado nas informações contidas no programa da auditoria e na documentação fornecida pelo auditado. Convém que o plano de auditoria considere o efeito das atividades da auditoria sobre os processos do auditado e forneça a base para um acordo entre o cliente da auditoria, a equipe da auditoria e o auditado com relação á condução da auditoria. Convém que o plano facilite a coordenação e a programação eficientes das atividades da auditoria de modo a atingir os objetivos de forma eficaz.

Convém que a quantidade de detalhes fornecida no plano de auditoria reflita o escopo e a complexidade da auditoria, bem como o efeito da incerteza em atingir os objetivos da auditoria. Na preparação do plano da auditoria, convém que o auditor líder esteja consciente dos seguintes pontos:

— as técnicas apropriadas de amostragem (ver Seção B.3);

— a composição da equipe auditora e sua competência coletiva;

— os riscos para a organização gerados pela auditoria.

Por exemplo, os riscos para a organização podem resultar da presença de membros de equipe auditora influenciando a saúde e segurança, a qualidade e o meio ambiente, e suas presenças podem representar ameaças aos produtos do auditado, serviços, pessoal ou infra-estrutura (por exemplo, contaminação em instalações que requerem salas limpas).

Para auditorias combinadas, convém que atenção particular seja dada às interações entre os processos operacionais e os objetivos e prioridades concorrentes dos diferentes sistemas de gestão.

6.3.2.2 A escala e conteúdo do plano de auditoria podem divergir, por exemplo, entre as auditorias iniciais e subseqüentes, bem como entre as auditorias internas e externas. Convém que o plano de auditoria seja suficientemente flexível para permitir mudanças que podem se tornar necessárias na medida em que as atividades da auditoria progridam.

Convém que o plano de auditoria inclua ou referencie o seguinte:

a) os objetivos da auditoria;

b) o escopo da auditoria, incluindo identificação das unidades organizacionais e funcionais, bem como os processos a serem auditados;

c) os critérios de auditoria e quaisquer documentos de referência;

d) as localizações, datas, tempos estimados e duração das atividades da auditoria a serem realizadas, incluindo as reuniões com a direção do auditado;

e) os métodos de auditoria a serem usados, incluindo a abrangência na qual a amostragem da auditoria é necessária para obter suficiente evidencia da auditoria e propósito do plano de amostragem, se aplicável;

f) os papéis e responsabilidades dos membros da equipe da auditoria, bem como dos guias e observadores;

g) a alocação de recursos apropriados para áreas críticas da auditoria.

Convém que o plano de auditoria também inclua o seguinte, se apropriado:

— identificação do representante do auditado na auditoria;

— o idioma de trabalho e do relatório da auditoria, se ele for diferente do idioma do auditor ou do auditado ou ambos;

— os tópicos do relatório de auditoria;

— preparativos de logística e de comunicação, incluindo preparativos específicos para os locais a serem auditados;

— quaisquer medidas específicas a serem tomadas para considerar o efeito da incerteza em atingir os objetivos da auditoria;

— assuntos relacionados à confidencialidade e segurança da informação;

— quaisquer ações de acompanhamento de auditorias anteriores;

— quaisquer atividades de acompanhamento para a auditoria planejada;

— coordenação com outras atividades de auditoria, no caso de auditoria conjunta.

O plano de auditoria pode ser analisado criticamente e aceito pelo cliente da auditoria e convém que seja apresentado para o auditado. Convém que quaisquer objeções pelo auditado sobre o plano da auditoria sejam solucionadas entre o líder da equipe da auditoria, o auditado e o cliente da auditoria.

6.3.3 Designando o trabalho para a equipe da auditoria

Convém que o líder de equipe de auditoria, em consulta com a equipe de auditoria, atribua responsabilidade a cada membro da equipe para auditar processos específicos, atividades, funções ou localidades. Convém que tais tarefas levem em conta a independência e competência de auditores e o uso eficaz de recursos, como também funções e responsabilidades diferentes de auditores, auditores em treinamento e especialistas.

Convém que as instruções à equipe de auditoria sejam mantidas, conforme apropriado, pelo líder da equipe de modo a alocar atribuições de trabalho e decidir sobre possíveis mudanças. As mudanças das atribuições do trabalho podem ser feitas a medida em que a auditoria progride para assegurar o cumprimento dos objetivos da auditoria.

6.3.4 Preparando documentos de trabalho

Convém que os membros da equipe de auditoria coletem e analisem criticamente as informações pertinentes às suas tarefas de auditoria e preparem documentos de trabalho, se necessário, para referência e registro de evidencia da auditoria. Tais documentos de trabalho podem incluir o seguinte:

— listas de verificação;

— planos de amostragem de auditoria;

— formulários para registro de informação, tais como evidências de suporte, constatações da auditoria e registros de reuniões.

Convém que o uso de listas de verificação e formulários não se restrinjam à abrangência das atividades da auditoria, os quais podem mudar como um resultado das informações coletadas durante a auditoria.

NOTA Diretriz sobre preparação de documentos de trabalho é apresentada na Seção B.4.

Convém que documentos de trabalho, incluindo registros resultantes de seu uso, sejam retidos no mínimo até a conclusão da auditoria ou como especificados no plano de auditoria. A retenção de documentos, depois da conclusão da auditoria, é descrita em 6.6. Convém que esses documentos que envolvam informações confidenciais ou proprietária, sejam salvaguardados adequadamente, a todo o momento, pelos membros da equipe de auditoria.

6.4 Conduzindo as atividades de auditoria

6.4.1 Geral

As atividades de auditoria são normalmente realizadas em uma seqüência definida conforme indicado na Figura 2. Esta seqüência pode ser variada para atender a circunstancias de auditorias especificas.

6.4.2 Conduzindo a reunião de abertura

O propósito de uma reunião de abertura é para:

a) confirmar o acordo de todas as partes (por exemplo, auditado, equipe auditora) quanto ao plano de auditoria;

b) apresentar a equipe auditora,

c) assegurar que todas as atividades planejadas da auditoria podem ser realizadas.

Convém que uma reunião de abertura seja realizada com a direção do auditado e, onde apropriado, com os responsáveis pelas funções ou processos a serem auditados. Durante a reunião convém que uma oportunidade para realizar perguntas seja dada.

Convém que o grau de detalhe seja consistente com a familiaridade do auditado com o processo de auditoria. Em muitas situações, por exemplo, em auditorias internas em uma pequena organização, a reunião de abertura pode simplesmente consistir em comunicar que uma auditoria está sendo realizada e explicar a natureza da auditoria.

Para outras situações de auditoria, a reunião pode ser formal e convém que os registros de presença sejam mantidos. Convém que a reunião seja presidida pelo líder da equipe de auditoria e que os seguintes pontos sejam considerados, se apropriado:

— apresentação dos participantes, incluindo observadores e guias e um resumo de suas funções;

— confirmação dos objetivos, escopo e critérios da auditoria;

— confirmação do plano de auditoria e outros ajustes pertinentes com o auditado, tais como o dia e hora da reunião de encerramento, e quaisquer reuniões intermediarias entre a equipe auditora e a direção do auditado, bem como quaisquer mudanças de última hora;

— apresentação dos métodos a serem usados para realizar auditoria, incluindo a informação ao auditado de que a evidencia da auditoria será baseada na amostragem da informação disponível;

— apresentação dos métodos para gerenciar os riscos para a organização, que podem resultar da presença dos membros da equipe auditora;

— confirmação dos canais formais de comunicação entre a equipe da auditoria e o auditado;

— confirmação do idioma a ser usado durante a auditoria;

— confirmação de que, durante a auditoria, o auditado será mantido informado do progresso da auditoria;

— confirmação de que os recursos e instalações necessários à equipe da auditoria estão disponíveis;

— confirmação de assuntos relativos à confidencialidade e segurança da informação;

— confirmação de procedimentos pertinentes de saúde, segurança no trabalho, emergência e segurança física para a equipe da auditoria;

— informação sobre o método de relatar as constatações de auditoria incluindo as classificações, se existirem;

— informações sobre condições nas quais a auditoria pode ser encerrada;

— informações sobre a reunião de encerramento;

— informações sobre como tratar as possíveis constatações encontradas durante a auditoria;

— informações sobre qualquer sistema para retroalimentação do auditado sobre as constatações ou conclusões da auditoria, incluindo reclamações ou apelações.

6.4.3 Executando a análise crítica da documentação durante a realização da auditoria

Convém que a documentação pertinente do auditado seja analisada criticamente para:

— determinar conformidade do sistema, tanto quanto documentado, com os critérios da auditoria;

— obter informações para apoiar as atividades da auditoria.

NOTA Orientação sobre como realizar análise crítica documental são fornecidas na Seção B.2

A análise crítica pode ser combinada com outras atividades da auditoria e pode continuar ao longo da auditoria, desde que isto não seja prejudicial para a eficácia da realização da auditoria.

Se a documentação adequada não puder ser fornecida dentro do tempo dado no plano de auditoria, convém que o líder da equipe auditora informe tanto a pessoa que gerencia o programa de auditoria quanto o auditado. Dependendo dos objetivos e escopo da auditoria, convém que uma decisão seja tomada sobre se a auditoria deve ser continuada ou suspensa, até que a documentação pertinente seja resolvida.

6.4.4 Comunicação durante a auditoria

Durante a auditoria, pode ser necessário fazer acordos formais para comunicação com a equipe da auditoria, como também com o auditado, o cliente da auditoria e, potencialmente, com entidades externas (por exemplo, órgãos regulatórios) especialmente onde requisitos legais exijam relatórios mandatórios de não conformidades.

Convém que a equipe de auditoria se comunique periodicamente para trocar informações, avaliar o progresso da auditoria, e redistribuir o trabalho entre os membros da equipe da auditoria, conforme necessário.

Durante a auditoria, convém que o líder da equipe de auditoria periodicamente comunique o progresso da auditoria e quaisquer questões ao auditado e ao cliente da auditoria, como apropriado. Convém que a evidência coletada durante a auditoria que indique um risco imediato e significativo para o auditado, seja relatada sem demora ao auditado e, como apropriado, ao cliente da auditoria. Convém que qualquer consideração sobre um assunto fora do escopo da auditoria seja anotada e seja relatada ao líder da equipe da auditoria, para possível comunicação ao cliente da auditoria e o auditado.

Quando a evidência da auditoria disponível indica que os objetivos da auditoria são inatingíveis, convém que o líder da equipe da auditoria relate as razões ao cliente da auditoria e ao auditado para definir a ação apropriada. Tal ação pode incluir a reconfirmação ou a modificação do plano de auditoria, mudanças nos objetivos da auditoria ou o seu escopo ou o seu encerramento

Qualquer necessidade de mudanças no plano da auditoria que possam se tornar aparente à medida em que a auditoria progride, convém que seja analisada criticamente e aprovada e, quando apropriado, pela pessoa que gerencia o programa de auditoria e pelo auditado.

6.4.5 Atribuindo papéis e responsabilidades dos guias e observadores

Guias e observadores (por exemplo, órgão regulatório ou outras partes interessadas) podem acompanhar a equipe de auditoria. Convém que eles não influenciem ou interfiram na realização da auditoria. Se isto não puder ser assegurado, convém que o líder da equipe da auditoria tenha o direito de negar aos observadores, a sua participação em certas atividades da auditoria.

Para os observadores, convém que quaisquer obrigações em relação à saúde e segurança pessoal, segurança e confidencialidade, sejam gerenciadas entre o cliente da auditoria e o auditado.

Convém que os guias designados pelo auditado prestem ajuda à equipe da auditoria e ajam por solicitação do líder da equipe da auditoria. Convém que suas responsabilidades incluam o seguinte:

a) apoiar os auditores na identificação de pessoas para participar das entrevistas e confirmar os horários;

b) providenciar acesso a locais específicos do auditado;

c) assegurar que regras relativas a segurança no local e procedimentos de segurança, sejam conhecidos e respeitados pelos membros da equipe auditora e observadores.

O papel do guia pode também incluir o seguinte:

— testemunhar a auditoria em nome do auditado;

— fornecer esclarecimento ou ajuda na coleta de informações.

6.4.6 Coletando e verificando informações

Convém que durante a auditoria, as informações pertinentes aos objetivos, escopo e critérios da auditoria, incluindo informações relativas às interfaces entre funções, atividades e processos, sejam coletadas por meio de amostragem apropriada e sejam verificadas. Convém que somente informação que seja verificável seja aceita como evidência de auditoria. Convém que as evidências de auditoria que levam às constatações da auditoria, sejam registradas. Se durante a coleta de evidências, a equipe de auditoria ficar ciente de riscos ou circunstâncias novos ou modificados convém que estas constatações sejam consideradas apropriadamente pela equipe

NOTA 1 Diretrizes sobre amostragem são apresentadas na Seção B.3

A Figura 3 fornece uma visão geral do processo de uma auditoria desde a coleta de informações até as conclusões da auditoria.

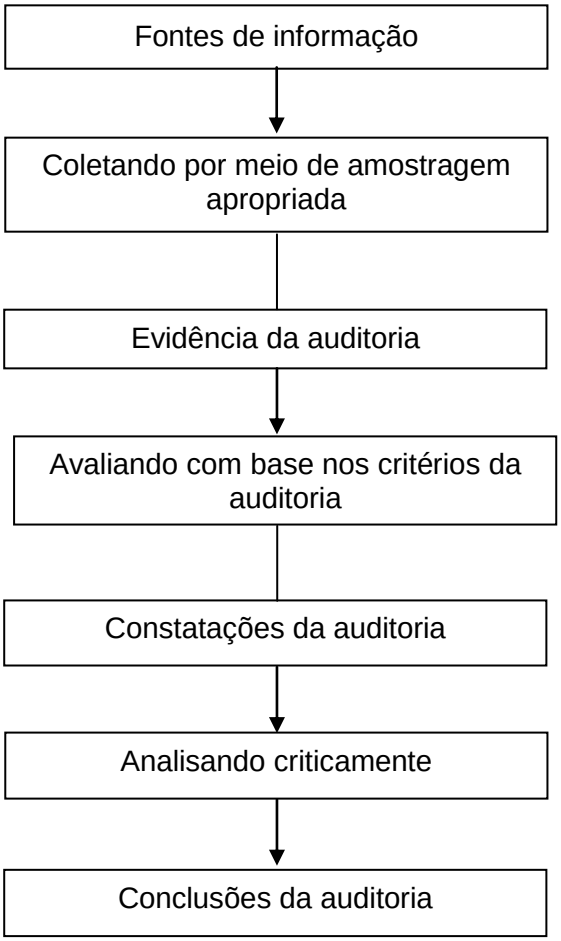


Figura 3 — Visão geral do processo de coleta e verificação de informações

Métodos para coletar informações incluem o seguinte:

— entrevistas;

— observações;

— análise crítica de documentos, incluindo registros.

NOTA 2 Diretrizes sobre fontes de informação são apresentadas na Seção B.5.

NOTA 3 Diretrizes sobre visita aos locais do auditado são apresentadas na Seção B.6.

NOTA 4 Diretrizes sobre como conduzir entrevistas são apresentadas na Seção B.7.

6.4.7 Gerando constatações de auditoria

Convém que as evidências de auditoria sejam avaliadas de acordo com os critérios de auditoria a fim de determinar as constatações da auditoria. Constatações da auditoria podem indicar tanto conformidade quanto não conformidade com os critérios de auditoria. Quando especificado pelo plano de auditoria, convém que as constatações de auditoria individual incluam a conformidade e boas práticas ao longo

das suas evidências de apoio, oportunidades para melhoria e quaisquer recomendações para o auditado.

Convém que sejam registradas as não conformidades e as evidências de auditoria que as suportam. Não conformidades podem ser classificadas. Convém que elas sejam analisadas criticamente com o auditado para obter o reconhecimento de que a evidência de auditoria é precisa e que as não conformidades são entendidas. Convém que todo empenho seja feito para solucionar qualquer opinião divergente relativa às evidências ou constatações da auditoria, e convém que sejam registrados os pontos não resolvidos.

Convém que a equipe auditora atenda às necessidades para analisar criticamente as constatações de auditoria, em estágios apropriados durante a auditoria.

NOTA Diretrizes adicionais sobre a identificação e avaliação das constatações de auditoria são apresentadas na Seção B.8

6.4.8 Preparando as conclusões da auditoria

Convém que a equipe da auditoria se comunique anteriormente à reunião de encerramento, para:

a) analisar criticamente as constatações da auditoria e quaisquer outras informações apropriadas coletadas durante a auditoria, de acordo com os seus objetivos;

b) acordar quanto às conclusões da auditoria, levando em conta a incerteza inerente ao processo de auditoria;

c) preparar recomendações, se especificado pelo plano de auditoria;

d) discutir sobre a auditoria de acompanhamento, se aplicável.

Conclusões da auditoria podem apontar assuntos tais como:

— a abrangência da conformidade com os critérios da auditoria e a robustez do sistema de gestão, incluindo a eficácia do sistema de gestão para atender os objetivos declarados;

— a implementação eficaz, manutenção e melhoria do sistema de gestão;

— a capacidade do processo de análise crítica pela direção para assegurar a contínua pertinência, adequação, eficácia e melhoria do sistema de gestão;

— o atingimento dos objetivos de auditoria, cobrindo o escopo de auditoria e atendendo o critério de auditoria;

— causas raiz das constatações, se incluído no plano da auditoria;

— constatações similares feitas em diferentes áreas que foram auditadas com o propósito de identificar tendências.

Se especificado pelo plano de auditoria, as conclusões da auditoria podem conduzir a recomendações para melhoria ou atividades futuras de auditoria.

6.4.9 Conduzindo a reunião de encerramento

Convém que seja realizada uma reunião de encerramento pelo líder da equipe da auditoria, para apresentar as constatações e conclusões da auditoria. Convém que a direção do auditado seja incluída como participante na reunião de encerramento e, onde apropriado os responsáveis pelas funções ou processos que foram auditados, podendo incluir o cliente da auditoria e outras partes. Se aplicável, convém que o líder da equipe da auditoria alerte o auditado sobre situações encontradas durante a auditoria, que podem diminuir a confiança colocada nas conclusões da auditoria. Se for definido no sistema de gestão ou pelo acordo com o cliente da auditoria, convém que os participantes concordem com o prazo do plano de ação relativo às constatações da auditoria.

Convém que o grau de detalhe seja consistente com a familiaridade do auditado com o processo da auditoria. Para algumas situações da auditoria, a reunião pode ser formal e com atas, e convém que as listas de presença sejam guardadas. Em outras circunstâncias, por exemplo, auditorias internas, a reunião de encerramento é menos formal e pode consistir apenas da comunicação das constatações e das conclusões da auditoria.

Se apropriado, convém que os seguintes pontos sejam explicados ao auditado na reunião de encerramento:

— advertir que a evidência da auditoria coletada foi baseada na amostragem das informações disponíveis;

— o método de relato;

— o processo de manuseio das constatações da auditoria e possíveis conseqüências;

— apresentação das conclusões e constatações da auditoria de tal modo que elas sejam conhecidas e entendidas pela direção do auditado;

— quaisquer atividades relativas ä pós-auditoria (por exemplo, implementação de ações corretivas, tratamento de reclamações de auditoria, processo de apelação)

Convém que quaisquer opiniões divergentes relativas às conclusões ou constatações da auditoria entre a equipe da auditoria e o auditado sejam discutidas e, se possível, resolvidas. Se não forem resolvidas, convém que sejam registradas.

Se especificado pelos objetivos da auditoria, podem ser apresentadas recomendações para melhorias. Convém que seja enfatizado que as recomendações não são obrigatórias.

6.5 Preparando e distribuindo o relatório de auditoria

6.5.1 Preparando o relatório de auditoria

Convém que o líder de equipe da auditoria relate os resultados da auditoria de acordo com os procedimentos do programa de auditoria.

Convém que o relatório da auditoria forneça um registro completo, preciso, conciso e claro da auditoria, e que inclua ou se refira ao seguinte:

a) os objetivos da auditoria;

b) o escopo da auditoria, particularmente a identificação das unidades organizacionais e funcionais ou os processos auditados;

c) identificação do cliente da auditoria;

d) identificação da equipe da auditoria e dos participantes do auditado na auditoria;

e) as datas e locais onde as atividades da auditoria foram realizadas;

f) os critérios da auditoria;

g) as constatações da auditoria e as evidências relacionadas;

h) as conclusões da auditoria;

i) uma declaração sobre o grau no qual os critérios de auditoria foram atendidos.

O relatório da auditoria também pode incluir ou pode se referir ao seguinte, se apropriado:

— o plano de auditoria incluindo a programação;

— um resumo do processo de auditoria incluindo obstáculos encontrados que possam diminuir a confiabilidade das conclusões da auditoria;

— a confirmação de que os objetivos da auditoria foram atendidos dentro do escopo da auditoria e de acordo com o plano de auditoria;

— quaisquer áreas dentro do escopo da auditoria não cobertas;

— um resumo cobrindo as conclusões da auditoria e as principais constatações da auditoria que os suportam;

— quaisquer opiniões divergentes e não resolvidas entre a equipe da auditoria e o auditado;

— oportunidades para melhoria, se especificado do plano de auditoria;

— boas práticas identificadas;

— o plano de ação de acompanhamento negociado, se existir;

— uma declaração da natureza confidencial dos conteúdos;

— quaisquer implicações para o programa da auditoria ou auditorias subseqüentes;

— a lista de distribuição do relatório de auditoria.

NOTA O relatório de auditoria pode ser desenvolvido antes da reunião de encerramento.

6.5.2 Distribuindo o relatório da auditoria

Convém que o relatório da auditoria seja emitido dentro de um período de tempo acordado. Se ele estiver atrasado, convém que as razões sejam comunicadas ao auditado e a pessoa que gerencia o programa de auditoria.

Convém que o relatório da auditoria seja datado, analisado criticamente e aprovado conforme apropriado, de acordo com os procedimentos do programa de auditoria.

Convém que o relatório de auditoria seja, então, distribuído às pessoas conforme definido nos procedimentos de auditoria ou no plano de auditoria.

6.6 Concluindo a auditoria

A auditoria está concluída quando todas as atividades planejadas da auditoria forem realizadas, ou de outra forma acordadas com o cliente da auditoria (por exemplo, pode haver uma situação não esperada que impeça a auditoria de ser concluída de acordo com o plano).

Convém que os documentos pertencentes à auditoria sejam retidos ou destruídos, conforme acordo entre as partes participantes e de acordo com os procedimentos do programa de auditoria e requisitos aplicáveis.

A menos que requerido por lei, convém que a equipe de auditoria e a pessoa que gerencia o programa de auditoria não revelem o conteúdo de documentos, quaisquer outras informações obtidas durante a auditoria, ou o relatório da auditoria, para qualquer outra parte, sem a aprovação explícita do cliente da auditoria e, onde apropriado, a aprovação do auditado. Se a revelação do conteúdo de um documento de auditoria for solicitada, convém que o cliente da auditoria e o auditado sejam informados o mais cedo possível.

Convém que lições aprendidas da auditoria sejam usadas no processo de melhoria continua do sistema de gestão das organizações auditadas.

6.7 Conduzindo ações de acompanhamento da auditoria

As conclusões da auditoria podem, dependendo dos objetivos da auditoria, indicar a necessidade para as correções ou ações corretivas, preventivas ou de melhoria. Tais ações são normalmente decididas e realizadas pelo auditado dentro de um período de tempo acordado. Se apropriado, convém que o auditado mantenha a pessoa que gerencia o programa de auditoria e a equipe auditora informada da situação dessas ações.

Convém que sejam verificadas a completeza e a eficácia das ações. Esta verificação pode ser parte de uma auditoria subseqüente.

7 Competência e avaliação de auditores

7.1 Geral

A confiança no processo de auditoria e a capacidade para atender seus objetivos dependem da competência dos indivíduos que estão envolvidos no planejamento e na realização das auditorias, incluindo os auditores e os líderes da equipe auditora. Convém que a competência seja avaliada por meio de um processo que considere o comportamento pessoal e a capacidade para aplicar conhecimento e habilidades, obtidas por meio da educação, experiência no trabalho, treinamento de

auditor e experiência de auditoria. Convém que este processo leve em consideração as necessidades do programa de auditoria e seus objetivos. Alguns dos conhecimentos e habilidades descritos em 7.2.3 são comuns para auditores de quaisquer disciplinas de sistema de gestão; outros são específicos de disciplinas de sistema de gestão individual. Não é necessário para cada auditor na equipe auditora ter a mesma competência; entretanto, a competência global da equipe da auditoria precisa ser suficiente para atingir os objetivos da auditoria.

Convém que a avaliação da competência do auditor seja planejada, implementada e documentada de acordo com o programa da auditoria, incluindo seus procedimentos para fornecer um resultado que seja objetivo, consistente, justo e confiável. Convém que o processo de avaliação inclua quatro passos mostrados a seguir:

a) determinar a competência do pessoal da auditoria para atender as necessidades do programa da auditoria;

b) b) estabelecer o critério de avaliação;

c) c) selecionar o método apropriado de avaliação;

d) d) realizar a avaliação.

Convém que o resultado do processo de avaliação forneça uma base para o seguinte:

— seleção dos membros da equipe auditora, conforme descrito em 5.4.4;

— determinação da necessidade para melhoria da competência (por exemplo, treinamento adicional);

— avaliação contínua do desempenho dos auditores.

Convém que os auditores desenvolvam, mantenham e melhorem suas competências através de um desenvolvimento profissional continuo e participação regular em auditorias (ver 7.6).

Um processo para avaliação dos auditores e líderes da equipe auditora está descrito em 7.4 e 7.5.

Convém que os auditores e os líderes da equipe auditora sejam avaliados com base nos critérios definidos em 7.2.2 e 7.2.3.

A competência requerida da pessoa que gerencia o programa de auditoria está descrita em 5.3.2.

7.2 Determinando competência do auditor para atender às necessidades do programa da auditoria

7.2.1 Geral

Ao decidir o conhecimento e habilidades apropriados requeridos do auditor, convém que sejam considerados o seguinte:

— o tamanho, natureza, e complexidade da organização a ser auditada;

— as disciplinas do sistema de gestão a ser auditado;

— os objetivos e a abrangência do programa de auditoria;

— outros requisitos tais como aqueles impostos por entidades externas, onde apropriados;

— o papel do processo da auditoria no sistema de gestão do auditado;

— a complexidade do sistema de gestão a ser auditado;

— a incerteza em atingir os objetivos de auditoria.

Convém que esta informação seja alinhada com aquelas listadas em 7.2.3.2, 7.2.3.3 e 7.2.3.4

7.2.2 Comportamento pessoal

Convém que os auditores possuam as qualidades necessárias para habilitá-los a agir de acordo com os princípios de auditoria conforme descrito na Seção 4. Convém que os auditores demonstrem comportamento profissional durante o desempenho das atividades de auditoria, incluindo os seguintes:

— ético, isto é, justo, verdadeiro, sincero, honesto e discreto;

— mente aberta, isto é, disposto a considerar idéias ou pontos de vista alternativos;

— diplomático, isto é, com tato para lidar com as pessoas;

— observador, isto é, estar atento à circunvizinhança e às atividades físicas;

— perceptivo, isto é, estar consciente e ser capaz de entender situações;

— versátil, isto é, ser capaz de prontamente se adaptar a diferentes situações;

— tenaz, isto é, persistente, focado em alcançar objetivos;

— decisivo, isto é, ser capaz de chegar a conclusões em tempo hábil, baseado em razões lógicas e análise;

— autoconfiante, isto é, ser capaz de agir e atuar independentemente, enquanto interage de forma eficaz com outros;

— agir com firmeza, isto é, ser capaz de atuar de forma ética e responsável, mesmo quando essas ações possam não ser sempre populares e possam algumas vezes resultar em desacordo ou confronto;

— aberto a melhorias, isto é, aprender a partir das situações e esforçar-se para obter melhores resultados da auditoria;

— sensibilidade cultural, isto é, observar e respeitar a cultura do auditado;

— colaborativo, isto é, interagir de forma eficaz com outros, incluindo, os membros da equipe auditora e o pessoal do auditado.

7.2.3 Conhecimentos e habilidades

7.2.3.1 Geral

Convém que os auditores possuam o conhecimento e habilidades necessários para atender aos resultados pretendidos das auditorias que eles irão realizar. Convém que todos os auditores possuam conhecimentos e habilidades genéricas e convém também que eles possuam conhecimentos e habilidades de disciplinas e setores específicos. Convém que os líderes da equipe auditora tenham conhecimento e habilidades adicionais necessárias para fornecer liderança à equipe auditora.

7.2.3.2 Conhecimento e habilidades genéricas de auditores de sistema de gestão

Convém que os auditores tenham conhecimento e habilidades nas áreas descritas abaixo:

a) **Princípios de auditoria, procedimentos e métodos**: conhecimento e habilidades nessa área permite ao auditor aplicar os princípios apropriados, procedimentos e métodos para diferentes auditorias, e para assegurar que as auditorias são realizadas de maneira consistente e sistemática. Convém que um auditor seja capaz de fazer o seguinte:

— aplicar princípios, procedimentos e métodos de auditoria;

— planejar e organizar o trabalho com eficácia;

— realizar a auditoria dentro da programação acordada;

— priorizar e enfocar os assuntos de importância;

— coletar informações através de entrevistas eficazes, escuta, observação e análise crítica de documentos, registros e dados;

— entender e considerar opiniões de especialistas;

— entender a conveniência e conseqüências de usar técnicas de amostragem para auditar;

— verificar a relevância e a precisão das informações coletadas;

— confirmar a suficiência e conveniência da evidência de auditoria para apoiar as constatações e conclusões da auditoria;

— avaliar aqueles fatores que possam afetar a confiabilidade das constatações e conclusões da auditoria;

— usar documentos de trabalho para registrar atividades de auditoria;

— documentar as constatações de auditoria e preparar os relatórios de auditoria apropriados;

— manter a confidencialidade e a segurança da informação, dados, documentos e registros;

— comunicar-se com eficácia, de forma oral e por escrito (tanto pessoalmente quanto pelo uso de interpretes e tradutores);

— entender os tipos de riscos associados com auditoria;

b) **Sistema de gestão e documentos de referência**: conhecimento e habilidades nessa área permite ao auditor compreender o escopo da auditoria e aplicar os critérios da auditoria, e convém que abranja o seguinte:

— normas do sistema de gestão ou outros documentos usados como critério de auditoria;

— a aplicação de normas do sistema de gestão pelo auditado e outras organizações, conforme apropriado;

— interação entre os componentes do sistema de gestão;

— reconhecimento da hierarquia dos documentos de referência;

— aplicação de documentos de referência a diferentes situações de auditoria.

c) **Contexto organizacional**: conhecimentos e habilidades nesta área permitem ao auditor compreender a estrutura do auditado, práticas de gestão e do negócio e convém que abranja o seguinte:

— tipos organizacionais, governança, tamanho, estrutura, funções e relacionamentos;

— conceitos de gestão e negócios em geral, processos e terminologia relacionada, incluindo planejamento, orçamento e gestão de pessoal;

— aspectos culturais e sociais do auditado.

d) **Requisitos legais e contratuais aplicáveis e outros requisitos que se aplicam ao auditado:** conhecimento e habilidades nessa área permite ao auditor estar consciente de, e trabalhar de acordo com os requisitos legais e contratuais da organização. Conhecimentos e habilidades específicas para a jurisdição ou para os produtos e atividades do auditado, convém que abranja o seguinte:

— leis e regulamentações e as agências que governam;

— terminologia legal básica;

— responsabilidade civil pelo fato do produto e contratação.

7.2.3.3 Conhecimento e habilidades de setores específicos e de disciplinas de auditores de sistema de gestão

Convém que os auditores tenham conhecimento e habilidades da disciplina e do setor específico que sejam apropriados para auditar o tipo particular do sistema de gestão e setor.

Não é necessário, para cada auditor na equipe auditora, ter a mesma competência; entretanto a competência global da equipe auditora precisa ser suficiente para atender os objetivos da auditoria.

Conhecimento e habilidades dos auditores na disciplina e setor específico inclui o seguinte:

— requisitos e princípios do sistema de gestão da disciplina específica e suas aplicações;

— requisitos legais pertinentes para a disciplina e o setor, de tal modo que o auditor esteja consciente dos requisitos específicos para a jurisdição e as obrigações do auditado, suas atividades e produtos;

— requisitos de partes interessadas pertinentes para a disciplina específica;

— fundamentos da disciplina e a aplicação de negócios e métodos técnicos específico da disciplina, técnicas, processos e práticas suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações da auditoria apropriada;

— conhecimento específico de disciplina relativo ao setor em particular, natureza de operações ou local de trabalho que está sendo auditado, suficiente para o auditor avaliar as atividades do auditado, processos, produtos, bens e serviços;

— princípios de gestão de risco, métodos e técnicas pertinentes para a disciplina e setor de tal modo que o auditor possa avaliar e controlar os riscos associados ao programa de auditoria.

NOTA Diretrizes e exemplos ilustrativos de conhecimentos e habilidades de disciplina específica dos auditores são fornecidos no Anexo A.

7.2.3.4 Conhecimento e habilidades genéricas de um líder da equipe da auditoria

Convém que os líderes da equipe de auditoria tenham habilidades e conhecimentos adicionais para gerenciar e prover liderança a equipe auditora, a fim de facilitar a eficácia e eficiência na realização da auditoria. Convém que o líder de uma equipe auditora tenha conhecimento e habilidades necessários para fazer o seguinte:

a) balanço das forças e fraquezas dos membros individuais da equipe auditora;

b) desenvolver um trabalho harmonioso de relacionamento entre os membros da equipe auditora;

c) gerenciar o processo de auditoria, incluindo:

— planejamento da auditoria fazendo uso eficaz dos recursos durante a auditoria;

— gerenciamento das incertezas em atingir os objetivos da auditoria;

— proteção da saúde e segurança dos membros da equipe auditora durante a auditoria, incluindo a garantia da conformidade dos auditores com os requisitos de saúde, segurança do trabalho e segurança física pertinentes;

— organização e orientação aos membros da equipe auditora;

— fornecimento de diretrizes e orientação para os auditores em treinamento;

— prevenção e resolução de conflitos, se necessário.

a) Representar a equipe auditora nas comunicações com a pessoa que gerencia o programa de auditoria, o cliente da auditoria e o auditado;

b) e) Conduzir a equipe auditora para alcançar as conclusões da auditoria;

c) f) preparar e concluir o relatório da auditoria.

7.2.3.5 Conhecimento e habilidades para auditoria de sistemas de gestão considerando múltiplas disciplinas

Os auditores que pretendem participar como um membro da equipe auditora em auditoria de sistemas de gestão que considere múltiplas disciplinas, convém que eles tenham a competência necessária para auditar pelo menos uma das disciplinas do sistema de gestão e tenham um entendimento da interação e sinergia entre os diferentes sistemas de gestão.

Convém que os líderes da equipe auditora que realizam auditorias de sistemas de gestão contendo múltiplas disciplinas, entendam os requisitos de cada uma das normas do sistema de gestão e reconheçam os limites de seus conhecimentos e habilidades em cada uma das disciplinas.

7.2.4 Atingindo a competência do auditor

Os conhecimentos e habilidades do auditor podem ser adquiridos usando uma combinação dos seguintes itens:

— experiência e treinamento/educação formal que contribua para o desenvolvimento do conhecimento e habilidades no setor e na disciplina do sistema de gestão que o auditor pretende auditar;

— programas de treinamento que cubram habilidades e conhecimentos genéricos do auditor;

— experiência em uma posição técnica, profissional ou gerencial pertinente que envolva o exercício de julgamento, tomada de decisão, solução de problemas e comunicação com gerentes, profissionais, pares, clientes e outras partes interessadas;

— experiência de auditoria adquirida sob a supervisão de um auditor na mesma disciplina.

7.2.5 Líderes de equipe de auditoria

Convém que um líder de equipe de auditoria tenha adquirido experiência adicional em auditoria para desenvolver o conhecimento e habilidades descritos em 7.2.3. Convém que essa experiência adicional tenha sido adquirida pelo trabalho sob a direção e orientação de um líder da equipe auditora diferente.

7.3 Estabelecendo critérios para avaliação do auditor

Convém que o critério seja qualitativo (tais como ter demonstrado comportamento pessoal, conhecimento ou desempenho de habilidades, seja em treinamento ou em local de trabalho) e quantitativo (tais como anos de experiência de trabalho e educação, número de auditorias realizadas, horas de treinamento de auditoria).

7.4 Selecionando o método apropriado de avaliação do auditor

Convém que a avaliação seja conduzida usando dois ou mais dos métodos selecionados, daqueles contidos na tabela 2. Ao usar a tabela 2, convém que seja observado o seguinte:

— os métodos descritos representam uma gama de opções e podem não ser aplicados em todas as situações;

— os vários métodos descritos podem diferenciar quanto a sua confiabilidade;

— convém que uma combinação de métodos seja usada para assegurar um resultado que seja objetivo, consistente, justo e confiável.

Tabela 2 — Possíveis métodos de avaliação

Método de avaliação	Objetivos	Exemplos
Análise crítica dos registros	Verificar a formação profissional do auditor	Análises de registros de educação, treinamento, emprego, credenciais e experiência em auditoria
Realimentação	Fornecer informações sobre como o desempenho do auditor é percebido	Pesquisas, questionários, referencias pessoais, testemunhos, reclamações, avaliação de Desempenho,análise crítica pelos pares
Entrevista	Avaliar o comportamento pessoal e a habilidade em comunicação para verificar informações e testar conhecimentos e para adquirir informações adicionais	Entrevista pessoal
Observação	Avaliar o comportamento pessoal e a capacidade para aplicar conhecimento e habilidade	Desempenho de papel, auditorias de testemunho e desempenho no trabalho
Exames	Avaliar o comportamento pessoal, conhecimentos e habilidades, e a sua aplicação	Testes orais e escritos, testes psicométricos ou psicotestes
Análise crítica pós auditoria	Fornecer informações sobre o desempenho do auditor durante a atividade de auditoria, identificar forças e fraquezas	Análise crítica do relatório da auditoria entrevista com o auditor líder, a equipe auditora e, se apropriado, realimentação do auditado

7.5 Conduzindo a avaliação do auditor

Convém que a informação coletada sobre a pessoa seja comparada com base no critério estabelecido em 7.2.3. Quando uma pessoa tem a expectativa de participar em um programa de auditoria, mas não preenche os critérios, convém que treinamento adicional, trabalho ou experiência em auditoria seja realizado e uma subseqüente reavaliação seja desempenhada.

7.6 Mantendo e melhorando a competência do auditor

Convém que os auditores e líderes da equipe auditora melhorem continuamente suas competências. Convém que os auditores mantenham suas competências em auditoria por meio de uma participação regular nas auditorias dos sistemas de gestão e no desenvolvimento profissional contínuo. Desenvolvimento profissional contínuo envolve a manutenção e a melhoria de competência. Isto pode ser atingido por várias maneiras, como por exemplo, experiência adicional de trabalho, treinamento,

estudos particulares, liderança, participação em reuniões, seminários e conferências ou outras atividades pertinentes.

Convém que a pessoa que gerencia o programa de auditoria estabeleça mecanismos adequados para a avaliação contínua do desempenho dos auditores e dos líderes da equipe auditora.

Convém que as atividades de desenvolvimento profissional contínuo levem em consideração o seguinte:

— mudanças nas necessidades do indivíduo e da organização responsável por realizar a auditoria;

— a prática de auditoria;

— normas pertinentes e outros requisitos.

Anexo A
(Informativo)

Diretrizes e exemplos ilustrativos de conhecimentos e habilidades de auditores de disciplinas específicas

A.1 Geral

Este anexo fornece exemplos genéricos de conhecimento e habilidades de auditores de disciplinas específicas de sistemas de gestão, os quais são usados como orientação para apoiar a pessoa que gerencia o programa de auditoria para selecionar ou avaliar os auditores.

Outros exemplos de conhecimento e habilidades de auditores de disciplinas específicas podem também ser desenvolvidos para sistemas de gestão. É recomendado que, onde possível, tais exemplos sigam a mesma estrutura geral para assegurar a compatibilidade.

A.2 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplina específica em gestão na segurança de transporte

Convém que conhecimento e habilidades relacionados à gestão na segurança de transportes e a aplicação de práticas, processos, técnicas e métodos de gestão da segurança do transporte sejam suficientes para permitir o auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— terminologia sobre gestão de segurança;

— entendimento sobre abordagem de sistema de segurança;

— avaliação de risco e sua mitigação;

— análise de fatores humanos relacionados à gestão da segurança no transporte;

— interação e comportamento humano;

— interação de processos, máquinas, pessoas e do ambiente do trabalho;

— danos potenciais e outros fatores no local de trabalho que afetem a segurança;

— métodos e práticas para investigação de incidentes e monitoramento do desempenho de segurança;

— avaliação de incidentes e acidentes operacionais;

— desenvolvimento proativo e reativo sobre o desempenho de métricas e medidas.

NOTA Para informações adicionais, ver a futura norma ISO 39001 desenvolvida pelo Comitê ISO/PC 241 sobre sistemas de gestão de segurança no tráfego rodoviário.

A.3 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplina específica em gestão do meio ambiente

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— terminologia sobre meio ambiente;

— estatísticas e métricas sobre meio ambiente;

— técnicas de monitoramento e ciência de medições;

— interação de ecossistemas e biodiversidade;

— mídia ambiental (por exemplo, ar, água, terra, fauna e flora);

— técnicas para determinação do risco (por exemplo, avaliação de aspectos/impactos ambientais, incluindo métodos para a avaliação de significância)

— avaliação do ciclo de vida;

— avaliação do desempenho ambiental;

— controle e prevenção de poluição (por exemplo, melhores técnicas disponíveis para o controle da poluição ou eficiência energética);

— redução na fonte, minimização de resíduos, reuso, reciclagem e práticas e processos de tratamento;

— uso de substâncias perigosas;

— quantificação e gestão de emissões de gases de efeito estufa;

— gestão de recursos naturais (por exemplo, combustíveis fósseis, água, flora, fauna e terra);

— projetos ambientais;

— divulgação e relatos ambientais;

— gestão cuidadosa de produtos;

— tecnologias renováveis e de baixo carbono.

NOTA Para informações adicionais ver normas desenvolvidas pelo Comitê ISO/TC 207 sobre gestão ambiental

A.4 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplinas específicas em gestão da qualidade

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— terminologia relativa à qualidade, gestão, organização, processo e produto, características, conformidade, documentação, processos de medição e auditoria;

— foco no cliente, processos relacionado ao cliente, monitoramento e medição da satisfação do cliente, tratamento de reclamações, código de conduta e resolução de divergências;

— liderança – papel da alta direção, gerenciamento para o sucesso sustentável de uma organização;

— enfoque da gestão da qualidade, geração de benefícios financeiros e econômicos por meio da gestão da qualidade, sistemas de gestão da qualidade e modelos de excelência;

— envolvimento de pessoas, fatores humanos, competência, treinamento e conscientização;

— abordagem por processos, análise de processo, técnicas de controle e capabilidade, métodos de tratamento de riscos;

— abordagem de sistemas para gestão (justificativa de sistema de gestão da qualidade e outros sistemas de gestão, documentação de sistema de gestão da qualidade), tipos e valores, projetos, planos de qualidade e gestão de configuração;

— melhoria contínua, inovação e aprendizado;

— enfoque baseado em fatos para tomada de decisão, técnicas de avaliação de riscos (identificação de risco, análise e avaliação), avaliação da gestão da qualidade (auditoria, análise critica e auto-avaliação), técnicas de medição e monitoramento, requisitos para processo de medição e equipamentos de medição, análise da causa raiz, técnicas estatísticas;

— características de processos e produtos, incluindo serviços;

— benefícios mútuos na relação com fornecedores, requisitos de sistema de gestão da qualidade e requisitos para produtos, requisitos particulares para gestão da qualidade de diferentes setores.

NOTA Para informações adicionais ver normas relacionadas desenvolvidas pelo Comitê ISO/TC 176 sobre gestão da qualidade.

A.5 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplinas específicas em gestão de registros

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— registros, processos de gestão de registros e sistemas de gestão para terminologia de registros;

— desenvolvimento do desempenho de métricas e medições;

— investigação e avaliação de práticas de registros por meio de entrevistas, observação e validação;

— análise de amostras de registros criados nos processos de negócios. Características chave de registros, sistemas de registros, controles e processos de registros;

— avaliação de risco (por exemplo, avaliação de riscos decorrentes de falha para criar, manter e controlar os registros de forma adequada dos processos de negócios da organização);

— o desempenho e adequação dos processos de registros para criar, capturar e controlar os registros;

— avaliação da adequação e desempenho de sistemas de registros (incluindo sistemas de negócios para criar e controlar os registros), a pertinência de ferramentas tecnológicas usadas, instalações e equipamentos estabelecidos;

— avaliação dos diferentes níveis de competência na gestão de registros requeridos em toda a organização e a avaliação desta competência;

— importância do conteúdo, contexto, estrutura, representação e informação de controle (metadados) requerido para definir e gerenciar os registros e os sistemas de registros;

— métodos para desenvolver instrumentos específicos de registros;

— tecnologias usadas para criação, captura, conversão e migração na preservação de longo tempo dos registros eletrônicos e digitais;

— identificação e importância da documentação de autorização para os processos de registros.

NOTA Para informações adicionais ver normas relacionadas desenvolvidas pelo Comitê ISO/TC 46/SC 11 sobre gestão de registros

A.6 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplinas específicas em resiliencia, segurança, prontidão e gestão da continuidade

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— processos, ciência e tecnologia baseados na gestão da resiliencia, segurança física, prontidão, resposta, continuidade e recuperação;

— métodos para o monitoramento e uso da inteligência;

— gerenciamento de riscos de eventos que causam transtornos (antecipar, evitar, prevenir, proteger, mitigar, responder e recuperar a partir de um evento que causa transtorno);

— avaliação de risco (valoração e identificação do ativo; avaliação, análise e identificação de risco) e análise de impacto (relativo a pessoas, ativos físicos e intangíveis, bem como ao meio ambiente);

— tratamento do risco (medidas adaptativas, proativas e reativas);

— métodos e práticas relativas à sensibilidade e integridade da informação;

— métodos para segurança pessoal e a proteção das pessoas;

— métodos e práticas para proteção de ativos e segurança física;

— métodos e práticas para a gestão da prevenção, intimidação e segurança física;

— métodos e práticas para mitigação de incidentes, respostas e gestão de crise;

— métodos e práticas para a gestão da continuidade, emergência e recuperação;

— métodos e práticas para monitoramento, medição e relato do desempenho (incluindo metodologias de teste e exercício).

NOTA Para informações adicionais ver normas relacionadas desenvolvidas pelos comitês ISO/TC 8, ISO/TC 223 e ISO/ TC 247 sobre gestão da resiliencia, segurança, prontidão e da continuidade.

A.7 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplinas específicas em gestão da segurança da informação

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— diretrizes sobre normas tais como ISO IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005;

— identificação e avaliação de requisitos dos clientes e partes interessadas;

— leis e regulamentações que tratam da segurança da informação (por exemplo, propriedade intelectual, conteúdo, proteção e retenção de registros da organização, proteção e privacidade de dados, regulamentação de controles criptográficos, anti-terrorismo, comercio eletrônico, assinaturas digital e eletrônicas, avaliação do ambiente de trabalho, ergonomia no ambiente de trabalho, interceptação da telecomunicação e monitoramento de dados (por exemplo, email, uso abusivo do computador, coleta de evidência eletrônica, teste de penetração, etc);

— processos, tecnologia e ciência baseada na gestão da segurança da informação;

— avaliação de risco (identificação, analise e avaliação) e tendências na tecnologia, ameaças e vulnerabilidades;

— gestão de risco de segurança da informação;

— métodos e praticas para controles da segurança da informação (eletrônico e físico);

— métodos e práticas para a sensibilidade e integridade da informação;

— métodos e práticas para medição e avaliação da eficácia do sistema de gestão da segurança da informação e dos controles associados;

— métodos e práticas para medição, monitoramento e registros de desempenho (incluindo testes, auditorias e análises críticas).

NOTA Para informações adicionais ver normas relacionadas desenvolvidas pelo comitê ISO/IEC JTC1 SC27 sobre gestão da segurança da informação.

A.8 Exemplo ilustrativo de conhecimento e habilidades de auditores de disciplinas específicas em gestão da segurança e saúde ocupacional

A.8.1 Habilidades e conhecimentos gerais

Convém que conhecimento e habilidades relacionados à disciplina e a aplicação de práticas, processos, técnicas e métodos de disciplinas específicas sejam suficientes para permitir ao auditor examinar o sistema de gestão e gerar conclusões e constatações de auditoria apropriada.

São exemplos de conhecimento e habilidades:

— identificação de danos, incluindo aqueles fatores que afetam o desempenho humano no ambiente de trabalho (tais como fatores físicos, químicos e biológicos, bem como gênero, idade, deficiência ou outros fatores de saúde ou psicológicos);

— avaliação de risco, determinação de controles e comunicação do risco [convém que a determinação de controles seja baseada na hierarquia de controles (ver OHSAS 18001:2007, 4.3.1)];

— avaliação de fatores humanos e de saúde (incluindo fatores psicológicos e fisiológicos) e os princípios para avaliá-los;

— métodos para monitoramento de exposição e avaliação dos riscos da saúde e segurança ocupacional (incluindo aqueles oriundos de fatores humanos mencionados acima ou relativos a higiene ocupacional) e relativos a estratégias para eliminar ou minimizar tais exposições;

— comportamento humano, interações pessoa a pessoa e interação de pessoas com equipamentos, processos e ambiente de trabalho (incluindo local de trabalho, princípios ergonômicos e de projeto seguro, tecnologia da informação e comunicação)

— avaliação de diferentes tipos e níveis da competência da segurança e saúde ocupacional requerida em toda a organização e avaliação desta competência;

— métodos para encorajar o envolvimento e a participação dos integrantes da força de trabalho;

— métodos para encorajar a saúde dos integrantes da força de trabalho, o bem estar e a auto-responsabilidade (em relação ao fumo, drogas, álcool, questões relativas ao peso, exercício físico, estresse, comportamento agressivo, etc.), tanto durante ao trabalho quanto na sua vida privada;

— o desenvolvimento, uso e avaliação do desempenho de métricas e medições proativas e reativas;

— princípios e práticas para identificar situações potenciais de emergência e para o planejamento, prevenção, resposta e recuperação depois da emergência;

— métodos para avaliação e investigação de incidentes (incluindo acidentes e doenças relativas ao trabalho);

— determinação e uso de informações relacionadas à saúde (incluindo exposição relacionada ao trabalho e monitoramento de dados de doenças), dando especial atenção a confidencialidade de aspectos particulares destas informações;

— entendimento de informações médicas (incluindo terminologia médica suficiente para entender dados relativos à prevenção de danos e doenças);

— sistemas de valores de limite de exposição ocupacional;

— métodos para monitoramento e relato sobre desempenho de saúde ocupacional e segurança;

— entendimento de requisitos legais e outros requisitos pertinentes para a segurança e saúde ocupacional para permitir ao auditor avaliar o sistema de gestão de segurança e saúde ocupacional;

A.8.2 Conhecimento e habilidades relacionadas ao setor que está sendo auditado

Convém que conhecimento e habilidades relativas ao setor que esta sendo auditado seja suficiente para permitir o auditor examinar o sistema de gestão dentro do contexto do setor e gerar conclusões e constatações da auditoria apropriadas.

São exemplos de conhecimento e habilidades:

— processos, equipamentos, matérias-primas, substancias perigosas, ciclos de processos, manutenção, logística, fluxograma organizacional, praticas de trabalho, programação de turno, cultura organizacional, liderança, comportamento e outros aspectos específicos da operação ou do setor;

— riscos e perigos típicos incluindo fatores humanos e de saúde para o setor;

NOTA 1:Para informações adicionais ver normas relacionadas desenvolvidas pelo grupo de projeto da OHSAS, sobre gestão de segurança e saúde ocupacional.

NOTA 2 DA ABNT:Para informações adicionais ver a norma ABNT NBR 18801 referente a sistema de gestão da segurança e saúde no trabalho.

Anexo B

(Informativo)

Diretrizes adicionais para auditores para planejamento e realização de auditorias

B.1 Aplicando métodos de auditoria

Uma auditoria pode ser realizada usando uma variedade de métodos de auditoria. Uma explicação dos métodos mais comuns usados em auditoria pode ser encontrada neste anexo. Os métodos de auditoria escolhidos para uma auditoria dependem dos objetivos da auditoria definidos, do escopo e critérios, bem como da duração e localização. Convém que a disponibilidade de auditor com competência e qualquer incerteza que surja da aplicação dos métodos de auditoria sejam considerados. Aplicando uma variedade e combinação de diferentes métodos de auditoria, pode otimizar a eficiência e eficácia do processo de auditoria e do seu resultado.

O desempenho de uma auditoria envolve uma interação entre indivíduos com o sistema de gestão que esta sendo auditado e a tecnologia usada para realizar a auditoria. A tabela B.1 fornece exemplos de métodos de auditoria que podem ser usados, de maneira única ou combinados, para atingir os objetivos da auditoria. Se uma auditoria envolve o uso de uma equipe de auditoria com múltiplos membros, tanto métodos, no local e remoto, podem ser usados simultaneamente.

NOTA Informações adicionais sobre visitas no local é dada na Seção B.6.

Tabela B.1 – Métodos de auditoria aplicáveis

Abrangência do envolvimento entre o auditor e o auditado	**Localização do auditor**	
	No local	**Remota**
Interação humana	Realizando entrevistas. Completando lista de verificações e questionários com a participação do auditado. Realizando análise crítica dos documentos com a participação do auditado. Amostragem	Por meio de comunicação interativa: - Realizando entrevistas. - Completando lista de verificação e questionários. - Realizando análise crítica documental com a participação do auditado.
Sem interação humana	- Realizando análise crítica dos documentos com a participação do auditado (ex: registros, análise de dados) - Observando o trabalho realizado - Realizando a visita no local - Completando listas de verificação - Amostragem (p. ex: produtos)	Realizando análise crítica documental (ex: registros, análise de dados) - Observando o trabalho realizado por meio de monitoramento, levando-se em conta requisitos sociais e legais. - Analisando dados
Atividades de auditoria no local são realizadas na localidade do auditado. Atividades de auditoria remota são realizadas em qualquer local que não o local do auditado, independentemente da distância. Atividade de auditoria interativa envolve a interação entre as pessoas da organização auditada e a equipe auditora. Atividades de auditoria não interativa não envolvem interação humana com pessoas que representam o auditado, mas envolve interação com equipamento, instalações e documentação.		

A responsabilidade da aplicação efetiva dos métodos de auditoria para quaisquer auditorias no estágio do planejamento, permanece ou com a pessoa que gerencia o programa de auditoria ou com o líder da equipe auditora. O líder da equipe auditora tem esta responsabilidade para realizar as atividades de auditoria.

A viabilidade das atividades de auditoria remota pode depender do nível de confiança entre o auditor e o pessoal auditado.

No nível do programa de auditoria, convém que seja assegurado que o uso de métodos de auditoria remota ou no local seja adequado e balanceado, para assegurar um atingimento satisfatório dos objetivos do programa de auditoria.

B.2 Realizando análise critica da documentação

Convém que os auditores considerem se:

— a informação contida nos documentos disponibilizados é:

— completa (todo conteúdo esperado está contido no documento);

— correta (o conteúdo está em conformidade com outras fontes confiáveis, tais como normas e regulamentações);

— consistente (o documento é consistente em si e com documentos relacionados);

— atual (o conteúdo está atualizado);

— o documento que está sendo analisado criticamente cobre o escopo da auditoria e provê informação suficiente para apoiar os objetivos de auditoria;

— o uso de tecnologias de comunicação e informação, dependendo dos métodos de auditoria, promove uma eficiente realização da auditoria: cuidado específico é necessário para a segurança da informação devido a regulamentações aplicáveis sobre proteção de dados (em particular para informações que permanecem fora do escopo da auditoria, mas que estão também contidas no documento).

NOTA Análise critica do documento pode dar uma indicação da eficácia do controle de documento no sistema de gestão do auditado.

B.3 Amostragem

B.3.1 Geral

Amostragem de auditoria é realizada quando não é prático ou é oneroso examinar todas as informações disponíveis durante uma auditoria, por exemplo, registros são muitos numerosos ou muito dispersos geograficamente para justificar o exame de cada item na população. Amostragem de auditoria de uma grande população é o processo de selecionar menos de 100% de itens dentro do conjunto total de dados disponíveis (população) para obter e avaliar a evidência sobre alguma característica daquela população a fim de formar uma conclusão com relação à população.

O objetivo da amostragem de auditoria é prover informação para o auditor ter confiança de que os objetivos de auditoria podem ou serão atingidos.

O risco associado com amostragem é que as amostras podem não ser representativas da população das quais elas são selecionadas, e então as conclusões do auditor podem ser tendenciosas e diferentes daquelas que seriam alcançadas se a população inteira fosse examinada. Podem existir outros riscos dependendo da variabilidade dentro da população a ser amostrada e do método escolhido.

Amostragens de auditoria tipicamente consideram os seguintes passos:

— estabelecendo os objetivos do plano de amostragem;

— selecionando a abrangência e composição da população a ser amostrada;

— selecionando um método de amostragem;

— determinando o tamanho da amostra a ser realizada;

— conduzindo atividade de amostragem;

— compilando, avaliando, reportando e documentando os resultados.

Quando da amostragem, convém que consideração seja dada a qualidade dos dados disponíveis, uma vez que amostragem insuficiente e dados imprecisos não fornecerão resultado útil. Convém que a seleção de uma amostra apropriada seja baseada tanto no método de amostragem como no tipo de dados requeridos, por exemplo, para inferir um comportamento particular modelo ou obter inferências ao longo de uma população.

Um relato sobre a amostra selecionada pode levar em consideração o tamanho da amostra, método de seleção e estimativas feitas em base na amostra e no nível de confiança.

Auditorias podem tanto ser usadas em amostragem baseada no julgamento (ver B 5.2) ou em amostragem estatística (ver B.5.3).

B.3.2 Amostragem baseada no julgamento

Amostragem baseada no julgamento depende de conhecimento, habilidade e experiência da equipe auditora (ver Seção 7).

Para amostragem baseada em julgamento, convém que seja considerado o seguinte:

— experiência anterior de auditoria dentro do escopo da auditoria;

— complexidade de requisitos (incluindo requisitos legais) para atingir os objetivos de auditoria;

— complexidade e interação dos processos da organização e dos elementos do sistema de gestão;

— grau de mudança na tecnologia, fator humano ou sistema de gestão;

— identificação previa, de áreas de risco críticas e de áreas para melhoria;

— resultado de monitoramento de sistemas de gestão.

Um obstáculo para a amostragem baseada em julgamento é que pode não existir uma estimativa estatística do efeito da incerteza nas constatações da auditoria ou nas conclusões alcançadas.

B.3.3 Amostragem estatística

Se a decisão é fazer uso de amostragem estatística, convém que o plano de amostragem seja baseado nos objetivos da auditoria e no que é conhecido sobre as características da população global, das quais as amostras serão tomadas.

— O projeto de amostragem estatística utiliza um processo de seleção de amostras baseado na teoria da probabilidade. Amostragem baseada em atributo é usada quando existem apenas dois possíveis resultados para cada amostra (por exemplo, certo/errado ou aprovado/reprovado). Amostragem baseada em variável é usada quando o resultado da amostra ocorre em um intervalo contínuo.

— Convém que o plano de amostragem leve em consideração se o resultado que está sendo examinado tem possibilidade de ser baseado em um atributo ou baseado em uma variável. Por exemplo, quando avaliando a conformidade dos formulários preenchidos com os requisitos estabelecidos em um procedimento,pode ser usada uma abordagem baseada em atributo. Quando

examinando a ocorrência de incidentes de segurança de alimentos ou do número de violações da segurança da informação, uma abordagem baseada em variável é provavelmente mais apropriada.

— os elementos chave que irão afetar o plano de amostragem de auditoria são:

— o tamanho da organização;

— o número de auditores qualificados;

— a freqüência de auditorias durante o ano;

— o tempo da auditoria em particular;

— quaisquer níveis de confiança requerido externamente.

— Quando um plano de amostragem estatístico é desenvolvido, o nível de risco da amostra que o auditor está disposto a aceitar, é uma consideração importante a ser avaliada. Isto é sempre referido como nível de confiança aceitável. Por exemplo, um risco de amostragem de 5% corresponde a um nível de confiança aceitável de 95%. Um risco de amostragem de 5% significa que o auditor está disposto a aceitar o risco de 5 em um total de 100 (ou 1 em 20) de amostras examinadas que não afetarão os valores reais que seriam vistos caso a população inteira fosse examinada.

— Quando uma amostra estatística é usada, convém que os auditores documentem apropriadamente o trabalho realizado. Convém que isto inclua uma descrição da população que está sendo amostrada, o critério de amostragem usado para a avaliação (por exemplo, o que é uma amostra aceitável), métodos e parâmetros estatísticos que foram usados, o número de amostras avaliadas e resultados obtidos.

B.4 Preparando documentos de trabalho

Quando da preparação de documentos de trabalho, convém que a equipe auditora considere as seguintes questões para cada documento:

a) Quais registros da auditoria serão criados pelo uso deste documento de trabalho?

b) Quais atividades da auditoria são afetadas por esse documento de trabalho em particular?

c) Quem será o usuário deste documento de trabalho?

d) Quais informações são necessárias para preparar este documento de trabalho?

Para auditorias combinadas, convém que os documentos de trabalho sejam desenvolvidos para evitar duplicação de atividade de auditoria devido a:

— agrupamento de requisitos similares oriundos de critérios diferentes;

— coordenação do conteúdo de listas de verificação e questionários relacionados.

Convém que os documentos de trabalho sejam adequados para contemplar todos aqueles elementos do sistema de gestão dentro do escopo da auditoria e pode ser fornecido em qualquer meio.

B.5 Selecionando fontes de informação

As fontes de informação selecionadas podem variar de acordo com o escopo e complexidade da auditoria e podem incluir o seguinte:

— entrevistas com o empregado e outras pessoas;

— observações de atividades e ambiente de trabalho ao redor, incluindo condições;

— documentos, tais como políticas, objetivos, planos, procedimentos, normas, instruções, licenças e permissões, especificações, desenhos, contratos e ordens de compra;

— registros, tais como registros de inspeção, atas de reuniões, relatórios de auditoria, registros de programas de monitoramento e os resultados de medições;

— dados sumarizados, análises e indicadores de desempenho;

— informações sobre os planos de amostragem do auditado e sobre os procedimentos para controle de amostragem e processos de medição;

— relatórios de outras fontes, por exemplo, realimentação dos clientes (feedback), medições e pesquisas externas, outras informações pertinentes de partes externas e classificação de fornecedores;

— base de dados e sites;

— simulação e modelagem.

B.6 Diretrizes sobre a visita no local do auditado

Para minimizar a interferência entre as atividades de auditoria e os processos de trabalho do auditado, e para assegurar a segurança e saúde ocupacional da equipe auditora durante a visita, convém que seja considerado o seguinte:

a) Planejamento da visita:

— assegurar permissão e acesso aquelas partes da localidade do auditado a serem visitadas, de acordo com o escopo da auditoria;

— prover informações adequadas (por exemplo, apresentação da empresa) aos auditores sobre segurança, saúde (por exemplo, quarentena), assuntos de segurança física e saúde no trabalho e normas culturais para visita incluindo solicitação e recomendação para vacinação e permissões, se aplicado;

— confirmar com o auditado que quaisquer requisitos de equipamento de proteção individual (EPI) estará disponível para equipe auditora, se aplicável;

— exceto para as auditorias *ad hoc* não planejadas, assegurar que o pessoal que está sendo visitado será informado sobre o escopo e objetivos da auditoria;

b) Atividades no local da auditoria:

— evitar quaisquer distúrbios desnecessários aos processos operacionais;

— assegurar que a equipe auditora esta usando o EPI apropriadamente;

— assegurar que os procedimentos de emergência sejam comunicados (por exemplo, saída de emergência, ponto de encontro);

— programar comunicação para minimizar interrupções;

— adaptar o tamanho da equipe auditora e o número de guias e observadores de acordo com o escopo da auditoria para evitar interferência com os processos operacionais, tão prático quanto possível;

— não tocar ou manipular quaisquer equipamentos, a menos que explicitamente permitido, mesmo sendo competente ou licenciado;

— Se um incidente ocorre durante a visita no local, convém que o líder da equipe auditora analise criticamente a situação com a organização auditada e, se necessário, com o cliente da auditoria para chegar a um acordo sobre se convém que a auditoria seja interrompida, reprogramada ou continuada;

— no caso de tirar fotos ou gravar imagens, pedir autorização da direção antecipadamente e considerar as questões de confidencialidade e segurança da informação, evitando tirar fotos de pessoas sem a sua permissão;

— caso tire cópias de documentos de quaisquer tipos, solicitar permissão antecipadamente e considerar as questões de confidencialidade e segurança da informação;

— ao fazer anotações, evitar coletar informações pessoais, a menos que sejam requeridas pelos objetivos de auditoria ou pelo critério de auditoria.

B.7 Realizando entrevistas

Entrevistas representam uma das mais importantes formas de coletar informações e convém que seja realizada de tal maneira a adaptar a situação a pessoa a ser entrevistada, seja pessoalmente ou por outros meios de comunicação.

Entretanto, convém que o auditor considere o seguinte:

— convém que entrevistas sejam realizadas com pessoas de funções e níveis apropriados que realizam as atividades ou tarefas dentro do escopo da auditoria;

— convém que entrevistas sejam normalmente conduzidas durante o horário normal de trabalho e, sempre que possível, no local de trabalho da pessoa que está sendo entrevistada;

— sempre que possível, deixar a pessoa que está sendo entrevistada à vontade antes e durante a entrevista;

— a razão para a entrevista e quaisquer anotações convém que sejam explicadas;

— entrevistas podem ser iniciadas pedindo às pessoas para descrever o seu trabalho;

— seleção cuidadosa do tipo de questão usada (por exemplo, usar questões abertas, fechadas);

— convém que os resultados de entrevistas sejam sumarizados e analisados criticamente com a pessoa entrevistada;

— convém agradecer às pessoas entrevistadas pela sua participação e cooperação.

B.8 Constatações de auditoria

B.8.1 Determinando as constatações de auditoria

Quando determinando as constatações de auditoria, convém que seja considerado o seguinte:

— acompanhamento de conclusões e registros de auditorias anteriores;

— requisitos do cliente de auditoria;

— constatações que excedam a prática normal ou oportunidades para melhoria;

— tamanho da amostra;

— categorização (se existir) das constatações da auditoria.

B.8.2 Registrando as conformidades

Para os registros de conformidade, convém que seja considerado o seguinte:

— identificação dos critérios de auditoria, com base no qual a conformidade é apresentada;

— evidencia da auditoria para apoiar a conformidade;

— declaração de conformidade, se aplicável.

B.8.3 Registrando não-conformidades

Para os registros de não-conformidade, convém que seja considerado o seguinte:

— descrição de ou referencia ao critério de auditoria;

— declaração da não-conformidade;

— evidência da auditoria;

— constatações relatadas na auditoria, se aplicável.

B.8.4 Tratando com constatações relacionadas a múltiplos critérios

Durante uma auditoria é possível identificar constatações relativas a múltiplos critérios. Quando um auditor identifica uma constatação relacionada a um critério de uma auditoria combinada, convém que o auditor considere o possível impacto sobre o critério similar ou correspondente de outros sistemas de gestão.

Dependendo dos arranjos com o cliente da auditoria, o auditor pode considerar:

— separar as constatações para cada critério; ou

— uma simples constatação, combinando as referências a múltiplos critérios.

Dependendo dos arranjos com cliente da auditoria o auditor pode orientar o auditado sobre como responder a estas constatações.

Bibliografia

[1] ISO 2859-4, Sampling procedures for inspection by attributes — Part 4: Procedures for assessment of declared quality levels

[2] ABNT NBR ISO 9000:2005, Sistemas de Gestão da Qualidade-Fundamentos e Vocabulário

[3] ABNT NBR ISO 9001, Sistemas de Gestão da Qualidade-Requisitos

[4] ABNT NBR ISO 14001, Sistemas de Gestão Ambiental-Requisitos com diretrizes para uso

[5] ISO 14050, *Environmental management — Vocabulary*

[6] ISO/IEC 17021:2011, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[7] ABNT NBR ISO/IEC 20000-1, Tecnologia da informação-Gestão de services-Parte 1:Requisitos de sistema de gestão em serviços

[8] ABNT NBR ISO 22000, Sistemas de gestão da segurança em alimentos-Requisitos para qualquer organização na cadeia

[9] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[10] ABNT NBR ISO/IEC 27001, Tecnologia da Informação-Técnicas de Segurança-Sistemas de Gestão da Segurança da Informação-Requisitos

[11] ABNT NBR ISO/IEC 27002, Tecnologia da informação-Técnicas de Segurança –Código de prática para gestão da segurança da informação

[12] ABNT NBR ISO/IEC 27003,Tecnologia da Informação-Técnicas de Segurança-Diretrizes para implementação de um sistema de gestão da segurança da informação

[13] ABNT NBR ISO/IEC 27004, Tecnologia da Informação-Técnicas de Segurança-Gestão de Segurança da Informação-Medições

[14] ABNT NBR ISO/IEC 27005, Tecnologia da Informação-Técnicas de Segurança-Gestão de riscos de segurançada informação

[15] ISO 28000, *Specification for security management systems for the supply chain*

[16] ISO 30301[1], *Information and documentation — Management system for records — Requirements*

[17] ABNT NBR ISO 31000, Gestão de riscos- Princípios e diretrizes

[1] To be published.

[18] ISO 39001[2], *Road traffic safety (RTS) management systems — Requirements with guidance for use*

[19] ABNT NBR ISO 50001, Sistemas de gestão de energia-Requisitos com diretrizes para uso

[20] ABNT NBR ISO Guide 73:2009, Gestão de riscos-Vocabulário

[21] OHSAS 18001:2007, *Occupational health and safety management systems — Requirements*

[22] *ISO 9001 Auditing Practices Group* papers available at:
www.iso.org/tc176/ISO9001AuditingPracticesGroup

[23] ISO 19011 additional guidelines[2] available at:
www.iso.org/19011auditing

[24] ABNT NBR 18801:2010 – Sistema de gestão da segurança e saúde no trabalho. Requisitos

[2] Under preparation.